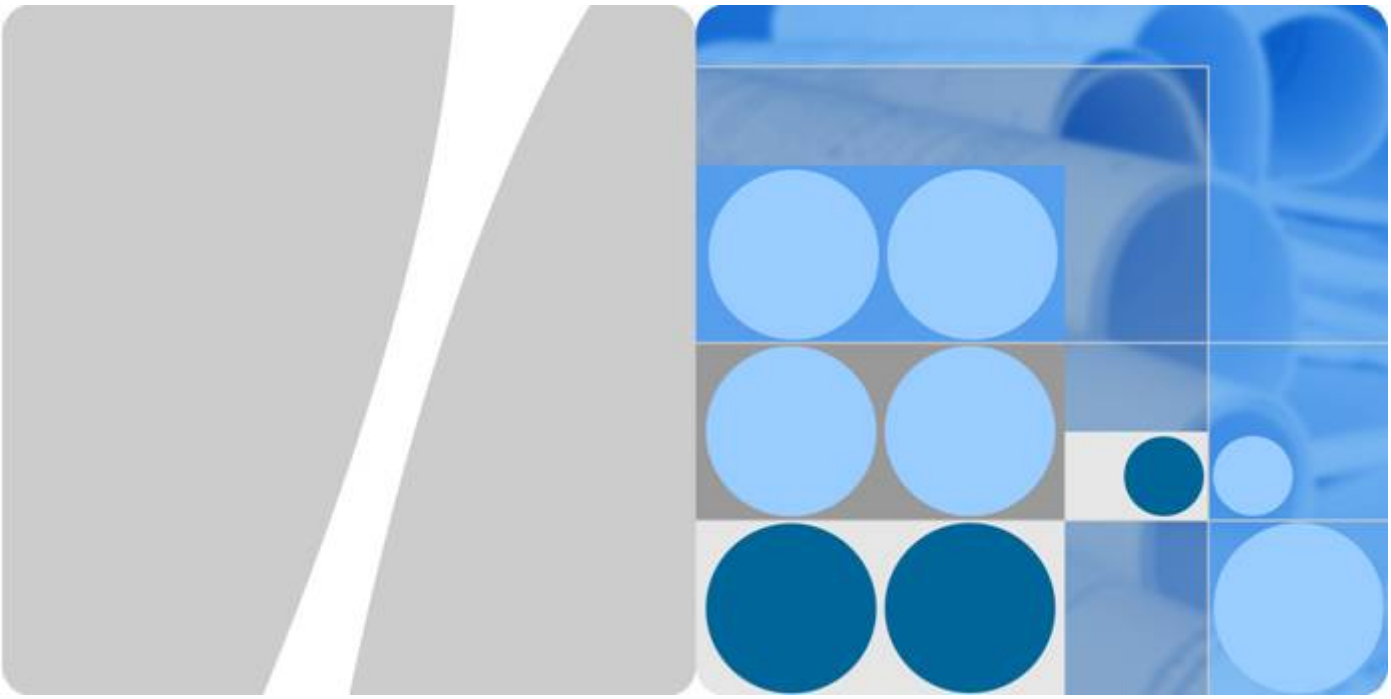


iManager U2000 Unified Network Management System

V200R014C60

Troubleshooting

Issue 03

Date 2015-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2015. All rights reserved.

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

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Version

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

Product Name	Version
iManager U2000	V200R014C60

Intended Audience

This document describes U2000 troubleshooting in terms of the troubleshooting procedure, information collection, fault location, fault rectification, and troubleshooting suggestions.

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

Copyright © Huawei Technologies Co., Ltd.

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

Command Conventions

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

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

GUI Conventions

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

Copyright © Huawei Technologies Co., Ltd.

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

The third commercial release has the following updates:

Fixed some bugs.

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

The second commercial release has the following updates:

Fixed some bugs.

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

Initial release.

Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document.....ii

1 Security Precautions (for Troubleshooting).....1

2 Basic Troubleshooting Principles.....3

3 Troubleshooting Process.....5

4 Collecting Fault Data.....7

5 U2000-Related Faults.....10

5.1 Solaris Troubleshooting.....11

5.1.1 Failure to Start the OS.....11

5.1.2 Failure to Log In to the GUI of the OS.....14

5.1.3 How to Solve the Problem Where the Monitor or KVM Cannot Access the GUI After the OS Is Installed on the Netra T4-1/Netra T4-2/Oracle T4-1/Oracle T4-2/T5220 Server.....15

5.1.4 Failure to Open Graphical Tools.....17

5.1.5 Failure to Eject a DVD.....17

5.1.6 Operation Abnormality Caused by Insufficient Disk Space.....18

5.1.7 Slow Running of the System Caused by Insufficient Memory.....18

5.1.8 Slow Running of the System Caused by Too High CPU Usage.....19

5.1.9 Failure to Connect the SUN Server and a Switch Because of an Auto-Negotiation Failure.....20

5.2 SUSE Linux Troubleshooting.....21

5.2.1 Failure to Log In to the GUI.....21

5.3 Sybase Database Troubleshooting.....22

5.3.1 Failure to Immediately Back Up the Sybase Database.....22

5.3.2 Failure to Start the Sybase Database.....23

5.3.3 Abnormal Startup of the Sybase Database.....30

5.3.4 How to Verify That the Sybase Database Is Running.....37

5.3.5 How to Check the Sybase Database Version.....38

5.3.6 How to Disable the Sybase Database Service.....39

5.4 SQL Server Database Troubleshooting.....41

5.4.1 Failure to Initialize the Database.....41

5.4.2 Failure to Immediately Back Up the SQL Server Database.....47

5.4.3 Usage of the imaptmdb Database Reaches Upper Limit Upon an Incorrect Password Modification.....48

5.5 U2000 Server Troubleshooting.....49

Copyright © Huawei Technologies Co., Ltd.

5.5.1 Failure to Start the U2000 Server....49
5.5.2 Cannot Back Up Data on the U2000 Server....54
5.5.3 Some U2000 Functions Fail to Work....54
5.5.4 Failure to Start Certain Processes of the U2000 Server....55
5.5.5 Some U2000 Functions Become Abnormal Due to the Change of the System Time....57
5.5.6 Data or Log Space of the U2000 Used Up....57
5.5.7 Abnormal Data Generated After the U2000 Restarts....58
5.5.8 A Message Displayed Indicating Not All Scripts Are Imported....58
5.5.9 Failure to Find a Uniquely Matched Trail During Script Importing....59
5.5.10 Message Indicating Unreachable Receive End Process Displayed During Script Exporting....60
5.5.11 How to Clear Alarms That an NE Reported Before Becoming Unreachable....60
5.6 Faults on a U2000 Client....61
5.6.1 Failure to Start a U2000 Client....61
5.6.2 Failure to Log In to the U2000 Server from a U2000 Client....61
5.6.3 User Account for Logging In to a U2000 Client Locked....64
5.6.4 U2000 Client Running Abnormally....65
5.6.5 Abnormal Exit of a U2000 Client Because of Inappropriate Input Method Editor Software....65
5.6.6 Abnormal NE Manager GUI for Certain Equipment on a U2000 Client....66
5.6.7 Connection Between the U2000 Client and Server that Are Running on the Same Machine Interrupted for a Short Period of Time After a Network Cable Is Removed....69
5.6.8 Time Inconsistency Between the U2000 Server and Client....70
5.6.9 Unsynchronized NE Configuration Information Is Not Displayed....71
5.6.10 How Do I Resolve the Problem Where the U2000 Client Fails to Be Installed Using CAU After the U2000 Has Been Upgraded?....71
5.7 U2000 Running Slowly....72
5.8 Veritas High Availability System Troubleshooting....74
5.8.1 HA System Status Overview....74
5.8.2 Principle of HA System Status Conversion....76
5.8.3 Causes of Failover on an HA System....78
5.8.4 Troubleshooting Policies for a Veritas High Availability System....80
5.8.5 Veritas Troubleshooting Cases....84
5.8.6 Failure to Connect the Primary and Secondary Sites (HA System, Solaris)....97
5.8.7 Failure to Separate the Primary and Secondary Sites (HA System, Solaris)....104
5.8.8 Failure to Forcibly Configure the Local End as the Primary Site (HA System, Solaris)....106
5.8.9 Common FAQ....111

6 Troubleshooting Basic Operation Faults on the U2000....116

6.1 License Management Troubleshooting....117
6.1.1 A Failure to Update the U2000 License File to a Commercial License File....117
6.1.2 Incorrect License Usage Information....118
6.1.3 How to Resolve the Problem that the License Does Not Take Effect....119
6.2 Security Management Troubleshooting....120
6.2.1 Failure to Create a U2000 User....120

Copyright © Huawei Technologies Co., Ltd.

6.2.2 U2000 User Is Locked....122
6.2.3 Failed to Start the Security Process....123
6.2.4 How to Configure the ACL for a Client with Multiple Network Adapters....125
6.2.5 Failure to Log In to a U2000 After the Old Password that Expires Is Changed....126
6.2.6 Message indicating Invalid Login Period Displayed During U2000 User Login....126
6.2.7 Users Having the Right to View Devices Outside the Assigned Management Domain....127
6.2.8 Cannot Find New NEs in the Main Topology....128
6.2.9 Inconsistency Between the Client Time and Time in the U2000 Log....129
6.2.10 Failure to Use the Log Forwarding Server....130
6.2.11 U2000 User Password Is Forgotten....132
6.3 Topology Management Troubleshooting....132
6.3.1 Failure to Find a Matched NE Explorer....133
6.3.2 When You Add a NE, the U2000 Prompts That the NE Already Exists....133
6.3.3 Failed to Add a Certain Type of NEs Correctly....134
6.3.4 Cannot Delete a Certain Type of NEs....135
6.3.5 Failed to Add an NE Manually....135
6.3.6 Incorrect Dialog Box Displayed During OSN NE Creation....138
6.3.7 SNMP NE Is Created as a Third-Party NE During Automatic Discovery....139
6.3.8 Frequent Change of Online Status and Offline Status for Some NEs on the U2000....139
6.3.9 Failure to Connect to a Large Number of GNEs on the U2000....140
6.3.10 Objects in the Topology View Are Overlapped....141
6.3.11 Added Topology Objects Are Not Displayed in the Topology View....141
6.3.12 Failed to Ping an NE Using the Ping Tool Provided by the U2000....142
6.3.13 Failed to Log In to a Managed NE Using the Telnet Tool Provided by the U2000 Client....142
6.3.14 Gateway NEs Are Unreachable....143
6.3.15 NE Does Not Exist or Has Been Deleted....143
6.3.16 No WDM NE Is Available for Creation After the U2000 Is Installed....144
6.3.17 A Database Operation Failure Is Reported During an NE Data Upload....144
6.3.18 Status Displayed in the NE Topology View Is Incorrect....145
6.3.19 Message Indicating an MDP Distribution Failure or a Server Response Failure Is Displayed During U2000 Operation....145
6.3.20 Inconsistency Between the WDM NE Quantity in the Topology View with the Actual Quantity....146
6.3.21 How to Process the NE License Alarm of the U2000 Server....148
6.3.22 NE Icon in the Topology Becomes Grey....149
6.3.23 NE Icons in the U2000 Topology View Changed to Blue....149
6.3.24 Time Inconsistency Between the U2000 and NEs....150
6.3.25 Link Display Exception....151
6.3.26 Failure to Display Tracing Status in the Clock View....152
6.3.27 Abnormal Display of NE Panel....152
6.3.28 High Usage of NE Management Process....153
6.3.29 High Usage of NE Management Process....153
6.3.30 LLDP Link Fails to Be Discovered....153

Copyright © Huawei Technologies Co., Ltd.

6.3.31 Main Topology Fails to Be Saved....154
6.3.32 Port Names Fail to Be Modified in Batches....154
6.3.33 NE Discovery Is Unavailable After an Upgrade....155
6.4 Performance Management Troubleshooting....155
6.4.1 PMS Cannot Monitor the ICMP Jitter Performance Data....155
6.4.2 How Do I Query Board Optical Power of NG WDM NEs....155
6.4.3 Failure to Collect Performance Data Due to an Incorrect SNMP Version....156
6.4.4 Failure to Collect Interface Traffic on ME60s....156
6.5 Configuration Failure Troubleshooting....156
6.5.1 A Menu/View Item Is Missing....156
6.6 Alarm Troubleshooting....157
6.6.1 Alarm and Event Postprocessing Function Is Unavailable....157
6.6.2 U2000 Cannot Obtain NE Alarm Information Because of IP Address Mismatch....157
6.6.3 An Alarm About Database Space Is Generated Because of Incorrect U2000 Database Settings....158
6.6.4 U2000 Cannot Receive NE Alarms....159
6.6.5 Cannot Find Some Reported Alarms on the U2000....164
6.6.6 U2000 Client Fails to Play Alarm Sound....164
6.6.7 Failed to Display the Alarm Panel and the Fault Main Menu....165
6.6.8 When a User Browses Alarms or Events, the **Filter** Dialog Box Cannot Be Displayed....166
6.6.9 Acknowledged and cleared alarms exist in the current alarm window....167
6.6.10 Alarm Time Displayed Abnormally....167
6.6.11 LinkDown and LinkUp Alarms Are Displayed After a Long Delay....169
6.6.12 SNMP Version Is Not Supported When Current NE Alarms Are Being Synchronized....170
6.6.13 NE Offline Alarm Is Not Displayed on the U2000 Although Some NEs Get Offline....171
6.6.14 Frequent Historical Alarm Reporting for a PTN NE....171
6.6.15 How Do I View Dumped Historical Alarms/Events?....172
6.6.16 An Alarm Is Not Cleared in Real Time....173
6.6.17 Alarms Cannot Be Cleared....173
6.6.18 Alarm Synchronization Failure Between the U2000 and NEs....174

7 MSTP Network Management Troubleshooting....176

7.1 SDH Trails Management Troubleshooting Cases....177
7.1.1 Insufficient Resources for Creating a Protection Subnet....177
7.1.2 Failure to Delete a Protection Subnet Node Due to Time or Space Division Cross-connections....178
7.1.3 How to Use the End-To-End Trail Management Function....179
7.1.4 Failure to Perform the Related Operations While Trail Creation Succeeded....179
7.1.5 Message Indicating that Cross-Connection Already Exists Displayed During Service Creation....180
7.1.6 Service Timeslot Conflict During Trail Creation....181
7.1.7 Failure to Find Routes During Trail Creation....182
7.1.8 Failure to Find the Reverse Route During Trail Creation....183
7.1.9 How to Select a Port When Creating a Trail....184
7.1.10 Failure to Find Protection Subnets During Creation of a VC12 or VC3 Service....185

Copyright © Huawei Technologies Co., Ltd.

7.1.11 Blank NE Panel Displayed During Trail Creation....186
7.1.12 Operation Timeout Occurs when Configuring Services on the U2000....186
7.1.13 Cannot Form Trails After Search....187
7.1.14 Incorrect Trail Generated After A Trail Search....187
7.1.15 Copying Trails Fails Due to Insufficient Resource....188
7.1.16 Failure to Copy and Paste All SDH Trail Records to an Excel File....190
7.1.17 A Modified Trail Displayed as Unchanged in the Trail Search Result....190
7.1.18 Failure to Browse the Created Trail....191
7.1.19 Cannot Modify an Existing Trail....192
7.1.20 No Cross-Connections in the NE Explorer for Trails in the Manage SDH Trail Window....193
7.1.21 Failed to Delete a Fiber/Cable....193
7.1.22 Inconsistent Timeslot Occupation Between the NE Explorer and the E2E Service Management Window....194
7.1.23 Cannot Open the SDH Trail Management Window....195
7.1.24 NE Cannot Be Added During SDH Trail Modification....195
7.1.25 SDH Trail Fails to Be Deleted....196
7.2 MSTP NE Configuration Troubleshooting Cases....196
7.2.1 Failure to Upload NE Data....196
7.2.2 No Data Returned During Query of NE Performance Data....197
7.2.3 SDH NEs Become Unreachable....197

8 WDM Network Management Troubleshooting....199

8.1 WDM Trails Management Troubleshooting....200
8.1.1 Incorrect Number of Searched-Out Client Trails....200
8.1.2 Failure to Create Trails on WSMD4 Boards....201
8.1.3 Incorrect Trail Rate....202
8.1.4 Cannot Use Trail Functions....203
8.1.5 Failure to Browse the Created WDM Trail....204
8.1.6 Failure to Create the WDM ASON Trail on the U2000 Because of NE Commissioning Times Out....205
8.1.7 How to Select a Port When Creating a Trail....206
8.1.8 Trail Data Is Not Synchronized During a WDM NE Upgrade....207
8.1.9 Inconsistent Timeslot Occupation Between the NE Explorer and the E2E Service Management Window....208
8.2 WDM NE Configuration Troubleshooting Cases....209
8.2.1 A Menu Item Is Missing....209
8.2.2 A WDM NE Cannot Be Opened....209
8.2.3 Allocating Existing OTN Subracks to Optical NEs....210

9 Troubleshooting Native Ethernet Trail Faults....212

9.1 Cannot Use Trail Functions....213

10 PTN Network Management Troubleshooting....214

10.1 Tunnels Are Not Displayed Completely....215

11 Router and Switch Management Troubleshooting.... 216

11.1 NE Channel Management Troubleshooting....218

Copyright © Huawei Technologies Co., Ltd.

11.1.1 Failed to Configure the Syslog Service....218
11.1.2 Failure to Report an Extension Error to the U2000....218
11.1.3 Multiple Duplicate Alarms Are Found....219
11.1.4 FTP Test Failure....220
11.1.5 Excess Historical NE Alarms Are Displayed on the U2000....220
11.1.6 Incorrect NETCONF Parameter Setting....221
11.2 Data Synchronization Troubleshooting....223
11.2.1 Failure to Synchronize Data and the Associated Error Message Displayed....223
11.2.2 A Message Is Displayed Indicating that Executing the SNMP Command Times Out During NE Synchronization....224
11.2.3 A Message Is Displayed Indicating that the Length a Replied SNMP Packet Exceeds the Maximum Value During Data Synchronization....225
11.3 QoS Management Troubleshooting....225
11.3.1 Failed to Deploy the Applying Policy on the GE Interface....225
11.3.2 Configurations Are Invalid Because of Problems with VTY Operation Rights....227
11.4 Troubleshooting LLDP Management....228
11.4.1 Failed to Synchronize LLDP Configurations....228
11.5 Ethernet OAM Management Troubleshooting....230
11.5.1 When a User Performs the Ethernet Link OAM Loopback Test, the System Prompts That the Port Is in the Discovered State and the Loopback Test Cannot Be Started....230
11.5.2 During the Deletion of the MD, MA, Local MEP, or Remote MEP, the System Prompts That the Object to Be Deleted Does Not Exist....232
11.6 MPLS-TP OAM Management Troubleshooting....232
11.6.1 **Failed to send the SNMP message** Is Displayed When MPLS-TP OAM Configurations Are Deployed....233
11.7 Change Audit Troubleshooting....233
11.7.1 In Change Audit, a User Cannot View and Compare the Configuration Files....234
11.8 Link Troubleshooting....235
11.8.1 Links Displayed in Red on the U2000....235
11.8.2 Failure to Automatically Discover Links Between Equipment....236
11.9 Some Information Is Not Displayed in the U2000 NE Explorer and Data Is Not Correctly Displayed on the NE Panel....238
11.10 Failed to Telnet to an NE by Right-clicking the NE Icon on the Main Topology....242
11.11 An NE5000E Is Displayed Abormally After Being Upgraded from a Single Chassis to a Cluster....243
11.12 Failed to Change an NE Interface Description....243
11.13 Failure to Create a Test Case on the NE Side....244
11.14 IP E2E Troubleshooting....244
11.14.1 Services Created by a User Cannot Be Viewed by Other Users After the U2000 Is Upgraded....244
11.14.2 Unavailability of Importing/Exporting Service Options....245
11.14.3 The Create PWE3 Service Window Flickers....246
11.14.4 A Label Allocation Conflict Occurs During the Creation of a Tunnel and a PWE3 Service....246
11.14.5 A PWE3 Service Automatically Discovered by the U2000 Is in the Discrete State....247
11.14.6 How to Delete a PWE3 Service from an Offline NE....247
11.14.7 The U2000 Fails to Query Service Access Interfaces....248

Copyright © Huawei Technologies Co., Ltd.

12 Troubleshooting for the Access Domain....250
12.1 Failure to Make Added MDUs Online....251
12.2 Failure to Add NEs....252
12.2.1 Fault Location for a Failure to Add NEs....252
12.2.2 Troubleshooting for a Failure to Add NEs....253
12.2.3 Analysis on Typical Cases....256
12.3 Failure to Display NE Alarms After an Active/Standby Switchover in a Veritas High Availability System....259
12.4 Message "NE license authority failed" Displayed During NE Creation....261
13 Security NE Management Troubleshooting....265
13.1 Security VPN Service....266
13.1.1 IPSec VPN Service Type Discovery Is Incorrect....266
13.1.2 Failed to Deploy IPSec VPN Services....266
13.2 Centralized Policy Configuration Troubleshooting....267
13.2.1 Failure to Discover or Display NE Configurations on the U2000....267
13.2.2 Failure to Discover Policies, with "TimeRange [time1] no found, make sure it is created or synchronize the NE please." Displayed....268
13.2.3 Failed to Verify, Deploy, or Audit a Policy, with "The ZONE is not found. Please check the NE configuration or synchronize the NE, and make sure zone [zone1] of priority set up." Displayed....269
13.2.4 Failure to Deploy a Policy, with "Conflict with current NE configuration of Interzone Packet-Filter" Displayed....271
13.2.5 Failure to Undeploy a Policy, with "Fail to undeploy" Displayed....272
13.3 Single-Point Web Configuration Troubleshooting....273
13.3.1 Attempt to Log in to the Web Interface Fails and a Message Is Displayed Indicating that the Authentication Fails or Expires....273
13.3.2 Failure to Repair the Web User Account, with "Failed to insert the user" Displayed....274
14 Common Faults and Solutions for the HedEx Helper....276
14.1 When You Access the HedEx Helper Through the Internet Explorer, initialize the progress bar has been at 0% or with Confused Styles....277
14.2 Blank Window Does Not Close When You Attempt to View Help Information by Pressing F1....278
14.3 Libraries Fail to Be Uploaded in IE8.0....280
14.4 The System Prompts "`Retrieving verify code failed`" When You Register with the HedEx Helper or Log In to the HedEx Helper with a User Name....281
14.5 A Blank Window Appears in the Firefox When You Press F1 on the EMS Interface....284
14.6 An Exception Occurs when You Export All the Remarks....286
14.7 Failed to Launch the U2000 Online Help on Solaris OS....286
14.8 "Firefox is already running, but is no responding" Is Displayed When a User Presses **F1** on Solaris-based U2000....288
14.9 Online Help Cannot Be Launched on the System Monitor Client....290
14.10 Help Is Not Displayed After F1 Is Pressed....291
14.11 The "The page cannot be displayed" Message Is Displayed Upon an Attempt to Visit the HedEx Helper....292
14.12 U2000 Help Invoked by F1 Is Displayed Unstably....292
A NMS Alarm Reference.... 295

Copyright © Huawei Technologies Co., Ltd.

A.1 NE_COMMU_BREAK....300
A.2 NE_NOT_LOGIN....303
A.3 ALARM_PERFORM_LOG_SIZE_CROSS_THRESHOLD....304
A.4 GNE_CONNECT_FAIL....305
A.5 The Device Is Offline....308
A.6 COMMU_BREAK_BTWN_NE_AND_BAKGNE....308
A.7 GNE_MGR_LIMIT_OVER....310
A.8 DB_ERR_AUTO_CLEAR_FRAGMENT_DATA....311
A.9 MGR_LIMIT_OVER....313
A.10 EMS_SERVER_STARTUP....314
A.11 SERVICE_OUTAGE....315
A.12 PROTECT_DEGRADED....316
A.13 GNE_NUM_LIMIT_OVER....317
A.14 XC_LICENSE_OVERFLOW....318
A.15 XC_LICENSE_UNEXPECTED....319
A.16 NE_COMMU_GNE_SWITCH....321
A.17 PROTECT_LOSS....322
A.18 LOOP_ALM....323
A.19 CLOSETO_MAX_CAPACITY....324
A.20 OVERFLOW_MAX_CAPACITY....325
A.21 NE_DATA_INCONSISTENCY....325
A.22 CLOSETO_AIR_LICENSE_LIMIT....326
A.23 OVERFLOW_AIR_LICENSE_LIMIT....327
A.24 ALM-33 The Server Is Disconnected from the Database....328
A.25 ALM-34 The Disk Usage Is Too High (Warning)....330
A.26 ALM-35 The Disk Usage Is Too High (Minor)....335
A.27 ALM-36 The Disk Usage Is Too High (Major)....339
A.28 ALM-38 The database process is abnormal....344
A.29 ALM-39 The database had exception logs....346
A.30 ALM-40 The ESN of the server does not match that in the License file....348
A.31 ALM-42 The Database Usage Is Too High (Warning)....349
A.32 ALM-43 The Database Usage Is Too High (Minor)....353
A.33 ALM-44 The Database Usage Is Too High (Major)....357
A.34 ALM-47 Memory Usage of Service Is Too High....361
A.35 ALM-50 Task execution failure alarm....362
A.36 ALM-51 The temporary Feature field of the OSS License file expires....364
A.37 ALM-52 The temporary Feature field of the OSS License file enters to the default state....365
A.38 ALM-53 High log space usage for the database....366
A.39 ALM-54 The swap Usage Is High....368
A.40 Communication with the Device Failed....371
A.41 ALM-100 The CPU Usage Is High....372

Copyright © Huawei Technologies Co., Ltd.

A.42 ALM-101 The Disk Usage Is Too High (Critical)....376
A.43 ALM-102 The Memory Usage Is Too High....380
A.44 ALM-103 The Database Usage Is Too High (Critical)....383
A.45 ALM-106 The OSS Service Is Terminated Abnormally....387
A.46 MAC Address Conflict....388
A.47 OMC license not exist....389
A.48 ALM-114 The Number of Login Attempts Reaches the Maximum....390
A.49 ALM-116 The Master Server Cannot Communicate with the Slave Server....391
A.50 ALM-117 Avalanche alarm....393
A.51 ALM-120 The number of records in the database table has reached the threshold....395
A.52 Predeploy device type no match....397
A.53 ALM-121 Sending Remote Notification Message Failed....398
A.54 ALM-123 The Digital Certificate Is to Expire....399
A.55 ALM-124 The Digital Certificate Has Expired....401
A.56 ALM-119 Alarm of the Switchover to the Standby Syslog Server....402
A.57 ALM-118 Alarm of the Failure to Connect the Master and Standby Syslog Servers....403
A.58 ALM-130 The Alarm Report Buffering Blocked....405
A.59 ALM-294 Expired OSS License File....406
A.60 ALM-295 OSS License File in Default State....407
A.61 ALM-296 The NE Capacity Reached the Threshold Alarm....408
A.62 ALM-297 The OSS License Expired....410
A.63 ALM-298 The User in the SMManagers Group Changes a User's Password....411
A.64 ALM-299 An OSS User Is Added to the Administrators, SMManagers or Sub Domain User Group....412
A.65 The status of the interface configured with IPSec services turns to **Down**....412
A.66 ALM-801 OSS License Beyond Limitation....413
A.67 OceanStor Storage System Alarm....414
A.68 ALM-1100 CPU abnormal....421
A.69 ALM-1101 Memory abnormal....422
A.70 ALM-1102 Environment abnormal....423
A.71 ALM-1103 HD abnormal....424
A.72 ALM-1119 Network interface status changed....425
A.73 Power Failure....429
A.74 Fan Failure....429
A.75 Hard Disk Failure....430
A.76 The Network Cable Is Disconnected....431
A.77 NIC in Half-Duplex Mode....432
A.78 Power Threshold Alarm....434
A.79 Database Size exceeds the threshold....435
A.80 The size of Sybase logs exceeds the threshold....436
A.81 The usage of the paged kernel memory on Windows exceeds the alarm threshold....437
A.82 The usage of the non-paged kernel memory on Windows exceeds the alarm threshold....438

Copyright © Huawei Technologies Co., Ltd.

A.83 The virtual memory of Windows is insufficient....439
A.84 The disk space for the virtual memory of Windows is insufficient....440
A.85 The swap space is insufficient....441
A.86 Database needs to be maintenanced....441
A.87 Database needs to be maintenanced....442
A.88 Database needs to be maintenanced....443
A.89 NE SSH Fingerprint Mismatch....444
A.90 Failure to Connect to an Integration Server....445
A.91 Failure to Connect to All Integration Servers....447
A.92 Abnormal Integration Information....449
A.93 OCH_TRAIL_POWER_ABNORMAL....450
A.94 Communication Failure of Alarm Reporting Channel....451
A.95 Buffer Overflow of Alarm Reporting Channel....451
A.96 A Member System in the Maintenance State....452
A.97 PSEUDOWIRE_OUTAGE....453
A.98 Trap numbers of NEs exceeded the threshold of NMS....454
A.99 NE Management by Multiple U2000s....455
A.100 Data Inconsistency....455
A.101 **tmp** Occupies Much Space....456
A.102 Veritas Resources Are Faulty....457
A.103 Veritas replication buffer exceeds the threshold....460
A.104 Manual Restoration Is Required After Primary-Primary Veritas Status....461
A.105 Veritas Heartbeat Is Interrupted....464
A.106 The Veritas data replication is interrupted....465
A.107 Veritas Resource Group Is Frozen....466
A.108 Veritas License Is a Temporary One....468
A.109 Veritas Process Is Faulty....469
A.110 Automatic Backup Operation Failed....470
A.111 Automatic Save Operation Failed....471
A.112 Automatic Recover Operation Failed....472
A.113 ALM-52003 Host cpu usage....473
A.114 ALM-52004 Host memory usage....475
A.115 ALM-52005 Virtual machine cpu usage....477
A.116 ALM-52006 Virtual machine memory usage....479
A.117 ALM-52008 Unable connect to vCenter Server....480
A.118 ALM-52009 Datastore usage on disk....482
A.119 FIBER_POWER_DEG....484
A.120 Database Backup....486
A.121 Unified Management Engine License Alarm....488
A.122 A Fault Occurs on the FTP or SFTP Server That Is Used to Execute ONT Loading Tasks....489
A.123 CLOCK_LINK_LOOP....490

Copyright © Huawei Technologies Co., Ltd.

A.124 The device is unwonted....491
A.125 NE type change....492
B Obtaining Technical Support....494
C Glossary and Abbreviations....495

Copyright © Huawei Technologies Co., Ltd.

1 Security Precautions (for Troubleshooting)

This topic describes basic troubleshooting principles. You must locate and rectify a fault based on the troubleshooting principles and precautions.

Troubleshooting Principles

Analyze, locate, and rectify a fault in compliance with the following principles:

- Restore system monitoring as soon as possible.
- Before locating a fault, collect the fault data in time, and save the collected data to a mobile storage medium or another computer on the network.
- When determining a troubleshooting scheme, evaluate the impact first to ensure the normal transmission of services.
- Refer to the documents related to third-party hardware or call the customer service center of third-party hardware to rectify faults of third-party hardware.
- If a fault cannot be located or rectified according to relevant manuals, contact the local **Huawei Global TAC Information** to seek for technical support. Cooperate with engineers from Huawei to shorten the duration of service interruption to the maximum.

Precautions

- Analyze the fault symptom and rectify the fault after locating the cause. If the cause is unknown, do not perform operations at random. This is to prevent the problem from being worsened. Rectifying the U2000 faults does not affect the running of NEs.
- Before rectifying a fault, keep all on-site records concerning the fault and do not delete any data or log randomly.
- To ensure customer network security and privacy, obtain the customer's agreement before collecting fault logs during troubleshooting.
- To ensure system security, using SFTP to upload files to the server or download files from the server during troubleshooting is recommended.
- Before a modification is performed, manually back up the U2000 data or export scripts to back up the U2000 data.
- After the system recovers, view the running status and ensure that the fault is rectified. Complete the associated troubleshooting report in a timely manner.
- After SetSolaris is enabled in Solaris OS, the **ossuser** user has the login permission only for accessing Secure Shell (SSH) services. The SSH login mode is recommended for your

Copyright © Huawei Technologies Co., Ltd.

system security. To use another login mode such as Telnet, you must enable the access permission for the Telnet service and the login user.

- After SetSUSE is enabled in SUSE Linux OS, the **ossuser** user has the login permission only for accessing Secure Shell (SSH) services. The SSH login mode is recommended for your system security. To use another login mode such as Telnet, you must enable the access permission for the Telnet service and the login user.

Collecting Fault Data

When a fault occurs on the U2000, see **Collecting Fault Data** in *Troubleshooting* to collect the fault data.

In addition to manual fault data collection, you can use the UEasy to collect data. On Solaris or SUSE Linux, the UEasy is stored in the **/opt/oss/server/tools/UEasy** directory. On Windows, the UEsay is stored in the **D:\oss\server\tools\UEasy** directory. For details about how to use the UEasy, see the **readme_en.txt** file in the storage directory.

NOTE

To ensure network security, obtain written authorization from the customer before collecting fault information. In addition, you must obey local laws or Huawei user privacy policies and take appropriate measures to ensure that user privacy data is fully protected.

Copyright © Huawei Technologies Co., Ltd.

2 Basic Troubleshooting Principles

This topic describes basic troubleshooting principles. You must locate and rectify a fault based on the troubleshooting principles and precautions.

Troubleshooting Principles

Analyze, locate, and rectify a fault in compliance with the following principles:

- Restore system monitoring as soon as possible.
- Before locating a fault, collect the fault data in time, and save the collected data to a mobile storage medium or another computer on the network.
- When determining a troubleshooting scheme, evaluate the impact first to ensure the normal transmission of services.
- Refer to the documents related to third-party hardware or call the customer service center of third-party hardware to rectify faults of third-party hardware.
- If a fault cannot be located or rectified according to relevant manuals, contact the local **Huawei Global TAC Information** to seek for technical support. Cooperate with engineers from Huawei to shorten the duration of service interruption to the maximum.

Precautions

- Analyze the fault symptom and rectify the fault after locating the cause. If the cause is unknown, do not perform operations at random. This is to prevent the problem from being worsened. Rectifying the U2000 faults does not affect the running of NEs.
- Before rectifying a fault, keep all on-site records concerning the fault and do not delete any data or log randomly.
- To ensure customer network security and privacy, obtain the customer's agreement before collecting fault logs during troubleshooting.
- To ensure system security, using SFTP to upload files to the server or download files from the server during troubleshooting is recommended.
- Before a modification is performed, manually back up the U2000 data or export scripts to back up the U2000 data.
- After the system recovers, view the running status and ensure that the fault is rectified. Complete the associated troubleshooting report in a timely manner.
- After SetSolaris is enabled in Solaris OS, the **ossuser** user has the login permission only for accessing Secure Shell (SSH) services. The SSH login mode is recommended for your

Copyright © Huawei Technologies Co., Ltd.

system security. To use another login mode such as Telnet, you must enable the access permission for the Telnet service and the login user.

- After SetSUSE is enabled in SUSE Linux OS, the **ossuser** user has the login permission only for accessing Secure Shell (SSH) services. The SSH login mode is recommended for your system security. To use another login mode such as Telnet, you must enable the access permission for the Telnet service and the login user.

Copyright © Huawei Technologies Co., Ltd.

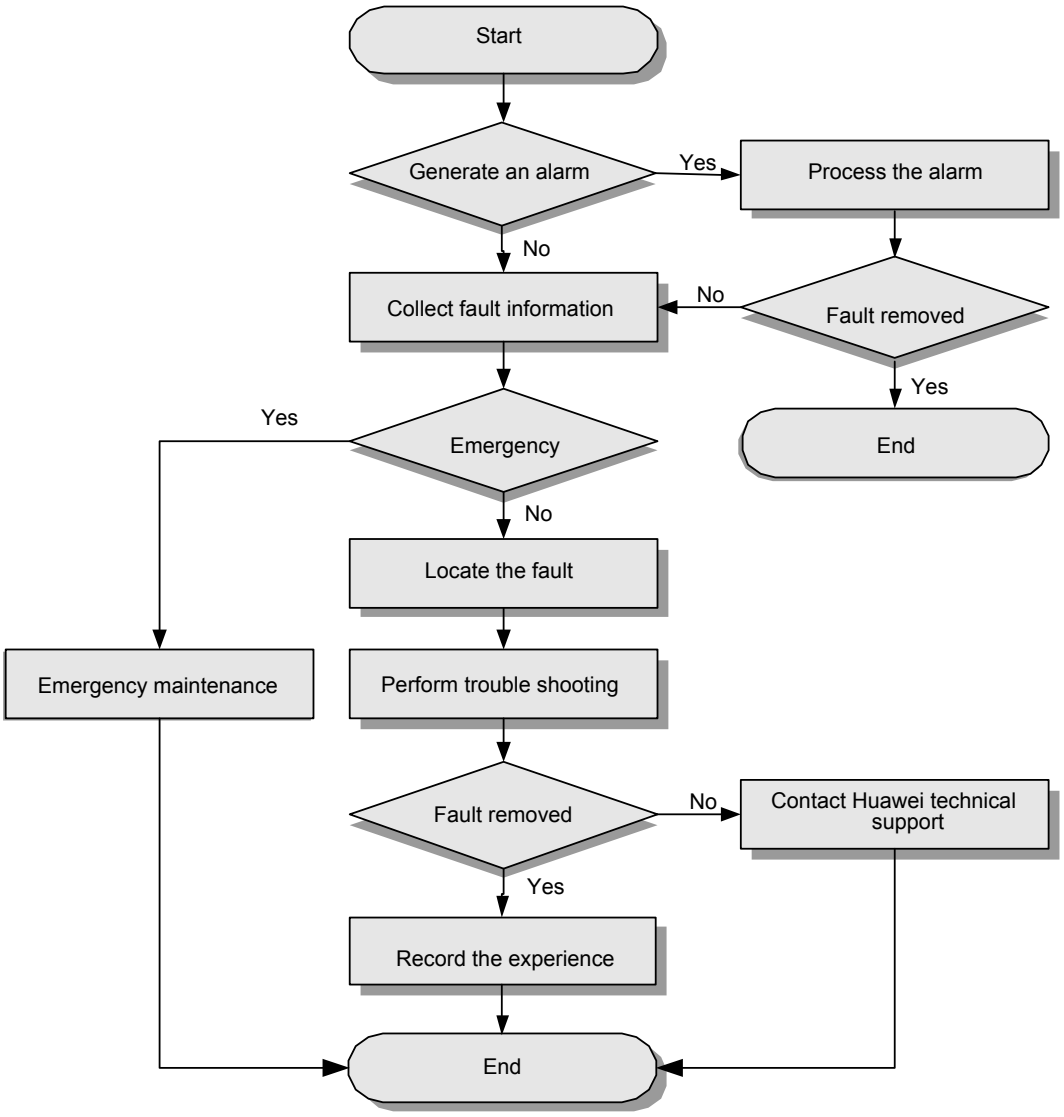
3 Troubleshooting Process

This topic describes the process of troubleshooting the U2000. If the U2000 does not work properly because of incorrect operations, external causes such as power failure, or U2000 software or hardware faults, the network may fail to be monitored. In this case, locate the fault and repair the system by referring to the troubleshooting process and observing the troubleshooting principles and precautions. If the problem persists, contact the local office or customer service center of Huawei.

Figure 3-1 shows the troubleshooting process.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Troubleshooting process



NOTE

- Normally, there are three stages of troubleshooting: fault location, information collection, and fault rectification.
- If an alarm is generated or an abnormal event occurs on the U2000, clear the fault as prompted.

Copyright © Huawei Technologies Co., Ltd.

4 Collecting Fault Data

In the case of a system fault, you must collect the related data in time to locate and rectify the fault.

When a fault occurs on the U2000, see **Table 4-1** to collect the fault data.

In addition to manual fault data collection, you can use the UEasy to collect data. On Solaris or SUSE Linux, the UEasy is stored in the **$IMAP_ROOT/tools/UEasy** directory. On Windows, the UEsay is stored in the **%IMAP_ROOT%\tools\UEasy** directory. For details about how to use the UEasy, see the **readme_en.txt** file in the storage directory.

NOTE

To ensure network security, obtain written authorization from the customer before collecting fault information. In addition, you must obey local laws or Huawei user privacy policies and take appropriate measures to ensure that user privacy data is fully protected.

Table 4-1 Fault data collection items

Collection Item	Description
Time and place	Time and place of a fault. The time should be accurate to the minute.
Symptom description	Symptom of a fault. Detailed description facilitates fault location.
Measures taken and result	After you take some preliminary troubleshooting measures in the field, new problems may occur. You must record in details the procedure for taking measures and the subsequent result.
Version information	View the version information about the U2000. ● On Solaris or SUSE Linux ,the default directory storing the **imap.cfg** file is **/opt/oss/server/etc/conf**. ● On Windows, the default directory storing the **imap.cfg** file is **D:\oss\server\etc\conf**. The version information about the U2000 is displayed in the last several lines of the **imap.cfg** file.

Copyright © Huawei Technologies Co., Ltd.

Collection Item	Description

	Do as follows to view system information:
	● On Solaris or SUSE Linux, do as follows to view system information:
	Log in to the OS as the **root** user. Then, run the following command:
	`# uname -a`
	● On SUSE Linux, you can also run the following command to view the version information about the SUSE Linux OS:
	`# cat /etc/SuSE-release`

	Do as follows to view the version information about the database.
	● On Solaris or SUSE Linux OS, run the following commands:
	`# su - dbuser`
	`$ isql -SDBSVR -Usa`
	NOTE
	Enter the database sa user password as prompted.
	`1> select @@version`
	`2> go`
	● On Windows, run the following commands in a CLI:
	`> isql -SDBSVR -Usa`
	NOTE
	Enter the database sa user password as prompted.
	`1> select @@version`
	`2> go`

IP address information	Run the following commands to view the IP address and MAC address: ● On Solaris or SUSE Linux, log in to the system as the **root** user and run the **ifconfig -a** command. ● On Windows, open a CLI and run the **ipconfig /all** command.
Alarm information	Collect the alarm information, especially information about U2000 alarms or abnormal events.
Log information	OS logs: ● On Windows: Choose **Start** > **Run**. Enter **eventvwr.msc** and then press **Enter**. In the **Event Viewer** dialog box, select the associated event name, right-click, and choose the associated option from the shortcut menu to save the OS logs. ● On Solaris: View OS logs in the **/var/adm** path. You can also navigate to the **/opt/SUNWexplo/bin/explorer** path and then collect log information about the OS. ● On SUSE Linux: View OS logs in the **/var/log**.
	Database logs: ● SQL Server 2008: the ERRORLOG files in the ***MSSQLServer 2008_installation_directory*\100\Setup Bootstrap\Log**. ● Sybase: **$SYBASE/$SYBASE_ASE/install/DBSVR.log**. For example: **/opt/sybase/ASE-15_0/install/DBSVR.log**.

Copyright © Huawei Technologies Co., Ltd.

Collection Item	Description
	U2000 logs: ● Server logs – On Windows: **%IMAP_ROOT%\server\var\logs**. For example: **D:\oss\server\var\logs**. – On Solaris: **$IMAP_ROOT/server/var/logs**. For example: **/opt/oss/server/var/logs**. – On SUSE Linux: **$IMAP_ROOT/server/var/logs**. For example: **/opt/oss/server/var/logs**. ● Client logs – On Windows: **%OSS_ROOT%\client\logs**. For example: **D:\oss\client\logs**. – On Solaris: **$OSS_ROOT/client/logs**. For example: **/opt/oss/client/logs**. ● On Solaris: **$OSS_ROOT/client/var/log**. For example: **/opt/U2000/client/var/log**. ● Operation logs (including historical records about installation, deployment, upgrade, patch installation, login, and other operations) – Windows: **%APPDATA%engineer.log** – Solaris: **:/var/tmp/engineer.log** – SUSE Linux: **/var/log/engineer.log** For details about how to collect log information about the U2000, see **Log Management** in the *U2000 Administrator Guide*.
Networking diagram	If the fault is caused by networking problems, you need to view the networking diagram.
ICMR-related files	If the server runs on Solaris or SUSE Linux, you must obtain the following ICMR-related files: ● Files in the **/etc/ICMR** path ● Files in the **/var/ICMR** path

Copyright © Huawei Technologies Co., Ltd.

5 U2000-Related Faults

About This Chapter

This topic describes how to troubleshoot the U2000-related faults.

5.1 Solaris Troubleshooting
This topic describes how to troubleshoot the faults on the U2000 running on Solaris.

5.2 SUSE Linux Troubleshooting
This topic describes how to troubleshoot the faults on the U2000 running on SUSE Linux.

5.3 Sybase Database Troubleshooting
This topic describes how to troubleshoot faults on the Sybase database.

5.4 SQL Server Database Troubleshooting
This topic describes how to troubleshoot faults on the SQL Server database.

5.5 U2000 Server Troubleshooting
This topic describes how to troubleshoot faults on the U2000 server.

5.6 Faults on a U2000 Client
This topic describes how to troubleshoot faults on a U2000 client.

5.7 U2000 Running Slowly
This section describes how to locate the slow U2000 operating problem.

5.8 Veritas High Availability System Troubleshooting
This topic describe how to troubleshoot faults on a Veritas high availability system.

Copyright © Huawei Technologies Co., Ltd.

5.1 Solaris Troubleshooting

This topic describes how to troubleshoot the faults on the U2000 running on Solaris.

5.1.1 Failure to Start the OS

The OS cannot be started or is restarted repeatedly. If such a fault occurs, users fail to access the login window.

The following table shows the procedure for locating and rectifying the fault.

Step	Symptom	Troubleshooting
1	No information is displayed.	Check whether the monitor and the server are properly connected.
2	Error messages are displayed.	Rectify the fault as prompted and by referring to the following symptoms: ● **OS Entering the Single-User Mode After Restart** ● **Repeated OS Startup** ● **Failure to Match the Monitor**
3	Unknown symptom.	Contact Huawei engineers for troubleshooting.

OS Entering the Single-User Mode After Restart

Symptom

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

NOTE

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

Possible Causes

The server is switched off or powered off illegally, which results in the fact that the running file system 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.

Procedure

Step 1 Log in to the OS as the **root** user.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Run the following command to restore the file system:

```
# fsck -y
```

NOTICE

- 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 on the server. Otherwise, the OS cannot recover.
- The **fsck** command can be used to rectify only common faults. For the fault on the Solaris startup parameters or kernel damage due to abnormal power failure, the command is invalid.

Step 3 Observe the command output. 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 asking you to restore the system is displayed again, run the **fsck -y** command repeatedly until such information is not displayed any more.

Step 4 Run the following commands to synchronize the files and restart the OS:

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

----End

Suggestion and Summary

It is prohibited to shut down the server illegally. Configuring the server with UPS (Uninterrupted Power Supply) recommended to effectively prevent power failures.

Repeated OS Startup

Symptom

On a single-server system, the message "Cannot open '/etc/path_to_inst' Program terminated." is displayed and the OS then starts repeatedly.

Possible Causes

The server is powered off abnormally or other abnormal operations are performed, which leads to the damage on the OS and a failure to open the **path_to_inst** system file. As a result, the OS fails to be started.

Procedure

Step 1 During self-check of the OS (before entering the OS), press **STOP+A** to exit the startup. The `ok` prompt is displayed.

Step 2 Insert the installation DVD of Solaris 10. To start installation by using a DVD and enter the single-user mode, run the following command:

```
ok boot cdrom -s
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Wait 5 minutes. When **SINGLE USER MODE** and **#** are displayed, the system enters the single-user mode.

Step 3 To search for the raw equipment name associated with the system root path, run the following command:

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

The following information is displayed:

NOTE

The command output varies according to the actual situation.

```
#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 preceding information, the raw partition associated with the root path (/) is **/dev/dsk/c1t0d0s0**.

Step 4 Set the raw partition associated with the root path to the **/mnt** path to restore the damaged OS.

```
# mount raw_equipment_name /mnt
```

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

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

Step 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** path:

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

Step 6 Run the following commands to synchronize the files and restart the OS:

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

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

----End

Failure to Match the Monitor

Symptom

After the workstation is started, a message is displayed indicating that the system does not match the monitor and the **/var/dt/Xerrors** file contains error messages.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

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

Procedure

Step 1 Repair the connections of peripherals (such as the mouse, keyboard, and monitor) as prompted.

Step 2 Stop the U2000 processes and the database process.

Step 3 Run the following commands to restart the workstation:

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

----End

5.1.2 Failure to Log In to the GUI of the OS

Symptom

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

Possible Causes

Abnormal shutdown may damage the file system and as a result, users cannot log in to the GUI after the Solaris OS is started. You can use the **fsck** command to restore the file system.

Procedure

Step 1 After the Solaris OS is started, enter the password of the **root** user as prompted. A CLI is displayed.

Step 2 Run the following command for several times to perform automatic fault rectification:

```
# fsck -y
```

NOTE

The **fsck** command can be used to rectify only common faults. This command does not work for the fault on the Solaris startup parameters or kernel damage due to abnormal power-off.

Step 3 Run the following commands to restart the workstation:

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

----End

Copyright © Huawei Technologies Co., Ltd.

5.1.3 How to Solve the Problem Where the Monitor or KVM Cannot Access the GUI After the OS Is Installed on the Netra T4-1/Netra T4-2/Oracle T4-1/Oracle T4-2/T5220 Server

Question

The OS was installed by using the quick installation DVD. After the Netra T4-1/Netra T4-2/Oracle T4-1/Oracle T4-2/T5220 is connected to the KVM, the GUI cannot be opened. How do I rectify this fault?

Answer

Step 1 **Optional:** If the firmware version of system controller is earlier than **3.2.1**, set the I/O mode, run the following commands:

eeprom output-device=screen

eeprom input-device=keyboard

NOTE

Log in to the controller of the server as the root user. Run the following command to view the version of the system controller firmware:

```
-> cd /HOST
-> ls
```

Step 2 To set the screen resolution and refresh rate, perform the following operations:

1. To view information about the current video board, run the following command:

   # **fbconfig -list**

   A message similar to the following will be displayed:

   ```
   Device File Name            Device Model     Config Program
   ----------------            ------------     --------------
   /dev/fbs/ast0              display          fbconf_xorg
   ```

   NOTE

   The value of */dev/fbs/ast0* differs according to on-site requirements.

2. **Optional:** If **Config Program** is displayed as **program not available**, run the following commands:

   # **ln -s** */dev/fbs/ast0* **/dev/fb**

   # **fbconfig -xserver Xorg**

3. To view the screen resolution and refresh rate supported for the current video board, run the following command:

   # **fbconfig -dev** */dev/fbs/ast0* **-res \?**

   A message similar to the following will be displayed:

   ```
   Valid values for -res option are:
              ...
              ...
   VESA_STD_640x480x60
   [1] Resolution is supported by monitor
   ```


Copyright © Huawei Technologies Co., Ltd.

```
[2] Preferred resolution for monitor
No EDID data for monitor.  Can not determine supported resolutions.

Use of an unsupported resolution can render the video display unusable.

Abbreviations such as "1280x1024x75" may also be used.
```

4. To view the current configurations for the video board, run the following command:

   # **fbconfig -dev** */dev/fbs/ast0* **-propt**

   A message similar to the following will be displayed:

```
--- Graphics Configuration for /dev/fbs/ast0 ---
xorg.conf: machine -- /etc/X11/xorg.conf
    Screen section:  "ast0"
    Device section:  "ast0"
    Monitor section: none

Video Mode: Not set

Screen Information:
    Remote Screen: Not set
```

5. The screen resolution and refresh rate are not set if **Video Mode** is set to **not set**. To set the screen resolution and refresh rate, run the following commands:

   # **fbconfig -dev** */dev/fbs/ast0* **-res** *1024x768x60* **now**

   A message similar to the following will be displayed:

```
fbconf_xorg: Unrecognized video mode, "1024*768*60"
fbconf_xorg: Use "1024*768*60" anyway (yes/no) ?
```

   Enter **y**, and then press **Enter**. A message similar to the following will be displayed:

```
Setting 1024x768x60
```

6. To view the current configurations for the video board, run the following command:

   # **fbconfig -dev** */dev/fbs/ast0* **-propt**

   The setting has taken effect if a message similar to the following is displayed.

```
--- Graphics Configuration for /dev/fbs/ast0 ---

xorg.conf: machine -- /etc/X11/xorg.conf
    Screen section:  "ast0"
    Device section:  "ast0"
    Monitor section: "ast0"

Video Mode: "VESA_STD_1024x768x60"

Screen Information:
    Remote Screen: Not set
```

Step 3 To restart the OS, run the following command. After the OS is restarted, connect the Netra T4-1/ Netra T4-2/Oracle T4-1/Oracle T4-2/T5220 to the KVM.

NOTE

If a message asking you to enter a user name is displayed on the monitor or KVM during the restart of the OS, ignore the message. The OS automatically accesses the login window.

sync;sync;sync;sync

Copyright © Huawei Technologies Co., Ltd.

```
# shutdown -y -g0 -i6
```

----End

5.1.4 Failure to Open Graphical Tools

Symptom

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

Possible Causes

The **DISPLAY** environment variable is not set on the GUI.

Procedure

Step 1 Log in to the GUI of the Solaris OS.

Step 2 Run the following commands to query the terminal number as the **root** user:

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

Step 3 Run the following commands to set the **DISPLAY** environment variable:

```
# 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
```

Step 4 Open the graphical tools again.

----End

5.1.5 Failure to Eject a DVD

Symptom

If a DVD is damaged or inserted to the DVD-ROM drive, when you use the **eject** command to open the drive, the message "Device busy" is displayed and the DVD cannot be ejected.

Possible Causes

- The DVD has not been used for a long time or is used incorrectly.
- Certain DVD data is in use.

Procedure

Step 1 If the DVD is damaged, reinstall the DVD-ROM drive and restart the OS.

Step 2 Ensure that no DVD data is being used.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Run the following command as the **root** user:

```
# svcadm disable -t volfs
```

Step 4 Press the eject button on the drive panel to take out the DVD from the DVD-ROM drive.

Step 5 Run the following command to resume the DVD-ROM drive:

```
# svcadm enable volfs
```

----End

5.1.6 Operation Abnormality Caused by Insufficient Disk Space

Symptom

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

Possible Causes

Normally, the disk usage cannot be larger than 80%.

Procedure

Step 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 paths such as /, **/opt**, and **/opt/oss** in the command output.

Step 2 If the size of the disk space exceeds the normal value, you must manually clean up the disk. For details, see the **Managing U2000 Files and Disks** in the *U2000 Administrator Guide*.

Step 3 If the disk space remains insufficient after the preceding operations are performed, check whether the hard disk configurations of the server meet network size requirements. Different network sizes require different hard disk configurations. For details, see the *U2000 Planning Guide*. If the hard disk configurations do not meet requirements, replace the hard disk.

----End

5.1.7 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

Step 1 To check the memory usage, run the following command as the **root** user:

Copyright © Huawei Technologies Co., Ltd.

```
# vmstat 2
```

The following information is displayed:

```
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 values in the **sr** column remain at a range from 200 to 300 page/sec, the physical memory may be insufficient.

Step 2 Close unnecessary applications.

Step 3 If the memory usage remains high, replace the physical memory.

----End

5.1.8 Slow Running of the System Caused by Too High CPU Usage

Symptom

The U2000 runs at a low speed.

Possible Causes

The CPU usage may be too high.

Procedure

Step 1 To check the memory usage, run the following command as the **root** user:

```
# vmstat 2
```

The following information is displayed:

```
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 period of time, the dominant frequency of the CPU will be the bottleneck of the running efficiency.

Step 2 Close unnecessary applications.

----End

Copyright © Huawei Technologies Co., Ltd.

5.1.9 Failure to Connect the SUN Server and a Switch Because of an Auto-Negotiation Failure

Symptom

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

Possible Causes

Some NICs do not support the auto-negotiation mode of 100 M full-duplex.

Procedure

Step 1 Run the following command as the **root** user to navigate to the **rc3.d** folder:

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

Step 2 Run the following commands and use **vi** commands to create and modify the file **S99set*bge***:

```
# 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)
```

Step 3 Run the following commands to modify attributes of the **S99setbge** file:

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

Step 4 Run the following commands to view attributes of the **S99setbge** file:

```
# ls -l S99setbge
```

Step 5 Run the following commands to restart the system to make the NIC configurations take effect:

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

Step 6 Run the following commands to check whether the NIC is successfully configured:

```
# 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
```


Copyright © Huawei Technologies Co., Ltd.

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

The mapping relations between the values of **link_duplex** and attributes are as follows:

- 0 indicates down.
- 1 indicates half duplex.
- 2 indicates full duplex.

----End

5.2 SUSE Linux Troubleshooting

This topic describes how to troubleshoot the faults on the U2000 running on SUSE Linux.

5.2.1 Failure to Log In to the GUI

Symptom

After the SUSE Linux OS is started, users cannot access the GUI.

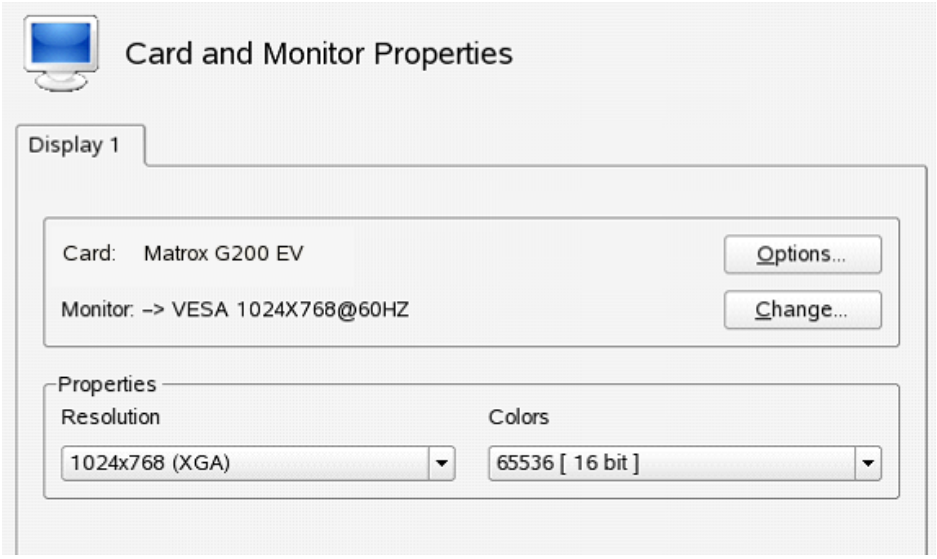
Possible Causes

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

Procedure

Step 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
```



Copyright © Huawei Technologies Co., Ltd.

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

Step 3 Click **OK**.

Step 4 In the dialog box that is displayed, click **Test**.

Step 5 After the test is carried out, click **OK**. In the dialog box that is displayed, click **Save**.

Step 6 In the dialog box that is displayed, click **Yes** to exit from the sax2 window.

Step 7 Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r now
```

----End

5.3 Sybase Database Troubleshooting

This topic describes how to troubleshoot faults on the Sybase database.

5.3.1 Failure to Immediately Back Up the Sybase Database

Symptom

The backup file does not exist in the path specified in a database backup task.

Possible Causes

The possible causes are as follows:

- The database is not started.
- The disk space is used up.
- Permissions for the backup path are incorrect.
- The password of the database user **sa** is not changed properly.
- Another user has logged in to the NMS Maintenance Suite client.
- Another database backup task is being executed.
- The NMS Maintenance Suite server is not started.

Procedure

Step 1 Check whether the database has been started. For details, see **5.3.4 How to Verify That the Sybase Database Is Running**.

Step 2 Check the disk space. For details, see **5.1.6 Operation Abnormality Caused by Insufficient Disk Space**.

Step 3 Check the permissions for and the owner of the backup path.

Run the **ls -al** command to check the permissions for the backup path. The owner of the backup path must be the **ossuser** user and the permissions to read, write, and execute the backup path

Copyright © Huawei Technologies Co., Ltd.

must be granted. For details about how to grant these permissions, see the common commands for the Solaris OS.

NOTE

- On Solaris OS or SUSE Linux OS, if the backup path already exists, assign permissions to the backup path based on the level. The backup path needs to belong to the **/opt** directory in order to prevent modification on the system directory from damaging the U2000 environment. You do not need to change the permission to the **/opt** path. The number of operation sets assigned to the **/opt/oss** directory is 750, and the number of operation sets assigned to other subdirectories under the **/opt** directory is 770.

  Run the following commands as the **root** user for all directories except for the last directory of the path:
  ```
  # chown ossuser:ossgroup path
  # chmod 770 path
  ```
  Run the following command for the last directory of the path:
  ```
  # chown -R ossuser:ossgroup path
  # chmod -R 770 path
  ```
  For example, if the path is **/opt/backup1/backup2**, run the following commands as user **root**:
  ```
  # chown ossuser:ossgroup /opt/backup1
  # chmod 770 /opt/backup1
  # chown -R ossuser:ossgroup /opt/backup1/backup2
  # chmod -R 770 /opt/backup1/backup2
  ```
- The backup directory must be an absolute path that contains letters, digits, underscores (_), or hyphens (-) and excludes the space, bracket, Chinese characters and so on. The path name cannot exceed 60 characters. For Windows, the backup directory must be located on the disk drive of the server.

Step 4 Ensure that the password of the database user **sa** has been changed according to the associated operation guide. If the password is changed improperly, restore the previous configuration and then use the NMS Maintenance Suite to change the password again. For details, see Chapter "Changing the Password of the Administrator of the Database" in the *U2000 Administrator Guide*.

Step 5 Ensure that all users have logged out of the NMS Maintenance Suite client.

Step 6 Check whether another database backup task is being executed. If such a task is being executed, back up the database after the task is complete.

Step 7 Run the following command as the **root** user to verify that the NMS Maintenance Suite is running:
```
# ps -ef | grep java
```
If the command output contains **/opt/OSSJRE/jre_sol/bin/java -server** or **/opt/OSSJRE/jre_linux/bin/java -server**, the NMS Maintenance Suite is running. If the command output does not contain **/opt/OSSJRE/jre_sol/bin/java -server**, run the following commands to start the NMS Maintenance Suite:
```
# cd /opt/OSSENGR/engineering
# ./startserver.sh
```

Step 8 If the problem persists, run the following commands to restart the NMS Maintenance Suite server:
```
# cd /opt/OSSENGR/engineering
# ./stopserver.sh
# ./startserver.sh
```

----End

5.3.2 Failure to Start the Sybase Database

Copyright © Huawei Technologies Co., Ltd.

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

The following table shows the procedure for locating and rectifying the fault.

Step	Fault Location	Troubleshooting
1	Check whether the disk usage exceeds the limit.	Rectify the fault by referring to **5.1.6 Operation Abnormality Caused by Insufficient Disk Space**.
2	Check whether the configuration file for the **dbuser** user contains error information.	Rectify the fault by referring to **Failure to Start the Sybase Database Because the Configuration File for the dbuser User Contains Incorrect Information**.
3	Check the log file contains error information.	Rectify the fault by referring to the following error messages: ● **Permission denied in Logs** ● **Shared memory segment *.krg is in use in Logs** ● **Incorrect Shared Memory Settings in Logs** ● **Failure to Open lv_master as Prompted in Logs**
4	Take other measures if the preceding measures do not work.	Contact Huawei engineers for troubleshooting.

Permission denied in Logs

Symptom

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

The **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path contains the following information:

```
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

If **Permission denied** is contained in the **DBSVR.log** file, the permissions for the log file are insufficient. As a result, the file cannot be read and the database server cannot be started.

NOTICE

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

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check the name of the user who will start the Sybase database. The correct user name is **dbuser**.

Step 2 Check the raw partition or the file where **Permission denied** is contained. Check whether the user who will start the Sybase database has the permissions for accessing the file. If such permissions are unavailable, assign the associated permissions for the user.

NOTE

The equipment files are stored in the **$SYBASE/data** path. You can change the permissions to an equipment file by running the **chmod 750** ***equipment_file_name*** command.

Step 3 Restart the database.

----End

Shared memory segment *.krg is in use in Logs

Symptom

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

The **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path contains the following message:

```
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. As a result, the **DBSVR.krg** and **DBSVR.srg junk** files exist in the **$SYBASE** or **$SYBASE/$SYBASE_ASE** path.

NOTICE

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

Procedure

Step 1 Log in to the OS as the **dbuser** user.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The default password of **dbuser** user is **Changeme_123**.

Step 2 Run the following commands to check whether the **DBSVR.krg** and **DBSVR.srg junk** files exist in the **$SYBASE** or **$SYBASE/$SYBASE_ASE** path:

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

Step 3 If the **DBSVR.krg** and **DBSVR.srg junk** files exist, run the following commands to delete them:

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

Step 4 Restart the database.

----End

Incorrect Shared Memory Settings in Logs

Symptom

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

The **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path contains the following information:

```
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 **system** file in the **/etc** path is not configured with correct shared memory.

NOTICE

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

Procedure

Step 1 Add **set shmsys:shminfo_shmmax=*Memory_Size*** to the end of the **system** file in the **/etc** path.

1. Run the following command to check the memory as the **root** user:

   ```
   # prtdiag
   ```

   The following information is displayed:

Copyright © Huawei Technologies Co., Ltd.

```
Memory size:2GB
```

NOTE

The command output varies according to the on-site equipment configurations.

2. Add **set shmsys:shminfo_shmmax=*Memory_Size*** to the end of the **system** file in the **/etc** path. Here, the value of *Memory_Size* is calculated as follows: Memory size (MB) x 1024 x 1024/2.

   For example, if the memory size is 2 GB (2048MB), the value of the *Memory_Size* is 2048 x 1024 x 1024/2, that is, 1073741824.

   Add the following content to the end of the **system** file in the **/etc** path:

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

   NOTE

   - On the GUI, open and modify the log file by referring to the *Solaris Online Help*.
   - On the CLI, modify the log file by running the **vi** command. For details, see the commands that are commonly used on Solaris.

Step 2 Restart the database.

----End

Failure to Open lv_master as Prompted in Logs

Symptom

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

The **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path contains the following information:

```
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.

NOTICE

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

Procedure

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

Step 2 Reinstall the U2000 and Sybase database.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

Reinstalling the database leads to the interruption of U2000 monitoring. Therefore, ensure that the database data has been backed up for data restoration.

Step 3 Restore the U2000 database data. For details, see the chapter "Backing Up and Restoring the U2000 Database" in the *U2000 Administrator Guide*.

Step 4 Restart the database.

----End

Failure to Start the Sybase Database Because the Configuration File for the dbuser User Contains Incorrect Information

Symptom

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

After a user uses the **su - dbuser** command to switch to the **dbuser** user and then runs the **showserver** command. The query result does not contain the dataserver or backupserver process.

Possible Causes

The possible causes are as follows:

- The **dbuser** user group does not exist.
- The **dbuser** user does not exist.
- The **.profile** file does not exist in the **home** directory of the **dbuser** user.
- The **.profile** file of the **dbuser** user contains incorrect information.

NOTICE

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

Procedure

Step 1 Run the following command to check whether the **dbuser** user group exists as the **root** user:

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

The following information is displayed:

```
......
dbuser::101:dbuser
......
```

If **dbuser** is displayed before the first **:**, the **dbuser** user group exists. Otherwise, run the following command as the **root** user to create the **dbuser** user group:

Copyright © Huawei Technologies Co., Ltd.

```
# groupadd dbuser
```

Step 2 Run the following command to check whether the **dbuser** user exists as the **root** user:

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

The following information is displayed:

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

If **dbuser** is displayed before the first **:**, the **dbuser** user exists. Otherwise, run the following command as the **root** user to create the **dbuser** user:

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

Step 3 Run the following commands to check whether the **.profile** file exists in the **home** directory of the **dbuser** user as the **root** user:

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

The following information is displayed:

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

If the command output contains **.profile**, the **.profile** file exists. Otherwise, run the following command as the **root** user to create the **.profile** file:

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

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

```
$ more .profile
```

The following information is displayed in Solaris OS:

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

The following information is displayed in SUSE Linux OS:

```
#!/bin/sh
PS1=$
export PS1
. /opt/sybase/SYBASE.sh
LANG=en_us.utf8
export LANG
```

If the preceding information is displayed, information contained in the **.profile** is correct. Otherwise, add the preceding information to the **.profile** file in the **/opt/sybase/** path as the **root** user.

Step 5 Run the following commands to set the host and authorities of the **/opt/sybase/** path to correct values:

```
# chmod -R 750 /opt/sybase
# chown -R dbuser:dbuser /opt/sybase
```

Step 6 Restart the database.

----End

Copyright © Huawei Technologies Co., Ltd.

5.3.3 Abnormal Startup of the Sybase Database

Locate and rectify the fault according to the log information.

Log Information	Troubleshooting
The equipment file cannot be opened.	Rectify the fault by referring to **dopen: open '/opt/sybase/data/lv_LogDB_dev' in Logs**.
suspect.	Rectify the fault by referring to **U2000 Start Failure Due to "suspect" in the Database Log**.
The disk allocated for the database logs is full.	Rectify the fault by referring to **Database Log Space Becoming Full**.
Other information except for the preceding ones is displayed.	Contact Huawei engineers for troubleshooting.

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

Symptom

In a single-server system, the **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path contains the following information:

```
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.)
```

NOTE

The information in brackets explains the associated message.

Possible Causes

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

Copyright © Huawei Technologies Co., Ltd.

Fault Diagnosis

Run the following commands to find the name of the database where the fault occurs as the **root** user:

```
# su - dbuser
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

```
1> select name,status from sysdatabases
2> go
```

The terminal displays:

NOTE

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

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

If **status** is **76**, physical file of the **LogDB** database is deleted by mistake.

Procedure

Step 1 Run the following commands to start the database as the **dbuser** user:

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

Step 2 Run the following command to log in to the database:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 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 command output, the correct value of **status** is **320**.

Step 4 Run the following commands:

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


Copyright © Huawei Technologies Co., Ltd.

Step 5 Run the following commands to start the database as the **dbuser** user:

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

Step 6 Run the following command to log in to the database:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 7 Run the following commands:

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

Step 8 Delete database devices.

1. Run the following commands to query the names of all database devices in the database:

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

   The following information is displayed:

   NOTE

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

   ```
   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 command output

Copyright © Huawei Technologies Co., Ltd.

The prefixes of the database device names are consistent with the name of the database to be restored. In this example, the name of the database to be restored is **LogDB** and the names of the database devices to be deleted are **LogDB_dev** and **LogDBlog_dev**.

3. Run the following commands to delete database devices:

```
1> sp_dropdevice database_device_name
2> go
```

In this example, the names of the database devices to be deleted are **LogDB_dev** and **LogDBlog_dev**. Run the following commands:

```
1> sp_dropdevice LogDB_dev
2> go
1> sp_dropdevice LogDBlog_dev
2> go
```

Step 9 Initialize the database. For details, see the associated contents in the administrator guide.

Step 10 Restore the database data. For details, see the associated contents in the administrator guide.

----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. This is to avoid database exceptions caused by incorrect operations.

U2000 Start Failure Due to "suspect" in the Database Log

Symptom

In the single-server system, the **$SYBASE/$SYBASE_ASE/install/DBSVR.log** log shows the failure to open the NE file, and the U2000 fails to start. In the high availability system, the AppService resource cannot go online.

The log 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

Generally, this fault occurs because of an 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 time. You must rectify the fault manually.

NOTICE

If the **master** database is suspended as prompted in logs, you must re-install the database or seek help from Sybase engineers.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the OS as the **root** user.

Step 2 Run the following commands to log in to the database as the **sa** user:

```
# su - dbuser
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 3 Run the following commands to update the database to be recovered:

```
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
```

Step 4 Run the following commands to restart the database server:

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

Step 5 Run the following commands to log in to the database as the **sa** user:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 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
```

Step 7 Run the following commands to restart the database server:

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

Step 8 Run the following commands to log in to the database as the **sa** user:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Copyright © Huawei Technologies Co., Ltd.

Step 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
```

Step 10 Run the following commands to restart the database server. The database recovers after the database server is restarted.

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

----End

Database Log Space Becoming Full

Symptom

In a single-server system, the database is started abnormally.

Information contained in the **DBSVR.log** file in the **$SYBASE/$SYBASE_ASE/install** path indicates that the database log space is full.

Possible Causes

The possible causes are as follows:

- Log truncation is not set.
- The value of the database size is too small.

Fault Diagnosis

Perform the following steps to locate the database with full log space:

1. Ensure that the U2000 application has been closed and the database has been started.
2. Run the following commands to search for the names of all databases as the **root** user:

   ```
   # su - dbuser
   $ isql -SDBSVR -Usa
   ```

   NOTE

   Enter the database administrator user password as prompted.

   In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

   ```
   1> sp_helpdb
   2> go
   ```

3. Run the following commands to locate the database with full log space:

   ```
   # su - dbuser
   $ isql -SDBSVR -Usa
   ```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

```
1> sp_helpdb database_name
2> go
```

In the command output, the number in the **free kbytes** column indicates the remaining space of database logs. Find the name of the database with full log space according to the message displayed.

NOTE

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.

Procedure

Step 1 Log in to the OS as the **root** user.

Step 2 Run the following commands to log in to the database as the **sa** user:

```
# su - dbuser
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 3 Run the following commands to update the database to be recovered:

```
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
```

Step 4 Run the following commands to restart the database server:

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

Step 5 Run the following commands to log in to the database as the **sa** user:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 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
```


Copyright © Huawei Technologies Co., Ltd.

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

Step 7 Run the following commands to restart the database server:

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

Step 8 Run the following commands to log in to the database as the **sa** user:

```
$ isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 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
```

Step 10 Run the following commands to restart the database server. The database recovers after the database server has been restarted.

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

----End

5.3.4 How to Verify That the Sybase Database Is Running

Question

How do I verify that the Sybase database is running?

Answer

Step 1 Log in to the OS as user **root**.

Step 2 Enter the CLI and run the following commands to check the Sybase process status:

```
# su - dbuser
$ cd /opt/sybase/ASE*/install
$ ./showserver
```

A message similar to the following will be displayed:

```
UID   PID  PPID   C    STIME TTY         TIME CMD
  dbuser  4195  4170   0 18:42:26 ?          70:35 /opt/sybase/ASE-15_0/bin/
dataserver -ONLINE:1,0,0x6505fd2a, 10000000000, 0x18fc
```


Copyright © Huawei Technologies Co., Ltd.

```
  dbuser  4563  4559   0 18:42:50 ?           0:00 /opt/sybase/ASE-15_0/bin/
backupserver -SDBSVR_back -e/opt/sybase/ASE-15_0/install
  dbuser  4170  4168   0 18:42:00 ?         546:12 /opt/sybase/ASE-15_0/bin/
dataserver -sDBSVR -d/opt/sybase/data/lv_master -e/opt
```

NOTE

- when NMS is not installed: If the displayed information contains **/opt/sybase/ASE-15_0/bin/backupserver -SDBSVR_back**, and **/opt/sybase/ASE-15_0/bin/dataserver -sDBSVR**, the Sybase database has been started.
- when NMS is installed: If the displayed information contains **/opt/sybase/ASE-15_0/bin/dataserver -ONLINE**, **/opt/sybase/ASE-15_0/bin/backupserver -SDBSVR_back**, and **/opt/sybase/ASE-15_0/bin/dataserver -sDBSVR**, the Sybase database has been started.

----End

5.3.5 How to Check the Sybase Database Version

Question

How do I perform the required check on the Sybase database version to see if it is correct after the Sybase database is installed?

Answer

Step 1 Log in to the OS as user dbuser.

NOTE

- To switch to the **dbuser** user, run the **su - dbuser** command.
- After the U2000 is installed, the password for the **dbuser** user is **Changeme_123**. For system security, modify the default password and remember the new password. For detail, see How to Change the OS User Password.

Step 2 Run the following commands:

```
$ cd /opt/sybase/OCS*/bin
$ ./isql -SDBSVR -Usa
```

NOTE

Enter the password of the database administrator as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Step 3 Run the following commands to check the Sybase database version:

```
1> use master
2> go
1> select @@version
2> go
```

NOTE

There must be a space between **select** and **@** in the **select @@version** command.

In Solaris OS, a message similar to the following will be displayed:

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


Copyright © Huawei Technologies Co., Ltd.

```
 Adaptive Server Enterprise/15.7/EBF 23462 SMP SP131 /P/Sun_svr4/OS 5.10/ase157s
        p131x/3896/64-bit/FBO/Mon Nov  3 21:04:21
2014


(1 row affected)
1>
```

The preceding message indicates that Sybase database version is SYBASE 15.7.

NOTE

EBF 23462 indicates the latest Sybase patch. The earlier Sybase patches are not displayed.

In SUSE Linux OS, a message similar to the following will be displayed:

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

Adaptive Server Enterprise/15.7/EBF 23724 SMP SP131 /P/x86_64/Enterprise Linux/
 ase157sp131x/3896/64-bit/FBO/Mon Nov  3 20:37:35
2014


(1 row affected)
```

The preceding message indicates that Sybase database version is SYBASE 15.7.

NOTE

EBF 23724 indicates the latest Sybase patch. The earlier Sybase patches are not displayed.

----End

5.3.6 How to Disable the Sybase Database Service

Question

How do I disable the Sybase database service?

Answer

Step 1 Perform the following operations to disable the Sybase database service in the single-server system:

1. Log in to the OS as user **root**.
2. Run the following commands to disable the Sybase database service:

   ```
   # su - dbuser
   $ cd /opt/sybase/OCS*/bin
   $ ./isql -SDBSVR -Usa
   ```

   NOTE

   Enter the password of the database administrator as prompted.

   In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

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

3. Run the following command to check whether the Sybase database service is disabled:

   # ps -ef | grep sybase

   If the following message is displayed, the Sybase database service has been disabled:

Copyright © Huawei Technologies Co., Ltd.

```
root  9629 14603   0 07:46:52 pts/3      0:00 grep sybase
```

Step 2 Perform the following operations to disable the Sybase database service at the primary site in the HA system:

NOTE

By default, the Sybase database service at the secondary site is not running.

- GUI mode:
  1. Log in to the primary site as user **root**.
  2. Run the following command to start the VCS client at the primary site:

     # **hagui&**
  3. Choose **File** > **New Cluster** from the main menu. In the window that is displayed, enter the IP address of the server and click **OK**.

     NOTE

     If you are not logging in to the VCS client for the first time, click a server record in the information list in the **Cluster Monitor** window.
  4. Enter the default user name **admin** and the initial password **Changeme_123** for the VCS client. For system security, modify the default password and remember the new password. For detail, see How to Change the admin User Password for Logging In to the VCS Client. Then click **OK**.
  5. On the VCS client of the primary site, right-click the **NMSServer** node and choose **Offline** > ***hostname*** from the shortcut menu.
  6. In the confirmation dialog box, click **Yes**.
  7. After the **NMSServer** node is dimmed, right-click the **BackupServer** node and choose **Offline** > ***hostname*** from the shortcut menu.
  8. In the confirmation dialog box, click **Yes**.
  9. After the **BackupServer** node is dimmed, right-click the **DatabaseServer** node and choose **Offline** > ***hostname*** from the shortcut menu.
  10. In the confirmation dialog box, click **Yes**.
- CLI mode:
  1. Log in to the primary site as user **root**.
  2. Run the following command to shut down the U2000:

     # **hares -offline NMSServer -sys** *hostname*
  3. Run the following command to disable the Sybase database service:

     # **hares -offline BackupServer -sys** *hostname*

     # **hares -offline DatabaseServer -sys** *hostname*

  NOTE

  hostname specifies the server name. You can run the **hostname** command to view the server name.

Run the following command to check whether the Sybase database service is disabled:

ps -ef | grep sybase

If the following message is displayed, the Sybase database service has been disabled:

```
root  9629 14603   0 07:46:52 pts/3      0:00 grep sybase
```

----End

Copyright © Huawei Technologies Co., Ltd.

5.4 SQL Server Database Troubleshooting

This topic describes how to troubleshoot faults on the SQL Server database.

5.4.1 Failure to Initialize the Database

The following table shows how to locate and rectify the fault according to the prompt or log information on Windows.

Fault Location	Troubleshooting
If a message is displayed in the DOS window, locate the fault as prompted.	If the following information is displayed, rectify the fault by referring to the corresponding solutions: ● **Failure to Log In to the Database** ● **Incorrect Parameter of Java Virtual Machine**
If no message is displayed in the DOS window, locate the fault by viewing the log information in the log file in the **U2000\server\database** path.	If the following information is displayed, rectify the fault by referring to the corresponding solutions: ● **Failed to open the database 'xxDB' in Logs** ● **Cannot insert duplicate key in object 'TrailService-Type' in Logs**
Locate the fault in either of the preceding conditions.	Contact Huawei engineers for troubleshooting.

Failure to Log In to the Database

Symptom

On Windows 2008, when the U2000 database is being initialized, the message **login database failure** is displayed.

Possible Causes

The possible causes 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

Step 1 Check whether the database has been started. If not, start it manually.

1. Double-click the database icon on the taskbar. The **SQL Server Service Manager** window is displayed.

Copyright © Huawei Technologies Co., Ltd.

2. Check whether the database server has been started.

   If **Start/Continue** is grayed out, the database has already been started. Otherwise, click **Start/Continue** to start the database server.

Step 2 Check and change the alias of the database server.

1. Choose **Start** > **Programs** > **Microsoft SQL Server** > **Client Network Utility**. On the **Alias** tab page, view the alias of the database server.

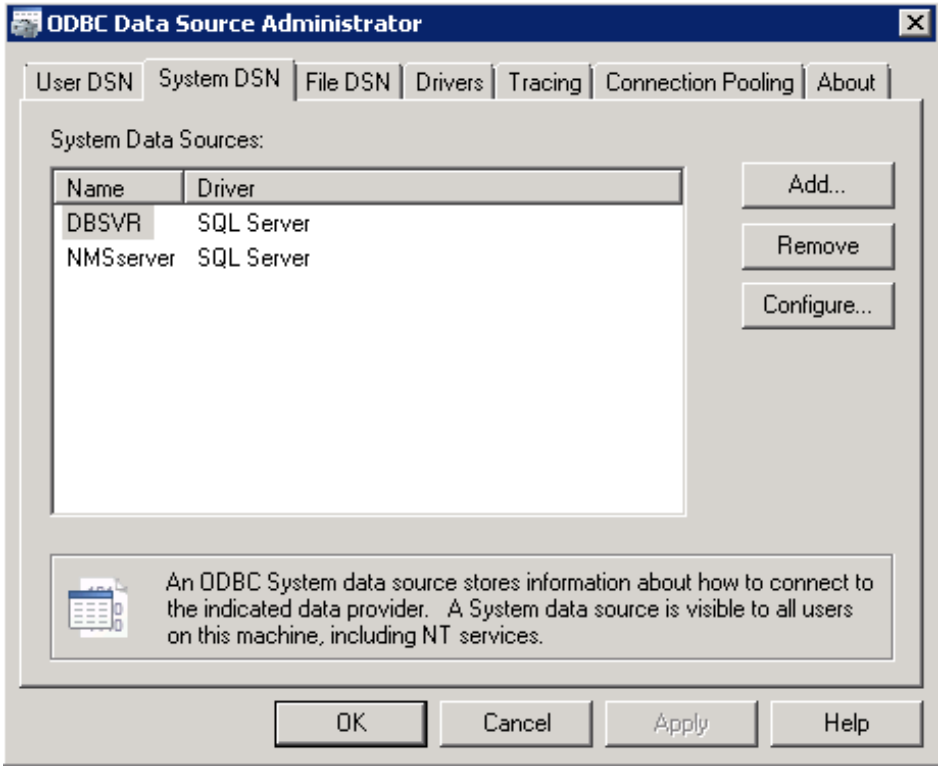
   The correct value of **Server alias** is **DBSVR**.

2. Initialize the database again.

   If the message "login database failure" is displayed again, the ODBC data source maybe configured incorrectly or may not be configured.

Step 3 Check and restore the configurations of the ODBC data source.

1. Choose **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**.



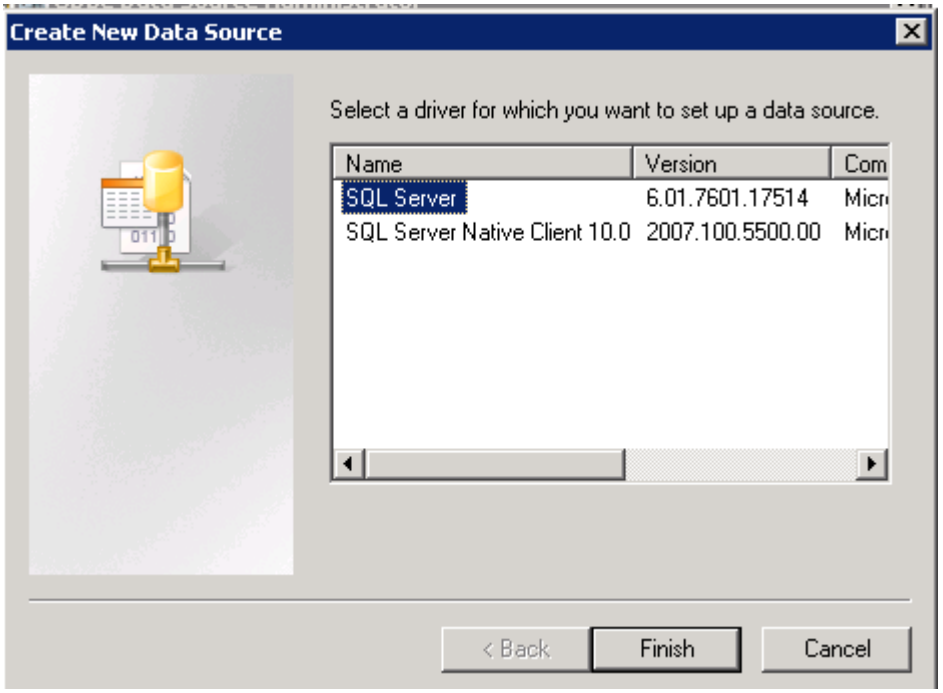
2. On the **System DSN** tab page, view the configuration of **DBSVR**.
   - If **DBSVR** already exists, select **DBSVR** and then click **Configure**, then perform the **Step 3.5**.
   - If **DBSVR** does not exist, click **Add**, then perform the **Step 3.3** and **Step 3.4** to add **DBSVR**.

   NOTE

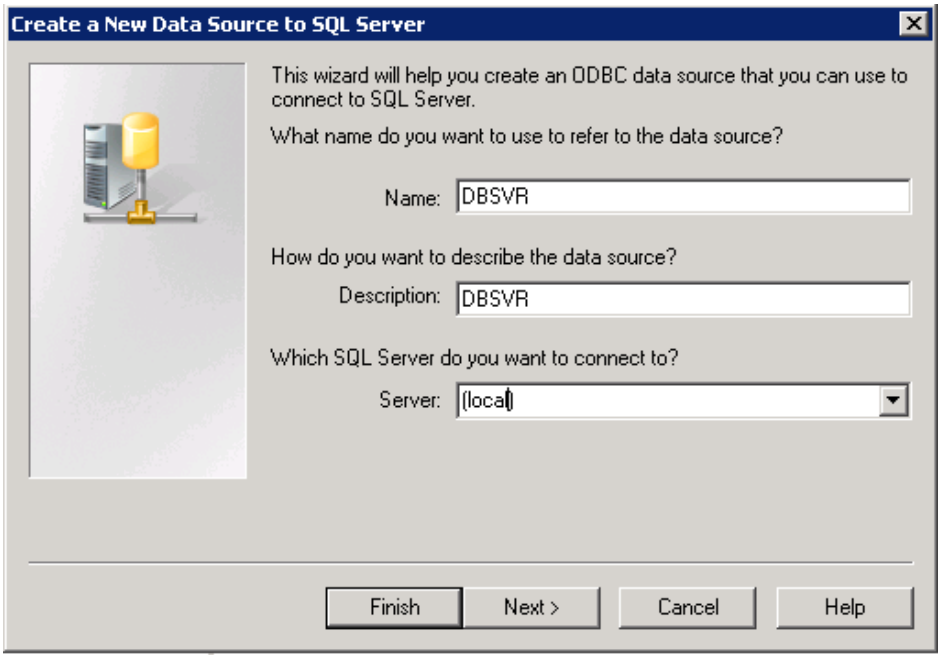
   Adding **DBSVR** is considered as an example.

3. On the **System DSN** tab page, click **Add**. In the **Create New Data Source** dialog box, select **SQL Server**.

Copyright © Huawei Technologies Co., Ltd.



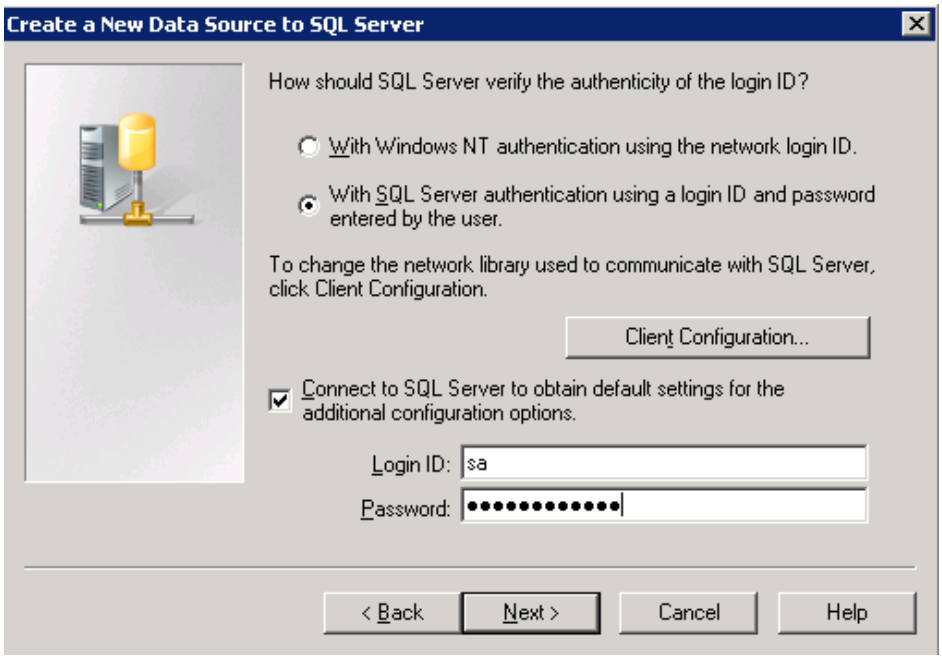
4. Click **Finish**. In the **Create a New Data Source to SQL Server** dialog box, enter the following information:



5. Click **Next**. In the **Create a New Data Source to SQL Server** dialog box, set parameters as follows:

Copyright © Huawei Technologies Co., Ltd.

- 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** text box, enter the database user name **sa** and the Password of the **sa**. If a password has been set, enter the password.



6. Click **Next**. In the dialog box that is displayed, select **Change the default database to:** and then select **master** from the drop-down list.
7. Click **Next**. In the dialog box that is displayed, keep the default settings.
8. Click **Finish**. Then, the **ODBC Microsoft SQL Server Setup** dialog box is displayed.
9. Click **Test Data Source...**. If the echo information contains **TEST COMPLETED SUCCESSFULLY!**, the U2000 applications have been connected to the database server.
10. Initialize the database again.

----End

Failed to open the database 'xxDB' in Logs

Symptom

Database initialization fails. The logs in the **D:\oss\engr\logs\logsServer** path contain the following information:

```
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 dbuser2008-08-06_10:27:51(CMSSQLConfig.mssqlSetDBOwner)    ERROR:Set
database xxDB's owner to dbuser 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
```


Copyright © Huawei Technologies Co., Ltd.

```
insufficient. For details, see the SQL Server error logs.
......
```

Possible Causes

Certain database files have been deleted or the disk space is insufficient.

Procedure

Step 1 Check the disk space.

Step 2 Run the following commands to delete the database:

```
> isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

```
1> drop database database_name
2> go
```

Deleting the **xxDB** database is considered as an example.

```
> isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

```
1> drop database xxDB
2> go
```

Step 3 Initialize the database again.

----End

Cannot insert duplicate key in object 'TrailServiceType' in Logs

Symptom

Database initialization fails. The logs in the **D:\oss\engr\logs\logsServer** path contain the following information:

```
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:\oss\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...
```


Copyright © Huawei Technologies Co., Ltd.

```
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

Step 1 Run the following commands at command prompts:

```
> isql -SDBSVR -Usa
```

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

```
1> sp_helpsort
2> go
```

The following information is displayed:

```
Chinese-PRC, binary sort
```

NOTE

If **Chinese-PRC** is displayed, the character set used by the database is Chinese. If **Chinese-PRC** is not displayed, the database needs to be installed again.

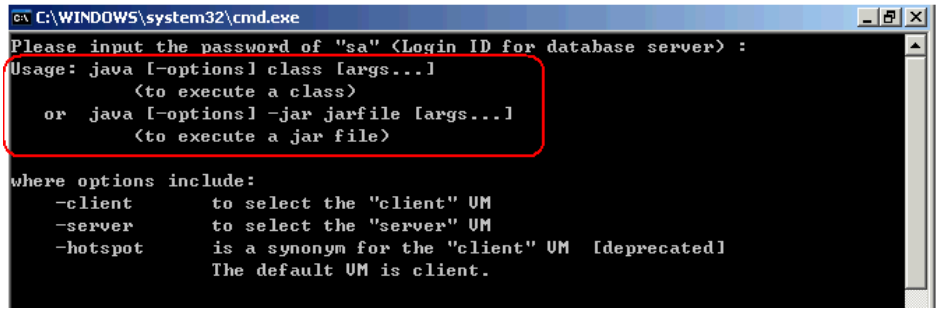
Step 2 Initialize the database again.

----End

Incorrect Parameter of Java Virtual Machine

Symptom

Database initialization fails. The following message is displayed:



Possible Causes

The symbol \ exists at the end of the IMAP_ROOT environment variable.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check and change the IMAP_ROOT environment variable. For details, see **Failure to Start the U2000 Because of Incorrect Environment Variables**.

Step 2 Initialize the database again.

----End

5.4.2 Failure to Immediately Back Up the SQL Server Database

Symptom

The backup file does not exist in the path specified in a database backup task.

The "Error Code: 1107329123. Failed to manually back up the database." message is displayed during backup.

Possible Causes

The possible causes are as follows:

- The database is not started.
- The disk space is used up.
- The password of the database user **sa** is not changed properly.
- Another user has logged in to the NMS Maintenance Suite client.
- Another database backup task is being executed.
- The NMS Maintenance Suite server is not started.

Procedure

Step 1 Ensure that the database has been started.

If the database icon in the Windows taskbar is , the database has been started.

Step 2 Check whether the backup path has sufficient space. On Windows, the available space for the local temporary directory or the local backup path is usually more than 1/3 of the local database size. The default local temporary directory is **D:\tmp**. The default local database path on the single-server system is **D:\data**. If the space is sufficient, delete unwanted files or move them to another disk.

Step 3 Ensure that the password of the database user **sa** has been changed according to the associated operation guide. If the password is changed improperly, restore the previous configuration and then use the NMS Maintenance Suite to change the password again. For details, see chapter "Changing the Password of the Administrator of the Database" in the *U2000 Administrator Guide*.

Step 4 Ensure that all users have logged out of the NMS Maintenance Suite client.

Step 5 Check whether another database backup task is being executed. If such a task is being executed, back up the database after the task is complete.

Step 6 Check whether the **msdaemon.exe** and **msserver.exe** processes have been started in the **Task Manager** window. If the process list contains the two processes, the NMS Maintenance Suite

Copyright © Huawei Technologies Co., Ltd.

is running. If the process list does not contain the two processes, the NMS Maintenance Suite is not running. Then, navigate to the **C:\OSSENGR\engineering** path and then double-click the **startserver.bat** file to start the NMS Maintenance Suite server.

Step 7 If the problem persists, do as follows to restart the NMS Maintenance Suite server: Navigate to the **C:\OSSENGR\engineering** path. Double-click the **stopserver.bat** file to stop the NMS Maintenance Suite server. Then, double-click the **startserver.bat** file to start the NMS Maintenance Suite server.

----End

5.4.3 Usage of the imaptmdb Database Reaches Upper Limit Upon an Incorrect Password Modification

Symptom

The alarm is generated when the usage of the imaptmdb database reaches the upper limit on the U2000 System Monitor.

Possible Causes

The password of the database user **sa** has been changed manually; as a result, a database abnormality occurs.

Fault Diagnosis

1. The associated description in the U2000 document shows that the imaptmdb database is used to store topology data.
2. The on-site information shows that the password of the database user **sa** has been manually changed before the fault occurs.

Procedure

Step 1 Shut down the U2000 server.

Step 2 After the U2000 server is shut down, log in to the U2000 System Monitor.

Step 3 Choose **Deploy** > **Change Database administrator Password** to modify the password.

Step 4 Restart the U2000 server to address the issue.

----End

Suggestion and Summary

- During U2000 daily maintenance, the MSuite must be used to modify the password of the database user **sa**. If the MSuite is not used, some configuration files may not be modified completely; as a result, a U2000 fault may occur.
- It is advisable to periodically modify the password of the **sa** user to ensure password security. For example, change the password every 3 months.

Copyright © Huawei Technologies Co., Ltd.

5.5 U2000 Server Troubleshooting

This topic describes how to troubleshoot faults on the U2000 server.

5.5.1 Failure to Start the U2000 Server

The U2000 server fails to start or certain processes of the U2000 are started repeatedly. The following table shows the order of locating and rectifying the fault in a single server system.

Step	Fault Location	Troubleshooting
1	Check whether the fault is caused by the U2000 coredump.	Rectify the fault by referring to **Abnormal Termination of the Server Application**.
2	Locate the fault as prompted.	Rectify the fault as prompted. ● **Failure to Connect to the Database** ● **Invalid License** ● **Failure to Start the U2000 Because of Incorrect Environment Variables**
3	Check whether the process cannot be started because the server is affected by viruses.	Use anti-virus software to remove viruses and refer to *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)* to re-install the U2000.
4	Attempt to restart the U2000 server. The server cannot be restarted.	Contact Huawei engineers for troubleshooting.

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

Step 1 Check whether any file whose name starts with **core.** exists in the following paths:

On Solaris or SUSE Linux:

- **/opt/oss**
- **/opt/oss/server**
- **/opt/oss/server/bin**

Copyright © Huawei Technologies Co., Ltd.

- **/opt/oss/server/platform/bin**

NOTE

The U2000 is installed in the **/opt/oss** path on Solaris or SUSE Linux is taken as an example.

On Windows:

- **D:\oss**
- **D:\oss\server**
- **D:\oss\server\bin**
- **D:\oss\server\platform\bin**

NOTE

The U2000 is installed in the **D:\oss** path on Windows is taken as an example.

Step 2 Collect the U2000 core dump file.

Step 3 Send the collected core dump file to Huawei engineers for troubleshooting.

----End

Failure to Start the U2000 Server Because of a U2000 Installation Error

Symptom

- A site provides the feedback that the U2000 server fails to start after the U2000 is installed on a Windows client.
- The U2000 server fails to start after the U2000 is installed on a PC.

Possible Causes

This problem is generally caused by an installation error. Possible causes are as follows:

1. Multiple versions of the SQL Server database have been installed on Windows. During installation of the U2000, the installation program automatically checks whether the SQL Server database has been installed. If the SQL Server database has been installed, a message will be displayed asking you whether to reuse the database. If two or more versions of the SQL Server database exist because of reasons such as incomplete uninstallation, this problem occurs.
2. The installation software package is not downloaded completely or some data is lost during transmission of the software package. In this scenario, the U2000 can be properly installed on the PC but the server fails to start properly.

Fault Diagnosis

Before the U2000 is installed, engineers have not checked the environment in strict compliance with chapter **Pre-installation Check** in *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)*. The troubleshooting roadmap is as follows:

1. Refer to chapter **Pre-installation Check** in *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)* to check the environment items one by one. Locate items that do not meet requirements for installing and operating the U2000. Refer to chapter **Pre-installation Check** to recover the problem items. In this case, the

Copyright © Huawei Technologies Co., Ltd.

cause of symptom one is that the environment check is not performed for the SQL Server database before the U2000 is installed.

2. Use the MD5 check tool to check whether the MD5 codes in the U2000 installation package on the server are the same as provided. If not, download the installation package again. The cause of symptom two is that the downloaded installation package is incorrect.

Procedure

Step 1 Refer to *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)* to download the U2000.

Step 2 Refer to *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)* to manually download the SQL Server database.

Step 3 Refer to *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)* to install the U2000 again.

----End

Suggestion and Summary

- During installation of the U2000 on Windows, engineers must perform operation in strict compliance with the *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)*. If not, unpredictable errors may occur.
- On Windows, install the U2000 on a specific computer and do not install software that is irrelevant to the U2000 or does not match the U2000 version.

Failure to Connect to the Database

Symptom

A message is displayed indicating a failure to connect to the database. In addition, the U2000 server cannot be started.

Possible Causes

The possible causes are as follows:

- 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.
- The IP address is changed, which causes a start failure.
- Other problems regarding the database occur.

Procedure

Step 1 Check whether the database has been started. If the database has not been started, start it manually.

Perform the following steps to check and start the database on Windows:

Copyright © Huawei Technologies Co., Ltd.

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 gray, the database has been 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.

Perform the following steps to check and start the database on Solaris or SUSE Linux:

1. Log in to the OS as the **dbuser** user.
2. Run the following commands to check whether the database has been started:
   ```
   $ cd $SYBASE/$SYBASE_ASE/install
   $ ./showserver
   ```
   Check whether the dataserver and backupserver processes are running. If these two processes do not exist, the database process has not been started.
3. Run the following commands to start the database:
   ```
   $ cd /opt/sybase/ASE-*/install
   $ ./startserver -f ./RUN_DBSVR
   $ ./startserver -f ./RUN_DBSVR_back
   ```
4. Run the following commands to check whether the database process is running:
   ```
   $ cd $SYBASE/$SYBASE_ASE/install
   $ ./showserver
   ```
   Check whether the dataserver and backupserver processes are running. If these two processes do not exist, the database process has not been started. If the database cannot be started, rectify the fault by referring to **5.3.2 Failure to Start the Sybase Database**.

Step 2 Check the communication between the U2000 and database.

- On Windows, see **Failure to Log In to the Database**.
- On Solaris or SUSE Linux, run the following commands to log in to the Sybase:
  ```
  # su - dbuser
  $ isql -SDBSVR -Usa
  ```

  NOTE

  Enter the database administrator user password as prompted.

  In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

  If the following message is displayed, communication between the U2000 and database is normal.
  ```
  1>
  ```
  Enter **quit** to exit the Sybase. If the preceding information is not displayed, rectify the fault according to the log information.

Step 3 If a start failure is caused by IP address changes, change the IP address. For details, see *U2000 Administrator Guide*.

Step 4 If the configuration file is damaged because the database user password has been changed illegitimately, re-set the password for the database user.

For details about how to re-set the database user password, see the *U2000 Administrator Guide*.

----End

Copyright © Huawei Technologies Co., Ltd.

Failure to Start the U2000 Because of Incorrect Environment Variables

Symptom

A message is displayed indicating that environment variables of the U2000 are set incorrectly.

Possible Causes

Environment variables are lost or changed.

Procedure

Step 1 Check the environment variables of the U2000. For details, see the *U2000 Single-Server System Software Installation and Commissioning Guide (Windows)*.

- 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 values of **IMAP_ROOT** and **OSS_ROOT**.
- On Solaris or SUSE Linux, run the following command as the **ossuser** user to query the values of environment variables. Take **IMAP_ROOT** as a example.
  ```
  $ echo $IMAP_ROOT
  ```

Step 2 Correct the environment variables of the U2000.

- On Windows: Assume that the U2000 is installed in the **D:\oss** path. The correct environment variable is **IMAP_ROOT=D:\oss\server**. if the environment variable is not **IMAP_ROOT=D:\oss\server**, re-set it manually.
- On Solaris or SUSE Linux: Assume that the U2000 is installed in the **/opt/oss** path. The value of the **$IMAP_ROOT** environment variable is **/opt/oss/server/etc/conf** by default. If the value of the **$IMAP_ROOT** environment variable is not **/opt/oss/server/etc/conf**, re-set it by running the following command as the **ossuser** user:
  ```
  $ IMAP_ROOT=/opt/oss/server;export IMAP_ROOT
  ```

----End

Failure to Start U2000 Services Because of an Authority Problem of the U2000 Installation Path

Symptom

After the U2000 workstation running on Solaris or SUSE Linux is restarted, the U2000 services fail to be started.

Possible Causes

An authority problem of the U2000 installation path occurs.

Procedure

Step 1 Log in to the OS as the **root** user.

Step 2 Change the owner of the U2000 installation path to **osssuser**. Then, run the following commands in the CLI:

Copyright © Huawei Technologies Co., Ltd.

```
# cd /opt
 # chown -R ossuser oss
```

Step 3 Restart the U2000.

----End

5.5.2 Cannot Back Up Data on the U2000 Server

Symptom

A user attempts to back up U2000 data on the current server, but a message is displayed indicating that FTP is disabled and data cannot be backed up.

Possible Causes

Generally, the message is displayed only when U2000 data is backed up to another computer. Therefore, the current server may be functioning improperly.

Procedure

Step 1 Shut down the U2000 and database properly. For details about how to shut down the U2000 and database, see *U2000 Administrator Guide*.

Step 2 After the U2000 and database are shut down, restart the server. The server will restore to the normal state after it is started successfully.

----End

5.5.3 Some U2000 Functions Fail to Work

Symptom

The feedback from a site shows that some functions on a U2000 client are unavailable. For example, the U2000 fails to manage a certain type of devices.

Possible Causes

Possible causes are as follows:

- Components to be involved functions are not installed, or the components are installed but instances are not installed for the involved functions.
- The U2000 license does not contain the associated function control items.
- The processes associated with the involved functions are not started or work incorrectly.

Procedure

Step 1 Log in to a U2000 client and check whether the processes associated with the involved functions are stopped. If the processes are stopped, start them.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- If a message indicating a lack of the associated function control item in the license is displayed during startup of a process, the obtained license is incorrect. Apply for a new license.
- If a process fails to be started, refer to **5.5.4 Failure to Start Certain Processes of the U2000 Server** to address the issue.

Step 2 If the associated function processes are not found on the U2000 client, no instance is deployed. Log in to the MSuite client. On the **Deployment Package** page, check whether an instance is deployed in the deployment package of the associated function. If the associated deployment package is available but no instance is found, add an instnace to the deployment package.

NOTE

For details about how to add instances, see the MSuite Help. On an MSuite client, press **F1** to navigate to the MSuite Help.

----End

5.5.4 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.
- The password of the database administrator is incorrect or not changed properly; as a result, some processes fail to be started.
- 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 and updated for the relevant functions.
- Ports are occupied.
- Some processes fail to be started due to exception power-off.
- On Windows, database software such as the Sybase client is installed on the U2000 server. An error occurs when processes access the database.
- In Windows, two dynamic library files **libeay32.dll** and **ssleay32.dll** are generated in the **C:\WINDOWS\system32** directory due to non-U2000 software installed on the U2000 server. As a result, the U2000 process fails to be started.
- On Windows, other software is installed on the U2000 server. As a result, some U2000 processes fail to start.
- The memory configurations of the U2000 server do not meet running requirements. As a result, some processes fail to start. For example, if the memory of the T5220 workstation is smaller than 8 GB, the desktop server process may fail to start.
- If 360 software has been installed on the site, some U2000 files will be deleted; as a result, the process cannot be started.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 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.

Step 2 Restart the U2000 and check whether the processes are started.

Step 3 Check whether the server IP address is changed. If the IP address is changed, ensure that it is changed according to the related operation guide. If the IP address is changed incorrectly, restore to the previous setting and then change the IP address again. For details, see section "Changing the System IP Address and Host Name" in the *U2000 Administrator Guide*.

Step 4 Check whether the password of the database administrator has been manually changed. If so, use the MSuite to change the password again.

Step 5 Ensure that licenses are obtained and updated for the relevant functions.

Step 6 If the account **root** has been used to start these processes but exits abnormally before the processes are started, perform the following steps:

1. Start the processes as the **root** user and exit after the processes are started.
2. Restart the OS.

Step 7 If a process, such as the CORBA NBI process, fails to be started, check the NBI settings or re-configure the NBI.

Step 8 Check whether the ports used by these processes are occupied.

Step 9 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 U2000 server.

Step 10 Uninstall the Sybase client if database software such as the Sybase client has been installed on the U2000 server running on Windows.

Step 11 In Windows, if dynamic library files **libeay32.dll** and **ssleay32.dll** are generated in the **C:\WINDOWS\system32** directory due to other software installed on the U2000 server, displace **libeay32.dll** and **ssleay32.dll** files to the directory of non-U2000 software installation or rename these files for backup.

Step 12 Installing U2000-irrelevant software on the U2000 server is not recommended. If the fault persists after the preceding operations are performed, uninstall the U2000-irrelevant software and restart the U2000 server.

Step 13 Check whether the hardware configurations of the U2000 server meet requirements. For the requirements, see the *U2000 Planning Guide*. If the hardware configurations do not meet requirements, replace the U2000 server.

Step 14 If this problem persists after the preceding operations, contact Huawei engineers.

Step 15 If the 360 software does not function properly, uninstall the 360 software and re-install the U2000.

----End

Copyright © Huawei Technologies Co., Ltd.

Suggestion and Summary

- When changing the IP address, follow the related operation guide. Otherwise, the U2000 may malfunction.
- Starting or stopping the U2000 as the ossuser user is recommended.
- On Windows, do not install database software such as the Sybase client on the U2000 server.

5.5.5 Some U2000 Functions Become Abnormal Due to the Change of the System Time

Symptom

After the system time has been changed, some U2000 functions become abnormal.

Possible Causes

If the system time of the server has been changed during the operation of the U2000, some functions (such as the scheduled dump function of the security Daemon) based on timer principles may become abnormal.

Procedure

Step 1 Shut down the U2000 and the database. For details, see the *U2000 Administrator Guide*.

Step 2 After the U2000 and the database are shut down, restart the OS. After the OS is restarted, the functions become normal.

NOTE

You must set the system time of the server properly before the U2000 has been installed, but not during the operation of the U2000. If the system time of the server needs to be changed during the operation of the U2000, you must stop U2000 services, change the system time, and then restart the U2000 server.

----End

5.5.6 Data or Log Space of the U2000 Used Up

Symptom

A user checks the U2000 database status on the **System Monitor** client. The result shows that the data or file space is full and alarms such as "The Database Usage Is Too High" are generated.

Possible Causes

The possible causes are as follows:

- A large number of alarms or events are reported within a short period of time.
- The threshold of the U2000 database usage is set to a small value.
- Parameters such as the period during which data is exported or dumped is not set properly and as a result the database usage is too high.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 If an alarm is generated, deal with the alarm according to the following troubleshooting suggestions:

- **A.31 ALM-42 The Database Usage Is Too High (Warning)**
- **A.32 ALM-43 The Database Usage Is Too High (Minor)**
- **A.33 ALM-44 The Database Usage Is Too High (Major)**
- **A.44 ALM-103 The Database Usage Is Too High (Critical)**

Step 2 Configure overflow dump. For example, configure log overflow dump, alarm overflow dump, event overflow dump, or performance overflow dump. For details, see the *U2000 Online Help*.

----End

Suggestion and Summary

Setting scheduled data dump is recommended. If the size of the data to be dumped reaches the threshold, the dumped data is saved as a file and deleted from the database. In this manner, the problem of insufficient database space is addressed.

5.5.7 Abnormal Data Generated After the U2000 Restarts

Symptom

Certain NEs are missing on the U2000 and topologies are displayed in a disorder manner.

Possible Causes

An exception occurs on the U2000 database.

Procedure

Step 1 Initialize the database. For details, see topoc **Initializing the U2000 Database** in the *U2000 Administrator Guide*.

Step 2 Manually recover the U2000 data. For details, see chapter **Backing Up and Restoring the U2000 Database** in the *U2000 Administrator Guide*.

----End

5.5.8 A Message Displayed Indicating Not All Scripts Are Imported

Symptom

Error code 1090614020 is displayed when users import scripts into the U2000.

Possible Causes

1. The NE capacity defined in the U2000 license file is insufficient.
2. The U2000 license registration does not take effect.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Update the U2000 license file. For details, see Chapter "Applying for and Updating the License" in the *U2000 Administrator Guide*.

Step 2 Shut down the U2000. For details, see Chapter "Shutting Down the U2000" in the *U2000 Administrator Guide*.

Step 3 Start the U2000. For details, see Chapter "Starting the U2000 System" in the *U2000 Administrator Guide*.

----End

5.5.9 Failure to Find a Uniquely Matched Trail During Script Importing

Symptom

During script importing on the U2000, an error message (with error code 1090614044) is displayed, indicating that no uniquely matched trail is found.

Possible Causes

The possible causes are as follows:

- Data of an NE that the trail traverses fails to be imported, which results in inconsistent cross-connections and fibers.
- Fiber data fails to be imported, which results in a failure to generate relevant optical multiplexing section (OMS) trails.
- Protection group data of an NE that the trail traverses fails to be imported, which results in inconsistent protection subnets.

Procedure

Step 1 On the U2000 from which the script is exported, locate trail A and view the cross-connections it belongs to. For details, see section 2.1.8 "Viewing WDM Trails" in the *Operation Guide for WDM End-to-End Management*.

Step 2 On the U2000 to which the script is imported, locate discrete services that belong to trail A in the discrete management window, and analyze the cause for these discrete services. For details, see section 2.1.3.2 "Viewing Discrete Services" in the *Operation Guide for WDM End-to-End Management*.

Step 3 The cause for why trail A is not generated can be inferred from the cause for discrete services. Then, seek a solution to search out trail A.

----End

Suggestion and Summary

This error does not indicate an import failure. It only reminds users of the fact that trail A existing on the U2000 from which the script is exported cannot be found after script importing.

Copyright © Huawei Technologies Co., Ltd.

5.5.10 Message Indicating Unreachable Receive End Process Displayed During Script Exporting

Symptom

When exporting of scripts on the U2000, an error message (with error code 1090611456) is displayed, indicating that the receive end process is unreachable.

Possible Causes

An optical network terminal (ONT) end-to-end (E2E) process is deployed on the U2000. The U2000 license, however, does not support ONT E2E functions. In this case, the process can be successfully started, but cannot load any functional module. Therefore, messages cannot be processed.

Procedure

Step 1 Delete instances that the U2000 license does not support. For details, see section "Deleting an Instance" in the *U2000 Administrator Guide*.

Step 2 Update the U2000 license. For details, see Chapter 3 "Applying for and Updating the License" in the *U2000 Administrator Guide*.

Step 3 Restart the U2000. For details, see Chapter 2 "Shutting Down the U2000 System" and chapter 1 "Starting the U2000 System" in the *U2000 Administrator Guide*.

----End

5.5.11 How to Clear Alarms That an NE Reported Before Becoming Unreachable

Symptom

When a user imports a script into the U2000, error 1090724220 is displayed, indicating that the NE management process cannot be found.

Possible Causes

Some components fail to be deployed during U2000 installation.

Procedure

Step 1 Log in an MSuite client and deploy domains. For details, see Chapter "U2000 Deployment" in the *U2000 Administrator Guide*.

Step 2 Deploy domains for new components. For details, see Chapter "U2000 Deployment" in the *U2000 Administrator Guide*.

----End

Copyright © Huawei Technologies Co., Ltd.

5.6 Faults on a U2000 Client

This topic describes how to troubleshoot faults on a U2000 client.

5.6.1 Failure to Start a U2000 Client

Symptom

- After a user double-clicks the shortcut icon of a U2000 client, but the login window is not displayed.
- The loading progress reaches 99% and stops for a long time during U2000 login.

Possible Causes

The possible causes are as follows:

- The files of the OS 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 illegitimate installation of the U2000 client.
- Hardware configurations of the computer on which the U2000 client is installed do not meet requirement.
- The memory usage is high on the U2000 server due to excessive exception events generated on the U2000.

Procedure

Step 1 If a prompt is displayed, locate and rectify the fault as prompted.

Step 2 On Windows, ensure that **core.jar** is available in **oss\client\client\productlib\base** on disk D. On Solaris, ensure that **core.jar** is available in **/opt/oss/client/client/productlib/base**.

Step 3 Uninstall the U2000 client and then install it again. For details, see the *U2000 Client Software Installation Guide*.

Step 4 Upgrade the hardware configurations of the computer on which the U2000 client is installed and reinstall the U2000 client.

Step 5 For details about how to handle exception events, see **ALM-47 Memory Usage of Service Is Too High** in *U2000 Troubleshooting*.

----End

5.6.2 Failure to Log In to the U2000 Server from a U2000 Client

Symptom

A user fails to log in to a U2000 client after a user name and a password have been entered in the login window.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The possible causes are as follows:

- The U2000 server does not work properly, the U2000 server fails to start properly, the disk on the U2000 server is full, or the memory usage of the U2000 server is high because many processes are started.
- An incorrect user name or password has been entered for logging in to the U2000 client.
- If the U2000 server runs on Windows, the ODBC data source is configured incorrectly or is not configured.
- If the U2000 server runs on Windows, the dynamic port of the SQL Server is not 1433; therefore, the U2000 server fails to connect to the database and login to the U2000 server from a U2000 client fails.
- The network between the client and server does not function properly.
- The license file is a temporary one or is damaged.
- The number of clients allowed in the license is restricted.
- The port between the client and server is shielded by firewall or viruses. In common mode, port 31037 is used by default. In SSL mode, port 31039 is used by default.
- 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 too many times of login failures.
- The IP address of the computer where the client is installed is not listed in the ACL.
- The OS time on the client is set incorrectly and the ILOG JTGO license is expired.
- The DCN is faulty.
- The 360 antivirus software has been installed on the server.
- The dfwModule fails to be loaded.
- The maximum client login limit has been reached.

Procedure

Step 1 If an error message is displayed, locate and rectify the fault as prompted.

Step 2 Check whether the server has been started properly. Ensure that the server runs properly, the disk space of the server is not used up, and not many processes are started on the server. If many processes are started on the server, the memory usage is high.

1. Ensure that the server has been started properly.

   You can log in to the U2000 System Monitor to view server information. If the server startup fails, see **5.5.4 Failure to Start Certain Processes of the U2000 Server** to address the issue.

2. Ensure that the disk space of the server is not used up.
   - To troubleshoot the full disk space on the server on Windows, perform the following operations:

     Check that disk C is fully used, delete log files, and restart the U2000.
   - To troubleshoot the full disk space on the server on Solaris or SUSE Linux, perform the following operations:

Copyright © Huawei Technologies Co., Ltd.

a. Check that the space usage of the **/opt** directory reaches 100%.

b. Run the following command to check the distribution of files larger than 100 MB.

```
# find /opt -size +200000 -print
```

Software runs abnormally because temporary files on the server are improperly large. Delete temporary files from the **/opt** directory if they occupy large space.

3. Ensure that not many processes are started on the server.

After the U2000 server is started, do not access the JDE desktop (switch to the CED environment for the U2000 on the live network). Start the U2000 in CLI mode.

Step 3 Verify that the entered user name and password are correct.

Step 4 If a message indicating that the license file is invalid when you log in to the U2000 client, rectify the license fault according to **6.1.3 How to Resolve the Problem that the License Does Not Take Effect** and log in to the U2000 client.

Step 5 Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).

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 file.

Step 6 If the U2000 server is installed on Windows, check and restore the ODBC data source settings on the U2000. For details, see Step 3 in **Failure to Log In to the Database**.

Step 7 Check whether the versions of the client and server are consistent. If the versions are inconsistent, a message will be displayed asking you to upgrade the client. In this case, try to upgrade or reinstall the client.

Step 8 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.

NOTE

Run the **ssl_adm -cmd query** command on the U2000 server to view the communication mode of the U2000 server. For details, see How to Set the Communication Mode on the U2000 server for the Single-Server System (Windows)How to Set the Communication Mode on the U2000 server for the Single-Server System (Solaris)How to Set the Communication Mode on the U2000 server for the Single-Server System (SUSE Linux)How to Set the Communication Mode of the Server in a High Availability System (Solaris, SUSE Linux).

Step 9 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
  ```

Step 10 Check whether the port between the client and server is shielded by firewall or viruses. Install a virus scanner, scan the entire disk, and remove viruses. If the client installed on the computer where the server belongs can log in to the server, but other clients cannot log in, check whether the port has been added to the Windows firewall. If not, perform the following operations to add the port to the Windows firewall:

Copyright © Huawei Technologies Co., Ltd.

NOTE

Windows Server 2008 is used as an example to describe the procedures for adding a port to a firewall. The procedures vary according to OSs. For specific procedures, see the Windows help.

1. Choose **Start** > **Control Panel**.
2. In the **Control Panel** window, click **windows Firewall**.
3. In the **windows Firewall** window, click **Advanced Setting**.
4. In the **Windows Firewall with Advanced Security** dialog box, choose **Inbound Rules** from the left navigation tree and from **New Rule** the right navigation tree.
5. In the **New Inbound Pule Wizard** dialog box, select **Port** and click **Next**.
6. In **Specific local ports**, set **Ports** and click **Next**.
7. Select **Allow the connection** and click **Next**.
8. Click **Next**, set **Name**, and click **Finish**.

Step 11 Log in to the U2000 client as the **admin** user and choose **Administration** > **NMS Security** > **ACL**.

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 Chapter "Security Management" in the *U2000 Administrator Guide*. If NAT is used for IP address translation for communication between the client and server, ensure that the translated IP address is permitted in the ACL.

Step 12 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**.

Step 13 Check whether the system time is the current time. If not, modify the system time.

Step 14 Check whether the 360 antivirus software has deleted some U2000 files. If yes, uninstall the 360 antivirus software and re-install the U2000.

Step 15 Log in to **NE Software Management**, check the process list, and start all the processes with **Automatic** startup mode.

Step 16 Create a user and use it to log in. For details, see "Setting the Maximum Number of Sessions" in *U2000 Administrator Guide*.

----End

5.6.3 User Account for Logging In to a U2000 Client Locked

Symptom

After a user enters a user name and password in the login dialog box of a U2000 client, the system displays a message indicating that the user account is locked.

Possible Causes

A user account is locked after three consecutive login attempts for the user fail.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the user is an illegal user who wants to invade the U2000.

Step 2 If the locked legal user is not the **admin** user, the user account can be unlocked by the **admin** user.

1. Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.
2. In the **NMS User Management** navigation tree, click the **User** node.
3. Right-click a user and choose **Unlock User** from the shortcut menu.

Step 3 If a legal user forgets the password, the **admin** user can initialize the database for the user.

1. Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.
2. In the **NMS User Management** navigation tree, click the **User** node.
3. Right-click a user and choose **Reset Password** from the shortcut menu.

Step 4 If the **admin** user is locked, the system automatically unlocks the user account after 30 minutes by default.

NOTE

You can set the automatic unlocking time in **Account Policy**. Choose **Administration** > **NMS Security** > **Security Policies** from the main menu. In the **Security Policy** dialog box, click the **Account Policy** tab, and then set **Auto Unlock**.

----End

5.6.4 U2000 Client Running Abnormally

Symptom

A U2000 client restarts repeatedly and operations are interrupted.

Possible Causes

The computer may be infected with viruses.

Procedure

Step 1 Check and remove the viruses by using antivirus software.

Step 2 Restart the U2000 client.

----End

5.6.5 Abnormal Exit of a U2000 Client Because of Inappropriate Input Method Editor Software

Symptom

On the U2000 client on which **Intelligent ABC Input Method Editor** or **Sogo Input Method Editor** is installed, the U2000 client exits abnormally and the GUI disappears.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

Certain software, such as **Intelligent ABC Input Method Editor** or **Sogo 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

Step 1 Upgrade the input method version or use another input method software.

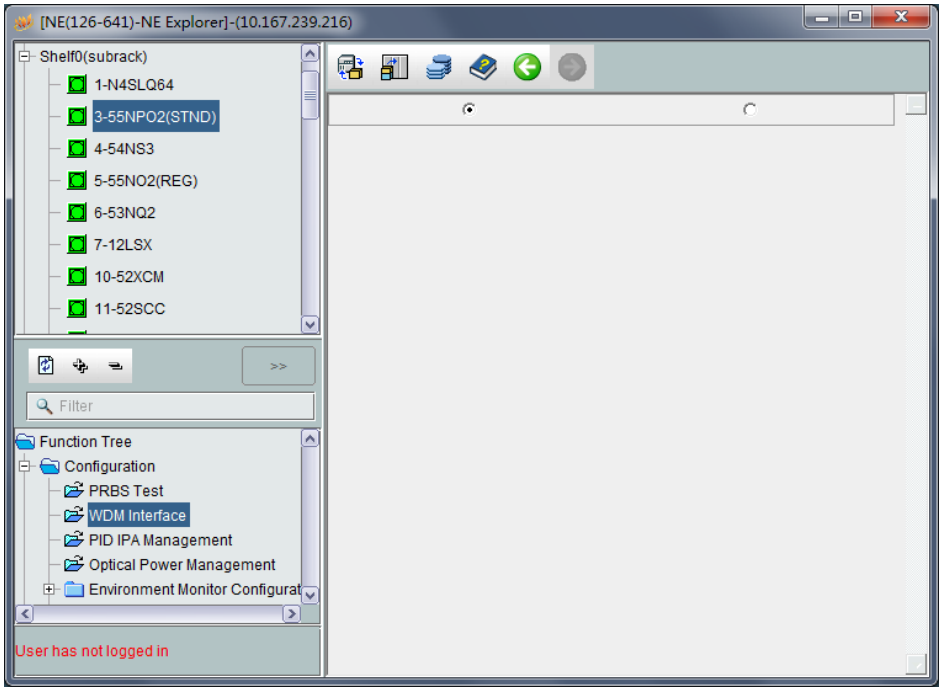
Step 2 Restart the U2000 client.

----End

5.6.6 Abnormal NE Manager GUI for Certain Equipment on a U2000 Client

Symptom

- On a U2000 client, open the NE Explorer, select some function items from the function tree, the right side GUI is grayed out or displayed abnormally.



- After the OS and U2000 are installed, a user opens the NE Explorer for an NG SDH or OTN NE but finds that the Web LCT server fails to be connected and the **WDM Interface** window cannot be opened.

Possible Causes

- For some NEs (such as the PTN series, RTN series, NG WDM series, and SLM 1630), the NE Explorer incorporates some web windows from the Web LCT. If the browser settings are inappropriate, these windows will be displayed abnormally. Probable causes are as follows:

Copyright © Huawei Technologies Co., Ltd.

- 1. The default browser is configured incorrectly.
- 2. The version of Internet Explorer is old (Windows only).
- 3. The security level of Internet Explorer is high.
- 4. A proxy server has been set on the browser.
- 5. The U2000 client is installed in a directory whose name contains double-byte characters, spaces, brackets, or Chinese characters.
- 6. The U2000 client and Simulator are running on the same computer. In addition, the Simulator forwards a lot of NEs, occupying numerous socket resources. Therefore, the U2000 client may fail to establish a connection to the Web LCT server.
- 7. The communication port of the Web LCT is occupied.

- The 360 software is installed.

Procedure

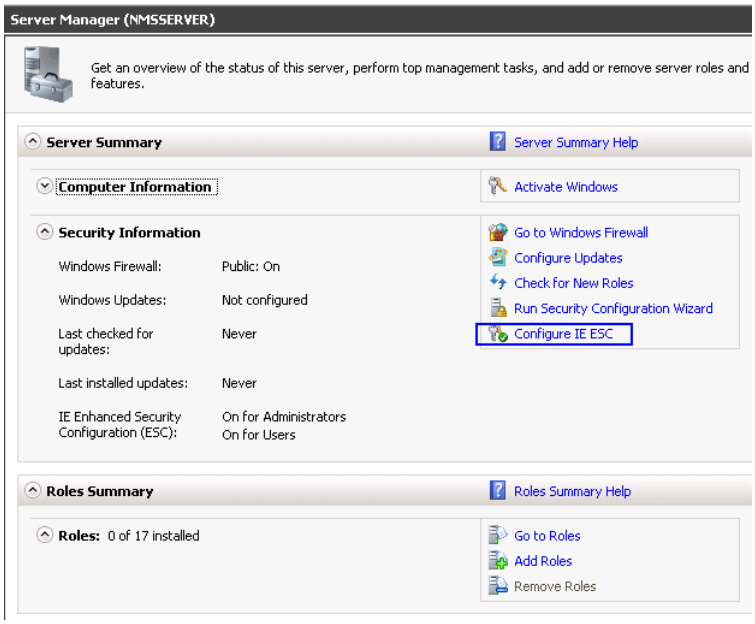
Step 1 Check whether the browser settings comply with the standards. On Windows, the default browser needs to be Microsoft Internet Explorer; on Solaris, the default browser needs to be Firefox browser.

Step 2 Check the version of Internet Explorer on Windows. If the version is earlier than 7.0, upgrade it to 7.0 or a later version.

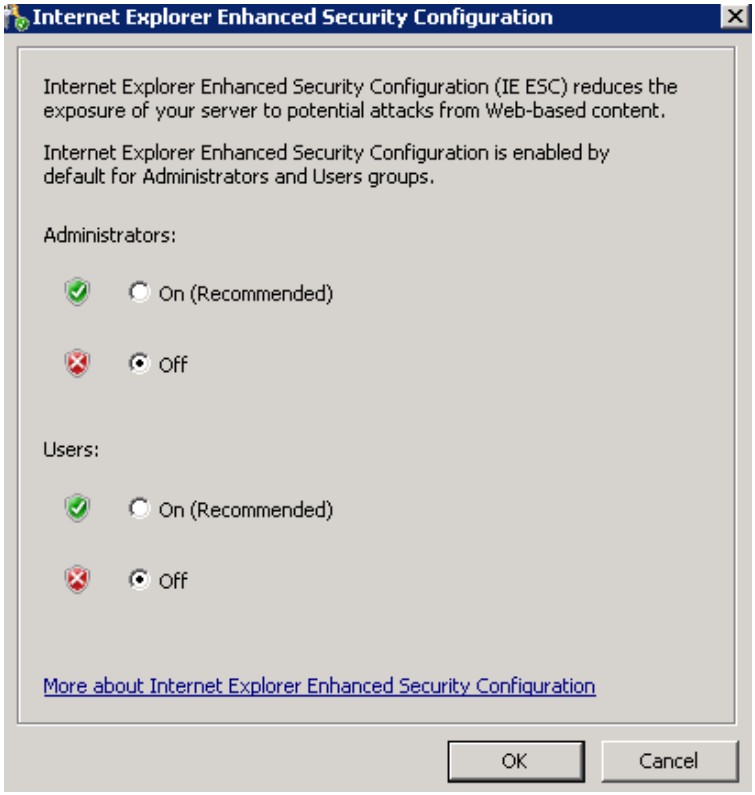
Step 3 Check the version of Microsoft Internet Explorer on Windows. If the security level of Microsoft Internet Explorer is set to high, the running of scripts is affected and the GUI becomes grayed out. To make the GUI display normally, you need to set the security level of the Internet Explorer to **Medium** or a lower level.

- In the Windows 2008 OS, the security level of Internet Explorer remains high by default. Therefore, you need to cancel the function as follows:
  1. Right-click the **Start** menu and choose **Computer** > **Server Manager** from the shortcut menu to access the **Server Manager** window.
  2. In the **Security Information** area on the **Server Summary** tab, click **Configure IE ESC**.

Copyright © Huawei Technologies Co., Ltd.



3. In the **Internet Explorer Enhanced Security Configuration** dialog box, set the status of the administrator and user to **Off**.



4. Click **OK**.
5. Double-click the **Internet Explorer** icon on the desktop to open the Microsoft Internet Explorer.
6. Choose **Tool** > **Internet Options** from the main menu.
7. In the **Internet Options** dialog box, select **Security**, and select **Local Intranet**. Then, set the security level of Internet Explorer to **Medium** level.

Copyright © Huawei Technologies Co., Ltd.

8. Click **Apply**.
9. Click **OK**.

- In the Windows 7 OS, the security level of Internet Explorer remains high by default. Therefore, you need to cancel the function as follows:
  1. Double-click the **Internet Explorer** icon on the desktop to open the Microsoft Internet Explorer.
  2. Choose **Tool** > **Internet Options** from the main menu.
  3. In the **Internet Options** dialog box, select **Security**, and select **Local Intranet**. Then, set the security level of Internet Explorer to **Medium** level.
  4. Click **Apply**.
  5. Click **OK**.

Step 4 Check whether Microsoft Internet Explorer is configured with the proxy server. If Microsoft Internet Explorer is configured with the proxy server, cancel the proxy server or disable the connection to the U2000 server through the proxy server.

Step 5 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.

Step 6 In the CLI, run the *netstat-ano* or *tasklist* command to query running processes and the ports they occupy. If any process occupies port 8090, end the process. Then restart U2000 processes.

Step 7 Add http://127.0.0.1 to **Trusted sites**.

1. Double-click the **Internet Explorer** icon on the desktop to open the Microsoft Internet Explorer.
2. Choose **Tool** > **Internet Options** from the main menu.
3. In the **Internet Options** dialog box, select **Security**, and select **Trusted sites**. Then click **Sites**, in the **Trusted sites** dialog box, add http://127.0.0.1 to **Trusted sites**.

Step 8 Check whether the 360 software is installed. If the software is installed, uninstall it.

Step 9 Close the U2000 client and restart the OS. Then open the U2000 client again.

----End

5.6.7 Connection Between the U2000 Client and Server that Are Running on the Same Machine Interrupted for a Short Period of Time After a Network Cable Is Removed

Symptom

A U2000 client and the 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 of time. On the U2000 client, the following message is displayed:

```
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, an NIC is selected as the communication link between the client and server. If an NIC is removed from the server, the

Copyright © Huawei Technologies Co., Ltd.

connection between the client and server may be interrupted. This is because the client may currently use the NIC that is connected to this network cable to communicate with the server.

Procedure

Step 1 Wait about 5 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 U2000 is restarted, do not remove any network cable at random. Connecting the hardware properly before the U2000 is installed is recommended.

5.6.8 Time Inconsistency Between the U2000 Server and Client

Fault Symptom

- Time is inconsistent between the U2000 server and client.
- The alarm occurrence time displayed on the U2000 client is later than the actual alarm occurrence time.

Fault Analysis

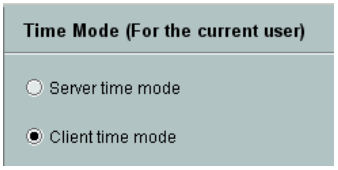
Although the time mode of the U2000 client is set to **Client time mode**, the time zones configured on the U2000 client and server are inconsistent because of their different OS time zones.

Procedure

Step 1 Ensure that the time mode of the U2000 client is set to **Client time mode**.

1. Choose **File** > **Preference** from the main menu.
2. In the **Preference** window, choose **Time Mode** from the navigation tree.

   In the **Time Mode** window, check whether the time mode of the U2000 client is set to **Client time mode**.



Step 2 Change the OS time zone of the client or server to make time zones consistent based on the actual situation. The Windows 2008 OS is used as an example to describe how to change the time zone of an OS.

1. On the desktop, choose **Start** > **Control Panel**. In the Control Panel, double-click **Date and Time**.
2. In the **Date and Time Properties** dialog box, click the **Time Zone** tab.

Copyright © Huawei Technologies Co., Ltd.

3. On the **Time Zone** tab, select a desired time zone from the drop-down list and click **OK**.

----End

5.6.9 Unsynchronized NE Configuration Information Is Not Displayed

Symptom

After configuring an NE, a user opens the **NE Configuration Data Management** window and clicks **Sync Info**. However, no unsynchronized information is displayed in the **NE Config Sync Info** dialog box.

NOTE

This case occurs on transport NEs.

Possible Causes

The **NE Config Sync Info** dialog box does not display unsynchronized NE configuration information, because the NE is configured by the user who queries the information. The user can only see an unsynchronized mark for the NE in the Main Topology.

The function of querying unsynchronized NE configuration information is closely related to NE users. The unsynchronized information caused by NE A cannot be queried by NE A on any NM clients. Only an unsynchronized mark is displayed for the NE in the Main Topology. Therefore, sometimes it is normal that no unsynchronized information is displayed in the **NE Config Sync Info** dialog box. The detailed process is as follows: User information is carried in the unsynchronized information. The NM compares the user information with that saved in itself. If the user information is consistent, the NM discards the unsynchronized information; otherwise, the NM displays the unsynchronized information. A workaround for this issue is to change the NE user and retry the query.

For example, there are two sets of NM, NM 1 and NM 2. NM 1 and NM 2 use user A and user B to manage NE 1 respectively. After user A deletes a board from NE 1 on NM 1, user B can see an unsynchronized mark and specific unsynchronized information on NM 2. After NM 1 and NM 2 exchange user A and user B (that is, NM 1 uses user B and NM 2 uses user A to manage NE 1), the unsynchronized information cannot be queried on NM 2.

Procedure

- No solution is required, because this issue does not affect operations.

----End

5.6.10 How Do I Resolve the Problem Where the U2000 Client Fails to Be Installed Using CAU After the U2000 Has Been Upgraded?

Symptom

How do I resolve the problem where the U2000 client fails to be installed using CAU after the U2000 has been upgraded?

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The Apache or Tomcat service was not started on the U2000 server.

Procedure

Step 1 Start the Apache process (on a Windows OS):

Log in to the server, access the command line interface (CLI), and run the following command:

```
D:/oss/server/3rdTools/apache/bin/httpd -k start -f D:/oss/server/etc/apache/conf/httpd.conf
```

NOTE

The **D:\oss\server\3rdTools\ftp** path needs to be accessed if the U2000 is installed in **D:\oss**. If the U2000 is not installed in **D:\oss**, change drive letter **D** in the command line based on the actual situations.

Step 2 Restart the Tomcat process.

Run the following command in the CLI:

```
python d:\oss\server\platform\bin\script\kill_daem\kill_Tomcat.pyc
python d:\oss\server\platform\bin\script\start_daem\start_Tomcat.pyc
```

NOTE

The **D:\oss\server\3rdTools\ftp** path needs to be accessed if the U2000 is installed in **D:\oss**. If the U2000 is not installed in **D:\oss**, change drive letter **D** in the command line based on the actual situations.

Step 3 Reinstall the client.

----End

5.7 U2000 Running Slowly

This section describes how to locate the slow U2000 operating problem.

The U2000 responds slowly to certain operations. For example, opening or closing a window takes more than three seconds on the U2000 client.

Locate and rectify the fault according to the steps shown in the following table.

Step	Fault Location	Troubleshooting
1	Check whether the number of non-gateway NEs managed by the gateway NE exceeds the limit. Generally, each gateway NE supports 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, add gateway NEs. Otherwise, ECC congestion may occur, which causes slow response to operations on the GUI.	Contact Huawei engineers for network division, ECC reconstruction, and DCN reconstruction.

Copyright © Huawei Technologies Co., Ltd.

Step	Fault Location	Troubleshooting
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 alarm database and log database are fully used.	If they are fully used, manually dump U2000 logs and alarms. For details, see the U2000 Help.
4	Check whether the communication between the U2000 and gateway NEs is normal. If a large packet loss ratio (such as 40% or above) exists on the network, packets need to be retransmitted. As a result, the U2000 responds slowly to the commands delivered to the transmission equipment and the response to operations on the GUI is slow too.	Restore the communication between the U2000 and gateway NEs. For details, see **6.3.9 Failure to Connect to a Large Number of GNEs on the U2000**.
5	Check whether the OS is normal. If the OS runs at a low speed, crashes, or restarts frequently, the problem may be caused by exceptions of the OS.	If the OS runs abnormally, rectify the fault by referring to **5.1.1 Failure to Start the OS**. **NOTE** If the Windows abnormality occurs because patches are not installed, install related patches. For details, see the Microsoft patch installation guide.
6	Check whether the disk usage exceeds the limit. Normally, the disk usage cannot be larger than 80%.	If the disk space exceeds the threshold, rectify the fault by referring to **5.1.6 Operation Abnormality Caused by Insufficient Disk Space**.
7	Check the hardware performance of the U2000 server.	Rectify the fault by referring to **5.1.7 Slow Running of the System Caused by Insufficient Memory** and **5.1.8 Slow Running of the System Caused by Too High CPU Usage**.
8	Check whether the virtual memory size of the computer where the client is installed is set to an improperly small value.	Configure the virtual memory to a partition with sufficient remaining space. On Windows XP, use the default value of Initial Size. On a computer that has 1 GB memory, the maximum memory size must be no less than 2 GB. On a computer that has more than 1 GB memory, the maximum memory size must be no less the physical memory size multiplied by 1.5.

Copyright © Huawei Technologies Co., Ltd.

Step	Fault Location	Troubleshooting
9	Check the memory usage of the computer where the client is installed.	● If the memory usage is improperly high, stop some non-U2000 processes. ● Check whether the hardware configurations of the computer where the client is installed meet running requirements for the U2000 client. If not, improve the hardware configurations.
10	If none of the preceding measures work, restart the U2000 client.	Restart the U2000 client.
11	Check whether the server to which the U2000 client is connected is taking any data backup or network-wide service operations that involve a large volume of data.	Back up data and perform network-wide service operations that involve a large volume of data at night.
12	Check U2000 server hardware performance.	If hardware performance is unsatisfactory, replace hardware and add memory.
13	The U2000 server is infected with viruses.	Run antivirus software to identify and remove viruses. To protect the server from network viruses and ensure that the U2000 runs securely, install patches on the operating system (OS), upgrade the antivirus software in time, and scan and remove viruses periodically.
14	Check the bandwidth between the U2000 server and client.	If the bandwidth fails to meet requirements, modify it.
15	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

5.8 Veritas High Availability System Troubleshooting

This topic describe how to troubleshoot faults on a Veritas high availability system.

5.8.1 HA System Status Overview

Based on the primary and secondary site faults, the U2000 HA system (Veritas hot standby) has different status. This topic describes the status.

Copyright © Huawei Technologies Co., Ltd.

Table 5-1 HA system status

System Status	Status of Primary and Secondary Sites	Remarks
Normal state	The primary site works properly. The secondary site works properly.	The AppService application runs on the primary site, the heartbeat connection is normal, the replication is from the primary site to the secondary site, and the secondary site works to protect the primary site.
Fault switching state	The primary site is faulty. The secondary site works properly.	The AppService application runs on the secondary site. The status details are as follows: ● Resource fault on the primary site: The heartbeat connection is normal and the replication is from the secondary site to the primary site. ● Primary site failure: The heartbeat connection is torn down and the replication is interrupted.
Primary-primary state	The primary site works properly. The secondary site works properly.	The AppService application runs on both the primary and secondary sites. The heartbeat connection is torn down and the replication is interrupted. This status is usually caused by a communication failure between the primary and secondary sites. The two sites may force each other to log out of a transport NE.

Copyright © Huawei Technologies Co., Ltd.

System Status	Status of Primary and Secondary Sites	Remarks
Recovery state	One site works properly. The other site is to be troubleshot.	The status details are as follows: ● If the status is caused by a network disconnection, the AppService application runs on the primary site, the heartbeat connection between the primary and secondary sites is normal, and no data is being replicated after the network fault is rectified. ● If the status is caused by a primary site failure, the AppService application runs on the secondary site, the heartbeat connection between the primary and secondary sites is normal, and no data is being replicated after the primary site fault is rectified.
Protection failure state	The primary site works properly. The secondary site is faulty.	The AppService application runs on the primary site, and the secondary site does not work to protect the primary site. The status details are as follows: ● If the status occurs because the sources on the secondary site are faulty or the resource groups on the primary and secondary sites are frozen, the heartbeat connection is normal and the replication is from the primary site to the secondary site. ● If the status is caused by a secondary site failure, the heartbeat connection is torn down and the replication is interrupted. ● If the status occurs because the SRL data exceeds the threshold, the heartbeat connection is normal, the replication is from the primary site to the secondary site, and data is not being replicated.
System failure state	The primary site is faulty. The secondary site is faulty.	Both the primary and secondary sites are faulty, no AppService application runs, the heartbeat connection is torn down, and the replication is interrupted.

5.8.2 Principle of HA System Status Conversion

The HA system status changes along with fault occurrence and rectification. This topic describes the principle of common HA system status conversion.

NOTE

Read **5.8.1 HA System Status Overview** before this topic.

Copyright © Huawei Technologies Co., Ltd.

If the HA system is in Normal state, the primary site acts as the active site, the secondary site acts as the standby site, and the U2000 runs on the primary site. **Figure 5-1** shows the conversion relationship between HA system status.

Figure 5-1 Conversion relationship between HA system status

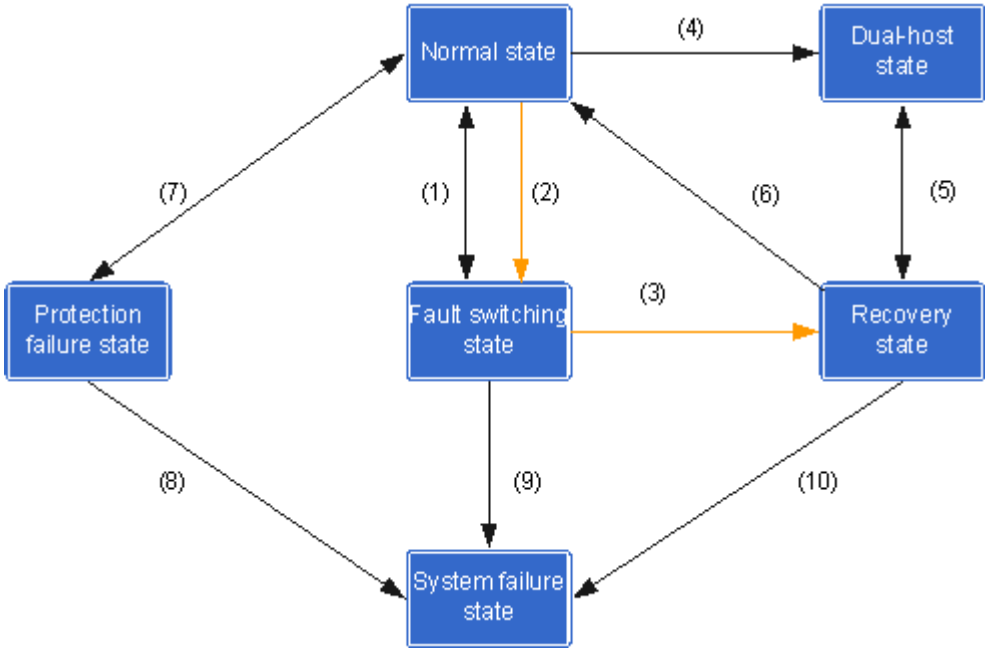


Table 5-2 shows the conversion relationship between and trigger factors for HA system status.

NOTE

- ←→ indicates that two status can be converted to each other.
- → indicates that only unidirectional conversion is available for two status.

Table 5-2 Status conversion relationship

No.	Status Conversion	Conversion Reason
(1)	Normal state←→Fault switching state	The resource on the primary site is faulty.
(2)	Normal state→Fault switching state	The primary site is powered off abnormally, has a hardware fault, or is broken down.
(3)	Fault switching state→ Recovery state	After the primary site fault is rectified, the HA system enters the Recovery state.

Copyright © Huawei Technologies Co., Ltd.

No.	Status Conversion	Conversion Reason
(4)	Normal state →Primary-primary state	The communication between the primary and secondary site has stopped for more than about 600 seconds. **NOTE** For Solaris HA system, if a separate heartbeat network and a separate replication network have been configured, the heartbeat between the primary and secondary sites uses the replication network if the communication on the heartbeat network is interrupted. In this scenario, the HA system status changes from Normal state to Primary-primary state only if the communication on both the heartbeat and replication networks has been stopped for more than about 600 seconds.
(5)	Primary-primary state→ Recovery state	After the DCN fault between the primary and secondary site is rectified, the HA system enters the Recovery state.
(6)	Recovery state→Normal state	The **Force Active of Local Site** operation is performed manually.
(7)	Normal state←→Protection failure state	● The resource on the secondary site is faulty. ● The secondary site fails. ● The resource groups on the primary and secondary sites are frozen. ● The SRL data exceeds the threshold.
(8)	Protection failure state→ System failure state	● The resource on the primary site is faulty. ● The primary site fails.
(9)	Fault switching state→ System failure state	● The resource on the secondary site is faulty. ● The secondary site fails.
(10)	Recovery state→System failure state	● The resource on the primary site is faulty. ● The primary site fails.

5.8.3 Causes of Failover on an HA System

This topic describes the causes of failover on an HA system. If the primary site does not function properly, services are automatically switched to the secondary site and the secondary site takes over the monitoring and management of networks. This ensures service protection.

Generally, the causes of a failover on an HA system are as follows:

NOTE

An automatic switching is triggered if the HA system is in the Normal state and one of the following conditions is met. If the HA system is not in the Normal state, an automatic switching is not triggered even if the following conditions are met.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

After the switching, the U2000 may not receive alarms. It is recommended that the client be reconnected and the primary site be configured on the U2000 again based on the the primary site's IP address after switching.

- **Cause 1:** A resource in the **AppService** resource group does not function properly. After the failover is complete, the HA system enters the Fault switching state.

  NOTE

  - If you manually stop the following resources, the HA system switchover is not triggered.
  - **BackupServer** is used to monitor the backup database server process. If the backup database server is faulty, the HA system switchover is not triggered.

  Table 5-3 Resources in the AppService resource group

Resource Name	Description
NMSServer	Used to monitor key U2000 processes. If a key U2000 process does not function properly, the U2000 automatically restart the process for three times. If three attempts fail, a failover occurs on the HA system. The HA system supports only the method of viewing non-key processes. **NOTE** To view non-key processes in standard mode and maximum mode, run the following command: # **cd /opt/oss/engr/OSSApp/process** To view non-key processes in standard mode, run the following command: # **cat process_std** To view non-key processes in maximum mode, run the following command: # **cat process_max**
DatabaseServer	Used to monitor database server processes. If the database server does not function properly, a failover occurs on the HA system.
DataFilesystem	Used to monitor the **lv_nms_data** volume. If the **lv_nms_data** volume does not function properly, a failover occurs on the HA system.
RVGPrimary	Used to monitor the RVG on the local site. If the RVG on the local site does not function properly, a failover occurs on the HA system.

Copyright © Huawei Technologies Co., Ltd.

Resource Name	Description
appNIC (Solaris) APPBOND (PC Linux)	Used to monitor the NIC associated with the U2000 application IP address. If the NIC does not function properly, a failover occurs on the HA system. **NOTE** ● For Solaris HA system, if an independent NMS application IP address without IPMP has been configured, the VCS does not monitor this resource. ● For Solaris HA system, if the system IP address without IPMP is used as the NMS application IP address, not the heartbeat or replication IP address, the VCS does not monitor this resource.

- **Cause 2:** The U2000 on the primary site abnormally powers off, has a hardware fault, or is broken down. A hardware fault may occur because of disasters such as earthquake, tsunami, or flood. The U2000 may be broken down because the operating system is damaged. After the failover is complete, the HA system enters the Fault switching state.
- **Cause 3:** The interval for interruption of heartbeat connections between the primary and secondary sites exceeds 600 seconds, the HA system enters the Primary-primary state.

  NOTE

  For Solaris HA system, if a separate heartbeat network and a separate replication network have been configured, the heartbeat between the primary and secondary sites uses the replication network if the communication on the heartbeat network is interrupted. In this scenario, the HA system status changes from Normal state to Primary-primary state only if the communication on both the heartbeat and replication networks has been stopped for more than about 600 seconds.

5.8.4 Troubleshooting Policies for a Veritas High Availability System

This topic describes the how to confirm the faults that commonly occur in a Veritas high availability system as well as the troubleshooting policies.

Checking the System Status

This topic describes how to check the system status. Checking the system status is the prerequisite for troubleshooting high availability system faults.

NOTE

If the server is configured with one NIC, the value of **Host name** is the host IP address of primary site. In this example, the values of **Host name** for master servers are **10.9.1.1** and **10.9.1.2**.

Normal state

On the primary or secondary site, run the following command to check the system status:

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

- If **Replication status** is displayed as **resync in progress (autosync)**, **Data status** is displayed as **inconsistent**, and the value of **Logging to** is becoming smaller, data is being duplicated between Primary and secondary sites.

Copyright © Huawei Technologies Co., Ltd.

- If **Replication status** is displayed as **replicating (connected)** and **Data status** is displayed as **consistent, up-to-date**, 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.

Information similar to the following is displayed:

```
Replicated Data Set: datarvg
Primary:
  Host name:                    10.9.1.1
  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:                    10.9.1.2
  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
```

If **Data status** is **consistent, up-to-date** and **Replication status** is **replicating (connected)**, the replication status between the primary and secondary site is normal and the high availability system is in the Normal state.

Primary-primary 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:         10.9.1.1
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:         10.9.1.2<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:
10.9.1.2: 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:

Copyright © Huawei Technologies Co., Ltd.

```
# vradmin -g datadg repstatus datarvg
Replicated Data Set: datarvg
Primary:
Host name:        10.9.1.2
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:
10.9.1.1: Pri or Sec IP not available or vradmind not running
```

NOTE

If an error message is displayed, the high availability is in the Primary-primary state.

Recovery state

On the primary or secondary site, run the following command to check the system status:

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

If the information contains **Primary-Primary configuration**, the high availability system is in the Recovery state. Information similar to the following is displayed:

```
Replicated Data Set: datarvg
Primary:
  Host name:                  10.9.1.1
  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:                  10.9.1.2
  RVG name:                   datarvg
  DG name:                    datadg
  Data status:                consistent, behind
  Replication status:         paused due to network disconnection
  Current mode:               asynchronous
  Logging to:                 SRL (397246 Kbytes behind, 37% full)
  Timestamp Information:      behind by 0h 36m 51s

Config Errors:
10.9.1.2:                   Primary-Primary configuration
```

Protection failure state

If one or more of the following conditions are met, the high availability system is in the Protection failure state state.

- **Symptom 1**: The **Veritas Resource Group Is Frozen** alarm is reported on the U2000 client.
- **Symptom 2**: The resources on the primary site of the high availability system are faulty or the secondary site of the high availability system fails.
- **Symptom 3**: The **Veritas Replication Data Is Not Synchronized** alarm is reported on the U2000 client.

  ```
  logging to DCM (needs dcm resynchronization)
  ```


Copyright © Huawei Technologies Co., Ltd.

is displayed after the
`# vradmin -g datadg repstatus datarvg`
command is run to view the replication status.

Fault switching state

If either or both of the following conditions are met, the high availability system is in the Fault switching state state.

- **Symptom 1**: The **Veritas Resources Are Faulty** alarm is reported on the U2000 client.
- **Symptom 2**: The primary site of the high availability system fails.

System failure state

Symptom: The primary and secondary sites are unavailable.

Detailed Fault Recovery Strategies for a High Availability System

This topic describes recovery strategies for a high availability system. When a fault occurs on a high availability system, use appropriate recovery strategies and methods to rectify the fault as required.

Recovery Strategy for the Primary-primary state

Symptom: When the network is disconnected, the high availability system enters the Primary-primary state. The **Veritas Data Replication Is Interrupted** and **Veritas Heartbeat is Interrupted** alarms are reported on the U2000 client. The transport NEs may preempt the resource of each other.

Recovery strategy:

1. Rectify the network fault. After the fault is rectified, the high availability system enters the Recovery state from the Primary-primary state. The **Veritas High Availability System Waits for Restoration** alarm is reported on the U2000 client.
2. Log in to the NMS Maintenance Suite on the primary site.
3. Choose **Deploy** > **Force Active of Local Site** to restore data replication relationships. The primary site becomes the active site after the operation.

Recovery Strategy for the Fault switching state

- **Symptom 1**: The resources on the primary site of the high availability system are faulty and the high availability system enters the Fault switching state. The **Veritas Resources Are Faulty** alarm is reported on the U2000 client.
- **Symptom 2**: The primary site of the high availability system fails.

Recovery strategy:

- Recovery strategy for symptom 1: Rectify the resource fault on the primary site. For details, see **A.102 Veritas Resources Are Faulty**.
- Recovery strategy for symptom 2:
  1. Rectify the primary site fault. For causes and troubleshooting methods, contact Huawei technical support engineers. After the fault is rectified, the high availability

Copyright © Huawei Technologies Co., Ltd.

system enters the Recovery state from the Primary-primary state. The **Veritas High Availability System Waits for Restoration** alarm is reported on the U2000 client.

2. Log in to the NMS Maintenance Suite on the secondary site.
3. Choose **Deploy** > **Force Active of Local Site** to restore data replication relationships. The secondary site becomes the active site after the operation.
4. After data is synchronized between the primary and secondary sites, manually switch U2000 applications back to the primary site to enable the primary site to monitor the network.

Recovery Strategy for the Protection failure state

- **Symptom 1**: The resource group is frozen and the **Veritas Resource Group Is Frozen** alarm is reported on the U2000 client.
- **Symptom 2**: The resources on the primary site of the high availability system are faulty or the secondary site of the high availability system fails.
- **Symptom 3**: The SRL data exceeds the threshold and the **Veritas Replication Data Is Not Synchronized** alarm is reported on the U2000 client.

Recovery strategy:

- Recovery strategy for symptom 1: If the resource group is temporarily frozen, run the **hagrp -unfreeze resource_group_name** command to unfreeze the resource group. If the resource group is permanently frozen, run the **hagrp -unfreeze resource_group_name -persistent** command to unfreeze the resource group.
- Recovery strategy for symptom 2: Rectify the secondary site fault. For causes and troubleshooting methods, contact Huawei technical support engineers.
- Recovery strategy for symptom 3: Wait until the data synchronization is complete. Alternatively, run the **vradmin -g datadg resync datarvg** command as the **root** user on the primary site.

Recovery Strategy for the System failure state

Symptom: The primary and secondary sites are unavailable.

Recovery strategy: Take emergency troubleshooting measures immediately. It is recommended that you start the emergency server, or troubleshoot one site for temporary network monitoring and management and then troubleshoot the other site. For causes and troubleshooting methods, contact Huawei technical support engineers.

5.8.5 Veritas Troubleshooting Cases

This topic describes the cases of troubleshooting faults on the Veritas.

Failure to Switch Between the Primary and Secondary Sites

Services fail to be switched between the primary and secondary sites in a high availability system (Veritas hot backup).

Locate and rectify the fault according to the steps shown in the following table.

Copyright © Huawei Technologies Co., Ltd.

Step	Fault Location	Troubleshooting
1	Check whether the high availability system is in the normal state.	If the system is in the revertive state or dual-host state, you must rectify the fault manually. For details, see **Detailed Fault Recovery Strategies for a High Availability System**.
2	Check whether the resources function properly.	Rectify the fault by referring to **A Resource or Resource Group in the Frozen State** and **A Resource in the Faulted State**.
3	Check whether the resource group is in the enabled state.	Rectify the fault by referring to **Primary/Secondary Switchover Failure Because the Resource Group at the Secondary Site Is Disabled** .
4	Check whether the communication between the primary and secondary sites is normal.	Rectify the fault by referring to **Failure to Communicate Between the Primary and Secondary Sites**.
5	Check whether the data on the primary site is consistent with the data on the secondary site.	Rectify the fault by referring to **Failure to Perform Data Replication Between the Primary and Secondary Sites**.
6	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

Failure to Perform Data Replication Between the Primary and Secondary Sites

The **vxrlink -g datadg -i 5 status datarlk** command is run on the primary server. After about 30 minutes, the system still displays a prompt indicating that a large amount of data is not yet synchronized. The alarm "Data Is Not Synchronized to the U2000 in a High Availability System" is generated.

Locate and rectify the fault according to the steps shown in the following table.

Step	Fault Location	Troubleshooting
1	Check whether the communication between the primary and secondary sites is normal.	Rectify the fault by referring to **Failure to Communicate Between the Primary and Secondary Sites**.

Copyright © Huawei Technologies Co., Ltd.

Step	Fault Location	Troubleshooting
2	Check whether the high availability system is in the normal state.	If the system is in the revertive or dual-host state, you must rectify the fault manually. For details, see **5.8.4 Troubleshooting Policies for a Veritas High Availability System**.
3	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

Failure to Communicate Between the Primary and Secondary Sites

Symptom

Data replication and service switchover cannot be performed between the primary and secondary sites. The alarm "VCS Replication Is Interrupted" is generated.

Possible Causes

The possible causes 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 configured incorrectly.
- The replication link between the primary and secondary sites is interrupted.

Procedure

Step 1 Run the following commands on the primary site to check the communication between the primary and secondary sites as the **root** user:

```
# ping IP_address_of_the_secondary_site
# ping IP_address_of_the_replication_NIC_on_the_secondary_site
```

NOTE

Run the **cat /etc/hosts | grep loghost** command on secondary site as the **root** user to query *IP address of the Master NIC on the secondary site*.

Generally, the bandwidth of the network between the primary and secondary sites is at least 2 Mbit/s and the packet loss ratio is smaller than 0.1%.

Step 2 Check whether replication NICs or the replication link functions properly.

Step 3 Check whether all the ports used by the high availability system are enabled.

Run the following command to query the enabled service ports as the **root** user:

```
# netstat -an
```

When the U2000 uses the Veritas HA system, you need to configure the ports required by the Veritas HA system. See **Table 5-4**.

Copyright © Huawei Technologies Co., Ltd.

Table 5-4 Veritas on primary and secondary sites of the HA system ports

Source End	Source Port	Protocol Type	Destination End	Destination Port	Description
U2000 Server	Any port	TCP	U2000 Server	12212	Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the high availability (HA) system, this port is used for servers at the primary site to notify the secondary site for cooperative deployment.
U2000 Server	Any port	TCP	U2000 Server	12213	Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for the primary site to notify the secondary site for cooperative deployment.
U2000 Server	Any port	TCP	U2000 Server	12214	Port for the msserver process. This port is used to for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary
U2000 Server	Any port	TCP	U2000 Server	12215	Port for the msserver process in SSL mode. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary sites.

Copyright © Huawei Technologies Co., Ltd.

Source End	Source Port	Protocol Type	Destination End	Destination Port	Description
U2000 Server	Any port	TCP	U2000 Server	14155	Port for the GCO WAC process on the Veritas HA system. This port is used for the WAC (Wdie-Area connector) process on the local cluster to listen to connection from remote clusters.
U2000 Server	4145	UDP	U2000 Server	4145	Port for Veritas volume replicator (VVR) heartbeat communication between the active and standby servers.
U2000 Server	Any port	TCP	U2000 Server	4145	This port is used for VVR to listen to the transport layer of the system.
U2000 Server	Any port	TCP	U2000 Server	8199	Port for the vradmind process of the VVR in a Veritas-based HA system. The active and standby servers communicate by means of the vradmind process through this port.
U2000 Server	Any port	TCP	U2000 Server	8989	Port for the in.vxrsyncd process of the VVR in a Veritas HA system. The active and standby servers communicate by means of the vradmind process through this port.

----End

A Resource or Resource Group in the Frozen State

Symptom

In the VCS Explorer, a lock in red is displayed for a resource or resource group.

Possible Causes

Users may forget to restore the resource or resource group after freezing it manually.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Using the Cluster Explorer

1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
2. Right-click, and choose **Unfreeze**.

Step 2 Using the Command Line

1. Log in to the site where the frozen resource group is located as the **root** user.
2. Run the following command to view the freezing mode of the resource group:

   # **hagrp -display** *resource group name*

   In the command output, if the value of the Frozen field is 1, the resource group is permanently frozen. Otherwise, the resource group is temporarily frozen.
3. Run the following commands to clear the Freeze state of the resource group:
   - If the resource group is temporarily frozen, run the following command:

     # **hagrp -unfreeze** *resource group name*
   - If the resource group is permanently frozen, run the following command:

     # **hagrp -unfreeze** *resource group name* **-persistent**

----End

A Resource in the Faulted State

Symptom

In the VCS Explorer, a cross in red is displayed for a resource. The resource is in the **Faulted** state. The alarm "VCS Resources Do Not Function Properly" is generated.

Possible Causes

The resource does not function properly. For example, the U2000 coredump occurs or U2000 processes or database processes are abnormal.

Procedure

Step 1 Check whether the U2000 processes or database processes are normal.

Step 2 Right-click the resource that is in the **Faulted** state and choose **Clear Fault** from the shortcut menu to rectify the fault.

Step 3 If services are performed on the primary server, right-click **AppService** and choose **Online** from the shortcut menu. The **AppService** resource group is in the **Online** state.

----End

Suggestion and Summary

If the U2000 still cannot work after the fault is rectified, 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.

Copyright © Huawei Technologies Co., Ltd.

Abnormal Disk Volume Status

Symptom

After the **vxprint -v** command is run to check the status of a disk volume, the result shows that the data volume is not in the **ACTIVE** or **ENABLED** state. After the **vxprint -l datarvg** command is run to check the status of datarvg, the result shows that the datarvg is in the **RECOVER** state. After the **vxprint -l datarlk** command is run to check the status of datarlk, the result shows that the datarlk is in the **RECOVER** state.

Possible Causes

The disk volume is restarted abnormally or some abnormal operations are performed.

Procedure

Step 1 Open a CLI

Step 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

Run the **vxdg list** command to query the value of *disk_group_name* and run the **vxprint -v** command to query the value of *volume_name*.

Step 3 Check whether the disk volume status and data replication status are correct. If they are correct, the fault is rectified successfully.

----End

Failure to Use the U2000 Upon a Fault on the Active Site

Symptom

The U2000 cannot be used properly.

Possible Causes

A fault occurs on the active site.

Procedure

- In the scenario where the connection between a client and the server is torn down, the active site is unavailable, and the U2000 applications are automatically switched to the standby site, perform the following steps:
  1. Log in to a U2000 client and connect the client to the server on the secondary site.
  2. Manage NEs through the U2000 server on the secondary site.
- In the scenario where the NEs on the U2000 preempt the resource of each other on a client and the server is in the dual-host state, perform the following steps:
  1. Shut down the U2000 server on the primary site. For details, see chapter "Shutting Down the U2000" in the *U2000 Administrator Guide*.

Copyright © Huawei Technologies Co., Ltd.

2. Log in to a U2000 client and connect the client to the server on the secondary site.
3. Manage NEs through the U2000 server on the secondary site.

- In the scenario where a fault occurs on the server because of damaged U2000 data and the primary and secondary sites are both unavailable, perform the following steps:
  1. Recover the backup data of the U2000. For details, see chapter "Backing Up and Restoring the U2000 Database" in the *U2000 Administrator Guide*.
  2. If there is no backup data, recover the data by using the script. For details, see chapter "Backing Up and Restoring the U2000 Database" in the *U2000 Administrator Guide*.

----End

High Availability System Frequently Entering the Dual-Host State

Symptom

The heartbeat between the primary and secondary sites is frequent interrupted, and the high availability system is in the dual-host state. As a result, the U2000 cannot work properly. The alarm "VCS Heartbeats Are Interrupted" or "Both Primary and Secondary Sites Enter the Primary State" is generated.

Possible Causes

The instability of the data communication network (DCN) between the primary and secondary sites leads to frequent interruption of heartbeat between the two sites. You can rectify the fault by changing the timeout period of heartbeat detection.

Procedure

Step 1 To display the current heartbeat settings, run the following command respectively on the primary and secondary sites:

```
# /opt/VRTSvcs/bin/hahb -display
```

Step 2 To change 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 heartbeat settings according to the period during which the network between the primary and secondary sites is interrupted. Besides an increase in the retry limit (**AYARetryLimit**), you can set the interval (**AYAInterval**) and timeout period (**AYATimeout**) in this manner also.

Step 3 After the DCN becomes stable, restore the heartbeat settings to default values.

----End

Suggestion and Summary

Modifying the timeout period of heartbeat detection applies only to the temporary avoidance of high availability system problems caused by the DCN instability. Therefore, troubleshooting in

Copyright © Huawei Technologies Co., Ltd.

time the problems of the unstable DCN between the primary and secondary sites and then restoring the heartbeat settings to default values is recommended.

High Availability System Abnormality Due to a DCN Fault

Symptom

The heartbeat connections between the primary and secondary sites become interrupted frequently. The high availability system enters the dual-host state many times and cannot work properly. The alarm "VCS Heartbeats Are Interrupted" or "Both Primary and Secondary Sites Enter the Primary State" is generated.

Possible Causes

The DCN between the primary and secondary site is unstable; as a result, the heartbeat connections between the primary and secondary site are interrupted frequently or the DCN is torn down.

Fault Diagnosis

1. Run the **vradmin -g datadg repstatus datarvg** command on the primary and secondary sites to check the data replication status. If the command output contains **needs dcm resynchronization** or **Primary-Primary configuration**, the data replication function of the high availability system is abnormal.
2. Log in to the VCS clients on both the primary and secondary sites. Check whether the **NMSServer** resource in the **AppService** resource group is marked red. If the **NMSServer** resource is not marked red, this problem does not arise from the **NMSServer** resource.
3. Run the **cat /var/adm/messages*** command on the primary site to view the system log file. The file content shows that the Rlink is interrupted and heartbeat connections are torn down frequently.

```
Dec  1 06:26:52 U2000S1B vxio: [ID 467919 kern.warning] WARNING: VxVM VVR vxio
V-5-0-266 Rlink datarlk disconnected from remote
Dec  1 06:29:28 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-18311 (U2000S1B) secondaryCluster lost connection to cluster
primaryCluster
Dec  1 06:33:13 U2000S1B Wac[17173]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-18311 secondaryCluster lost connection to cluster primaryCluster
Dec  1 06:33:13 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-18313 (U2000S1B) TCP/IP connection via connector from cluster
secondaryCluster to cluster primaryCluster is hung; intentionally
disconnecting. Auto-reconnect will occur however you may wish to examine the
wac resource on system 10.18.9.186
Dec  1 06:34:07 U2000S1B vxio: [ID 754354 kern.warning] WARNING: VxVM VVR vxio
V-5-0-233 Node 10.160.2.146 disconnected from node 10.18.9.186
Dec  1 06:36:42 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-50908 Remote cluster primaryCluster has faulted.  Determining if global
group AppService should be failed over to local cluster
Dec  1 06:36:42 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-50910 Local cluster was determined to be the next suitable failover
target for Group AppService. Initiating online of group
Dec  1 06:36:42 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS CRITICAL
V-16-1-50513 Remote cluster 'primaryCluster' has faulted
Dec  1 06:36:42 U2000S1B Had[16949]: [ID 702911 daemon.notice] VCS ERROR
V-16-1-51071 ALERT[CFAULT-primaryCluster-primaryCluster] Remote cluster
primaryCluster has faulted
Administrative action is required.
```


Copyright © Huawei Technologies Co., Ltd.

4. The result shows that the problem arises because of a DCN fault.

Procedure

Step 1 Restore the DCN between the primary and secondary sites.

NOTE

The possible causes of a network fault are as follows:

- The bandwidth of connections between the primary and secondary sites does not meet the minimum requirement of the high availability system. In this case, learn about network bandwidth from the customer, apply for a proper bandwidth from the customer in time to solve the problem.
- Network quality deteriorates after the network is interrupted. In this case, run the **ping -s gateway_address packet_size** command on the primary and secondary sites and view the packet loss ratio in the command output to locate the fault. Generally, the packet size ranges from 1400 to 8400.

Step 2 After the network fault is rectified, run the following command to check the system status:

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

- If the command output contains **Replication status: logging to DCM (needs dcm resynchronization)**, data accumulates after the DCN recovers. In this case, you must run the **vradmin -g datadg resync datarvg** command on the primary site.

```
Replicated Data Set: datarvg
Primary:
  Host name:                    Primary_datarep
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 16
  SRL name:                     srl_vol
  SRL size:                     3.00 G
  Total secondaries:            1

Secondary:
  Host name:                    Secondary_datarep
  RVG name:                     datarvg
  DG name:                      datadg
  Data status:                  consistent, behind
  Replication status:           logging to DCM (needs dcm resynchronization)
  Current mode:                 asynchronous
  Logging to:                   DCM (contains 5638848 Kbytes) (SRL protection
logging)
Timestamp Information:      N/A
```

- If the command output contains **Primary-Primary configuration**, the high availability system is in the Recovery state after the DCN recovers. If the client and upper-layer OSS are connected to the primary site, log in to the primary site and run the **Force Active of Local Site** command. If the client and upper-layer OSS are connected to the secondary site, log in to the secondary site and run the **Force Active of Local Site** command.

```
Replicated Data Set: datarvg
Primary:
  Host name:                    GD_T2000_3_P
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 14
  SRL name:                     srl_vol
  SRL size:                     3.00 G
  Total secondaries:            1

Primary (acting secondary):
  Host name:                    GD_T2000_4_S
```


Copyright © Huawei Technologies Co., Ltd.

```
  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 580928 Kbytes) (failback logging)
  Timestamp Information:    N/A

Config Errors:
GD_T2000_3_P:             Primary-Primary configuration
```

----End

Primary/Secondary Switchover Failure Because the Resource Group at the Secondary Site Is Disabled

Symptom

When a primary/secondary switchover is performed on the high availability system, a message indicating a VCS resource error is displayed. The switchover fails.

Possible Causes

The resource group at the secondary site is disabled and cannot go online.

Procedure

- GUI mode:
  1. Log in to the OS as user **root**.
  2. Open a CLI.
  3. Run the following command to start the VCS client:

     ```
     # hagui&
     ```

     NOTE

     If the OS was just restarted, wait 10 to 15 minutes. After the process starts, run the **hagui&** command.
  4. Choose **File** > **New Cluster**. Then, enter the server IP address and click **OK**.

     NOTE

     If you are not logging in to the VCS client for the first time, click a server record in the information list in the **Cluster Monitor** window.
  5. Enter the user name and password for VCS login.

     NOTE

     The default VCS user name is **admin** and the default password is **Changeme_123**. To ensure system security, change the default password in time. If the default password has been changed, enter the new password.
  6. Ensure that the datarvg resource in the **VVRService** resource group has been enabled.

     Right-click the datarvg resource and check whether the **Enabled** option is selected. If this option is selected, it has been enabled.

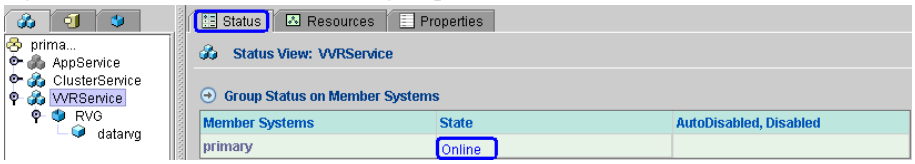
Copyright © Huawei Technologies Co., Ltd.

If this option is not selected, select it.

In the dialog box that is displayed, click **Yes**.

7. Ensure that the **VVRService** resource group has been started.

   Select the **VVRService** resource group, click the **Status** tab, and check whether the value in the **State** column is **Online**. If **Online** is displayed as shown in the following figure, the **VVRService** resource group has been started.



   If the **VVRService** resource group has not been started, do as follows to start it:

   a. Right-click the **VVRService** resource group and choose **Online** > ***host name*** from the shortcut menu.

   b. In the dialog box that is displayed, click **Yes** to make the resource group online.

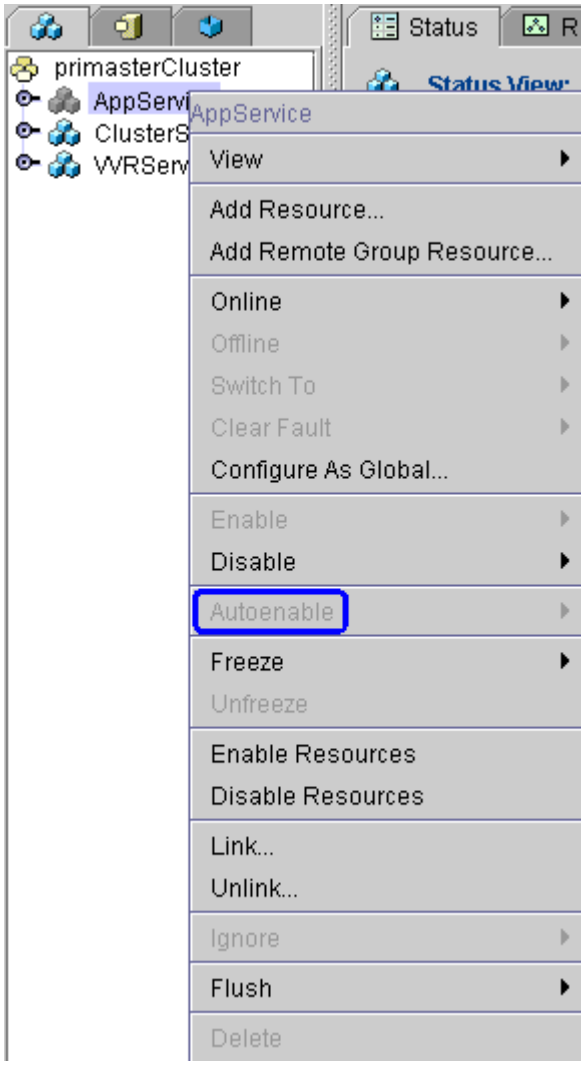
8. Ensure that all resources in the **AppService** resource group have been enabled.

   Right-click a resource in the **AppService** resource group and check whether the **Enabled** option is selected. If this option is selected, the resource has been enabled.

Copyright © Huawei Technologies Co., Ltd.

If this option is not selected, you must select it. Repeat this operation on every resource in the **AppService** resource group.

9. **Optional:** Ensure that **Autoenable** of the **AppService** resource group has been grayed out, as shown in the following figure.



   - If **Autoenable** has been grayed out, no action is required.
   - If **Autoenable** has not been grayed out, click **Autoenable** to gray it out.

10. Click **File** > **Save Configuration** to save the settings.

- CLI mode:
  1. Log in to the OS as the **root** user.
  2. Run the following commands to start the U2000 server:

```
# haconf -makerw  > /dev/null 2>&1
# hares -modify datarvg Enabled 1
# haconf -dump -makero
```

----End

Copyright © Huawei Technologies Co., Ltd.

5.8.6 Failure to Connect the Primary and Secondary Sites (HA System, Solaris)

This topic describes how to troubleshoot the failure to connect the primary and secondary sites.

Mismatch of Replication Volume Sizes

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating a mismatch of replication volume sizes and asking you to modify the replication volume sizes.

Possible Causes

- The hardware configurations on the primary and secondary sites are inconsistent.
- The replication volume sizes on the primary and secondary sites are different.
- The SRL volume sizes on the primary and secondary sites are different.

Procedure

Step 1 Run the following command on the primary and secondary sites to view the replication volume and SRL volume sizes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

The replication volume and SRL volume are named lv_nms_data and srl_vol, and their sizes are 33554432/2/1024/1024 = 16 GB and 2097152/2/1024/1024 = 1 GB respectively.

Step 2 On the site whose replication volume size is smaller, perform the following operations to expand the volume to the same size on the other site:

- Expand the srl_vol volume. Suppose that the srl_vol volume is to be expanded to 2 GB.
  1. Run the **hagui&** command to log in to the VCS client. Select **AppService**, right-click, and choose **Offline** > ***host name*** from the shortcut menu to stop the NMS and database.
  2. Run the following command to check whether the server has sufficient space:

     # **vxassist -g datadg maxgrow srl_vol**

     Information similar to the following is displayed:

     ```
     Volume srl_vol can be extended by 2736128 to: 4833280 (2360Mb)
     ```

     As indicated by the preceding information, the srl_vol volume can be expanded to 2.3 GB at most.
  3. Run the following command to expand the srl_vol volume to 2 GB:

Copyright © Huawei Technologies Co., Ltd.

vxresize -g datadg srl_vol 2g

- Expand the lv_nms_data volume. Suppose that the lv_nms_data volume is to be expanded to 50 GB.

  1. Run the **hagui&** command to log in to the VCS client. Select **AppService**, right-click, and choose **Offline** > ***host name*** from the shortcut menu to stop the NMS and database.
  2. Run the following command to check whether the server has sufficient space:

     # **vxassist -g datadg maxgrow lv_nms_data**

     Information similar to the following is displayed:

     ```
     Volume lv_nms_data be extended by 140777472 to: 140879872 (68789Mb)
     ```

     As indicated by the preceding information, the lv_nms_data volume can be expanded to 67 GB at most.
  3. Run the following command to expand the lv_nms_data volume to 50 GB:

     # **vxresize -F ufs -g datadg lv_nms_data 50g**
  4. Run the following command to delete the DCM log:

     # **/usr/sbin/vxassist -g datadg -f remove log lv_nms_data nlog=0**
  5. Run the following command to add a DCM log:

     # **vxprint**

     Information similar to the following is displayed:

     ```
     ... ...
     v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
     pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
     sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
     pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
     sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
     ... ...
     ```

     - If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

       # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

     - If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

       # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

----End

Nonexistence of Replication Volumes

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating nonexistence of replication volumes and asking you to create replication volume sizes.

Possible Causes

The replication volume or SRL volume of the primary or secondary site does not exist.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the following command on the primary site to view the replication volume and SRL volume names and sizes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

The replication volume and SRL volume are named lv_nms_data and srl_vol, and their sizes are 33554432/2/1024/1024 = 16 GB and 2097152/2/1024/1024 = 1 GB respectively.

Step 2 Run the following commands on the secondary site to create lv_nms_data volume and add a DCM log for the lv_nms_data volume:

vxassist -g datadg make lv_nms_data 16g

vxprint

Information similar to the following is displayed:

```
... ...
v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
... ...
```

- If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

- If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

Step 3 Run the following command on the secondary site to create srl_vol volume:

vxassist -g datadg make srl_vol 1g

----End

Replication Volumes Not in Active State

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating that the replication volumes are mot in active state and asking you to repair the replication volumes.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The replication volumes are damaged and enter the non-active state.
- The SRL volume is damaged and enters the non-active state.

Procedure

Step 1 Run the following command to check the status of replication and SRL volumes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

As indicated by the preceding information, the replication and SRL volumes are in active state and enabled.

Step 2 If any of the replication or SRL volumes is not in active state, run the following command to repair it:

vxrecover -bs

----End

No DCM Logs for Replication Volumes

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating that the replication volumes have no DCM logs and asking you to add DCM logs.

Possible Causes

DCM logs are deleted or not created.

Procedure

Step 1 Run the following command to add DCM logs:

vxprint

Information similar to the following is displayed:

```
... ...
v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
... ...
```


Copyright © Huawei Technologies Co., Ltd.

- If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

- If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

----End

Inconsistent Database Passwords for the Primary and Secondary Sites

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating that the database **sa** user passwords or database user passwords for the primary and secondary sites are inconsistent and asking you to change the passwords to the same one.

Possible Causes

The database passwords have been set to different ones during the installation of primary and secondary sites, or the database password for one site has been changed using the MSuite after the sites are installed.

Procedure

Step 1 Change the database **sa** user passwords or database user passwords to the same one for the primary and secondary sites. For details, see **Change Database administrator Password** or **Change Database User Password** in the *iManager U2000 Administrator Guide*.

----End

Database Abnormality

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating that the database is abnormal.

Possible Causes

- After the NMS and database are installed, the database user password is changed manually, rather than using the MSuite. As a result, the database user password is different from that recorded on the NMS.
- The database fails to start.
- A fault occurs on the database.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 If the database user password has been changed manually, change it back to the original password. Ensure that you use the MSuite to change the database user password and the database user password is consistent for the primary and secondary sites.

Step 2 Contact Huawei technical support engineers to locate the database fault.

----End

Failure to Connect to the MSuite on the Peer Site

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating a failure to connect to the MSuite on the peer site.

Possible Causes

- The network between the primary and secondary sites is disconnected.
- The MSuite on the secondary site is not started.

Procedure

Step 1 Run the **ping** command to verify that the network between the primary and secondary sites is connected.

Step 2 Start the MSuite on the secondary site. For details, see **Starting the Process of the MSuite Server** in the *U2000 Administrator Guide*.

----End

Unavailable Replication IP Address

Symptom

During the connection of the primary and secondary sites, a message is displayed indicating that the replication IP address is unavailable.

Possible Causes

- Replication NICs on the primary and secondary sites do not function properly.
- The DCN between the primary and secondary sites is interrupted.
- The replication IP addresses of the primary and secondary sites are not reachable.

Procedure

Step 1 On the primary and secondary sites, run the following command to check whether the replication IP addresses exist:

ifconfig -a

Copyright © Huawei Technologies Co., Ltd.

If the command output does not contain replication IP addresses, reset replication IP addresses. For details, see chapter **Pre-configuring the U2000** in the *U2000 HA System Software Installation and Commissioning Guide (Solaris)* or *U2000 Remote HA System Software Installation and Commissioning Guide (SUSE Linux, PC Server)*.

Step 2 On the primary and secondary sites, run the following command to check whether the NICs where the replication IP addresses are located are in marked **UP** and **RUNNING**, but not **DUPLICATED**:

ifconfig -a

- If the command output does not contain **UP**, run the **ifconfig** *NIC name* **up** command to make the NIC status **UP**.
- If the command output does not contain **RUNNING**, verify that NICs are properly connected.
- If the command output contains **DUPLICATED**, IP addresses may be occupied and you must reset IP addresses.

Step 3 On the primary and secondary sites, run the following command to check whether the replication IP addresses of the primary and secondary sites are reachable:

ping *remote replication IP address*

If the primary and secondary sites can ping through each other, the replication IP addresses of the primary and secondary sites are reachable.

----End

Unavailable Heartbeat IP Address

Symptom

During a connection between the primary and secondary sites, a message is displayed indicating that heartbeat IP addresses are not reachable.

Possible Causes

- Heartbeat NICs on the primary and secondary sites do not function properly.
- The DCN between the primary and secondary sites is interrupted.
- The heartbeat IP addresses of the primary and secondary sites are not reachable.

Procedure

Step 1 On the primary and secondary sites, run the following command to check whether the heartbeat IP addresses exist:

ifconfig -a

If the command output does not contain heartbeat IP addresses, reset heartbeat IP addresses. For details, see chapter **Pre-configuring the U2000** in the *U2000 HA System Software Installation and Commissioning Guide (Solaris)*.

Step 2 On the primary and secondary sites, run the following command to check whether the NICs where the heartbeat IP addresses are located are in marked **UP** and **RUNNING**, but not **DUPLICATED**:

Copyright © Huawei Technologies Co., Ltd.

ifconfig -a

- If the command output does not contain **UP**, run the **ifconfig** *NIC name* **up** command to make the NIC status **UP**.
- If the command output does not contain **RUNNING**, verify that NICs are properly connected.
- If the command output contains **DUPLICATED**, IP addresses may be occupied and you must reset IP addresses.

Step 3 On the primary and secondary sites, run the following command to check whether the heartbeat IP addresses of the primary and secondary sites are reachable:

ping *peer heartbeat IP address*

If the primary and secondary sites can ping through each other, the heartbeat IP addresses of the primary and secondary sites are reachable.

----End

5.8.7 Failure to Separate the Primary and Secondary Sites (HA System, Solaris)

This topic describes how to troubleshoot the failure to separate the primary and secondary sites.

NMS and Database Not Shut Down

Symptom

During the separation of the primary and secondary sites, a message is displayed indicating that the NMS and database must be shut down to prevent incomplete database data and NMS failure on the secondary site and asking you whether to continue.

Possible Causes

The NMS and database are not shut down.

Procedure

Step 1 Click **No**. Manually shut down the NMS and database before separating the primary and secondary sites.

NOTICE

If you click **Yes** to forcibly separate the primary and secondary sites, data on the database of the secondary site may be incomplete and the NMS on the secondary site may be abnormal. Therefore, forcibly separating the primary and secondary sites is not recommended.

----End

Copyright © Huawei Technologies Co., Ltd.

Incomplete Replication

Symptom

During the separation of the primary and secondary sites, a message is displayed indicating that the replication is incomplete or abnormal and the forcible separation may result in an NMS abnormality on the secondary site and asking you whether to continue.

Possible Causes

- The SRL volume has accumulated data.
- Data in the SRL volume overflows.
- The replication status is not up-to-data.

Procedure

Step 1 Click **No**. The system does not forces the primary site to be separated from the secondary site. If the problem persists, contact Huawei technical support engineers to troubleshoot the problem.

NOTICE

If **Yes** is clicked, the system forces the primary site to be separated from the secondary site and the U2000 on the secondary site may not function properly. Separating the primary and secondary sites is not recommended.

----End

Failure to Connect to the MSuite on the Peer Site

Symptom

During the separation of the primary and secondary sites, a message is displayed indicating a failure to connect to the MSuite on the peer site.

Possible Causes

- The network between the primary and secondary sites is disconnected.
- The MSuite on the secondary site is not started.

Procedure

Step 1 Run the **ping** command to verify that the network between the primary and secondary sites is connected.

Step 2 Start the MSuite on the secondary site. For details, see **Starting the Process of the MSuite Server** in the *U2000 Administrator Guide*.

----End

Copyright © Huawei Technologies Co., Ltd.

5.8.8 Failure to Forcibly Configure the Local End as the Primary Site (HA System, Solaris)

This topic describes how to troubleshoot the failure to forcibly configure the local end as the primary site.

Mismatch of Replication Volume Sizes

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating a mismatch of replication volume sizes and asking you to modify the replication volume sizes.

Possible Causes

- The hardware configurations on the primary and secondary sites are inconsistent.
- The replication volume sizes on the primary and secondary sites are different.
- The SRL volume sizes on the primary and secondary sites are different.

Procedure

Step 1 Run the following command on the primary and secondary sites to view the replication volume and SRL volume sizes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

The replication volume and SRL volume are named lv_nms_data and srl_vol, and their sizes are 33554432/2/1024/1024 = 16 GB and 2097152/2/1024/1024 = 1 GB respectively.

Step 2 On the site whose replication volume size is smaller, perform the following operations to expand the volume to the same size on the other site:

- Expand the srl_vol volume. Suppose that the srl_vol volume is to be expanded to 2 GB.
  1. Run the **hagui&** command to log in to the VCS client. Select **AppService**, right-click, and choose **Offline** > ***host name*** from the shortcut menu to stop the NMS and database.
  2. Run the following command to check whether the server has sufficient space:

     # **vxassist -g datadg maxgrow srl_vol**

     Information similar to the following is displayed:

     ```
     Volume srl_vol can be extended by 2736128 to: 4833280 (2360Mb)
     ```


Copyright © Huawei Technologies Co., Ltd.

As indicated by the preceding information, the srl_vol volume can be expanded to 2.3 GB at most.

3. Run the following command to expand the srl_vol volume to 2 GB:

   # **vxresize -g datadg srl_vol 2g**

- Expand the lv_nms_data volume. Suppose that the lv_nms_data volume is to be expanded to 50 GB.

  1. Run the **hagui&** command to log in to the VCS client. Select **AppService**, right-click, and choose **Offline** > ***host name*** from the shortcut menu to stop the NMS and database.
  2. Run the following command to check whether the server has sufficient space:

     # **vxassist -g datadg maxgrow lv_nms_data**

     Information similar to the following is displayed:

     ```
     Volume lv_nms_data be extended by 140777472 to: 140879872 (68789Mb)
     ```

     As indicated by the preceding information, the lv_nms_data volume can be expanded to 67 GB at most.
  3. Run the following command to expand the lv_nms_data volume to 50 GB:

     # **vxresize -F ufs -g datadg lv_nms_data 50g**
  4. Run the following command to delete the DCM log:

     # **/usr/sbin/vxassist -g datadg -f remove log lv_nms_data nlog=0**
  5. Run the following command to add a DCM log:

     # **vxprint**

     Information similar to the following is displayed:

     ```
     ... ...
     v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
     pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
     sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
     pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
     sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
     ... ...
     ```

     - If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

       # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

     - If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

       # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

----End

Nonexistence of Replication Volumes

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating nonexistence of replication volumes and asking you to create replication volume sizes.

Possible Causes

The replication volume or SRL volume of the primary or secondary site does not exist.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the following command on the primary site to view the replication volume and SRL volume names and sizes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

The replication volume and SRL volume are named lv_nms_data and srl_vol, and their sizes are 33554432/2/1024/1024 = 16 GB and 2097152/2/1024/1024 = 1 GB respectively.

Step 2 Run the following commands on the secondary site to create lv_nms_data volume and add a DCM log for the lv_nms_data volume:

vxassist -g datadg make lv_nms_data 16g

vxprint

Information similar to the following is displayed:

```
... ...
v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
... ...
```

- If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

- If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

Step 3 Run the following command on the secondary site to create srl_vol volume:

vxassist -g datadg make srl_vol 1g

----End

Replication Volumes Not in Active State

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating that the replication volumes are mot in active state and asking you to repair the replication volumes.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The replication volumes are damaged and enter the non-active state.
- The SRL volume is damaged and enters the non-active state.

Procedure

Step 1 Run the following command to check the status of replication and SRL volumes:

vxprint -v

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg      ENABLED  33554432 -        ACTIVE   -       -
v  opt          fsgen        ENABLED  60821952 -        ACTIVE   -       -
v  rootvol      root         ENABLED  31464192 -        ACTIVE   -       -
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -       -
v  swapvol      swap         ENABLED  12587712 -        ACTIVE   -       -
```

As indicated by the preceding information, the replication and SRL volumes are in active state and enabled.

Step 2 If any of the replication or SRL volumes is not in active state, run the following command to repair it:

vxrecover -bs

----End

No DCM Logs for Replication Volumes

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating that the replication volumes have no DCM logs and asking you to add DCM logs.

Possible Causes

DCM logs are deleted or not created.

Procedure

Step 1 Run the following command to add DCM logs:

vxprint

Information similar to the following is displayed:

```
... ...
v  backup       fsgen        ENABLED  161493120 -       ACTIVE   -       -
pl backup-01    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk01-05    backup-01    ENABLED  161493120 0       -        -       -
pl backup-02    backup       ENABLED  161493120 -       ACTIVE   -       -
sd disk04-03    backup-02    ENABLED  161493120 0       -        -       -
... ...
```


Copyright © Huawei Technologies Co., Ltd.

- If the command output contains two **pl**s, the system has been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=2**

- If the command output contains only one **pl**, the system has not been configured with disk mirroring. To add DCM logs, run the following command:

  # **/usr/sbin/vxassist -g datadg addlog lv_nms_data logtype=dcm nlog=1**

----End

Inconsistent Database Passwords for the Primary and Secondary Sites

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating that the database **sa** user passwords or database user passwords for the primary and secondary sites are inconsistent and asking you to change the passwords to the same one.

Possible Causes

The database passwords have been set to different ones during the installation of primary and secondary sites, or the database password for one site has been changed using the MSuite after the sites are installed.

Procedure

Step 1 Change the database **sa** user passwords or database user passwords to the same one for the primary and secondary sites. For details, see **Change Database administrator Password** or **Change Database User Password** in the *iManager U2000 Administrator Guide*.

----End

Database Abnormality

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating that the database is abnormal.

Possible Causes

- After the NMS and database are installed, the database user password is changed manually, rather than using the MSuite. As a result, the database user password is different from that recorded on the NMS.
- The database fails to start.
- A fault occurs on the database.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 If the database user password has been changed manually, change it back to the original password. Ensure that you use the MSuite to change the database user password and the database user password is consistent for the primary and secondary sites.

Step 2 Contact Huawei technical support engineers to locate the database fault.

----End

Failure to Connect to the MSuite on the Peer Site

Symptom

When you attempt to forcibly configure the local site as the primary site, a message is displayed indicating a failure to connect to the MSuite on the peer site.

Possible Causes

- The network between the primary and secondary sites is disconnected.
- The MSuite on the secondary site is not started.

Procedure

Step 1 Run the **ping** command to verify that the network between the primary and secondary sites is connected.

Step 2 Start the MSuite on the secondary site. For details, see **Starting the Process of the MSuite Server** in the *U2000 Administrator Guide*.

----End

5.8.9 Common FAQ

This topic describes common FAQs for a high availability system.

How to Check Whether the U2000 Processes of the High Availability System (Solaris, PC Linux) Are Started

Question

How to check whether the U2000 processes of the high availability system (Solaris, PC Linux) are started?

Answer

Step 1 Log in to the OS of the active site as the **ossuser** user.

Step 2 Check the U2000 processes.

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

```
$ daem_ps
```


Copyright © Huawei Technologies Co., Ltd.

Information similar to the following is displayed:

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

NOTE

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

The process is stopped if the displayed information is empty.For the high availability system (Solaris), you can still view information about the **imapwatchdog** and **ResourceMonitor** processes after the U2000 is stopped. This is because the two processes are used to monitor high availability system alarms and will be automatically enabled after the U2000 is stopped.

----End

How to End the U2000 Processes of the High Availability System (Solaris, PC Linux)

Question

How do I end the U2000 processes of the high availability system (Solaris, PC Linux)?

Answer

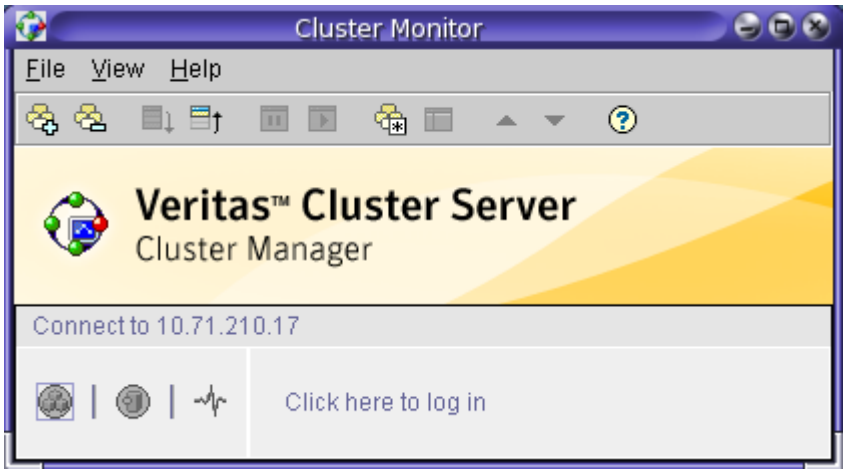
Step 1 Log in to the OS of the active site as the **root** user.

Step 2 Stop the U2000 server processes.

- GUI mode:

  1. Open a terminal window, run the following command:

     ```
     # hagui&
     ```

     NOTE

     If the login dialog box is not displayed and a message appears indicating that the current status is **STALE_ADMIN_WAIT**, run the **# hasys -force** ***host name of node*** command.

  2. Click **Connect to** ***Cluster name***.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If you are logging in to the VCS for the first time, you need to create a new Cluster.

1. Click **File** > **New Cluster**.
2. Enter the IP address of application network.
3. Click **OK**.

3. Enter the user name and password for VCS login.

   NOTE

   The default VCS user name is **admin** and the default password is **Changeme_123**. To ensure system security, change the default password in time. If the default password has been changed, enter the new password.

4. Click **OK**.
5. Choose **AppService** from the navigation tree.
6. Click the **Resources** tab. Right-click **NMSServer** and choose **Offline** > ***Host name*** from the shortcut menu.

   Wait about 1 minute. If the **NMSServer** icon changes to grey, the U2000 processes have been stopped.

- CLI mode:

  # **hares -offline NMSServer -sys** *hostname*

----End

How Do I Ensure Proper Connections to VVR and MSuite Ports on the Primary and Secondary Sites?

Question

How do I ensure proper connections to VVR and MSuite ports on the primary and secondary sites?

Answer

Step 1 Check whether a firewall has been set on the network between the primary and secondary sites. If a firewall has been set, permit VVR and MSuite ports into the firewall.

Step 2 On the primary and secondary sites, log in to the OS as the **root** user.

Step 3 On the primary and secondary sites, verify that the VVR ports used by the peer site can be connected.

NOTE

- Ports 4145, 8199, and 8989 are VVR ports.
- The following uses port 8199 as an example.

1. Run the following commands to check whether the VVR ports used by the peer site can be connected:

   ```
   # cd /opt/install/OSSICMR/bin
   # chmod 750 Hacheck.sh
   # ./Hacheck.sh Peer site application IP address
   ```

   Enter the password for the **ossuser** user used by the peer site.

   - Verify that port 4145, 8199, or 8989 is connected properly.

Copyright © Huawei Technologies Co., Ltd.

- If ports 4145, 8199, and 8989 all fail to be connected, go to step **3.2**.

2. Run the following commands to view the PID of the process that uses the port:
   - On Linux OS, run the following command:
     ```
     # netstat -ntlp | grep -w 8199
     ```
     Information similar to the following is displayed:
     ```
     tcp        0      0 :::8199                 :::*                    LISTEN
     979/
     ```
   - On Solaris OS, run the following commands:
     ```
     # cd /proc
     # pfiles * > /tmp/proc.txt
     # more /tmp/proc.txt
     ```
     Information similar to the following is displayed:
     ```
     979:   /opt/oss/server/conf/../bin/DmsSyslogCollector

       Current rlimit: 4096 file descriptors

       13: S_IFREG mode:0644 dev:32,88 ino:52929 uid:0 gid:0 size:892888

           O_WRONLY|O_CREAT|O_TRUNC

           /opt/oss/server/conf/log/DmsSyslogCollector20080226_133400.log

       14: S_IFSOCK mode:0666 dev:323,0 ino:22704 uid:0 gid:0 size:0

           O_RDWR

        SOCK_DGRAM

        SO_SNDBUF(57344),SO_RCVBUF(57344)

        sockname: AF_INET 0.0.0.0  port: 8199
     ```
   Port 8199 is used by the process 979.
3. View the process.
   ```
   # ps -ef |grep 979
   ```
   Information similar to the following is displayed:
   ```
   root 20161  2440   0 14:56:37 pts/1       0:00 grep 979
   root   979 25685   0   Feb 20 ?           8:17 /opt/oss/server/conf/../bin/
   DmsSyslogCollector
   ```
   Process 979 is DmsSyslogCollector.
4. Run the **kill** *PID* command to stop the process after confirming that it can be stopped.

NOTICE

Stop the process only after you confirm that it can be stopped. Otherwise, the U2000 may fail to run properly.

Step 4 On the primary and secondary sites, verify that the MSuite ports can be connected.

NOTE

- Ports 12212, 12213, 12214, and 12215 are MSuite ports.
- The following uses port 12212 as an example.

1. Run the following commands to check whether MSuite ports are occupied:
   - On Linux OS, run the following command:

Copyright © Huawei Technologies Co., Ltd.

```
# netstat -ntlp | grep -w 12212
```

- If no command output is returned, the ports are not occupied and can be connected.
- If a command output is returned and contains the information below, the ports are occupied by process 979. Then go to step 4.2.

```
tcp        0      0 :::12212                :::*                    LISTEN
979/
```

- On Solaris OS, run the following commands:

```
# cd /proc
# pfiles * > /tmp/proc.txt
# more /tmp/proc.txt
```

- If a command output is returned but does not contain the information below, the ports are not occupied and can be connected.
- If a command output is returned and contains the information below, the ports are occupied by process 979. Then go to step 4.2.

```
979:   /opt/oss/server/conf/../bin/DmsSyslogCollector

  Current rlimit: 4096 file descriptors

  13: S_IFREG mode:0644 dev:32,88 ino:52929 uid:0 gid:0 size:892888

      O_WRONLY|O_CREAT|O_TRUNC

      /opt/oss/server/conf/log/DmsSyslogCollector20080226_133400.log

  14: S_IFSOCK mode:0666 dev:323,0 ino:22704 uid:0 gid:0 size:0

      O_RDWR

   SOCK_DGRAM

   SO_SNDBUF(57344),SO_RCVBUF(57344)

   sockname: AF_INET 0.0.0.0  port: 12212
```

2. View the process.

```
# ps -ef |grep 979
```

Information similar to the following is displayed:

```
root 20161  2440   0 14:56:37 pts/1       0:00 grep 979
root   979 25685   0   Feb 20 ?           8:17 /opt/oss/server/conf/../bin/
DmsSyslogCollector
```

Process 979 is DmsSyslogCollector.

3. Run the **kill** *PID* command to stop the process after confirming that it can be stopped.

NOTICE

Stop the process only after you confirm that it can be stopped. Otherwise, the U2000 may fail to run properly.

----End

Copyright © Huawei Technologies Co., Ltd.

6 Troubleshooting Basic Operation Faults on the U2000

About This Chapter

This topic describes how to troubleshoot basic operation faults on the U2000.

6.1 License Management Troubleshooting
This describes how to rectify the common faults of license management.

6.2 Security Management Troubleshooting
This describes how to rectify the common faults of security management.

6.3 Topology Management Troubleshooting
This describes how to rectify the common faults of topology management.

6.4 Performance Management Troubleshooting
This describes how to rectify the common faults in performance management.

6.5 Configuration Failure Troubleshooting
This topic describes how to troubleshoot common configuration failures.

6.6 Alarm Troubleshooting
This describes how to rectify the common faults of alarms.

Copyright © Huawei Technologies Co., Ltd.

6.1 License Management Troubleshooting

This describes how to rectify the common faults of license management.

NOTE

If the license file is lost, search for the email received when the license is obtained.

6.1.1 A Failure to Update the U2000 License File to a Commercial License File

Fault Symptom

The license file of the U2000 cannot be updated to a commercial license file.

Fault Analysis

- The to-be-updated license file is an expired temporary license file.
- The license item is incorrect.
- The ESN of the U2000 server is different from the ESN in the U2000 license file.
- The obtained license is incorrect. The license information does not match the version information. Alternatively, the number of licenses used is inconsistent with the number of licenses authorized by the U2000.
- The login user of the client does not have rights to update license files.
- When commercial license files are uploaded to Solaris- or SUSE Linux-based servers, the transfer mode, user name, or directory is incorrect.
- Temporary and commercial license files coexist in the **License** directory on the server.
- The device types supported by the new license are different from those supported by the original license.
- The function items supported by the new license are less those supported by the original license.
- The number of clients supported by the new license is different from that supported by the original license.

Procedure

Step 1 Ensure that the updated license file does not expire.

Step 2 If the license item is incorrect, please apply for a new license.

Step 3 Check whether the ESN in the license file is the same as that ESN of the U2000 server. If not, apply for a new license.

Step 4 Check whether the U2000 version in the license file is the same as the U2000 version to be installed. If U2000 version in the license file is different from the U2000 version to be installed, apply for the required license file.

Step 5 Ensure that the login user of the client has rights to update license files.

You are recommended to log in as user **admin**.

Copyright © Huawei Technologies Co., Ltd.

Step 6 Upload a commercial license file to the correct directory on Solaris- or SUSE Linux-based servers in ASCII mode as an appropriate user.

- On Solaris OS, upload the license file to the **/export/home/ossuser** path on the server as user **ossuser**.
- On SUSE Linux OS, upload the license file to the **/export/home/ossuser** path on the server as user **ossuser**.
- In a high availability (HA) system, upload the new license file to the server at the primary site.

Step 7 Ensure that only a commercial license file exists in the **license** directory.

Step 8 Update the license file. Choose **Help** > **License Management** > **License Information** from the main menu. In the dialog box that is displayed, click **Update License**. In the **Open** dialog box, select the new license file and click **Open**.

NOTE

In an HA system, you need to log in to the U2000 client at the secondary site to update license files.

Step 9 Check whether The device types supported by the new license are different from those supported by the original license.If not, the license is updated as follows:

- If the device types supported by the new license are more than the device types supported by the original license and the added device types are supported by the current version, the license can be updated. If the added device types are not supported by the current version, the license cannot be updated.
- If the device types supported by the new license are less than the device types supported by the original license and no NEs of the reduced device types are created in the NMS, the license can be updated. If certain NEs of the reduced device types are created in the NMS, the license cannot be updated.

Step 10 Check whether the function items supported by the new license are less those supported by the original license. If the function items supported by the new license are less those supported by the original license, the license cannot be updated.

Step 11 Check whether The number of clients supported by the new license is different from that supported by the original license. If not, the license is updated as follows:

- If the number of clients supported by the new license is less than that supported by the original license but the number of online clients is less than the number of clients supported by the new license, the license can be updated. If the number of online clients is greater that the number of clients supported in the new license, the license cannot be updated.
- If the number of clients supported by the new license is greater than that supported by the original license, the license can be updated.

----End

6.1.2 Incorrect License Usage Information

Fault Symptom

A customer provides the feedback that the license usage information displayed on the U2000 is incorrect. To view license usage information, perform the following operations:

Copyright © Huawei Technologies Co., Ltd.

1. Log in to the U2000 client.
2. Choose **Help** > **License Management** > **License Information**.
3. In the **License Information** dialog box, view the license condition.

Fault Analysis

The confirmation with the customer shows that a device has been deleted from the U2000, but not in a proper way. As a result, configurations of the device still remain in the database.

Procedure

Step 1 Navigate to the **%IMAP_ROOT%\server\cbb\ip\dmf\bin** path.

NOTE

%IMAP_ROOT% specifies the installation directory of the U2000.

Step 2 Execute the **runConvertLicense.bat** file to update the calculation for U2000 license usage.

----End

6.1.3 How to Resolve the Problem that the License Does Not Take Effect

Question

A message is displayed indicating that the license of the U2000 is invalid. As a result, the U2000 cannot be started or certain functions cannot be used.

How do I resolve this problem?

Answer

The possible causes are as follows:

- The license item is incorrect.
- The time setting of the OS is incorrect.
- Check and rectify the fault on Solaris or SUSE Linux based on the following items:
  1. The date of the OS is the current date.
  2. Check whether the ESN is correct.

     You can obtain the ESN tool according to the *U2000 License Usage Guide* to check the ESN.
  3. A unique license file exists in the **/opt/oss/server/etc/conf/license** path.

     If more than one license files exist in the path, you must delete redundant license files manually.
  4. The NIC used during license application must be the NIC actually used on the server.

     If the NICs are different, you must apply for a new license.
  5. The license file must be transferred in the ASCII format.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can check the license file by running the **vi** command. If each line of the license file ends with the **^M** symbol, the license file is uploaded in binary mode. You must re-upload the license file.

6. The license file must comply with the U2000 version.
7. Check whether an error has occurred during the license file transfer.

   If an error has occurred, transfer the license file again or download the license file to the **/opt/oss/server/etc/conf/license** directory. Restart the U2000 and check whether the license takes effect.

- Check for and rectify the fault on Windows according to the following precautions:

  NOTE

  Suppose that the U2000 is installed in the **D:\oss** directory.

  1. Ensure that the date of the OS is the current date.
  2. Check whether the ESN is correct.

     You can obtain the ESN tool according to the *U2000 License Instructions* to check the ESN.
  3. A unique license file exists in the **D:\oss\server\etc\conf\license** path.

     If more than one license files exist in the path, you must delete redundant license files manually.
  4. The NIC used during license application must be the NIC actually used on the server.

     If the NICs are different, you must apply for a new license.
  5. The license file must comply with the U2000 version.
  6. Check whether an error has occurred during the license file transfer.

     If an error has occurred, transfer the license file again or download the license file to the D:\oss\server\etc\conf\license directory. Restart the U2000 and check whether the license takes effect.

----End

6.2 Security Management Troubleshooting

This describes how to rectify the common faults of security management.

6.2.1 Failure to Create a U2000 User

Fault Symptom

During creation of a U2000 user, an error message is displayed, as shown in **Figure 6-1**.

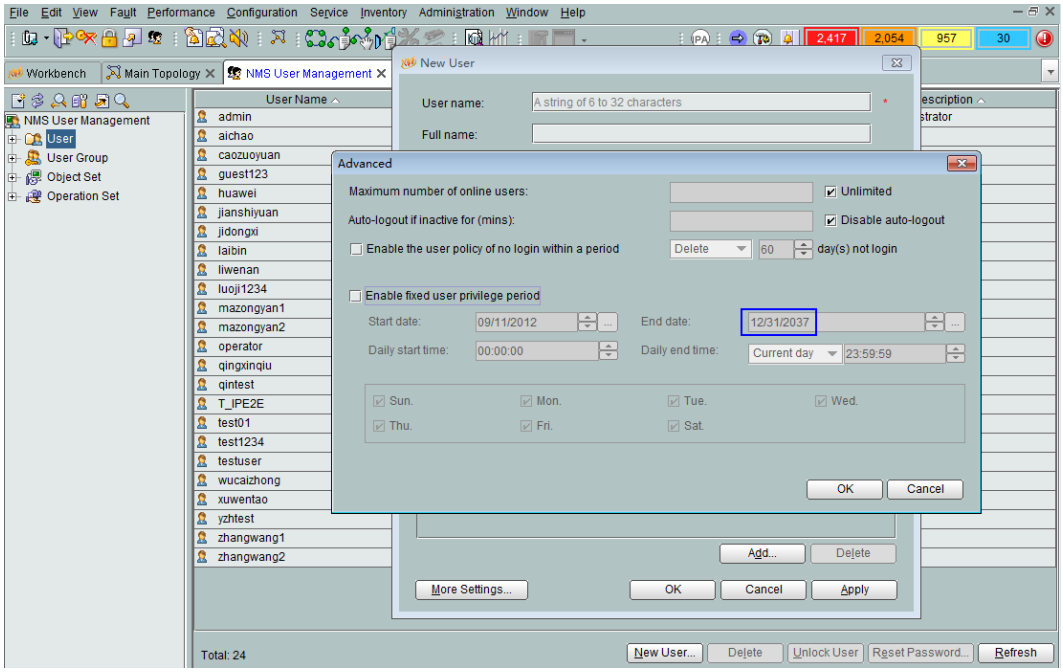
Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Error description

Fault Analysis

A user creates a U2000 user on the U2000 without customizing the validity end date. The U2000 automatically sets the end date 2037-12-31, as shown in **Figure 6-2**. The U2000 server then saves the end date as the UTC time. If the U2000 user is created on the Western Hemisphere, its validity end date will be set to 2038-1-1, rather than 2037-12-31. The date 2038-1-1, however, exceeds the default end date of a U2000 user. As a result, the U2000 user fails to be created.

Figure 6-2 Cause analysis



Copyright © Huawei Technologies Co., Ltd.

Procedure

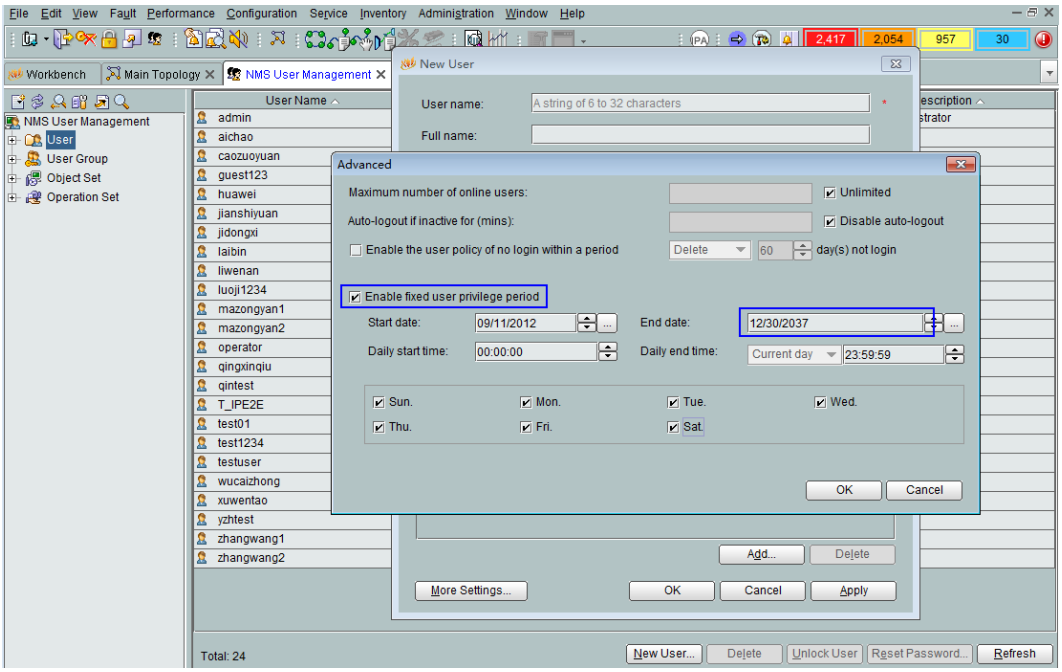
Step 1 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).

Step 2 In the **NMS User Management** navigation tree, select the **User** node and click **New User** in the main window.

The **New User** dialog box is displayed.

Step 3 Click **Advanced** and set the validity end date to a date before 2037-12-31, for example, 2037-12-30, and then create the U2000 user again, as shown in **Figure 6-3**.

Figure 6-3 Setting method



----End

6.2.2 U2000 User Is Locked

Fault Symptom

Log in to the U2000 through a client. The user gets locked after incorrect passwords are entered for three successive times.

How to solve the problem that a U2000 user is locked?

Operation Impact

If the locked user is not manually unlocked, the U2000 automatically unlocks the user within 30 minutes. The default value is 30 minutes and you can change the value.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- The locked user is not **admin**.
  1. Log in to the U2000 as a user with the rights of a **SMManagers group** or higher.
  2. Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).
  3. In the **NSM User Management** navigation tree, click **User**.
  4. In the user information list, select the record of the locked user and right-click it. Then select **Unlock User** on the shortcut menu.

     The user is then unlocked.
- The **admin** user is locked.
  1. The U2000 automatically unlocks the user within 30 minutes. The default value is 30 minutes and you can change the value.

----End

6.2.3 Failed to Start the Security Process

Fault Symptom

The security process cannot be started on the U2000 System Monitor.

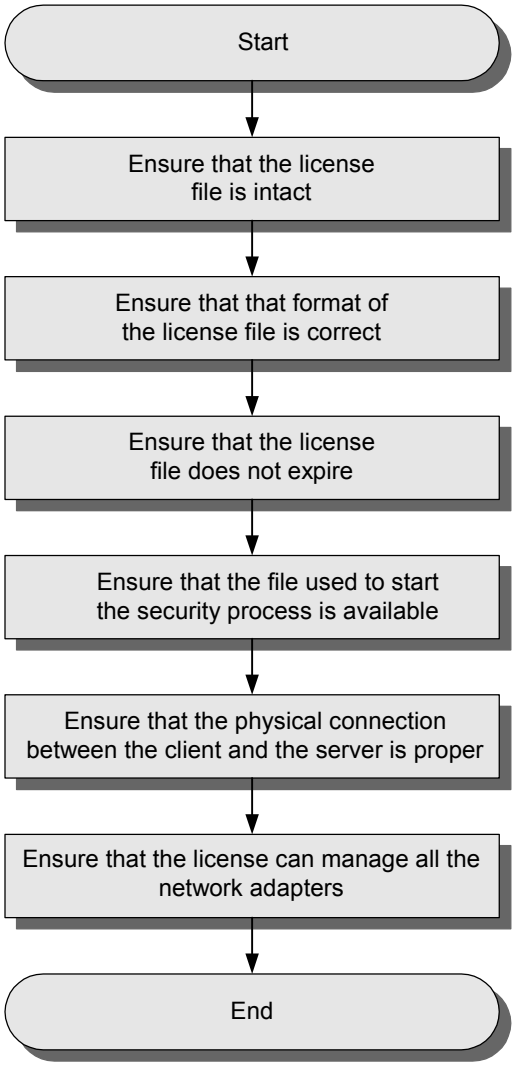
Fault Analysis

- The license file is damaged.
- The format of the license file is unidentifiable for Solaris or SUSE Linux.
- The license file is not unique or expires.
- The security process start file is unavailable.
- The network adapter is not correctly connected.
- The network adapter on the U2000 server is replaced, which invalidates the license.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 6-4 Troubleshooting flowchart of the fault that the security process cannot be started



Procedure

Step 1 Ensure that the license file is intact.

Open the license file locally to check whether it can be opened and displayed normally.

Step 2 For Solaris or SUSE Linux, check whether the license file transmitted to the server is in ASCII format.

Connect to the server that receives files through SFTP/FTP and transmit files directly.

The license generated by the tool is for Windows. Therefore, the format of the license file is different from the text file on Solaris or SUSE Linux. By transmitting the file in ASC mode to the Solaris or SUSE Linux server, the file can be converted into acceptable format.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Ensure that the license does not expire.

Ensure that only one license file exists in the license directory and the license file is an officially released one.

If the U2000 prompts that the license has expired, purchase a new license as soon as possible.

Step 4 Ensure that the security process start file **sm_agent.xml** is available.

On Windows, check whether this file exists in **%IMAP_ROOT%\etc\conf**; on Solaris or Linux, check whether this file exists in **$IMAP_ROOT/etc/conf**.

Step 5 Ensure that the client and the server are connected properly, the network adapters work normally, and the cables are correctly connected to the network adapters.

Step 6 Ensure that the license covers all the NICs of the U2000 server. Check whether the ESN corresponding to the MAC address of the network interface on the server exists in the license file. An ESN is a string consisting of 40-digit numerals or letters obtained by encrypted calculation on the MAC addresses of the U2000 server network interface.

On Windows, this license file is in **%IMAP_ROOT%\etc\conf\license**; on Solaris or Linux, it is in **$IMAP_ROOT/etc/conf/license**.

The license is bundled with the NICs. Ensure that the ESN of the NICs of the U2000 server is added when you apply for a license. Replacing a NIC invalidates the license. In this case, you need to apply for a new license.

----End

6.2.4 How to Configure the ACL for a Client with Multiple Network Adapters

Fault Symptom

If you add only the IP address of the first network adapter on a client with multiple network adapters to the ACL, sometimes you cannot access the U2000 server through this client. The U2000 prompts that the IP address is not in the ACL.

Fault Analysis

The U2000 server performs access control according to IP addresses. The U2000 server takes a random IP address of the client with multiple network adapters as the request IP address. If the request IP address is not the IP address of the first network adapter, you cannot access the U2000 server. Thus, you need to add all the IP addresses of the client with multiple network adapters to the ACL.

Procedure

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

Step 2 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).

Copyright © Huawei Technologies Co., Ltd.

Step 3 In the **NSM User Management** navigation tree, click the user corresponding to this client and then click **ACL**.

Step 4 On the **ACL** tab, click **Set System ACL**.

Step 5 On the **System ACL** window, click **Add**.

Step 6 On the **New System Access Control Item** window, enter the IP addresses or network segment of the multi-network adapter client. Then click **OK**.

NOTE

Make sure that all the IP addresses of the client with multiple adapters are added to the system ACL.

Step 7 Return to the **Set System ACL** dialog box, click **Close**.

Step 8 On the **ACL** tab, select the check boxes of **Use all the ACLs**.

Step 9 Click **Apply**.

----End

6.2.5 Failure to Log In to a U2000 After the Old Password that Expires Is Changed

Fault Symptom

During login to a U2000 client, an error message is displayed, indicating that the U2000 user uses an expired password. This problem persists after the user **admin** changes the password of the U2000 user.

Fault Analysis

- The U2000 server or client software malfunctions.
- User configurations are incorrect.

Procedure

Step 1 Check that the U2000 server software and client software function properly by logging in to the U2000 client as another user.

Step 2 View user configurations on the U2000 client and check whether **Forbid user to change password** is set to **Yes**. If yes, the user does not have the permission to change the password.

Step 3 Assign the U2000 user the permission for changing the password as the user **admin**, and then change the password as the U2000 user.

----End

6.2.6 Message indicating Invalid Login Period Displayed During U2000 User Login

Symptom

During U2000 user login, the message **Invalid login period** is displayed.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The current login time is not within the scope of the configured valid login period.

Procedure

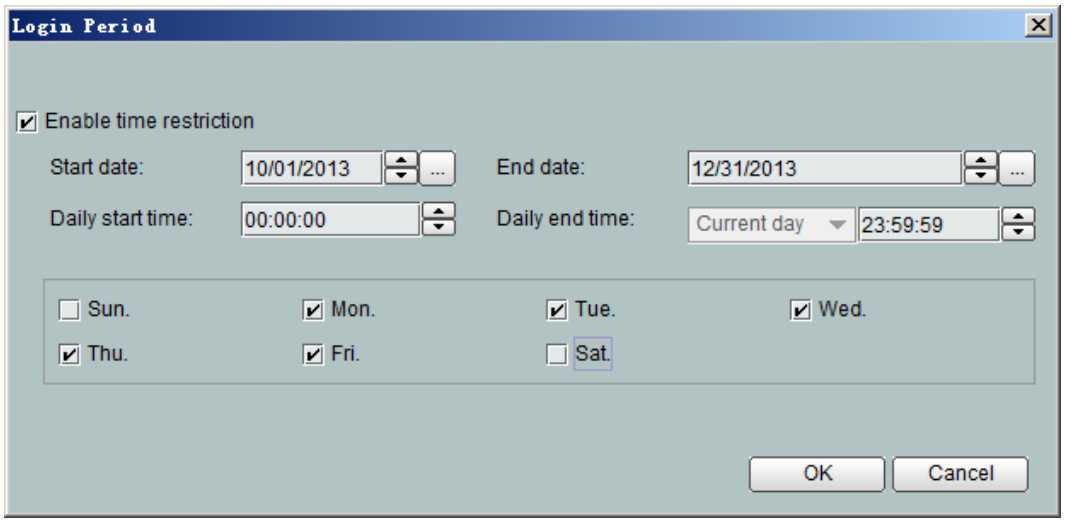
Step 1 Log in to the U2000 as the **SMManagers** user.

Step 2 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).

Step 3 In the **NMS User Management** navigation tree, choose the **User** node and then select a login user.

Step 4 View the valid login period in the **Login period** area on the **Details** tab.

Step 5 Click ... next to **Login period**. In the dialog box that is displayed, modify the user login time as required.



----End

6.2.7 Users Having the Right to View Devices Outside the Assigned Management Domain

Symptom

The management domain (excluding **All Objects**) and operation rights are assigned to the **huawei01** user group, and the **huawei** user is added to the **huawei01** user group. After the **huawei** user logs in to the U2000 client, the user can view not only the devices within the management domain but also the devices outside the management domain in the **Main Topology**.

Possible Causes

The **huawei** user belongs to not only the **huawei01** use group but also other user groups and inherits the management domains of other user groups.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

Step 2 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).

Step 3 In the **NMS User Management** navigation tree, choose the **User** node and select the **huawei** user.

Step 4 View the user group to which the **huawei** user belongs on the **User Groups** tab.

Step 5 Select all user groups except for **huawei01** and click **Delete**.

Step 6 In the **Confirm** dialog box, click **Yes**.

Step 7 Verify permissions. Log in to the U2000 client as the **huawei** user. In the **Main Topology**, you can view the devices only in the management domain.

----End

Suggestion and Summary

After a user is added to a user group, the user inherits the management domain and the operation rights of the user group. After a user is added to multiple user groups, the user inherits the combination of the management domains and operation rights of all these user groups.

6.2.8 Cannot Find New NEs in the Main Topology

Symptom

A user cannot see the new NEs in the **Main Topology**.

Possible Causes

The new NEs are not within the management domain of the user group.

Procedure

Step 1 Check the user group.

1. Log in to the U2000 as the **SMManagers** user.
2. Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **OSS User Management** from the main menu (application style).
3. In the **NMS User Management** window, expand the **User** node and select the user that needs to be checked.
4. In the right pane, click the **User Group** tab to check the user group.

   NOTE

   Plan the user group that manages the new NEs if the user belongs to several user groups.

Step 2 Add the new device to the user group's domain.

Copyright © Huawei Technologies Co., Ltd.

1. In the **NMS User Management** navigation tree, expand the **User Group** node and choose the user group that manages the new device.
2. On the **Domain** tab page in the right pane, check the management domain of the user group and add the new NEs into the management of the user group.
   - If the user group is authorized using a user-defined object set, perform the following steps:
     a. In the **NMS User Management** navigation tree, expand the **Object Set** node and select the user group's object set.
     b. On the **Members** tab page in the right pane, click **Select**.
     c. In the **Available Devices and Object Sets** area of the **Select Object Set Member** dialog box, expand all nodes and select the new device.
     d. Click to move the new device to the **Selected Devices and Object Sets** area.
     e. Click **OK**.
   - If the user group is authorized using the device mode, perform the following steps:
     a. On the **Domain** tab page in the right pane, click **Select**.
     b. In the **Select Domain** dialog box, click **More** in the **Authorization Mode** area and select **Device**.
     c. In the **Available Objects** area, select the new device.
     d. Click to move the new device to the **Selected Objects** area.
     e. Click **OK**.

Step 3 Permissions: Log in to the U2000 client. The new NEs are displayed in the **Main Topology**.

----End

Suggestion and Summary

When configuring the management domain of a user group, you can add object sets and devices. If a new NE is not displayed for a user, add the NE to the management domain of the user. Another way to configure management domains is to add subnets. After an NE is added to a subnet for which a user has rights, the NE will be automatically added to the management domain of the user. The subnet way is recommended.

6.2.9 Inconsistency Between the Client Time and Time in the U2000 Log

Symptom

The operation time stored in the operation logs, security logs, and system logs is different from that on the U2000 client.

Possible Causes

- The time on the server or client is incorrect.
- The time zone on the server or client is incorrect.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Correct the time on the server or client.

- On Windows, perform the following operations:
  1. Open the Control Panel and click **Clock, Language, and Region**.
  2. In the **Clock, Language, and Region** dialog box, click **Date and Time**.
  3. In the dialog box that is displayed, click **Change date and time** and perform configurations based on the local time.
  4. Click **OK**.
- On Solaris and SUSE Linux, perform the following operations:
  1. Log in to the MSuite client.
  2. Choose **Deploy** > **Change Time Zone** from the main menu.
  3. In the **Modify System Time Zone** dialog box, set the time according to the local time.
  4. Click **OK**.

Step 2 Correct the time zone of the server or client.

- On Windows, perform the following operations:
  1. Open the Control Panel and click **Clock, Language, and Region**.
  2. In the **Clock, Language, and Region** dialog box, click **Date and Time**.
  3. In the dialog box that is displayed, click **Change time zone** and perform configurations based on the local time.
  4. Click **OK**.
  5. Restart the OS.
- On Solaris and SUSE Linux, perform the following operations:
  1. Log in to the MSuite client.
  2. Choose **Deploy** > **Change Time Zone** from the main menu.
  3. In the **Modify System Time Zone** dialog box, set the time zone according to the local time zone.
  4. Click **OK**.
  5. Restart the OS.

----End

6.2.10 Failure to Use the Log Forwarding Server

Symptom

After the log forwarding parameters are configured on the U2000 client, forwarded logs are not displayed in the Syslog server path.

Possible Causes

The function of writing U2000 logs to the Syslog database is not enabled.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the U2000 server.

- Solaris/SUSE Linux: Log in to the server as the **ossuser** user.
- Windows: Log in to the server as the **administrator** user.

Step 2 Open the **IMAP_logsvc.xml** file, and set **syslogReportFlag** of the log to **1**. The function of writing the logs into the Syslog database is enabled.

- Solaris/SUSE Linux: **/opt/oss/server/etc/conf/IMAP_logsvc.xml**
- Windows: **D:\oss\server\etc\conf\IMAP_logsvc.xml**

The following is an example of writing the system logs, operation logs, and security logs of the U2000 into the Syslog database.

```
<syslog name="syslogReport">
<logType name="41">
<!-- Report switch: 0 - Off; 1 - On. This swtich is for system logs. The switch is
turned off by default. -->
<param name="syslogReportFlag">1</param>
<!-- Report level control: Only the logs at the same level or a higher level are
reported. The default value is 2 (Risk). -->
<!-- Log level are 0:warning, 1:minor, 2:risk -->
<param name="syslogReportLevel">2</param>
</logType>
<logType name="42">
<!-- Report switch: 0 - Off; 1 - On. This swtich is for operation logs. The switch
is turned off by default. -->
<param name="syslogReportFlag">1</param>
</logType>
<logType name="43">
<!-- Report switch: 0 - Off; 1 - On. This swtich is for security logs. The switch
is turned off by default. -->
<param name="syslogReportFlag">1</param>
<!-- Report level control: Only the logs at the same level or a higher level are
reported. The default value is 1 (Minor). -->
<!-- Log level are 0:warning, 1:minor, 2:risk -->
<param name="syslogReportLevel">1</param>
</logType>
</syslog>
```

Step 3 After the modification is complete, save the file.

Step 4 Run the following commands to import **IMAP_logsvc.xml** to the database:

- Solaris/SUSE Linux: **SettingTool -cmd import -file** */opt/oss/server/etc/conf/IMAP_logsvc.xml*
- Windows: **SettingTool -cmd import -file** *D:\oss\server\etc\conf\IMAP_logsvc.xml*

Step 5 Restart the LogService.

svc_adm -cmd restartsvc *LogService*

NOTE

When log service is restarted, all the dependent services will also be restarted.

View other services that depend on the log service. For details, see section **Monitoring the U2000 Processes** in the *Administrator Guide*.

Step 6 Log in to the U2000 client and configure the log forwarding parameters.

----End

Copyright © Huawei Technologies Co., Ltd.

Suggestion and Summary

If the log forwarding service is enabled, a U2000 performance fault may occur. Do not enable the log forwarding service when this function is not required.

6.2.11 U2000 User Password Is Forgotten

Symptom

The password for a U2000 user is forgotten.

Possible Causes

The password for a U2000 user is forgotten.

Fault Diagnosis

- If the password for the **admin** user is forgotten, reinstall the U2000 to retrieve the password. There are no other ways to retrieve the password. Therefore, keep the password secure.
- If the user is not a security administrator, reset its password as a security administrator. If the user is a security administrator (not **admin**), reset its password as another security administrator.

Procedure

Step 1 Log in to the U2000 client as a security administrator.

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

Step 3 In the **NMS User Management** navigation tree, expand the **User** node. Right-click the user whose password is to be reset and choose **Reset Password**.

Step 4 In the **Reset Password** dialog box, set **New password** and **Confirm password** and click **OK**.

NOTE

If the **Require user to change password on next login** check box is selected, users need to change the passwords next time they log in to the U2000 client. You are advised to select the **Require user to change password on next login** check box to improve the security of the U2000 system.

Step 5 In the **Information** dialog box, click **OK**.

----End

Related Information

None

6.3 Topology Management Troubleshooting

This describes how to rectify the common faults of topology management.

Copyright © Huawei Technologies Co., Ltd.

6.3.1 Failure to Find a Matched NE Explorer

Symptom

An error (error code: 1090724220) is displayed indicating that no matched NE Explorer is found when an NE is being created on the U2000.

Possible Causes

Some domains fail to be deployed during U2000 installation.

Procedure

Step 1 Log in an MSuite client and deploy domains. For details, see Chapter "U2000 Deployment" in the *U2000 Administrator Guide*.

Step 2 Deploy domains for new components. For details, see Chapter "U2000 Deployment" in the *U2000 Administrator Guide*.

----End

6.3.2 When You Add a NE, the U2000 Prompts That the NE Already Exists

Fault Symptom

When you attempts to add a NE, the U2000 prompts that the NE already exists.

Fault Analysis

The NE is already added to the U2000.

Procedure

- Method 1:
  1. In the topology view, check whether the NE icon exists. If so, the NE is already added to the U2000.
- Method 2:
  1. Choose **File** > **Find** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **Topology** > **Search** from the main menu (application style).
  2. Set the conditions in the **Search** dialog box.

     NOTE

     The **Auto search with specified keyword** check box is selected by default. After a user specify the filter criteria, the **Search** dialog box automatically displays the search result.

     If the **Auto search with specified keyword** check box is cleared, you need to click **Search** to display the search result after you specify the filter criteria.

Copyright © Huawei Technologies Co., Ltd.

3. If the search result is available in the **Search** dialog box, the NE is already added to the U2000.

----End

6.3.3 Failed to Add a Certain Type of NEs Correctly

Fault Symptom

Failed to add a certain type of NEs such as the NE40s on the U2000. When the auto-discovery function is used, the U2000 identifies a device of this type as a third-party NE. When the manual adding function is used, the system prompts that the NE type is incorrect.

Fault Analysis

- The U2000 does not have enough licenses of this type of NEs.
- This type of NEs is not registered with the U2000 of the current version.
- A required NE management component is not installed.

Procedure

Step 1 Ensure that the U2000 has enough licenses of this type of NEs.

1. Log in to the U2000 client.
2. Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).
3. In the **License Information** dialog box, select **Resource Control Item**.
4. Check the number of licenses consumed by this type of NEs.

   Check the information entries of this type of NEs. Check the corresponding **License Capacity** and **License Consumprion** to ensure that there are enough licenses.

Step 2 Ensure that this type of NEs has been registered with the U2000 of the current version.

1. Right-click in the topology view and choose **New** > **NE** on the shortcut menu.
2. On the Object Type tree of the **Create NE** dialog box, check the NE types registered with the U2000.

NOTE

If this type of NEs is not registered with the U2000, upgrade the U2000 to enable the U2000 to manage this type of NEs.

Step 3 Download software packages from the Huawei Support website, replace the existing installation files, and install the required component.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3.4 Cannot Delete a Certain Type of NEs

Fault Symptom

On the U2000, a user cannot delete a certain type of NEs such as MA5600 or S6500 series NEs. A message is displayed indicating that the server is functioning improperly.

Fault Analysis

- The memory usage of NE management processes is abnormal.
- The log database runs out of space.

Procedure

Step 1 Restarts NE management processes.

1. Log in to the System Monitor client.
2. In the main window, click the **Service Monitor** tab.
3. On the **Service Monitor** tab, select a desired NE process, click **Service Management**, and choose **Stop the Service** from the drop-down list. Alternatively, right-click the desired NE process and choose **Stop the Service** from the shortcut menu.
4. In the **Confirm** dialog box, click **Yes**.
5. Wait until the process is stopped by the U2000.
6. After the process is stopped, select the process, click **Service Management**, and choose **Start the Service** from the drop-down list. Alternatively, right-click the process and choose **Start the Service** from the shortcut menu.
7. After the NE process is started, you can delete the NE on the U2000 client again.

Step 2 Expand the RouterMgrDB database.

----End

6.3.5 Failed to Add an NE Manually

Fault Symptom

Failed to add an NE manually.

Fault Analysis

- The U2000 server is infected with viruses.
- A required component is not installed. For example, RTN NEs cannot be added if RTN NE management components are not installed.
- A required module of the NE is not installed. For example, when a user attempts to add an OptiX OSN 8800, the U2000 informs the user that related modules are missing.
- The basic configured route is unreachable.
- The configured ACL filters out IP addresses.
- There is no available disk space on the U2000 server.

Copyright © Huawei Technologies Co., Ltd.

- The U2000 does not have enough licenses of this type of NEs.
- SNMP parameters are set incorrectly.
- The firewall on the NE is not configured correctly.
- The NE exists on the U2000.
- The **System Log Collector** is abnormal.
- The selected NE type is incorrect.
- The database space is insufficient.
- The ECC channel over which MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs are transmitted does not function properly.
- No communication port is found.
- An interface IP address conflict occurs.
- The management IP address of the NE already exists on the U2000.

Procedure

Step 1 Run antivirus software to identify and remove viruses. To protect the server from network viruses and ensure that the U2000 runs securely, install patches on the operating system (OS), upgrade the antivirus software in time, and scan and remove viruses periodically.

Step 2 Use the MSuite to check whether required components are installed. If not, install them and deploy domains for them. For details about how to deploy domains, see "U2000 Deployment" of "MSuite" in *U2000 Administrator Guide*.

Step 3 Use the MSuite to check whether NE instances are missing. If any are missing, add them. After that, deploy domains for the deployment package of the NE. For details about how to deploy domains, see "U2000 Deployment" of "MSuite" in *U2000 Administrator Guide*.

Step 4 Ensure that the NE is connected normally.

Check whether the NE can be pinged.

Step 5 If the NE is connected normally, make sure that the ACL is correct.

Check whether the configured ACL filters out IP addresses.

Step 6 Check whether the disk space usage is 100% on the U2000 server.

If there is no available disk space, clean up the disk on the U2000 server.

Step 7 Check whether the licenses are sufficient.

1. Log in to the U2000 client.
2. Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).
3. In the **License Information** dialog box, select **Resource Control Item**.
4. Check the number of licenses consumed by this type of NEs.

Copyright © Huawei Technologies Co., Ltd.

Check the information entries of this type of NEs. Check the corresponding **License Capacity** and **License Consumption** to ensure that there are enough licenses.

When you create an NE manually, if the U2000 prompts that the licenses are insufficient and asks you to contact Huawei Technologies Co., Ltd. to obtain more licenses, do as prompted and update the licenses.

Step 8 If the NE is connected normally but the U2000 prompts that the NE does not respond, make sure that the SNMP parameters are set correctly.

Check whether the SNMP parameters configured on the NE are consistent with those configured during the creation of the NE on the U2000. If not, modify the SNMP parameters configured on the U2000.

Step 9 If the NE is connected correctly and SNMP parameters are set correctly, ensure that the configuration of the firewall on the NE is correct.

If the configuration of the firewall on the NE is not correct, modify the configuration by referring to the **configuration guide** for this NE.

Step 10 Check whether this NE exists on the U2000. If it has been added to the U2000, you do not need to add it.

Ensure that the MAC address of the NE is unique. To check whether the NE has been added to the U2000, perform the following steps:

Press **Ctrl**+**F**. In the **Search** dialog box that is displayed, enter the keyword and click **Locate** > **Locate to Topo**. Then, you can locate this NE.

Step 11 Check whether the **System Log Collector** runs normally.

1. Log in to the U2000 System Monitor.
2. In the main window of the U2000 System Monitor, click the **Service Monitor** tab and check whether the status of the **System Log Collector** is **Running**.

   If this process is not started, start this process and set **Startup Mode** to **Automatic**.

Step 12 Check whether the selected NE type is correct.

Step 13 Check whether the alarm indicating database needs to be maintenanced. For details, see **A.88 Database needs to be maintenanced**.

Step 14 Ensure that the ECC channels between gateway NEs and non-gateway NEs are working properly.

Step 15 If no communication port is found, check DCN links and ensure that the route configurations of the NBI do not conflict with those of NEs.

If the route configurations of the NBI conflict with those of NEs, modify route configurations to eliminate conflicts.

Step 16 Delete the conflicting IP address.

Step 17 Delete the NE with the conflicted management IP address from the U2000 and re-add the new NE.

----End

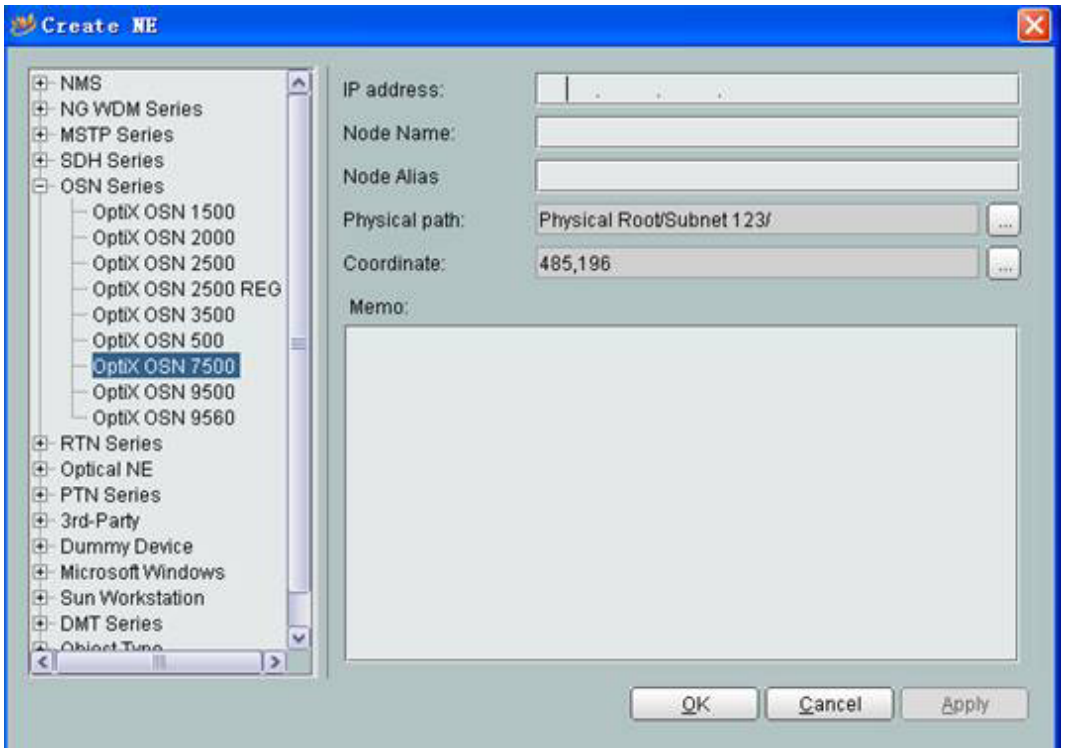
Copyright © Huawei Technologies Co., Ltd.

6.3.6 Incorrect Dialog Box Displayed During OSN NE Creation

Fault Symptom

When a user creates an optical switch node (OSN) NE, the **Create NE** dialog box for creating a router domain NE is displayed, as shown in **Figure 6-5**.

Figure 6-5 Error description



Fault Analysis

The OSN NE management process nemgr_sdh starts properly. Maybe not all processes on the U2000 are stopped when OSN NMS management components are added in the MSuite. As a result, loaded components on the client and components on the server are inconsistent.

Procedure

Step 1 Perform the following steps to restart all processes on the U2000:

1. Double-click the shortcut icon on the desktop to start the MSuite.
2. In the **Login** dialog box, select a server from the **Server** drop-down list.
3. In the **Login** dialog box, enter a user name and password.
4. Click **Login**. You can login to the System Monitor client.
5. In the main window, click the **Service Monitor** tab.

Copyright © Huawei Technologies Co., Ltd.

6. On the **Service Monitor** tab page, click **Service Management** and select **Stop All Services**; or from the main menu select **Administration** > **Stop All Services**.
7. In the dialog box that is displayed, click **Yes**.
8. Wait patiently until all processes are stopped.
9. After all processes are stopped, on the **Service Monitor** tab page, click **Service Management** and select **Start All Services**; or from the main menu select **Administration** > **Start All Services**.

Step 2 After all processes on the U2000 are started, create NEs again on the client.

----End

6.3.7 SNMP NE Is Created as a Third-Party NE During Automatic Discovery

Fault Symptom

An SNMP NE is created as a third-party NE during automatic discovery.

NOTE

This case is applicable to routers and switches.

Fault Analysis

- The associated process is not started; therefore, the SNMP NE is created as a third-party ICMP NE.
- The read community in SNMP parameters for automatic NE discovery is inconsistent with that of the agent; therefore, the SNMP NE is created as a third-party ICMP NE.
- The started agent is an unknown agent; therefore, the SNMP NE is created as a third-party SNMP NE.

Procedure

1. Check whether the agent is started.
   a. Log in to the System Monitor.
   b. Click the **Service Monitor** tab, and select the associated process in the **Process Name** column.
   c. If **Status** of the process is not **Running**, right-click the process and choose **Start the Service** from the shortcut menu.
2. On the U2000, reset SNMP parameters for automatic NE discovery.
3. Check whether the agent is a known agent.

6.3.8 Frequent Change of Online Status and Offline Status for Some NEs on the U2000

Fault Symptom

The online status and offline status of certain NEs frequently change on the U2000.

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

- The same user name is used to login to the NE on another U2000 client.
- The number of NEs exceeds the threshold set on the U2000.
- The disk space of the U2000 server is insufficient.
- If the high availability system is in the primary-primary state, the transport NEs may preempt the resource of each others.

Procedure

Step 1 Check whether the same NE user is used to access the NE on another client.

Step 2 Check whether the number of NEs exceeds the threshold set on the U2000. For details, see chapters "Performance Indicators" and "Management Capability" in the *U2000 Product Description*.

Step 3 Check the disk space of the server. Normally, the disk usage cannot exceed 80%. If the disk usage exceeds 80%, clean up the disk. You can delete and back up the associated files to free the disk space.

Step 4 If the high availability system is in the primary-primary state, take measures according to **A.104 Manual Restoration Is Required After Primary-Primary Veritas Status**.

----End

6.3.9 Failure to Connect to a Large Number of GNEs on the U2000

Fault Symptom

The U2000 server is running properly, but a large number of gateway network elements (GNEs) fail to connect to the U2000.

Fault Analysis

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

Procedure

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

NOTE

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

Step 2 If GNEs can be connected, check the ECC link of the GNEs. Choose **Communication** > **NE ECC Link Management** in the NE Explorer to view ECC links.

Step 3 If hundreds of ECC links exist and change frequently, the number of non-GEs connected to the GNEs exceeds the threshold. As a result, ECC storm occurs.

Copyright © Huawei Technologies Co., Ltd.

Step 4 It is recommended that you disable the ECC ports on certain optical cards, and divide and plan ECC subnets after locate the fault that causes the ECC storm. This helps to reduce potential risks.

NOTE

For the specific maximum number of non-GNEs connected to a GNE, see the product description of the related version. If the actual number exceeds the threshold, change the number based on the planning information.

----End

6.3.10 Objects in the Topology View Are Overlapped

Symptom

When there are multiple objects in the topology view, the names of objects are overlapped and cannot be seen clearly.

Procedure

You can solve the problem by using one of the following methods as required:

- On the main menu bar, choose **View** > **Create** > **Subnet** to create a subnet. Then classify objects in different subnets.
- On the main menu bar, choose **View** > **Layout** .
- On the main menu bar, choose **View** > **Display Setting** > **Filter** to select the filter tree template. Only specified types of objects are displayed in the view.
- On the main menu bar, choose **View** > **Zoom** to set the label display mode, label font, or viewing type.

6.3.11 Added Topology Objects Are Not Displayed in the Topology View

Symptom

The added topology objects, such as the NEs and subnets, are not displayed in the topology view.

Possible Causes

The following are the possible reasons:

- NEs are added to the server, but there is a delay before the data is synchronized to the client.
- The corresponding NEs and subnets are not displayed in the topology view if they are filtered in **Filter**. You can disable the filtering option to display the corresponding devices and subnets.

Procedure

1. The view is automatically refreshed after the NE is added for a certain time. The period depends on the network communication. If the view is not automatically refreshed for a

Copyright © Huawei Technologies Co., Ltd.

long time, the data packet may be lost because of the unstable network. You can choose **View** > **Refresh** form the main menu or click on the toolbar to refresh the view.

2. If the filter tree is configured not to display this type of NEs or subnets, do as follows:
   a. Choose **View** > **Display Setting** > **Filter** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **View** > **Show** > **Filter** from the main menu (application style).
   b. In the **Filter Tree** group box, click the **Filter tree**, select the related filter tree template.
   c. In the **Filter** area, select the **Object Name**, **NE** and **Subnet**.

6.3.12 Failed to Ping an NE Using the Ping Tool Provided by the U2000

Fault Symptom

On the U2000, select an NE, right-click, and then choose **Tool** > **Ping** from the shortcut menu. The NE cannot be pinged and a message indicating operation timeout is displayed. If you use command lines to ping the NE, the NE can be pinged.

NOTE

This case is applicable to routers and switches.

Fault Analysis

The Ping tool provided by the U2000 relies on the build-in ICMP tool to implement its function. That is, the operation of the Ping tool depends on the running status of the topology process. In this case, the NE cannot be pinged because the **eam_agent** process is not started. To ping the NE, you must manually start this process.

Procedure

Step 1 Log in to the U2000 System Monitor.

Step 2 Click the **Service Monitor** tab and select **eam_agent**.

Step 3 Select **Process Name**, right-click, and then choose **Start the Service** from the shortcut menu.

----End

6.3.13 Failed to Log In to a Managed NE Using the Telnet Tool Provided by the U2000 Client

Fault Symptom

Failed to log in to an NE by selecting the NE, right-clicking, and choosing **Tool** > **Telnet** from the U2000 client.

NOTE

Using STelnet is recommended because of its higher security than Telnet.

Copyright © Huawei Technologies Co., Ltd.

NOTE

This case is applicable to routers and switches.

Fault Analysis

- The firewall configuration of the U2000 is incorrect.
- If the Telnet tool provided by the U2000 is used to log in to an NE, the U2000 client communicates with the U2000 server and informs the U2000 server of Telnet operations. Then, the U2000 server serves as an agent to return operation results to the U2000 client. Therefore, login to the NE can succeed only if the Telnet tool provided by the U2000 is used.

Procedure

Step 1 Log in to the U2000 System Monitor.

Step 2 Click the **Service Monitor** tab and Set **Process Name** to **necomm_agent**.

Step 3 Right-click and choose **Start the Service** from the shortcut menu.

----End

6.3.14 Gateway NEs Are Unreachable

Fault Symptom

The U2000 server is running properly, but a large number of gateway NEs are unreachable.

Fault Analysis

The fibers/cables connecting Ethernet ports are faulty.

Procedure

Step 1 Verify that Ethernet ports are connected by properly functioning fibers/cables.

----End

6.3.15 NE Does Not Exist or Has Been Deleted

Fault Symptom

When a user deletes a newly added NE (such as OSN 6800), the U2000 displays an error message indicating that the NE does not exist or has been deleted.

Fault Analysis

The data displayed on the client is consistent with the data in the U2000 database.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the System Monitor and check the status of the topu and WDM NE management processes.

Step 2 If the processes are normal, restart the U2000 server.

----End

6.3.16 No WDM NE Is Available for Creation After the U2000 Is Installed

Fault Symptom

No WDM NE is available for creation after the U2000 is installed.

Fault Analysis

The transport component package was not decompressed to the expected directory.

Procedure

Step 1 Decompress the transport component package and reinstall the U2000.

----End

6.3.17 A Database Operation Failure Is Reported During an NE Data Upload

Fault Symptom

A database operation failure is reported during an NE data upload.

Fault Analysis

The NE name contains illegal characters.

Procedure

Step 1 Correct the NE name.

Step 2 Use Navigator to log in to the NE and run the following command:

```
cfg-verify
```

Step 3 Delete the NE on the U2000.

Step 4 Restart the nemgr_trans process.

Step 5 Add the NE on the U2000 and upload its data.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3.18 Status Displayed in the NE Topology View Is Incorrect

Fault Symptom

A type of NEs can be pinged, but the topology view shows that the NEs are offline and cannot be upgraded or deleted.

NOTE

This case is applicable to routers and switches.

Fault Analysis

- The fireware is configured to be unable to access this type of NEs.
- A temporary license is used to add this type of NEs to the U2000 and then replaced by a formal license. The formal license, however, does not include the management license for this type of NEs.

Operation Procedure

Procedure

Step 1 Change configurations of the firewall to cancel the access restriction on this type of NEs.

Step 2 Apply for and load a correct formal license.

NOTICE

Control mechanisms for temporary licenses and formal licenses are different. You can add NEs only to the U2000 that is loaded with formal licenses.

----End

6.3.19 Message Indicating an MDP Distribution Failure or a Server Response Failure Is Displayed During U2000 Operation

Symptom

- When a device is being added to the U2000, a message indicating an MDP distribution failure or a server response failure is displayed.
- When some query commands (such as board query commands) or path search commands (such as WDM path search commands) are executed on the U2000, "error code : 1090611456" is displayed.

Possible Causes

- Components to be involved functions are not installed, or the components are installed but instances are not installed for the involved functions.

Copyright © Huawei Technologies Co., Ltd.

- The U2000 license does not contain the associated function control items.
- The processes associated with the involved functions are not started or work incorrectly.

Procedure

Step 1 Log in to a U2000 client and check whether the processes associated with the involved functions are stopped. If the processes are stopped, start them.

NOTE

- If a message indicating a lack of the associated function control item in the license is displayed during startup of a process, the obtained license is incorrect. Apply for a new license.
- If a process fails to be started, refer to **5.5.4 Failure to Start Certain Processes of the U2000 Server** to address the issue.

Step 2 If the associated function processes are not found on the U2000 client, no instance is deployed. Log in to the MSuite client. On the **Deployment Package** page, check whether an instance is deployed in the deployment package of the associated function. If the associated deployment package is available but no instance is found, add an instnace to the deployment package.

NOTE

For details about how to add instances, see the MSuite Help. On an MSuite client, press **F1** to navigate to the MSuite Help.

Step 3 If the component required for the function has been installed, an instance has been deployed, and the process corresponding to the function is running properly, restart the U2000 server to resolve the MDP distribution failure or server response failure.

----End

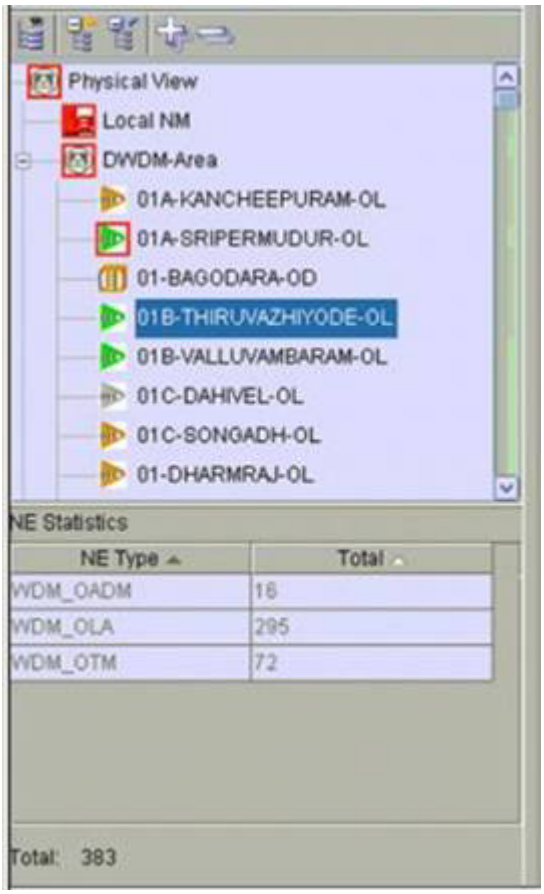
6.3.20 Inconsistency Between the WDM NE Quantity in the Topology View with the Actual Quantity

Fault Symptom

The WDM NE quantity displayed in the lower-left corner of the window is inconsistent with the actual quantity as in **Figure 6-6**.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-6 Error description



Fault Analysis

The U2000 provides the function of collecting statistics about wavelength WDM NEs but the collected statistics are about optical NEs only. In general, an optical NE consists of several types of NEs. Thus, the number of wavelength NEs displayed in the topology view is inconsistent with the actual number. Generally, the number of NEs displayed in the topology view is smaller than the actual number. Enable the NE report function to collect the number of all NEs. Perform the following steps.

Procedure

Step 1 Choose **Inventory** > **Physical Inventory** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **Physical Inventory** from the main menu (application style). Choose **NE** from the **Physical Inventory Type** navigation tree.

Step 2 Click the **By NE Statistics** or **By Subnet Statistics** tab. Select the NE type from the **Statistics Type** drop-down list and set **Statistics Scope**.

The NE records in accordance with the statistics type are displayed in the query result area.

Step 3 **Optional:** If no statistics type in the drop-down list meets the requirement, you can customize a statistics type. Perform the following steps:

Copyright © Huawei Technologies Co., Ltd.

1. Select **Customize** from the **Statistics Type** drop-down list.
2. In the **Customize NE Statistics Type** dialog box, click **New**.
3. In the **New Customize NE Statistics Type** dialog box, set related parameters, and then click **OK**.
4. In the **Customize NE Statistics Type** dialog box, click **OK**.

In the query result area, information about the NE statistics types that meet the set conditions is displayed.

----End

6.3.21 How to Process the NE License Alarm of the U2000 Server

Fault Symptom

The number of used licenses exceeds the preset threshold. In the fault alarms, the license alarm is generated.

If the number of NEs managed by the U2000 reaches the upper threshold, you cannot add a new NE.

Fault Analysis

When the number of NE managed by the U2000 exceeds the preset threshold, an NE license alarm of the U2000 server is generated.

Procedure

The NE license alarm of the U2000 server is generated.

1. Log in to the U2000 client.
2. Choose **Help** > **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (application style).
3. In the **Alarm Configuration for License Resource Item Capacity** dialog box, view NE License Alarm Setting.

   NOTE

   If the license threshold is too low, set the license threshold to a proper value.
4. If the license threshold is reasonable, Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).
5. In the **License Information** dialog box, select the **Resource Control Item** tab to view the NE license consumption.

   NOTE

   Apply for new licenses if the licenses are used up.

Copyright © Huawei Technologies Co., Ltd.

6.3.22 NE Icon in the Topology Becomes Grey

Symptom

An NE icon in the topology changes from green to grey.

Possible Cause

1. Firewall configurations on the NE are incorrect.
2. The NE connection is abnormal.
3. The management IP address of the NE is changed.
4. The gateway or mask of the NMS server is changed and the NMS server fails to connect to the NE.

Procedure

Step 1 Ensure that the firewall configurations on the NE are correct.

Check whether the firewall configurations on the NE are correct and ensure that UDP port 161 is used to send and receive packets. If the firewall configurations are incorrect, correct the configurations according to the configuration guide for the NE.

Step 2 If the firewall configurations are correct, ensure that the NE connection is normal.

Run the **Ping** command to check whether the NE is connected.

Step 3 If the NE connection is normal, ensure that the management IP address of the NE is correct.

If the management IP address of the NE is changed, the NE icon will change from green to grey. Delete the NE from the NMS and use the new management IP address to add the NE.

Step 4 If the management IP address of the NE is correct, check the NMS server.

Check whether the gateway or mask of the NMS server is correct.

----End

6.3.23 NE Icons in the U2000 Topology View Changed to Blue

Symptom

The NE icons in the U2000 topology view change to blue.

Possible Causes

The ICMP communication between the U2000 server and NEs is normal, but the SNMP communication is abnormal.

Fault Diagnosis

The colors of NE icons in the topology view identify different NE status. A blue NE icon specifies that the NE is in the unknown state. Generally, an NE icon turns blue when the ICMP communication is normal but the SNMP communication is abnormal.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the SNMP parameters configured on the U2000 and NE are consistent.

1. Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).
2. Select an NE and click **Test**.
   - If the communication fails, check whether the SNMP parameters configured on the U2000 and NE are consistent.
   - If the communication succeeds, go to **Step 2**.

Step 2 Check the ACL control on the SNMP read and write community names on the NE.

Change the ACL control and allow the IP address of the U2000 server to access NEs using SNMP.

----End

6.3.24 Time Inconsistency Between the U2000 and NEs

Symptom

On the local network, the time on NEs is inconsistent with that on the U2000.

Possible Causes

- The NE synchronization mode is not set on the U2000.
- Two U2000s monitor the same NE. As a result, the NE time is inconsistent with the U2000 time.

Procedure

Step 1 Configure time consistency on the U2000.

1. Choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (application style).
2. Choose an NE whose time is inconsistent with the U2000 time from the object tree and click
3. Click **Close** in the **Operation Result** dialog box that is displayed.
4. Select one or more NEs in the list, right-click and choose **Synchronize with NM Time** from the shortcut menu.
5. In the **Time Synchronization Operation** dialog box, click **Yes**. In the **Operation Result** dialog box, click **Close**.
6. Click **Apply**. In the **Operation Result** dialog box, click **Close**.

Step 2 Exist one U2000 and implement **Synchronize with NM Time**. For details, see **Step 1**.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Log in to the System Monitor Client, modify the time zone or time, and restart the OS.

----End

Suggestion and Summary

Determine the synchronization mode for time on the U2000 and NEs. The U2000 provides the following synchronization modes:

1. Synchronizes NE time to the U2000 time.
2. Synchronizes NE time to the NTP server time.
3. Synchronizes NE time to the standard NTP time.

6.3.25 Link Display Exception

Symptom

Links between NEs are not displayed or marked in red or yellow in the Main Topology after a user logs in to the U2000 client.

Possible Causes

- Filter criteria are set in the Main Topology, which causes that links between NEs are not displayed.
- Data is inconsistent between the U2000 and NEs.
- The protocol status of the link source interface is Down, and the link is displayed in red on the U2000.

Procedure

Step 1 Choose **View** > **Display Setting** > **Filter** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **View** > **Show** > **Filter** from the main menu (application style). Or in the Main Topology of the U2000 client, click on the toolbar. On the **Filter** tab, select the desired link information from the **Topology Filter** navigation tree.

NOTE

The Main Topology displays information about subnets, NEs, and links that are selected from the **Topology Filter** navigation tree. For those unselected objects, the related information will not be displayed.

Step 2 Synchronize NE data. For details, see "Synchronizing NE Data" in section "Keeping Data Consistency Between the U2000 and NEs" of the *U2000 Operation Guide for Common Features*.

NOTE

For routers, switches, access, and security NEs, ensure that the SNMP and Telnet (or STelnet) parameters and the xFTP service are configured correctly before synchronizing NE data.

Step 3 Rectify the fault of the source interface.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3.26 Failure to Display Tracing Status in the Clock View

Symptom

An NE has been configured with a clock link on a U2000 client. The clock link, however, is not displayed in the clock view. As a result, the tracing relationship between NEs and the clock synchronization status cannot be obtained.

Possible Causes

The filter criteria have been configured in the clock view; as a result, the clock link between NEs cannot be displayed.

Procedure

Step 1 Log in to a U2000 client.

Step 2 Choose **View** > **Main Topology** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** (application style).

Step 3 Choose **Clock View** from the **Current View** drop-down list to access the **Clock View** window.

Step 4 Choose **View** > **Display Setting** > **Filter** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **View** > **Show** > **Filter** from the main menu (application style). or click in the toolbar of the topology. In the right pane, click the **Filter** tab.

Step 5 Choose the link information to be displayed from the **Topology Filter** navigation tree.

NOTE

Ensure that the information associated with the clock link is selected, such as **LINK**, **Link Level**, and **Clock Link Tracing Type**.

----End

6.3.27 Abnormal Display of NE Panel

Symptom

The NE panel cannot be opened.

Possible Causes

The NE management process malfunctions.

Procedure

Step 1 Log in to the System Monitor and restart the NE management process.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3.28 High Usage of NE Management Process

Symptom

The U2000 reports high usage of the NE management process.

Possible Causes

The quantity of a series of NEs exceeds the management capability of the NE management process.

Procedure

Step 1 Deploy new domains to expand the U2000 management capability for such series of NEs. For details, see **Deploying Domains** in the *Administrator Guide*.

----End

6.3.29 High Usage of NE Management Process

Symptom

The U2000 fails to create connections.

Possible Causes

The NE is busy when data is synchronized, resulting in a failure to synchronize some data.

Procedure

Step 1 Modify the timeout period of the **SNMP** parameter to improve the success rate of SNMP operations.

1. Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).
2. Select the SNMP parameter record of the NE and click **Display**. Alternatively, double-click the record. Then modify **Timeout Interval** to a larger value.

----End

6.3.30 LLDP Link Fails to Be Discovered

Symptom

The U2000 fails to discover an LLDP link automatically.

Possible Causes

The source and sink NE of the LLDP link uses a name longer than 64 characters.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Change the NE name to be shorter than 64 characters.

----End

6.3.31 Main Topology Fails to Be Saved

Symptom

A user saves changes in the Main Topology and logs out. However, after the user logs in to the client again, the Main Topology does not reflect the changes.

Possible Causes

Multiple users perform operations simultaneously.

Procedure

Step 1 Select all NEs in the Main Topology and save changes. Then re-log in to the client.

----End

6.3.32 Port Names Fail to Be Modified in Batches

Symptom

On the U2000, port names fail to be modified in batches.

Possible Causes

The U2000 client does not provide a batch modification function. The modification must be performed by running a script.

Procedure

Step 1 Choose **Administration** > **Back Up/Restore NMS Data** > **Import/Export Script File** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **System** > **Back Up/Restore NMS Data** > **Import/Export Script File** from the main menu (application style).

Step 2 Click the **Export** option button.

Step 3 Click the **TXT** or **XML** option button.

Step 4 Set **Script File Type** to **NE Port Naming File**.

Step 5 In the **Export NE List** area, select the desired NEs.

Step 6 Click **Create File Directory** and create a directory for saving the script to be exported.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The script file is saved on the U2000 server. On Windows, the backup directory is **%IMAP_ROOT%\script**. On Solaris and SUSE Linux, the backup directory is **$IMAP_ROOT/script**. You can create another directory under it.

Step 7 Enter the directory name and click **OK**.

Step 8 Select the created directory and click **Apply**.

Step 9 In the **Confirm** dialog box, click **OK**.

A progress bar appears showing the status of the export.

Step 10 In the **Import/Export Script File** window, import the script to modify port names in batches.

----End

6.3.33 NE Discovery Is Unavailable After an Upgrade

Symptom

After the U2000 is upgraded, the NE discovery function (**File** > **Discover** > **NE**) is unavailable.

Possible Causes

The ***U2000 client installation directory*****\client\client\style\users** directory is not updated.

Procedure

Step 1 Delete or rename the directory.

----End

6.4 Performance Management Troubleshooting

This describes how to rectify the common faults in performance management.

6.4.1 PMS Cannot Monitor the ICMP Jitter Performance Data

How to resolve the problem wherein the PMS cannot monitor the ICMP jitter performance data?

Q:

How to resolve the problem wherein the PMS cannot monitor the ICMP jitter performance data?

A:

You can identify the problem as follows:

The version of the NE VRP platform must be 5.6 or later.

6.4.2 How Do I Query Board Optical Power of NG WDM NEs

Copyright © Huawei Technologies Co., Ltd.

Description

On the U2000, I cannot query the optical power of boards on NG WDM NEs.

Procedure

1. Set Internet Explorer as the default browser of the operating system (OS).
2. Set Internet Explorer as the default browser again.
3. Set the security level of the Internet Explorer to a low level.
4. Restart the tomcat and weblct processes and then restart the U2000 client.

6.4.3 Failure to Collect Performance Data Due to an Incorrect SNMP Version

Q:

Performance data collection fails because the SNMP version is incorrect.

A:

If SNMPv1 is used to communicate with the U2000, the values of some performance indicators cannot be collected. It is advisable to use SNMPv2c or SNMPv3 to add devices and then collect performance data.

6.4.4 Failure to Collect Interface Traffic on ME60s

Q:

The U2000 fails to collect interface traffic on ME60s.

A:

If the server hardware configurations exceed the lower limits, hardware resources meet bottlenecks after a lot of performance tasks are created; as a result, performance data cannot be collected. To address the problem, delete unnecessary performance instances on device subinterfaces before collecting interface traffic.

6.5 Configuration Failure Troubleshooting

This topic describes how to troubleshoot common configuration failures.

6.5.1 A Menu/View Item Is Missing

Symptom

A Menu/View Item Is Missing.

Possible Causes

Probable causes of the absence of an NE- or board-level menu/view item:

- The U2000 has not logged in to the NE.

Copyright © Huawei Technologies Co., Ltd.

- The NE or board version is old and does not support the function.
- The NE or board does not support the function.
- The required license is not loaded or has expired.
- The NE login account is invalid or has insufficient rights.

Procedure

Step 1 Check whether the U2000 has logged in to the NE. If it has not, right-click the NE and choose **Login** from the shortcut menu.

Step 2 Check the NE version. Specifically, right-click the NE and choose **Properties** from the shortcut menu. In the **Properties** dialog box, check **NE Software Version(VRC)** on the **NE Properties** tab. Then consult the product description to determine whether the NE version supports this function. If the NE version is old and does not support this function, upgrade the NE version or retry with a version that supports the function.

Step 3 If the NE version supports this function, check whether the required license has been installed.

Step 4 Verify that the NE login account is valid and has sufficient rights. If it is invalid or has insufficient rights, log it off and retry with an account with more rights, for example, the **admin** account.

----End

6.6 Alarm Troubleshooting

This describes how to rectify the common faults of alarms.

6.6.1 Alarm and Event Postprocessing Function Is Unavailable

Symptom

When setting the alarm and event postprocessing policy, if you enter special characters such as %, &, @, or ^ in the process name for **Postprocessing Action**, the alarm and event postprocessing may fail to be started.

Possible Causes

In different OSs, special characters such as %, &, @, and ^ in the file name indicate different meanings. Thus, the execution status of an executable file varies according to the specific OS.

Procedure

Do not set **Postprocessing Action** with special characters such as %, &, @, and ^ to name a file.

6.6.2 U2000 Cannot Obtain NE Alarm Information Because of IP Address Mismatch

Copyright © Huawei Technologies Co., Ltd.

Fault Symptom

SNMP parameters are set on the U2000. The U2000, however, cannot receive trap packets sent from the NE or process received trap packets. As a result, NE alarm information cannot be obtained.

Fault Analysis

- Cause 1: Trap parameters on the NE, for example, the U2000 IP address, are configured incorrectly.
- Cause 2: The source address of the trap packets sent by the NE is different from the management address of the NE configured on the U2000.

Procedure

- For cause 1: Re-set the trap parameters on the NE.

  A router NE is used as an example to describe how to set trap parameters. For details, see **6.6.4 U2000 Cannot Receive NE Alarms**.
- For cause 2: Re-add the NE.
  1. Delete this NE from the U2000.
     a. Select this NE in the Main Topology.
     b. On the main menu bar, choose **Edit** > **Delete**.
     c. In the **Confirm** dialog box, click **Yes**.
     d. In the **Deletion Result** dialog box, click **Close**.
  2. Re-add this NE and make sure the management address of this NE is the same as the source address of trap packets.
     a. Choose **File** > **New** > **NE** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **File** > **New** > **NE** from the main menu (application style).
     b. Set the NE parameters in the **Create NE** dialog box.
     c. Click **OK**. The **Information** dialog box is displayed .
     d. In the **Information** dialog box,click **OK**.

----End

6.6.3 An Alarm About Database Space Is Generated Because of Incorrect U2000 Database Settings

Fault Symptom

After the U2000 is installed in Windows OS, the U2000 receives an alarm about database space.

Fault Analysis

The space allocated to database **MCDB** is too small. As a result, an alarm is generated on the U2000. Log in to the System Monitor and click the **Database Monitor** tab. Information about database **MCDB** is displayed in red.

Copyright © Huawei Technologies Co., Ltd.

Context

The SQL 2008 is used as an example.

Procedure

Step 1 Choose **Programs** > **Microsoft SQL Server** > **Enterprises Mananger**.

Step 2 In the **Microsoft SQL Server** navigation tree, expand **SQL Server Group** > **(local)(Windows NT)**, and then click **Database**.

Step 3 Select **MCDB** .

Step 4 Right-click and choose **Properties** from the shortcut menu.

Step 5 In the **MCDB Properties** dialog box, click the **Data Files** tab.

Step 6 Select **MCDBdata** from the database file list.

Step 7 Change the value in **Space allocated**. For example, change the value from **300** to **1000**.

Step 8 Click **OK**.

Step 9 Log in to the System Monitor and click the **Database Monitor** tab.

Step 10 In the information list, select **MCDB** and right-click it. Then select **Refresh** on the shortcut menu.

If this record changes from red to black, it indicates that the U2000 does not generate the related database space alarm any more.

----End

6.6.4 U2000 Cannot Receive NE Alarms

Fault Symptom

The U2000 cannot receive NE alarms.

Alarms occur on NEs but are not reported to the U2000.

Fault Analysis

- The server disk space is full.
- The database space is insufficient.
- Alarm masking is enabled on NEs, so that alarms are discarded.
- The fault service processes is abnormal.
- The **The number of records in the database table has reached the threshold** and **The Database Usage Is Too High (Critical)** alarms are displayed on the U2000, indicating that alarms cannot be dumped in the database. Therefore, alarms cannot be reported to the database.
- The priority of board software is higher than that of NE software.

Copyright © Huawei Technologies Co., Ltd.

- The trap IP address for disk array has not bee configured. For a HA system, you need to assign two Trap IP to the disk array. Each Trap IP corresponds to the NMS application IP address configured on each server.
- Other possible causes for Router series, Switch series, PTN 6900 series, Access series and Security NEs are as follows:
  - The SNMP parameters on NEs are incorrect.
  - NEs that do not support fragmentation exist on the network, and SNMP packets that exceed the maximum packet size will be dropped.
  - The firewall on the U2000 server does not allow the UDP 162 port to receive alarms.
  - The Trap sending function is not enabled for the associated feature on NEs.
  - The network is not stable.

Procedure

- Clean up the disk space of the server.
- Manually dump alarm.
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
  2. In the navigation tree on the left of the **Task Management**, choose **Manual Dump**.
  3. In the task list of the **Task Management** window, right-click **Alarm Manual Dump** or **Event Manual Dump**, and then choose **Run**.
- Modify the rules of alarm masking.
  1. Choose **Fault** > **Settings** > **Mask Rules** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Mask Rules** from the main menu (application style).
  2. In the **Mask Rule** window, view and modify the masking rules.
- Restart the fault service process
  1. Log in to the System Monitor client.
  2. In the main window, click the **Service Monitor** tab.
  3. On the **Service Monitor** tab, select **FaultService** process, click **Service Management**, and choose **Stop the Service** from the drop-down list. Alternatively, right-click the desired NE process and choose **Stop the Service** from the shortcut menu.
  4. In the **Confirm** dialog box, click **Yes**.
  5. Wait until the process is stopped by the U2000. After the process is stopped, select the process, click **Service Management**, and choose **Start the Service** from the drop-down list. Alternatively, right-click the process and choose **Start the Service** from the shortcut menu.
  6. After the fault service process is started, U2000 can receive NE alarms.
- Board software downgrade:
  1. Refer to the related chapters of *User Guide (NE Software Management)*.
- Clear the **The number of records in the database table has reached the threshold** and **The Database Usage Is Too High (Critical)**alarms .

Copyright © Huawei Technologies Co., Ltd.

1. Clear the **The Database Usage Is Too High (Critical)** alarm. For details, see **A.44 ALM-103 The Database Usage Is Too High (Critical)**.
2. Clear the **The number of records in the database table has reached the threshold** alarm. For details, see **A.51 ALM-120 The number of records in the database table has reached the threshold**.

- Perform the following operations if the U2000 cannot receive alarms generated on Router series, Switch series, PTN 6900 series, Access series and Security NEs:
  - Configure SNMP parameters on NEs.

    NOTE

    Configuring SNMPv3 on routers is used as an example.

    1. Run the following command to log in to the NE CLI:
       - **telnet** *NE IP Address*
       - **stelnet** *NE IP Address*

       NOTE

       Using STelnet (if supported) to log in to NEs is recommended.
    2. Run the following command to access the system view:

       system-view
    3. Run the following command to enable SNMP:

       snmp-agent sys-info version *v3*
    4. Run the following command to configure the SNMP user group:

       snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]
    5. Run the following command to configure SNMP user information:

       snmp-agent usm-user v3 *user-name group-name* [[**authentication-mode** { **md5** | **sha** } *password*] [**privacy-mode des56** *password*]] [**acl** *acl-number*]
    6. Run the following command to enable the function of sending traps on NEs:

       snmp-agent trap enable
    7. Run the following command to configure the U2000 server, the trap target host:

       snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | { **public-net** | **vpn-instance** *vpn-intance-name* }] **params securityname** *security-string* [**v3 authentication** | **privacy**] [**private-netmanager**] [**notify-filter-profile** *profile-name* | **ext-vb**]

       NOTE

       The **v3** version in the command must be consistent with the in-use SNMP version. Otherwise, the U2000 fails to receive the traps sent by NEs.
    8. Run the following command to specify the source interface that sends traps:

       snmp-agent trap source *interface-type interface-number*

       NOTE

       Ensure that an IP address is assigned to the source interface for sending trap packets and the IP address is reachable for the U2000.
  - Run the **snmp-agent packet max-size** *byte-count* command to set the SNMP packet size to prevent NEs that do not support fragmentation from discarding packets.

Copyright © Huawei Technologies Co., Ltd.

- Configure that the firewall on the U2000 server allows UDP port 162 to receive alarms.
- Perform the following operations to restart the TrapReceiver0101 process of the U2000:
  1. Choose **Start** > **Run**. In the **Run** dialog box, enter **services.msc** and press **Enter**.
  2. In the **Services** window, right click **Internet Connection Sharing (ICS)** and choose **Stop** from the shortcut menu.
  3. Right click **Internet Connection Sharing (ICS)** and choose **Properties** from the shortcut menu. In the dialog box that is displayed, set **Startup type** to **Manual** and click **OK**.
  4. Open the **Windows Task Manager** and click the **Processes** tab.
  5. Right click **EmfTrapReceiver.exe** and choose **End Process** from the shortcut menu.
  6. In the dialog box that is displayed, click **End Process**.
  7. Log in to the System Monitor client.
  8. Right click **TrapReceiver0101** on the **Service Monitor** tab and choose **Start the Service** from the shortcut menu.
- Run the following command to enable the Trap sending function for the associated feature on the NE:

  snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

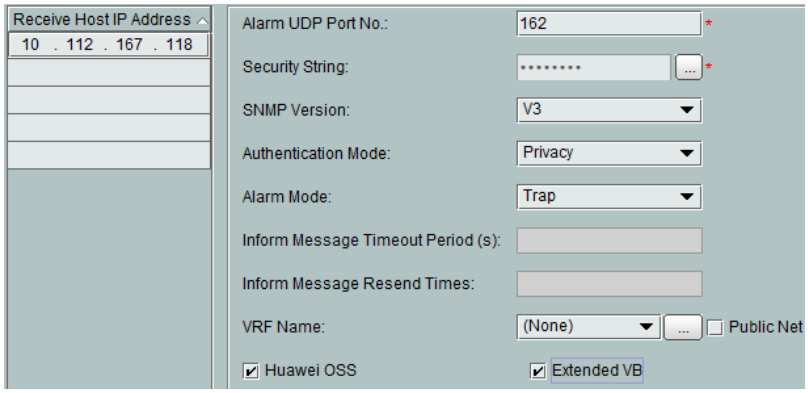
  NOTE

  Using sequence numbers to ensure alarm reliability is recommended. If devices and the VRP platform versions do not support the sequence number, use the Inform mode.

  Using sequence numbers can ensure alarm reliability and prevent alarm loss. Perform the following operations:

  Configuration on the U2000

  1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
  2. Choose **System Management** > **NE Channel Management** > **Trap Service** from the service tree.
  3. On the **Trap Service** tab page, click **Synchronize** to synchronize alarms from the NE.
  4. Right-click and choose **Create** from the shortcut menu. In the dialog box that is displayed, set the associated parameters and click **Huawei OSS** and **Extended VB**.



Copyright © Huawei Technologies Co., Ltd.

5. Click **OK**.

Configuration on the NE

1. Run the following command to access the system view:

   system-view

2. Run the following command to start the SNMP agent:

   snmp-agent

3. Run the following command to add the **private-netmanager** option to the destination host of the NE:

   snmp-agent target-host trap address udp-domain *X.X.X.X* **params securityname privacy v3 private-netmanager ext-vb**

   NOTE

   - *X.X.X.X* specifies the IP address of the destination host. Here, set it to the IP address of the U2000 server.
   - If the NE has been configured with the private-netmanager attribute before sending an alarm, the NE alarm generation time recorded on the U2000 is the same as that recorded on the NE. If the NE has not been configured with the private-netmanager attribute before sending an alarm, the NE alarm generation time recorded on the U2000 is the U2000 server time when the U2000 receives the trap packet from the NE.
   - If the SNMPv3 protocol is not used, add **cipher** next to the **securityname**. SNMPv3 is recommended because it is more secure.

- Perform the following operations if the U2000 cannot receive alarms generated on MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs:
  - Disable alarm suppression.
    1. Right-click an NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
    2. Select an NE in the NE Explorer and choose **Alarm** > **NE Alarm Suppression** from the function tree. Alternatively, select a board in the NE Explorer and choose **Alarm** > **Alarm Suppression** from the function tree.
    3. Change the value of **Status** to **Not Suppressed** for the associated event.
  - Configure automatic alarm reporting.
    1. Right-click an NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
    2. Select an NE in the NE Explorer and choose **Alarm** > **Alarm Severity and Auto Reporting** from the function tree. Alternatively, select a board in the NE Explorer and choose **Alarm** > **Alarm Severity and Auto Reporting** from the function tree.
    3. Change the value of **Auto Reporting Status** to **Reported** for the associated event.
  - Disable alarm reversion.
    1. Right-click an NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
    2. Select an NE in the NE Explorer and choose **Alarm** > **NE Alarm Attributes** from the function tree. Alternatively, select a board in the NE Explorer and choose **Alarm** > **Alarm Reversion** from the function tree.

Copyright © Huawei Technologies Co., Ltd.

3. Change the value of **Alarm Reversion** to **Disable** or **Reversion Status** to **Disable** for the associated alarm.

----End

6.6.5 Cannot Find Some Reported Alarms on the U2000

Symptom

The U2000 receives alarms, but these alarms are not displayed in the **Browse Current Alarm** or **Browse Historical Alarm** window.

Possible Causes

- Some alarms are filtered out by setting the filter criteria or the alarm template.
- The alarms are dumped.

Procedure

- Modify filtering criteria.
  1. Click **Filter** in the browse window or query alarm window. Check and modify the filter criteria in the **Filter** dialog box.
  2. Click **OK**.
- Query the alarms in the dump directory.
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
  2. Select a task type in the **Task Management** window and query the file saving directory of this task type.
     - Select **Alarm/Event Log Dump**.

       Right-click and choose **Attribute** from the shortcut menu and check **File path** on the **Extended Parameters** tab.
     - Select **Alarm Overflow Dump**or**Event Overflow Dump**.

       Right-click **Attribute** and check the **File path** from the **Extended Parameters** tab.
     - Select the task of **Alarm Manual Dump** or **Event Manual Dump**.

       Right click **Run** and check the **Dump path** in the **Run** dialog box.
  3. Query the alarms in the dump directory.

----End

6.6.6 U2000 Client Fails to Play Alarm Sound

Fault Symptom

Although the player of the U2000 client runs normally and the managed NE generates an alarm, the U2000 client fails to play the alarm sound.

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

- The U2000 user has stopped the current alarm sound or stopped the alarm sound permanently.
- The format of the audio files is incorrect.

Procedure

- Turning on the alarm sound.
  1. Choose **Fault** > **Stop the Alarm Sound Permanently** (traditional style) from the main menu or select **Fault Management** in **Application Center** and choose **Browse Alarm** > **Disable Alarm Sound** (application style) from the main menu is selected. Ensure that this item is not selected.
  2. Choose **Fault** > **Stop the Current Alarm Sound** (traditional style) from the main menu or select **Fault Management** in **Application Center** and choose **Browse Alarm** > **Disable Current Alarm Sound** (application style) from the main menu is selected. Ensure that this item is not selected.
- Modifying the format of the audio files.
  1. Choose **File** > **Preferences** from the main menu
  2. In the **Preferences** dialog box, click the **Sound Settting** tab.
  3. In the right pane of the dialog box, set the sound and sound file of the alarm of various severity levels, and the format of audio files for alarms to ***.wav**.
  4. Click **OK** or **Apply**.

----End

6.6.7 Failed to Display the Alarm Panel and the Fault Main Menu

Fault Symptom

The client fails to display the alarm panel and the **Fault** main menu.

Fault Analysis

If **Fault Process** does not start, the client cannot display the alarm panel and the **Fault** main menu.

Procedure

Step 1 Log in to the U2000 System Monitor.

Step 2 On the **Service Monitor** tab, select **Fault Process**.

Step 3 Right-click it, and then choose **Start the Process** from the shortcut menu.

Step 4 Make sure that **Fault Process** runs normally. Then, exit from the U2000 System Monitor.

Step 5 Log in to the U2000 client again.

----End

Copyright © Huawei Technologies Co., Ltd.

6.6.8 When a User Browses Alarms or Events, the Filter Dialog Box Cannot Be Displayed

Fault Symptom

When the user browses alarms or events, the **Filter** dialog box cannot be displayed.

Fault Analysis

- If the startup template is configured in the **Template Management** window, the **Filter** dialog box is not displayed after the client is started, and the window for browsing current alarms is displayed.
- If the default template is configured in the **Template Management** window, the **Filter** dialog box is displayed.
- In the **Alarm Local Terminal Settings** area in the **Preferences** window, the **Filter** will not be displayed.

  NOTE

  If a default template is configured, the **Filter** dialog box is not displayed during alarm/event browsing no matter whether the function of displaying the **Filter** dialog box is configured. The window for opening the template is displayed by default.

Procedure

- In the alarm/event browsing window, click **Filter** to open the **Filter** dialog box.
- If the **Filter** dialog box is automatically displayed after the alarm/event browsing window is accessed, perform the following operations:
  - Cancel a startup template.
    1. Choose **Fault** > **Settings** > **Template Management** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Template Management** from the main menu (application style).
    2. In the **Template Management** window, select a template with **Status** as **Startup Template**, right-click, and choose **Startup Template** from the shortcut menu.
  - Cancel a default template.
    1. Choose **Fault** > **Settings** > **Template Management** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Template Management** from the main menu (application style).
    2. In the **Template Management** window, view template types. Select a template with **Status** as **Default Template**, right-click, and choose **Default Template** from the shortcut menu.

       NOTE

       A default template can be configured for only one type of template. A default template can be deleted after the associated template type is selected.
  - Configure the function of automatically displaying the **Filter** dialog box.
    1. Choose **File** > **Preferences** from the main menu

Copyright © Huawei Technologies Co., Ltd.

2. In the **Preferences**, expand the **Alarm Local Terminal Settings** node from the navigation tree and choose **Alarm/Event Filtering**.
3. In the **Alarm/Event Filtering** area, select **Display the Filter dialog box**.

----End

6.6.9 Acknowledged and cleared alarms exist in the current alarm window

Symptom

Why is an acknowledged and cleared alarm displayed in the **Browse Current Alarm** window?

Possible Causes

This alarm is displayed because a life cycle has been set for this alarm. An acknowledged and cleared alarm whose life cycle has not ended is still displayed in the **Browse Current Alarm** window.

Procedure

Step 1 Choose **Fault** > **Settings** > **Options** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Options** from the main menu (application style).

Step 2 In the **Alarm Options** dialog box, choose **Lifecycle** from the navigation tree.

Step 3 In the **Lifecycle** area, set the life cycle to **0** for acknowledged and cleared alarms.

Step 4 Click **OK**.

Refresh the **Browse Current Alarm** window. The acknowledged and cleared alarm is not displayed. You can find the alarm in the **Browse Historical Alarm** window.

----End

Suggestion and Summary

To remove acknowledged and cleared alarms from the **Browse Current Alarm** window, set the life cycle to **0** for these alarms.

6.6.10 Alarm Time Displayed Abnormally

Symptom

The alarm time on the client is displayed abnormally.

Possible Causes

- The time zone or time of the client or server is set incorrectly.
- The time zone or time of the NE is set incorrectly.

Copyright © Huawei Technologies Co., Ltd.

Fault Diagnosis

The alarm time can be displayed in three modes: NE time, server time, client time. If the times or time zones configured for the NE, server, and client are different, you can use the following formula to check whether the alarm time on the U2000 is displayed incorrectly.

NOTE

- The time, time zone, and DST of an NE are represented by Te, Ze, and De.
- The time, time zone, and DST of the server are represented by Ts, Zs, and Ds.
- The time, time zone, and DST of the client are represented by Tc, Zc, and Dc.

Time Mode	Time	Time zone	DST	Alarm Time Displayed on the Client
NE Time	Te	Ze	De	Tc + (Ze-Zc) + (De-Dc)
Server Time	Ts	Zs	Ds	Tc + (Zs-Zc) + (Ds-Dc)
Client Time	Tc	Zc	Dc	Te+ (Zc-Ze) + (Dc-De)

If the alarm time displayed on the U2000 is different from the calculation result, the alarm time is incorrect. Check whether the time and time zone configured on the NE, server, and client are correct. If not, correct the configurations.

Procedure

Step 1 Correct the time on the client or server.

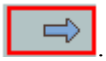
- On Windows, perform the following operations:
  1. Open the Control Panel and click **Date and Time**.
  2. In the **Date and Time** dialog box, set the time zone and time according to the local time zone and time.
  3. Click **OK**.
- On Solaris and SUSE Linux, perform the following operations:
  1. Log in to the MSuite client.
  2. Choose **Deploy** > **Change Time Zone** from the main menu.
  3. In the **Modify System Time Zone** dialog box, set the time zone and time according to the local time zone and time.
  4. Click **OK**.

NOTE

After changing the time zone, restart the OS as prompted for the changes to take effect.

Step 2 Change the NE time zone or time.

Copyright © Huawei Technologies Co., Ltd.

- Perform the following operations for access NEs:
  1. In common user mode, run the **display time** command to view the current system time.
  2. Switch to the privilege mode. Run the **timezone** or **time** commands to change the system time zone or time to the same as the local time and time zone.
- Perform the following operations for Router series, Switch series and Security NEs:
  1. Run the **display clock** command to view the current system time:
  2. Run the **clock timezone** or **clock datetime** commands to change the system time zone or time to be the same as the local time and time zone.
- Perform the following operations for MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs:
  - View and modify the NE time zone.
    1. Choose **Configuration** > **NE Batch Configuration** > **NE Time Localization Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Batch Configuration** > **NE Time Localization Management** from the main menu (application style).
    2. In the right pane, select an NE and click .
    3. Select a correct time zone from the **Time Zone** drop-down list.
    4. Click **Apply**.
  - View and modify the NE time.
    1. Choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (application style).
    2. In the left pane, select an NE and click  .
    3. Click **Synchronize with NM Time** to synchronize the NE time.

----End

6.6.11 LinkDown and LinkUp Alarms Are Displayed After a Long Delay

Fault Symptom

When you run the **shutdown** or **undo shutdown** command on a device, the link Up or link Down alarm is displayed in the alarm browser after a long delay.

NOTE

This case is applicable to routers and switches.

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

NEs whose VRP versions are earlier than V500R007 use a mechanism with a two-seconds delay to send LinkDown and LinkUp alarms. If N alarm destination NEs are configured, the total delay of link alarms is 2N seconds at most.

Procedure

Step 1 Make sure that the performance indicators of the U2000 are normal. For example, no resource is abnormally occupied.

Step 2 Right-click the NE in the topology view and choose **NE Explorer** from the shortcut menu.

Step 3 Choose **NE Channel Management** > **Trap Service** from the service tree.

Step 4 On the **Trap Service** tab page, view the alarm service list and delete unnecessary trap receiving devices.

Step 5 Perform a link Up or link Down test to check whether the alarm delay is back to normal.

NOTE

The delay of link alarms affects the refreshing of link status in the topology view. If the status of links cannot be refreshed in a timely manner, check whether the fault is caused by the delay in sending alarms. If so, refer to the preceding operation procedure to rectify the fault.

----End

6.6.12 SNMP Version Is Not Supported When Current NE Alarms Are Being Synchronized

Symptom

Right-click a router or switch in the Main Topology and choose **Synchronize Current Alarms** from the shortcut menu. A message is displayed indicating that the SNMP version is not supported.

NOTE

This case is applicable to routers and switches.

Cause Analysis

Alarm reliability in Inform mode is configured for the NE. This mode requires that the SNMP version be SNMPv2c.

Procedure

Step 1 Select the NE in the Main Topology and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** (traditional style) from the main menu or select **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** (application style) from the main menu.

Step 2 Click **Reset**.

Copyright © Huawei Technologies Co., Ltd.

Step 3 In the dialog box that is displayed, click the **SNMPv2 Parameters** tab. Then select the desired template from existing templates and click **OK**.

If the desired template is unavailable, click **Add** to add the template.

Step 4 In the **Confirm** dialog box, click **Yes**.

Step 5 Click **OK**.

----End

6.6.13 NE Offline Alarm Is Not Displayed on the U2000 Although Some NEs Get Offline

Symptom

Some NEs get offline, but no NE offline alarm is displayed on the U2000.

NOTE

This case is applicable to routers and switches.

Cause Analysis

NE offline alarms are masked by setting the relevant alarm masking rules. Therefore, these alarms are not displayed in the alarm list. The alarm masking rules can be modified in order to make the alarms unmasked.

Procedure

Step 1 Choose **Fault** > **Settings** > **Mask Rules** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Mask Rules** from the main menu (application style).

Step 2 Select an enabled alarm masking rule, right-click, and choose **Property** from the shortcut menu.

Step 3 On the **Basic Setting** tab page, check the settings of the alarm masking rule.

1. If **Alarm name** is selected, check that the NE offline alarm is not selected. If **Alarm name** is not selected, go to the next step.
2. In the **Severity** and **Type** areas, check that the severity and type of NE offline alarms are not selected. If the severity or type has been selected, clear the relevant check box.

Step 4 Click **OK**.

----End

6.6.14 Frequent Historical Alarm Reporting for a PTN NE

Symptom

A PTN NE reports historical alarms repeatedly.

Possible Causes

The login user of the PTN NE does not log out normally, causing this alarm reporting issue.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Administration** > **NE Security Management** > **NE Login Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **NE Login Management** from the main menu (application style).

Step 2 In the window that is displayed, select an NE from the Object Tree and click .

Step 3 Click the **NE Login Management** or **Online User Management** tab, select the PTN NE, and click **Logout** or **Forced Logout**.

----End

6.6.15 How Do I View Dumped Historical Alarms/Events?

Symptom

The dumped historical alarms/events cannot be queried in the historical alarm/event window.

Possible Causes

The dumped alarms/events were deleted from the database.

Procedure

- Periodic dump
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style) from the from the main menu
  2. In the navigation tree on the left of the **Task Management** window, choose **Database Capacity Management**.
  3. In the **Task Management** window, double-click the **Alarm/Event Log Dump** task in the task list.
  4. In the **Attribute** dialog box, click the **Extended Parameters** tab.

     You can view the dumped historical alarms/events in **File path**.
- Overflow dump
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style) from the from the main menu.
  2. In the navigation tree on the left of the **Task Management** window, choose **Overflow Dump**.
  3. In the **Task Management** window, double-click the **Alarm Overflow Dump** or **Event Overflow Dump** task in the task list.
  4. In the **Attribute** dialog box, click the **Extended Parameters** tab.

     You can view the dumped historical alarms/events in **File path**.

Copyright © Huawei Technologies Co., Ltd.

- Manual dump

  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style) from the from the main menu.
  2. In the navigation tree on the left of the **Task Management** window, choose **Manual Dump**.
  3. In the **Task Management** window, right-click the **Alarm Manual Dump** or **Event Manual Dump** task in the task list, then choose **Run**.

     You can view the dumped historical alarms/events in **Dump path**.

----End

6.6.16 An Alarm Is Not Cleared in Real Time

Symptom

After an NE-side fault is rectified, the alarm corresponding to the fault persists on the MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs.

Possible Causes

The NE time is incorrect, inconsistent with the MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs time.

Procedure

Step 1 Choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Batch Configuration** > **NE Time Synchronization** from the main menu (application style).

Step 2 In the left pane, select an NE and click .

Step 3 Click **Synchronize with NM Time** to synchronize the NE time.

----End

6.6.17 Alarms Cannot Be Cleared

Symptom

Alarms cannot be cleared in the **Browse Current Alarm** window.

Possible Causes

The NE where the alarms have occurred is offline.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 If the NE does not need to be managed, delete it. Then the U2000 automatically clears its alarms. (The U2000 erases all related information upon NE deletion.)

For details about how to delete an NE, see Deleting NEs.

Step 2 If the NE needs to be managed, bring it online and clear its alarms.

For details about how to bring an NE online, see **6.3.22 NE Icon in the Topology Becomes Grey**.

----End

6.6.18 Alarm Synchronization Failure Between the U2000 and NEs

Symptom

- The optical fiber is abnormal, but the associated alarm on the U2000 is cleared.
- When the associated physical port on the NE recovers, the alarm on the U2000 is not cleared.

NOTE

This case applies only to routers and switches.

Cause Analysis

Huawei OSS is not selected when the user configures a sequence number mode on the U2000, or the **private-netmanager** attribute is not configured for alarms sent on the NE side. As a result, the U2000 server time when the U2000 receives trap packets from NEs, not the actual alarm generation time on NEs, is recorded as the NE alarm generation time on the U2000.

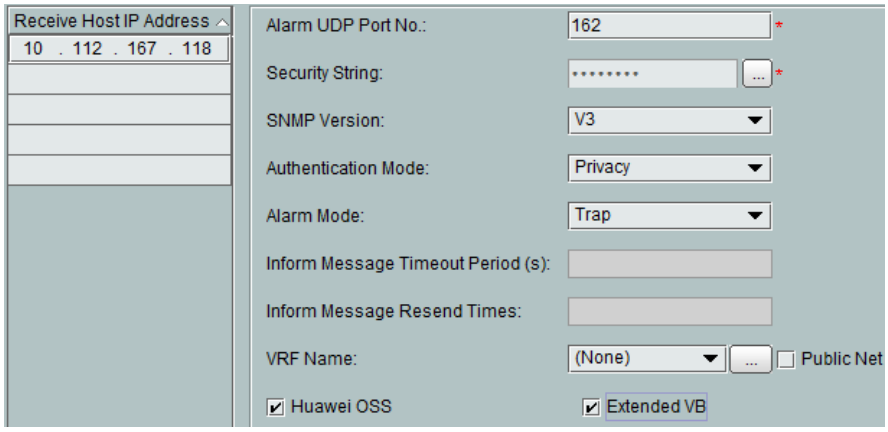
Procedure

NOTE

Simple Network Management Protocol version 3 (SNMPv3) is more secure than SNMPv1 and SNMPv2c. Using SNMPv3 is recommended.

- **Configuration on the U2000**
  1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
  2. Choose **System Management** > **NE Channel Management** > **Trap Service** from the service tree.
  3. On the **Trap Service** tab page, click **Synchronize** to synchronize alarms from the NE.
  4. Right-click and choose **Create** from the shortcut menu. In the dialog box that is displayed, set the associated parameters and click **Huawei OSS** and **Extended VB**.

Copyright © Huawei Technologies Co., Ltd.



5. Click **OK**.

- **Configuration on the NE**

1. Run the following command to access the system view:

   system-view

2. Run the following command to start the SNMP agent:

   snmp-agent

3. Run the following command to add the **private-netmanager** option to the destination host of the NE:

   snmp-agent target-host trap address udp-domain *X.X.X.X* **params securityname privacy v3 private-netmanager**

   NOTE

   X.X.X.X specifies the IP address of the destination host. Here, set it to the IP address of the U2000 server.

   If the SNMPv3 protocol is not used, add **cipher** next to the **securityname**. SNMPv3 is recommended because it is more secure.

Copyright © Huawei Technologies Co., Ltd.

7 MSTP Network Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot the commonly seen faults on MSTP network management.

7.1 SDH Trails Management Troubleshooting Cases
This topic describes how to troubleshoot the commonly seen faults on SDH end-to-end configuration.

7.2 MSTP NE Configuration Troubleshooting Cases

Copyright © Huawei Technologies Co., Ltd.

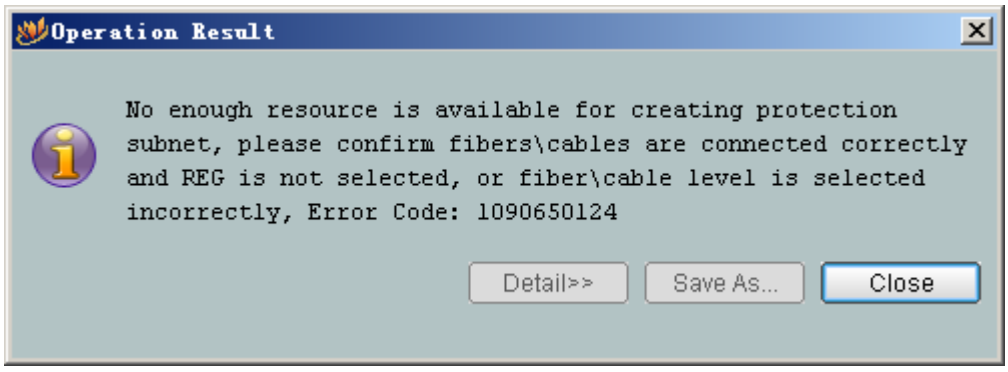
7.1 SDH Trails Management Troubleshooting Cases

This topic describes how to troubleshoot the commonly seen faults on SDH end-to-end configuration.

7.1.1 Insufficient Resources for Creating a Protection Subnet

Symptom

In the window for creating a protection subnet, a user selects NEs and clicks **Next**. An error message is displayed indicating insufficient resources. Error code: 1090650124.



Possible Causes

The possible causes are as follows:

- No fiber connection exists between NEs.
- Not all NEs are selected. For example, eight NEs exist in a ring but only seven NEs are selected.
- The order for selecting NEs is different from the order for connecting fibers.
- The protection subnet level does not match the fiber level. For example, the protection subnet level is STM-16 while the fiber level is STM-4.
- Fiber links are used by other protection subnets.
- The protection channel in the protection subnet carries trails.
- The values of **MSP Sharing** for the two optical ports at the two ends of the fiber are inconsistent.

Procedure

Step 1 Verify that all NEs are selected properly, including the number of selected NEs and the order of NE selection (clockwise or anticlockwise).

Step 2 Verify that fibers of the same level have been connected between NEs.

Step 3 Verify that the fiber level matches the protection subnet level.

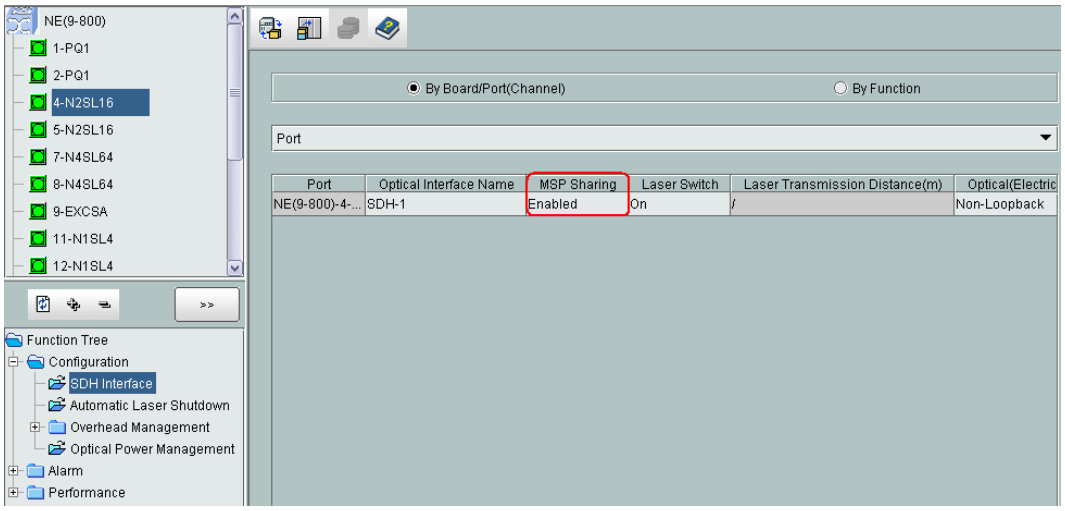
Step 4 Verify that fibers are not used by other protection subnets.

Copyright © Huawei Technologies Co., Ltd.

Step 5 Verify that the protection channel in the protection subnet does not carry trails.

Step 6 Ensure that the values of **MSP Sharing** for the two optical ports at the two ends of the fiber are the same.

Step 7 If resource insufficiency is reported when a multiplex section protection (MSP) ring that shares VC4 timeslots is created, verify that **MSP Sharing** is enabled on the source and sink ports of fibers.



----End

7.1.2 Failure to Delete a Protection Subnet Node Due to Time or Space Division Cross-connections

Symptom

A user fails to delete a protection subnet node.

Possible Causes

There are time division cross-connections on the NE. In this situation, nodes cannot be deleted to prevent service interruption.

NOTE

- Time division cross-connections are service cross-connections between different VC12 timeslots. That is, cross-connections pass through different VC12 timeslots on an NE, for example, timeslots 1 at one end and timeslots 9 at the other end.
- Space division cross-connections are service cross-connections between the same VC12 timeslots but different VC4 timeslots.

Procedure

Step 1 Adjust the trials to ensure that there is no time or space division cross-connection on the NE.

Step 2 Delete the protection subnet node.

----End

Copyright © Huawei Technologies Co., Ltd.

Suggestion and Summary

OptiX Metro 1000s have this restriction.

7.1.3 How to Use the End-To-End Trail Management Function

Symptom

- A new U2000 user cannot create an SDH trail.
- A user cannot create an SDH trail on an RTN NE.
- **SDH Protection Subnet** is missing from the main menu **Service**.

Possible Causes

The SDH_RTN end-to-end license is not loaded or the original license has expired.

Procedure

Step 1 Load or update the SDH_RTN E2E license file on the U2000.

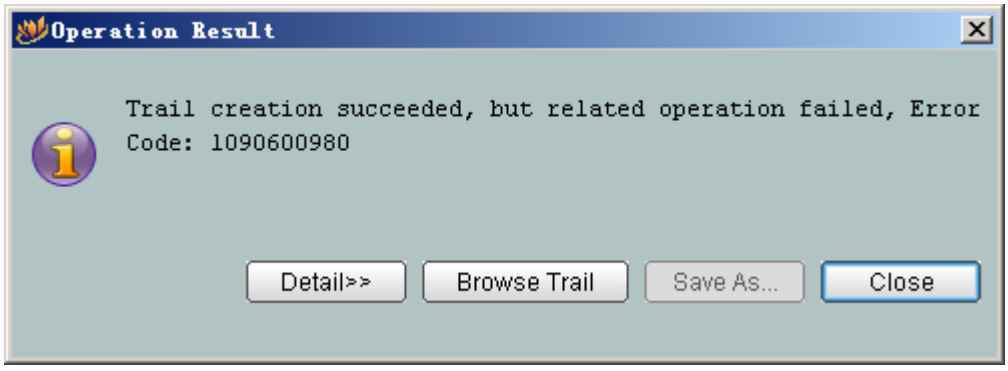
Step 2 Create a trail by using the end-to-end trail management function. For details, see Chapter **SDH and Radio Trails Management>Creating SDH Trails** in the *OG for MSTP and Radio Services Management*.

----End

7.1.4 Failure to Perform the Related Operations While Trail Creation Succeeded

Symptom

In the window for creating a trail, a user clicks **Apply** to apply new trails after routes have been calculated. A message is displayed indicating that the trail is created but failed to be applied. Error code: 1090600980, 1090601227.



Possible Causes

An activated trail can be created on the U2000 in two steps: Create a deactivated cross-connection and then apply the cross-connection to NEs for activation. Errors usually occur on the cross-

Copyright © Huawei Technologies Co., Ltd.

connection application. Failure causes will be displayed if you click **Detail>>** in the **Operation Result** dialog box. Common causes include:

- Communications between NEs and the U2000 are interrupted.
- NEs are busy.
- Cross-connection resources on NEs are insufficient.
- Cross-connections to be activated conflict with those existing on NEs.

Procedure

Step 1 Check that the NEs communicate with the U2000 properly.

Step 2 Choose **Configuration** > **NE Configuration Data Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Configuration Data Management** from the main menu (application style). Upload NE configuration data.

Step 3 **Optional:** Adjust the timeslots of the trail if the failure reason is no enough cross-connection.

Step 4 Activate the created trail.

1. Choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (application style).
2. In the **Set Trail Browse Filter Criteria** dialog box, specify the filter criteria and click **Filter All**.
3. Right-click the new trail that is deactivated or partially activated and choose **Activate** from the shortcut menu. In the **Confirm** dialog box, click **Yes**.

----End

Suggestion and Summary

Do not select **Active the trail** when creating a trail if you want to create deactivated trails. Ensure that NEs communicate with the U2000 successfully during trail creation.

7.1.5 Message Indicating that Cross-Connection Already Exists Displayed During Service Creation

Symptom

When creating a trail, a user clicks **Apply**. An error is displayed indicating that the cross-connection exists. Error code: 38747.

Possible Causes

This error message is reported from an NE to the U2000, indicating that the cross-connection to be activated exists on the NE. This error occurs because data on the U2000 is inconsistent with data on the NE. Generally, the following causes lead to data inconsistency:

Copyright © Huawei Technologies Co., Ltd.

- The cross-connection is created on the NE on a CLI.
- An NE is managed by two sets of U2000, called U2000 A and U2000 B. Data changes on U2000 A cannot be updated automatically to U2000 B.

Procedure

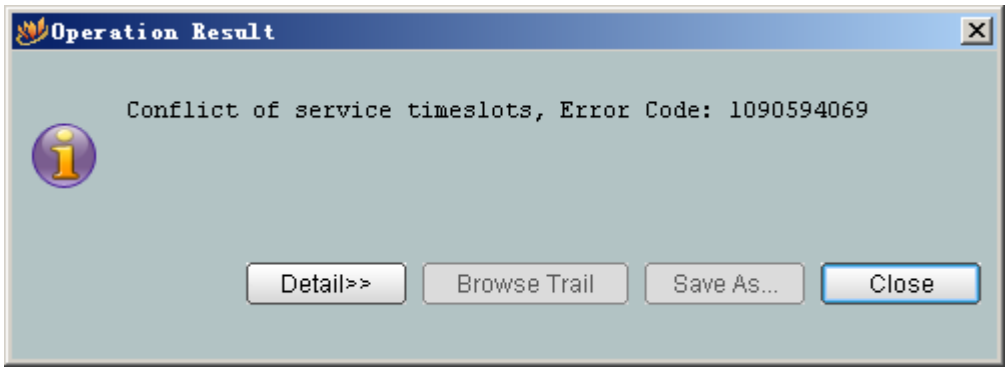
Step 1 Open the service configuration window in the NE Explorer, click **Query** to query cross-connections from NEs. Find the conflicting cross-connection and re-create the trail with an idle timeslot.

----End

7.1.6 Service Timeslot Conflict During Trail Creation

Symptom

In the dialog box for creating a trail, a user clicks **Apply** to apply the new trail after routes have been calculated. A message is displayed indicating a timeslot conflict. Error code: 1090594069.



Possible Causes

Usually, the error occurs during trail configuration if the source or sink port of a cross-connection to be created is used by a discrete service. Deal with the discrete service and create a trail again.

Procedure

Step 1 Synchronize data from the NEs traversed by the trail.

1. Check that the NEs communicate with the U2000 properly.
2. Choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (application style). Uploading the NE data to the U2000, so that the data on the U2000 is consistent with the data on NEs.
3. Adjust the timeslots of the trail if the failure reason is no enough cross-connection.
4. Activate the created trail. For details, see **SDH and Radio Trails Management>Maintaining SDH Trails>Locking or Unlocking an SDH Trail** in the *OG for MSTP and Radio Services Management*.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether the discrete service is in use. If the discrete service is in use, convert it to a mono nodal trail and then create a trail again.

Step 3 If the discrete service is no longer in use, delete it before creating a trail again.

NOTE

For details on how to handle discrete services, see **SDH and Radio Trails Management>Creating SDH Trails>Creating SDH Trails by Trail Search>Discrete Service Causes and Handling Measures** in the *OG for MSTP and Radio Services Management*.

----End

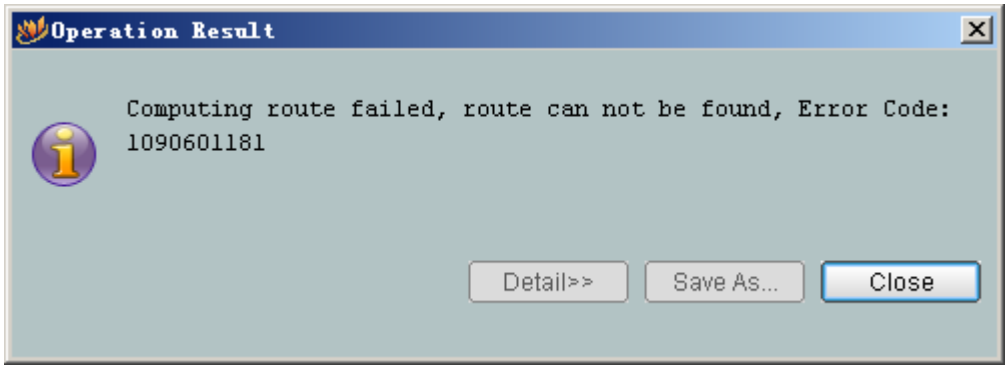
Suggestion and Summary

Clear discrete services in a timely manner to avoid timeslot conflicts. Convert mono nodal discrete services that are in use to a mono nodal trail. Delete discrete services that are not in use to release resources.

7.1.7 Failure to Find Routes During Trail Creation

Symptom

After a user selects the source NE and sink NE, an error message is displayed during route calculation indicating that routes cannot be found. Error code: 1090601181, 1090601396, 1090601358.



Possible Causes

The possible causes are as follows:

- No fiber connection exists between the source and sink NEs.
- The fiber between the source and sink NEs is disabled.
- No VC4 server trail or Link server trail exists for lower order trails.
- VC4 server trails or Link server trails are disabled.
- No protection subnet has been created for links on the NEs whose main control board versions are 4.XX.XX.XX.
- Routes are not selected based on the direction of the protection subnet involved.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Verify that fibers between NEs are connected properly and are enabled.

Step 2 **Optional:** Verify that VC4 trails or link server trails exist for lower order trails. Create the required server trails if they do not exist. If VC4 server trails are disabled, enable it.

Step 3 **Optional:** Verify that there are protection subnets for the NEs whose main control board versions are 4.XX.XX.XX. If no protection subnet has been created for the NEs, create one.

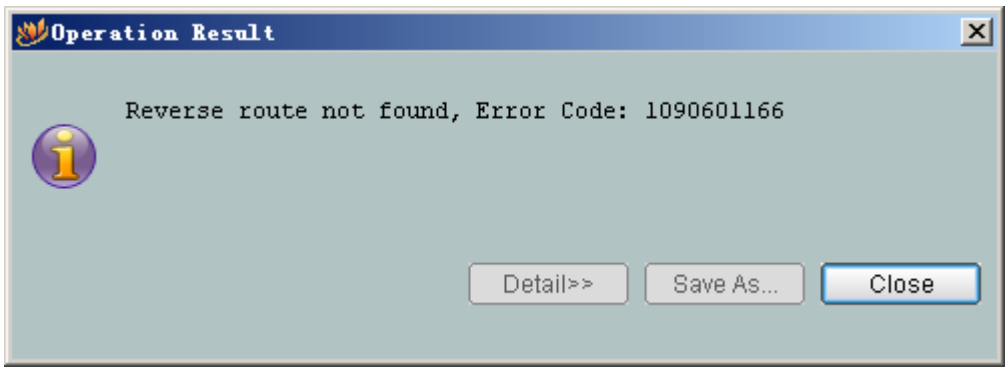
Step 4 Create a trail again. For details, see **SDH and Radio Trails Management > Creating SDH Trails** in *OG for MSTP and Radio Services Management*.

----End

7.1.8 Failure to Find the Reverse Route During Trail Creation

Symptom

During trail creation, an error message is displayed indicating that the reverse route cannot be found. Error code: 1090601166.



Possible Causes

The forward and reverse working trails in a unidirectional protection ring are routed differently. If the forward route has sufficient resources while the reverse route encounters resource insufficiency, the error message is displayed. For example, the VC4 trail for the reverse route does not exist or the VC4 trail is disabled.

Procedure

Step 1 Create a VC4 trail or enable the VC4 trail accordingly for the reverse route in a unidirectional protection ring.

NOTE

- Click **Service** > **SDH Trail** > **Create SDH Trail** to create a VC4 trail.
- Click **Service** > **SDH Trail** > **Manage SDH Trail**. In the displayed window, right–click a disabled VC4 trail and choose **Enabled** to enable the VC4 trail.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Create a trail again. For details, see Chapter **SDH and Radio Trails Management>Creating SDH Trails** in the *OG for MSTP and Radio Services Management*.

----End

7.1.9 How to Select a Port When Creating a Trail

Symptom

Ports cannot be specified when a trail is configured on the U2000 in end-to-end (E2E) mode.

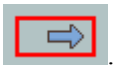
Possible Causes

- Cause 1: SDH NNIs are not configured for an NE whose control board version is 4.XX.XX.XX.
- Cause 2: In some scenarios, some ports are not used by any cross-connections or fiber connections when a trail is being created on the U2000 in E2E mode. However, the so-called idle ports cannot be specified. A possible cause is that NE data is not sufficiently uploaded to the U2000, resulting in data inconsistency between the U2000 and NEs.
- Cause 3: The specified ports are used by other fiber connections or service when the trail is configured.

Procedure

Step 1 Solution 1: Configure SDH NNIs for the NE whose control board version is 4.XX.XX.XX. For details, see Chapter **SDH and Radio Protection Subnets Management > Creating an SDH NNI** in the *OG for MSTP and Radio Services Management*.

Step 2 Solution 2: Synchronize data between the U2000 and NEs.

1. Choose **Configuration** > **NE Configuration Data Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Configuration Data Management** from the main menu (application style).
2. Select one or more NEs from the Object Tree and click  .
3. Select one or more NEs whose login status is **Yes** from the **Configuration Data Management List**.
4. **Optional:** For NEs whose login status is **No**: Choose **Administration** > **NE Security Management** > **NE Login Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **NE Login Management** from the main menu (application style). In the window that is displayed, log in to the NEs.

   NOTE

   If the NEs cannot be logged in to, adjust the DCN between the NEs and the U2000 to ensure proper communication, and then upload the NE data.
5. Click **Upload**. Alternatively, right-click and select **Upload** from the shortcut menu.
6. Click **OK** in the confirmation dialog box.
7. Click **Close** in the **Operation Result** dialog box.

Copyright © Huawei Technologies Co., Ltd.

8. Choose the port again to create a trail.
9. **Optional:** If NE data still cannot be uploaded after you take the preceding steps, log in to the System Monitor, find the E2E process Nml_sdh, and restart it.

NOTICE

Exercise caution because restarting the process may interrupt services.

Step 3 Solution 3: Delete fibers connected to the ports to be specified.

NOTE

Before deleting fibers, verify that the fibers are not planned fibers. If they are planned fibers, the trail plan may be incorrect and you need to adjust trail routes and select other ports.

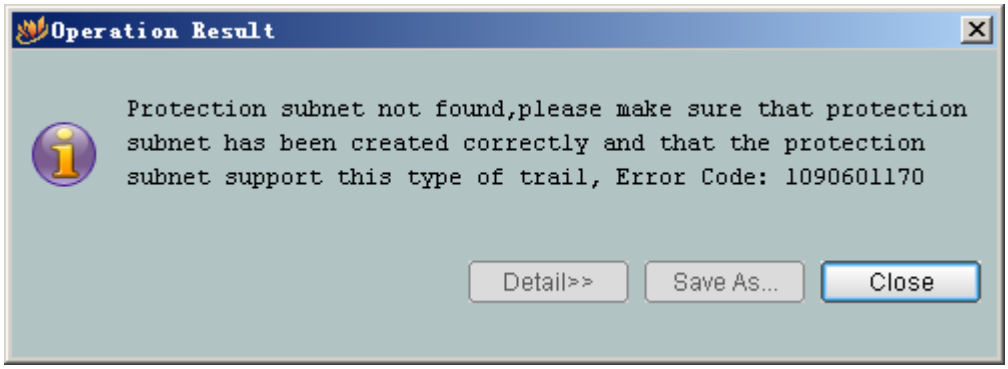
1. Choose **Inventory** > **Fiber/Cable/Microwave Link** > **Fiber/Cable/Microwave Link Management** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Inventory** > **Fiber/Cable/Microwave Link** > **Fiber/Cable/Microwave Link Management** from the main menu (application style).
2. Right-click the desired fibers/cables and choose **Delete Fiber/Cable** from the shortcut menu. The **Warning** dialog box is displayed. Click **OK** to delete the fibers/cables.
3. In the **Result** dialog box, click **Close**.

----End

7.1.10 Failure to Find Protection Subnets During Creation of a VC12 or VC3 Service

Symptom

When a user creates a VC12 or VC3 service, an error message is displayed indicating that protection subnets cannot be found. Error code: 1090601170.



Possible Causes

The VC12 or VC3 service being created traverses NEs whose main control board versions are 4.XX.XX.XX, but no protection subnet has been created for links on these NEs.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create protection subnets on NEs whose main control board versions are 4.XX.XX.XX.

Step 2 Create a VC12 or VC3 trail again. For details, see Chapter **SDH and Radio Trails Management>Creating SDH Trails** in the *OG for MSTP and Radio Services Management*.

----End

7.1.11 Blank NE Panel Displayed During Trail Creation

Symptom

When a user selects an NE during trail creation, the U2000 displays an error message, indicating that the target process does not exist. Then a blank NE Panel is displayed.

Possible Causes

The U2000 is busy with an excessive number of concurrent tasks and cannot allocate sufficient thread resources for opening the NE Panel.

Procedure

Step 1 Close the NE Panel and **Create SDH Trail** window.

Step 2 Choose **Service** > **SDH Trail** > **Create SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Create SDH Trail** from the main menu (application style). And then select the NE again.

----End

7.1.12 Operation Timeout Occurs when Configuring Services on the U2000

Symptom

A timeout message is displayed on the U2000 when Ethernet services are configured on an OSN 3500.

Possible Causes

The required U2000 management process is not fully started.

Procedure

Step 1 Check how many OSN 3500s encounter service configuration timeouts.

- If multiple or all OSN 3500s encounter timeouts, log in to the System Monitor client and restart the nemgr_sdh process for the OSN 3500s. Then configure services again.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

Restarting the nemgr_sdh process will make NEs unmanageable within a short period.

- If only one OSN 3500 encounters timeouts, resolve communication failures or NE faults for that OSN 3500. Then configure services again.

----End

7.1.13 Cannot Form Trails After Search

Symptom

After configuring cross-connections on NEs, I search for SDH trails. However, no new SDH trail is formed after the search.

Possible Causes

- Fiber connections between line boards are incorrect.
- Cross-connections are configured incorrectly on NEs.
- Configurations on NEs are not synchronized to the U2000 database.

Procedure

Step 1 Check fiber connections between line boards and verify that the line boards on which the cross-connections have been configured are connected properly by fibers.

Step 2 Verify that cross-connections are configured correctly on NEs.

Step 3 Upload NE data to the U2000 if NE configurations are not synchronized to the U2000 database.

1. Choose **Configuration** > **NE Configuration Data Management** from the main menu.
2. Select the NEs with unsynchronized cross-connection configurations and click **Upload**.
3. In the dialog box that is displayed, click **Close**.

----End

Suggestion and Summary

It is not recommended that a user creates cross-connections in the NE Explorer and configures trails using trail search. If necessary, select a suitable cross-connection protection mode.

7.1.14 Incorrect Trail Generated After A Trail Search

Symptom

In the NE Explorer, a user creates several trails. On the U2000, however, only one trail is generated after a trail search. In addition, the displayed trail is incorrect.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

During trail creation, the trail protection mode needs to be set to PP or SNCP, rather than no protection or MSP. Therefore, redundant cross-connections are created on the NEs whose main control board versions are 4.XX.XX.XX.

Fault Diagnosis

1. The analysis of the generated trail shows that this trail has multiple sources and sinks, rather than single source and sink.
2. After cross-connections on involved NEs are checked, it is found that involved ports on these NEs have multiple logical systems.
3. After involved discrete cross-connections are checked, it is found that they are generated due to a lack of a source or sink and unnecessary cross-connections are generated on these NEs.
4. It is verified that the user creates the cross-connections in the NE Explorer and generates the trail using a trail search.

Procedure

Step 1 Delete redundant dual-fed and single-receiving cross-connections.

Step 2 Create normal cross-connections again.

Step 3 Search for SDH trails.

----End

Suggestion and Summary

It is not recommended that a user create cross-connections in the NE Explorer and configure trails using trail search. If necessary, select a suitable cross-connection protection mode.

7.1.15 Copying Trails Fails Due to Insufficient Resource

Symptom

In the trail copying window, there is one record in the **Available Timeslots/Port** list, but no record in the **Current Number of Copying** list. A user fails to add a record from the **Available Timeslots/Port** list to the **Selected Timeslots/Port** list.

Possible Causes

- Some resources displayed in the **Available Timeslots/Port** list are occupied by discrete cross-connections.
- Server trail resources are used by other trails.

Procedure

Step 1 Seek out the cross-connection that uses the resource in the **Available Timeslots/Port** list. Locate the resource in the **Available Timeslots/Port** list that is used by the cross-connection and do not select this record for trail copying.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Right-click the trail to be copied and choose **Browse Relevant Server Trails** from the shortcut menu.

Step 3 In the **Manage SDH Trail** window, right-click the server trail that is used by other trails and choose **Browse Relevant Client Trails** from the shortcut menu.

Step 4 In the **Manage SDH Trail** window, check whether other trails use resources of the server trail.

NOTE

You cannot use server trail resources that are used by other trails to perform a trail copying.

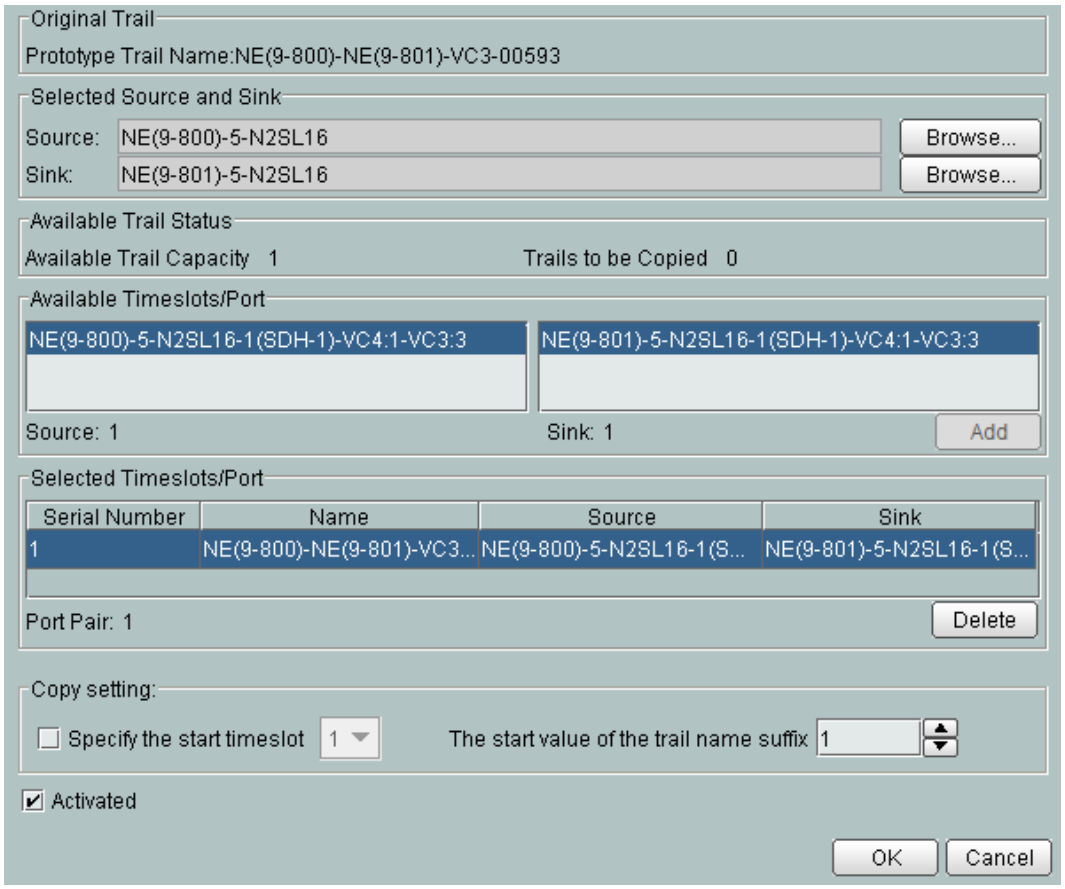
Step 5 Perform trail copying again.

----End

Suggestion and Summary

On the U2000, after trail copying is complete, new trails use the same server trails, source and sink NEs, boards, ports, and higher order timeslots.

Available Capacity of Trail specifies the number of trails available for copying; **Current Number of Copying** specifies the number of trails can be added to the trail copying list. As shown in the following figure, only one copying trail can be created, and one trail is added to the trail copying list. Therefore, **Current Number of Copying** is **0**, and the **Add** button is dimmed.



Copyright © Huawei Technologies Co., Ltd.

7.1.16 Failure to Copy and Paste All SDH Trail Records to an Excel File

Symptom

There are a large number of records in the SDH trail management window. Without dragging the scroll box, a user presses **Ctrl+A** to select all records, and then copies and pastes the selected records to an Excel file. Some SDH trail records, however, are omitted from the Excel file.

Possible Causes

The SDH trail list is divided into different pages and the buffer saves the information of only trails displayed in the current page. In this case, without dragging the scroll box, a user can only copy trails displayed in the current page by pressing **Ctrl+A** and **Ctrl+C**.

Procedure

Step 1 In the trail management window, click **Save As**. In the dialog box that is displayed, select the desired records and save them by setting **Start row**, **End row**, and **File name**.

NOTE

You can specify the path and format for the exported file. The following file formats are supported: XLS, TXT, HTML, and CSV. By default, the exported file is saved in the client/report directory.

Step 2 Click **OK**. In the **Information** dialog box, click **Yes** to open the file.

----End

Suggestion and Summary

To save memory and enhance running efficiency, the SDH trail list is divided into different pages and information about trails only on the current page is saved into the buffer. Without dragging the scroll box, a user can only copy trails displayed in the current page by pressing **Ctrl+A** and **Ctrl+C**. A user can export all trail data by clicking **Save As**, and specify parameters in the dialog box that is displayed.

7.1.17 A Modified Trail Displayed as Unchanged in the Trail Search Result

Symptom

A user adds a node to an Ethernet trail and sets relevant trunk links, VBs and VLAN information correctly. After a trail search, however, the trail does not change accordingly, and the new node becomes discrete. This problem recurs on all associated existing trails after a trail search.

Possible Causes

The user does not select the **Delete existing trails from network layer before searching** check box before the trail search.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check that all information added on the NE is correct and complies with the Ethernet trail generation rules.

Step 2 Select the **Delete existing trails from network layer before searching** check box before the trail search.

Step 3 Perform the Ethernet trail search.

----End

7.1.18 Failure to Browse the Created Trail

Symptom

A U2000 user (user A, a non-admin user) has permission to browse SDH trails but fails to browse the new trail on the U2000.

Possible Causes

- User A is not authorized to browse the new trail. To solve the problem, user **admin** needs to authorize user A to browse this trail.
- Because the SDH alarm table is too large, the Nml_sdh process is automatically ended or cannot start up.

Procedure

Step 1 For cause 1, grant the permission for SDH trails to user A.

1. Log in to the U2000 as user **admin**.
2. Choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (application style).
3. In the **Set Trail Browse Filter Criteria** dialog box, set the filter criteria and click **Filter All**. The trails are displayed in the list.
4. Right-click the trail and choose **Authorize to User** from the shortcut menu.
5. In the dialog box that is displayed, select user A from **Available Users** in the left pane. Then, click .
6. Click **OK**.

Step 2 For cause 2, contact Huawei technical support engineers for a solution.

----End

Suggestion and Summary

- In the **Manage SDH Trail** window, you can authorize a maximum of 50 trails at a time. If you are a non-admin user but want to view all trails, do as follows: Choose **Service** > **SDH Trail** > **Manage SDH Service Authority** from the main menu (traditional style);

Copyright © Huawei Technologies Co., Ltd.

alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Service Authority** from the main menu (application style). In the window that is displayed, select **Confer all trails** and click **OK**.

- Authorization is not needed during trail creation.

7.1.19 Cannot Modify an Existing Trail

Symptom

You have rights to modify SDH trails and have been given authority for the existing trail to be modified.

Possible Causes

- The trail is locked and therefore cannot be modified.
- The trail is in the **Partially Active** state and therefore cannot be modified.

Procedure

Step 1 Log in to the U2000.

Step 2 Choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (application style).

Step 3 In the **Set Trail Browse Filter Criteria** dialog box, set the filter criteria and click **Filter All**. The trails are displayed in the list.

Step 4 If the trail is locked, perform the following operations:

- Right-click the trail and choose **Unlock** from the shortcut menu. After the trail is unlocked, select it, click **Create/Modify** and choose **Modify Trail** or **Modify Manually** to modify the trail.

Step 5 If the trail is in the **Partially Active** state, perform the following operations:

- Right-click the trail and choose **Activate** from the shortcut menu. After the trail is activated, select it, click **Create/Modify** and choose **Modify Trail** or **Modify Manually** to modify the trail.

----End

Suggestion and Summary

The U2000 can lock out important trails. You cannot modify, delete, activate, or rename the locked SDH trails. Locking or unlocking an SDH trail does not affect services that are running.

Copyright © Huawei Technologies Co., Ltd.

7.1.20 No Cross-Connections in the NE Explorer for Trails in the Manage SDH Trail Window

Symptom

The **Manage SDH Trail** window displays some trails whose cross-connections do not exist in the NE Explorer.

Possible Causes

Cross-connections have been deleted on NEs, but the U2000 does not obtain this information and therefore displays outdated trail information in the **Manage SDH Trail** window.

Procedure

Step 1 Check the setting of the configuration item **bIsdeleteTrailByXC** in the **server\nml\nmlsdh\conf\cfg\nmlsdh.cfg** file. If the configuration item is disabled, this symptom is normal. If it is enabled, proceed to the next step.

Step 2 Choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (application style).

Step 3 Click **Maintenance** and choose **Synchronize**. In the dialog box that is displayed, select the NEs traversed by the trail, select the **Fiber synchronization** and **Cross synchronization** check boxes, and click **Synchronize**.

NOTE

Synchronize is available only to the users with "Maintenance Group" authority or higher.

Step 4 Choose **Service** > **SDH Trail** > **Search for SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Search for SDH Trail** from the main menu (application style).

Step 5 Choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **SDH Trail** > **Manage SDH Trail** from the main menu (application style).

Step 6 In the **Manage SDH Trail** window, check trail information. Trails whose cross-connections have been deleted should disappear.

----End

7.1.21 Failed to Delete a Fiber/Cable

Symptom

A fiber/cable fails to be deleted because "It is not allowed to delete the link." or "There are protection subnets,trails,or virtual fibers on the fibers/cables."

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The fiber/cable carries protection subnets, trails, or virtual fibers/cables and therefore cannot be deleted.

Procedure

Step 1 In the Main Topology, right-click the NE from which a fiber/cable needs to be deleted and choose **Query Relevant Fibers** from the shortcut menu.

Step 2 Select the fiber/cable to be deleted and click **Delete Fiber/Cable**.

NOTICE

When you delete fibers/cables, the protection subnets, trails, and virtual fibers/cables carried by them will also be deleted. Therefore, delete fibers/cables only when necessary. Before deleting fibers/cables, you can export network-wide data to a script.

Step 3 In the **Warning** dialog box, click **OK**.

----End

7.1.22 Inconsistent Timeslot Occupation Between the NE Explorer and the E2E Service Management Window

Symptom

When a user configures a service in the NE Explorer and E2E service management window, the timeslots displayed as occupied are different in the two places.

Possible Causes

Data is inconsistent between the U2000 and NEs.

Procedure

Step 1 Verify that data is consistent between the U2000 and NEs.

1. Set Telnet/STelnet parameters. For details, see Setting NE Telnet/STelnet Parameters by Using a Template and Manually Modifying NE Telnet/STelnet Settings.
2. Synchronize NE data.

   In the topology view or navigation tree, right-click the desired NE and choose **Synchronize NE Configuration Data** from the shortcut menu.

Step 2 Search for trails.

- To search for SDH trails, refer to the "Searching for SDH Trails" section (under **SDH and Radio Trails Management** > **Creating SDH Trails** > **Creating SDH Trails by Trail Search**) in *OG (MSTP and Radio Services Management)*.

Copyright © Huawei Technologies Co., Ltd.

- To search for WDM trails, refer to the "Searching for WDM Trails" section (under **WDM Trails Management** > **Creating WDM Trails**) in *OG (WDM Services Management)*.

----End

7.1.23 Cannot Open the SDH Trail Management Window

Symptom

The SDH trail management window cannot be opened as usual.

Possible Causes

- The SDH E2E management process (Nml_sdh) is not running.
- No thread resources can be allocated because the memory usage is high.

Procedure

Step 1 Restart the Nml_sdh process.

NOTICE

This operation will render related NEs temporarily unreachable.

Step 2 Collect stack information during the restart and send the information to Huawei technical support engineers.

----End

7.1.24 NE Cannot Be Added During SDH Trail Modification

Symptom

When I attempt to add an NE to a created SDH trail, the U2000 displays an error message indicating that cross-connections are incorrect.

Possible Causes

The NE you attempt to add does not have sufficient cross-connection resources.

Procedure

Step 1 Check cross-connection resources on the NE and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

7.1.25 SDH Trail Fails to Be Deleted

Symptom

I cannot delete an SDH trail.

Possible Causes

- After the SDH trail is deactivated, data of involved NEs become inconsistent between the U2000 and NEs.
- Some cross-connections of the trail have been deleted but some others remain.

Procedure

Step 1 For cause 1, synchronize data from the NEs traversed by the trail.

1. Ensure that the U2000 successfully communicates with the NEs.
2. Choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (application style). Upload NE data to the U2000 to maintain data consistency.
3. If the deletion fails because cross-connection resources are insufficient, adjust timeslots.

Step 2 For cause 2, delete the remaining cross-connections. For details, see **SDH and Radio Trails Management > Creating SDH Trails>Creating SDH Trails by Trail Search>Deleting Discrete Services** in *OG for MSTP and Radio Services Management*.

----End

7.2 MSTP NE Configuration Troubleshooting Cases

7.2.1 Failure to Upload NE Data

Symptom

An error (error code: 1090593555) is displayed when users upload the data of the OptiX OSN 3500 to the U2000.

Possible Causes

Certain boards that the current U2000 cannot manage exist on NEs.

Procedure

Step 1 Check whether certain boards that the current U2000 cannot manage exist on NEs. If such boards exist, use either of the following method to rectify the fault:

1. Pull out the boards. For details, see Chapter "U2000 Deployment" in the *Parts Replacement*.

Copyright © Huawei Technologies Co., Ltd.

2. Upload NE configurations again. For details, see Chapter "Keeping Data Consistency Between the U2000 and NEs" in the *Operation Guide for Common Features*.

1. Upgrade the current U2000 version to support these boards.
2. Upload NE configurations again. For details, see Chapter "Keeping Data Consistency Between the U2000 and NEs" in the *Operation Guide for Common Features*.

----End

7.2.2 No Data Returned During Query of NE Performance Data

Symptom

An error (error code: 1090646029) is displayed indicating that no data is returned when users query the ET1 performance of MSTP devices.

Possible Causes

The IP performance event monitoring of the ET1 board is disabled.

Procedure

Step 1 In the NE Explore, select the required board. Choose **Performance** > **IP Performance Event Monitor Status** from the Function Tree.

Step 2 In the window that is displayed, click **Search**. In the query result area, check **Monitor Status** of Ethernet port performance of the board.

Step 3 Set **Monitor Status** to **Disabled**, and then click **Apply**.

Step 4 Set **Monitor Status** to **Enabled**, and then click **Apply**.

----End

7.2.3 SDH NEs Become Unreachable

Symptom

SDH NEs become unreachable to the NE management process.

Possible Causes

When an NE management process manages an excessive number of NEs, SDH NEs may become unreachable. In that event, move some NEs to a new or lightly loaded NE management process.

Procedure

Step 1 Choose **Administration** > **Settings** > **NE Partition** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **Settings** > **NE Partition** from the main menu (application style).

Step 2 Select a node in the left pane. The right pane will show the NE name and other information of the node.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **Migrate NE/Move to**.

NOTE

- For transport NEs, the button is **Migrate NE**.
- For other NEs, the button is **Move to**.

Step 4 In the **Migrate NE** dialog box, select the NEs you want to move out in the **Available NEs** area and add them to the **Selected NEs** area. If an NE is associated with other NEs, the system will prompt you to move the associated gateway and non-gateway NEs as well. Click **Yes** to move these NEs.

Step 5 Select a record in the **Select Target NE explorer** area and click **OK**.

Step 6 Observe the operation progress in the **Move NE** dialog box.

Step 7 When the progress reaches 100%, click **Close**.

----End

Copyright © Huawei Technologies Co., Ltd.

8 WDM Network Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot the commonly seen faults on WDM network management.

8.1 WDM Trails Management Troubleshooting
This topic describes how to troubleshoot the commonly seen faults on WDM network management.

8.2 WDM NE Configuration Troubleshooting Cases

Copyright © Huawei Technologies Co., Ltd.

8.1 WDM Trails Management Troubleshooting

This topic describes how to troubleshoot the commonly seen faults on WDM network management.

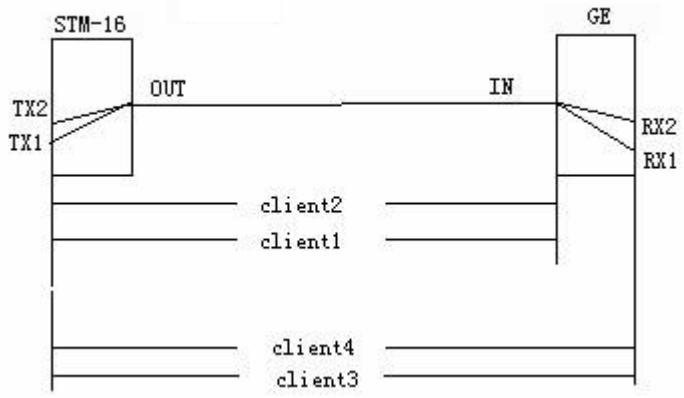
8.1.1 Incorrect Number of Searched-Out Client Trails

Symptom

After a trail search is complete, the searched-out trails are twice the number of actual Client trails in the **Manage WDM Trail** window.

Possible Causes

The error is caused by inconsistent transmission rate at the two ends of the Client trail. As shown in the following figure, one end of the trail is at STM-16 rate, and the other is at GE rate.



Trails are searched layer by layer. Cross-connections with higher transmission rate are searched first and those with lower transmission rate are searched later.

- When the search starts from left to right by STM-16 cross-connection, client1(TX1--IN) and client2(TX2--IN) are searched out. These two trails terminated at the IN port of the board on the right.
- When the search starts from right to left by GE cross-connection, client3(TX1--RX1) and client4(TX2--RX2) are searched out. Their server trail is client1.

In this case, two unnecessary trails (client1 and client2) are searched out because the rates at the two ends are different and Client trail is terminated at the IN or OUT port.

When both ends are at GE rate, only two correct trails (TX1--RX1 and TX2--RX2) are searched out.

Procedure

Step 1 In the NE Explorer, check whether the cross-connection configuration of the boards at both ends is correct.

Step 2 If the cross-connection configuration is incorrect, adjust the cross-connection rate.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Upload the data of related NEs to the U2000.

Step 4 Search for trails again.

----End

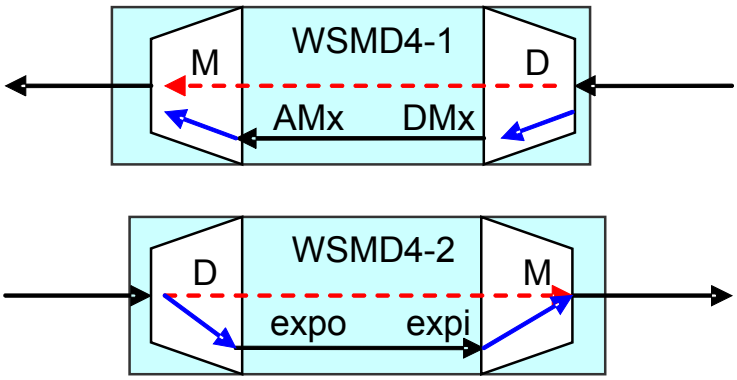
8.1.2 Failure to Create Trails on WSMD4 Boards

Symptom

After a user creates and applies a trail in a network with WSMD4 boards, an error is reported.

Possible Causes

- For WSMD boards (for example, WSMD4 and BWSMD2 boards), multiplexing and demultiplexing signals can be applied both in the eastbound and in the westbound directions, as shown in Figure-1. Routes calculated by the U2000 must traverse a board two times. The U2000 may create a cross-connection between any two ports and create the red cross-connection (wrong route) on an NE. Actually, the U2000 should create the blue cross-connections on the NE.

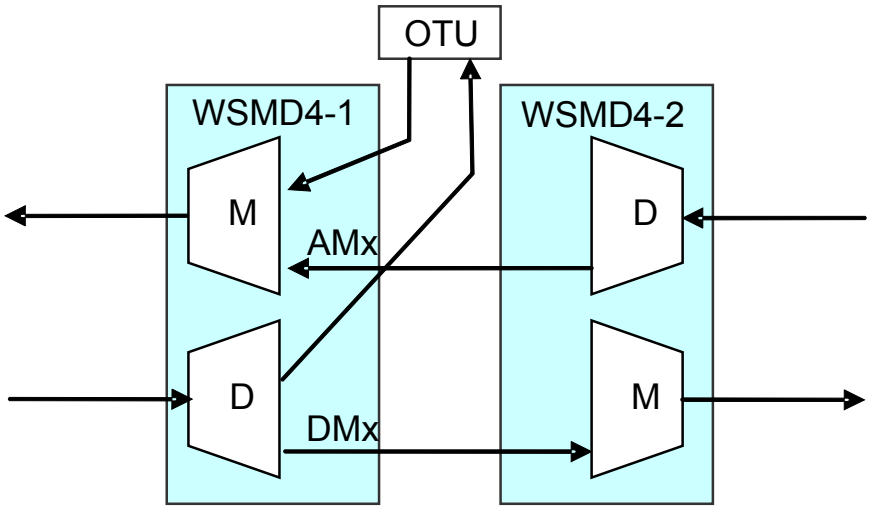


- If no route constraints are specified during trail creation, the route may fail to be applied to NEs.

Procedure

Step 1 As shown in the following figure, multiplexing and demultiplexing are performed in the same direction. Both the sent and received wavelengths of the OTU board traverse the WSMD4-1 board.

Copyright © Huawei Technologies Co., Ltd.



Step 2 Specify route constraints during trail creation. Specifically, designate the explicit links, explicit nodes, and excluded nodes.

----End

8.1.3 Incorrect Trail Rate

Symptom

After a user deletes a Client trail at GE rate in the NE Explorer and creates a cross-connection at STM-64 rate, the bearer rate of the new trail is still GE.

Possible Causes

- If the source and sink of the searched-out trail are the same as those of a deleted trail that has customized information, the customized information will take effect on this new trail.

  NOTE

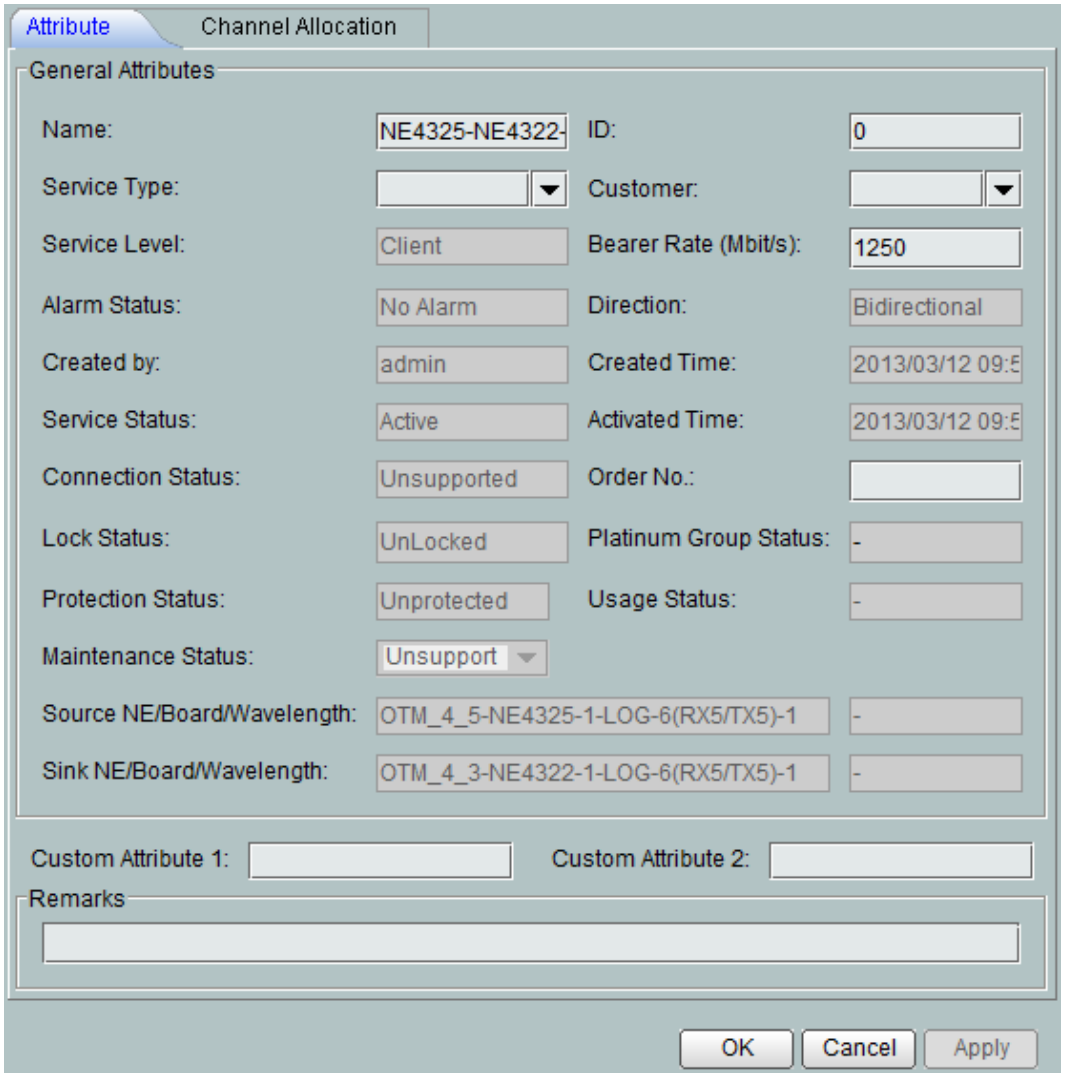
  The bearer rate of a trail can be specified by a user. The U2000 preserves the customized information of a trail if the trail is deleted from the network layer or deleted indirectly. For example, a fiber is deleted or a cross-connection is deleted in the NE Explorer.

- The customized information will be overwritten if scripts are imported to the U2000.

Procedure

Step 1 In the **Manage WDM Trail** window, right-click a trail in the list and choose **Details** from the shortcut menu.

Copyright © Huawei Technologies Co., Ltd.



Step 2 Enter the required rate in the **Bearer Rate(Mbit/s)** text box.

Step 3 Click **OK**.

----End

8.1.4 Cannot Use Trail Functions

Symptom

- An NMS user cannot create a WDM trail or an error occurs during trail creation.
- Trails are displayed incorrectly.
- Trails cannot be found by a trail search or the found trails cannot be combined.

Possible Causes

- The required license is not loaded or has expired.
- The OTN service management package for the network service management component has not been deployed or the Nml_common and Nml_otn processes are not running.

Copyright © Huawei Technologies Co., Ltd.

- Data is inconsistent between the U2000 and NEs.
- WDM NEs have been configured incorrectly.
- Fiber connections are missing or incorrect wavelengths have been specified.
- Logical fibers have not been created or logical wavelengths have not been specified.
- Cross-connections have not been created or electrical cross-connections have been configured incorrectly.
- Discrete services exist.
- Did not search trail.

Procedure

Step 1 Load or update the required license in the license file of the U2000.

Step 2 The **OTN** Service Management deployment package in the Network Service Management component has been deployed, and the **Nml_common** and **Nml_otn** processes have been started.

Step 3 Verify that WDM NE has been configured correctly and data is consistent between the U2000 and NEs. If data is inconsistent, upload NE data.

Step 4 Create a trail by using the end-to-end trail management function. For details, see "Creating WDM Trails" (under "WDM Trails Management") in *OG for WDM Services Management*.

Step 5 Verify that fiber connections are ready and correct wavelengths have been specified. Otherwise, trails may fail to be created or found.

Step 6 Verify that logical fibers have been created or logical wavelengths have been specified. Otherwise, trails may fail to be created or combined after being found.

Step 7 Verify that cross-connections have been created and electrical cross-connections have been configured correctly. If configurations are incorrect, modify them.

Step 8 Verify that no discrete services exist. Otherwise, trail creation will fail. If discrete services exist, delete them and re-create them.

Step 9 Choose **Service** > **WDM Trail** > **Search for WDM Trail** from the main menu to search for trail.

Step 10 If end-to-end WDM trails fails to be created, please set the explicit route to solve this.

Step 11 If a trail fails to be created, verify that board attributes are correct, search for trails, and create the trail again.

----End

8.1.5 Failure to Browse the Created WDM Trail

Symptom

A U2000 user (user A, a non-admin user) has rights to browse WDM trails but fails to browse the new trail on the U2000.

User B (with the monitoring or operation rights) has replaced the license but cannot browse created SDH trails on the U2000.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

Users A and B are not authorized to browse the new trail. To solve the problem, user **admin** needs to authorize users A and B to browse this trail.

Procedure

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

Step 2 Choose **Service** > **WDM Trail** > **Manage WDM Trail** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **WDM Trail** > **Manage WDM Trail** from the main menu (application style).

Step 3 In the **Set Trail Browse Filter Criteria** dialog box, set the filter criteria and click **Filter All**. The trails are displayed in the list.

Step 4 Right-click the trail and choose **Authorize to User** from the shortcut menu.

Step 5 In the dialog box that is displayed, select user from **Available Users** in the left pane. Then, click .

Step 6 Click **OK**.

----End

Suggestion and Summary

In the **Manage WDM Trail** window, you can authorize a maximum of 50 trails at a time. If you are a non-admin user but want to view all trails, do as follows: Choose **Service** > **WDM Trail** > **Manage WDM Service Authority** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **WDM Trail** > **Manage WDM Service Authority** from the main menu (application style). In the window that is displayed, select **Confer all trails** and click **OK**.

8.1.6 Failure to Create the WDM ASON Trail on the U2000 Because of NE Commissioning Times Out

Symptom

When a user attempts to create a WDM ASON trail in the **ASON Trail Management** window, the U2000 displays an error message indicating that the server is busy or the equipment is performing other operations. When the user makes the second attempt, the U2000 informs that the trail already exists on NEs.

Possible Causes

NE commissioning times out. After the U2000 displays the error message, NEs continue with the commissioning and then successfully add the trail.

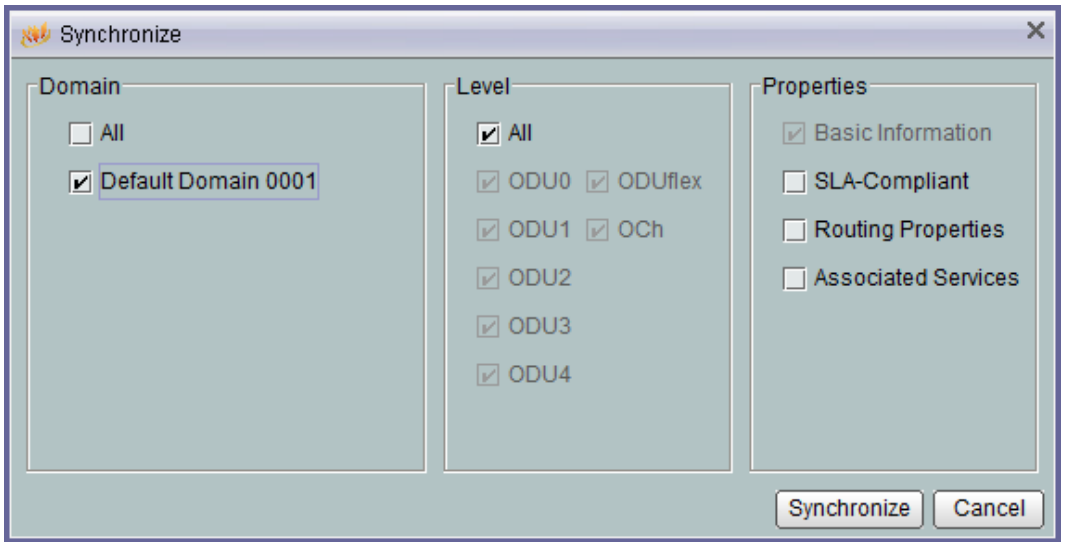
Procedure

Step 1 In the **ASON Trail Management** window, click **Synchronize**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 In the **Synchronize** dialog box, select the ASON domain of the source node and click **Synchronize** as shown in **Figure 8-1**.

Figure 8-1 Synchronize



NOTE

After a successful network-wide synchronization, ASON LSPs that exist on NEs will be synchronized to the U2000.

----End

8.1.7 How to Select a Port When Creating a Trail

Symptom

Ports cannot be specified when a trail is configured on the U2000 in end-to-end (E2E) mode.

Possible Causes

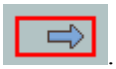
- Cause 1: In some scenarios, some ports are not used by any cross-connections or fiber connections when a trail is being created on the U2000 in E2E mode. However, the so-called idle ports cannot be specified. A possible cause is that NE data is not sufficiently uploaded to the U2000, resulting in data inconsistency between the U2000 and NEs.
- Cause 2: The specified ports are used by other fiber connections when the trail is configured.

Procedure

Step 1 Solution 1: Synchronize data between the U2000 and NEs.

1. Choose **Configuration** > **NE Configuration Data Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Configuration Data Management** from the main menu (application style).

Copyright © Huawei Technologies Co., Ltd.

2. Select one or more NEs from the Object Tree and click  .
3. Select one or more NEs whose login status is **Yes** from the **Configuration Data Management List**.
4. **Optional:** For NEs whose login status is **No**: Choose **Administration** > **NE Security Management** > **NE Login Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **NE Login Management** from the main menu (application style). In the window that is displayed, log in to the NEs.

   NOTE

   If the NEs cannot be logged in to, adjust the DCN between the NEs and the U2000 to ensure proper communication, and then upload the NE data.
5. Click **Upload**. Alternatively, right-click and select **Upload** from the shortcut menu.
6. Click **OK** in the confirmation dialog box.
7. Click **Close** in the **Operation Result** dialog box.
8. Choose the port again to create a trail.

Step 2 Solution 2: Delete fibers connected to the ports to be specified.

NOTE

Before deleting fibers, verify that the fibers are not planned fibers. If they are planned fibers, the trail plan may be incorrect and you need to adjust trail routes and select other ports.

1. Choose **Inventory** > **Fiber/Cable/Microwave Link** > **Fiber/Cable/Microwave Link Management** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Inventory** > **Fiber/Cable/Microwave Link** > **Fiber/Cable/Microwave Link Management** from the main menu (application style).
2. Right-click the desired fibers/cables and choose **Delete Fiber/Cable** from the shortcut menu. The **Warning** dialog box is displayed. Click **OK** to delete the fibers/cables.
3. In the **Result** dialog box, click **Close**.

----End

8.1.8 Trail Data Is Not Synchronized During a WDM NE Upgrade

Symptom

After a WDM NE is upgraded, WDM trail data fails to be updated on the U2000.

Possible Causes

Data is inconsistent between the U2000 and NEs.

Procedure

Step 1 Delete the WDM trails that traverse the upgraded WDM NE.

For details, see the "Deleting a WDM Trail" section (under **WDM Trails Management** > **Maintaining WDM Trails**) in *WDM Services Management*.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Create the WDM trails.

For details, see the "Creating WDM Trails" section (under **WDM Trails Management**) in *WDM Services Management*.

Step 3 Search for WDM trails.

For details, see the "Searching for WDM Trails" section (under **WDM Trails Management** > **Creating WDM Trails**) in *WDM Services Management*.

----End

Suggestion and Summary

If WDM trails are updated or modified after being created, delete the trails before performing other operations.

8.1.9 Inconsistent Timeslot Occupation Between the NE Explorer and the E2E Service Management Window

Symptom

When a user configures a service in the NE Explorer and E2E service management window, the timeslots displayed as occupied are different in the two places.

Possible Causes

Data is inconsistent between the U2000 and NEs.

Procedure

Step 1 Verify that data is consistent between the U2000 and NEs.

1. Set Telnet/STelnet parameters. For details, see Setting NE Telnet/STelnet Parameters by Using a Template and Manually Modifying NE Telnet/STelnet Settings.
2. Synchronize NE data.

   In the topology view or navigation tree, right-click the desired NE and choose **Synchronize NE Configuration Data** from the shortcut menu.

Step 2 Search for trails.

- To search for SDH trails, refer to the "Searching for SDH Trails" section (under **SDH and Radio Trails Management** > **Creating SDH Trails** > **Creating SDH Trails by Trail Search**) in *OG (MSTP and Radio Services Management)*.
- To search for WDM trails, refer to the "Searching for WDM Trails" section (under **WDM Trails Management** > **Creating WDM Trails**) in *OG (WDM Services Management)*.

----End

Copyright © Huawei Technologies Co., Ltd.

8.2 WDM NE Configuration Troubleshooting Cases

8.2.1 A Menu Item Is Missing

Symptom

- When configuring an OptiX OSN 1800 on the U2000, a user cannot find the shortcut menu item **Modify Port**.
- On the U2000 client, the **WDM Interface** window cannot be completely displayed in the NE Explorer.

Possible Causes

Probable causes of the absence of an NE- or board-level menu item:

- The U2000 has not logged in to the NE.
- The NE or board version is old and does not support the function.
- The NE or board does not support the function.
- The license does not support the function.
- The NE login account is invalid or has insufficient rights.

Procedure

Step 1 Check whether the U2000 has logged in to the NE. If it has not, right-click the NE and choose **Login** from the shortcut menu.

Step 2 Check the NE version. Specifically, right-click the NE and choose **Properties** from the shortcut menu. In the **Properties** dialog box, check **NE Software Version(VRC)** on the **NE Properties** tab. Then consult the product description to determine whether the NE version supports this function. If the NE version is old and does not support this function, upgrade the NE version or retry with a version that supports the function.

Step 3 If the NE version supports this function, check whether the required license has been installed.

Step 4 Verify that the NE login account is valid and has sufficient rights. If it is invalid or has insufficient rights, log it off and retry with an account with more rights, for example, the **admin** account. Then open the **WDM Interface** window again.

----End

8.2.2 A WDM NE Cannot Be Opened

Symptom

On the U2000, double-clicking an OTN NE cannot show the NE Panel, and the NE Explorer cannot be opened from the shortcut menu.

Possible Causes

The nemgr_trans process fails to be started.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Start the nemgr_trans process.

Step 2 If failed, initialize the database.

NOTICE

When the operation are performed, the services will be interrupted.

Step 3 Restore MOs or scripts.

NOTICE

When the operation are performed, the services will be interrupted.

----End

8.2.3 Allocating Existing OTN Subracks to Optical NEs

Question

The U2000 allows WDM subracks to be directly displayed in the Main Topology without creating an optical NE (such as OTM, OADM, or OLA). For such subracks, users cannot learn about optical NE types from node icons. (Optical NE types reflect node functions.) Some users may require a function that allows them to allocate existing subracks to optical NEs. If signal flows (internal fiber connections) have been created for existing subracks, the subracks cannot be directly allocated to optical NEs and related NEs cannot be directly deleted and then recreated on the U2000. If users can allocate existing subracks to optical NEs without deleting internal fiber connections, they will be relieved of the tremendous workload brought by deletion and recreation.

Answer

Step 1 In the NE Explorer, choose **Configuration** > **Fiber/Cable Synchronization** from the navigation tree.

Step 2 In the right pane, click **Synchronize** to maintain fiber/cable consistency between the U2000 and the NE.

- If the **Fiber/Cable on the NE Only** or **Fiber/Cable on the NMS Only** area has records, select all the records and click **Create Fiber/Cable**. In the dialog box that is displayed, click **Closed**. The synchronized fibers/cables are displayed in the **Synchronized Fiber/Cable** list.
- If conflicting fibers/cables exist, they cannot be created. Click **Delete Fiber/Cable** to delete the fibers/cables that have not been created on the U2000 or NE. Then recreate the remaining fibers/cables.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Choose **Configuration** > **NE Configuration Data Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Configuration Data Management** from the main menu (application style).

Step 4 In the **NE Configuration Data Management** window, choose an NE from the navigation tree and click .

Step 5 In the right pane, select all NEs and click **Initialize Data on NMS**.

After the initialization, all the selected NEs will enter the initialized state and therefore become preconfigured.

Step 6 Based on node types, create optical NEs and allocate OTN subracks to them.

Step 7 Choose **Configuration** > **NE Configuration Data Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **NE Configuration Data Management** from the main menu (application style).

Step 8 In the **NE Configuration Data Management** window, choose an NE from the navigation tree and click .

Step 9 In the right pane, select all NEs and click **Upload**. In the confirmation dialog box, click **OK** to upload NE data.

Step 10 View the signal flows (internal fiber connections) of the OTN subracks in the optical NEs. You will see the signal flows that have been created for the subracks before the subracks are allocated to optical NEs.

----End

Copyright © Huawei Technologies Co., Ltd.

9 Troubleshooting Native Ethernet Trail Faults

About This Chapter

This topic describes how to troubleshoot faults on native Ethernet trails.

9.1 Cannot Use Trail Functions

Copyright © Huawei Technologies Co., Ltd.

9.1 Cannot Use Trail Functions

Symptom

- A user NMS user cannot create an E-Line or E-LAN trail.

Possible Causes

The required license is not loaded or has expired.

Procedure

Step 1 Load or update the required license in the license file of the U2000.

Step 2 Create a trail by using the end-to-end trail management function. For details, see "Operation Tasks" in *OG for Native Ethernet Services Management*.

----End

Copyright © Huawei Technologies Co., Ltd.

10 PTN Network Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot the commonly seen faults on PTN network management.

10.1 Tunnels Are Not Displayed Completely

Copyright © Huawei Technologies Co., Ltd.

10.1 Tunnels Are Not Displayed Completely

Symptom

Some tunnels are not displayed on the **Manage Tunnel** tab page.

Possible Causes

Some tunnels are filtered out against the filter criteria configured during automatic IP service discovery.

Procedure

- Choose **Service** > **Search for Service** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **Search for Service** from the main menu (application style).
- Do not set filter criteria. Click **Start**.
- On the **Discovery Result** tab page, view the discovered IP services.
- Select one or more IP services in the service list and click **Jump Service** to switch to the service management window to locate the service and view or modify it.

----End

Copyright © Huawei Technologies Co., Ltd.

11 Router and Switch Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot router and switch management.

11.1 NE Channel Management Troubleshooting
This describes how to rectify the common faults in NE channel management.

11.2 Data Synchronization Troubleshooting
This topic describes how to troubleshoot commonly seen data synchronization faults.

11.3 QoS Management Troubleshooting
This describes how to rectify the common faults in QoS management.

11.4 Troubleshooting LLDP Management
This describes how to rectify the common faults in LLDP management.

11.5 Ethernet OAM Management Troubleshooting
This describes how to rectify the common faults in Ethernet OAM management.

11.6 MPLS-TP OAM Management Troubleshooting
This describes how to rectify the common faults in MPLS-TP OAM management.

11.7 Change Audit Troubleshooting
This topic describes how to troubleshoot change audit.

11.8 Link Troubleshooting
This topic describes the method of troubleshooting common link faults.

11.9 Some Information Is Not Displayed in the U2000 NE Explorer and Data Is Not Correctly Displayed on the NE Panel

11.10 Failed to Telnet to an NE by Right-clicking the NE Icon on the Main Topology

11.11 An NE5000E Is Displayed Abormally After Being Upgraded from a Single Chassis to a Cluster

11.12 Failed to Change an NE Interface Description

Copyright © Huawei Technologies Co., Ltd.

11.13 Failure to Create a Test Case on the NE Side

11.14 IP E2E Troubleshooting

This topic describes how to troubleshoot commonly seen IP E2E faults.

Copyright © Huawei Technologies Co., Ltd.

11.1 NE Channel Management Troubleshooting

This describes how to rectify the common faults in NE channel management.

11.1.1 Failed to Configure the Syslog Service

Fault Symptom

The Syslog service configured on the U2000 is invalid.

Fault Analysis

The information center is disabled on the device.

Procedure

Step 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then choose **Tool** > **Telnet** on the shortcut menu.

Step 2 Enter the password.

Step 3 Run the **system-view** command to enter the system view.

Step 4 Run the **info-center enable** command to enable the information center.

----End

11.1.2 Failure to Report an Extension Error to the U2000

Fault Symptom

An NE just returns a general error message. Hence, Users are unaware of what caused the configuration failure or how to change parameters during next configuration.

Fault Analysis

The SNMP extension error code function is not enabled on the NE.

Procedure

Step 1 Telnet or STelnet to an NE. Run the **system** command to open the system view. Then, run the following command to check whether the SNMP extend error code function is enabled on the NE.

NOTE

Using STelnet (if supported) to log in to the device is recommended. STelnet is more secure.

disp current-configuration configuration | incl snmp-agent extend

If a blank message is displayed, the function is disabled on the NE.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Run the following command to enable the function:

snmp-agent extend error-code enable

Step 3 Repeat Step 1 to verify the configuration.

display current-configuration configuration | incl snmp-agent extend

If the following information is displayed, the function is enable on the NE.

```
snmp-agent extend error-code enable
```

----End

11.1.3 Multiple Duplicate Alarms Are Found

Symptom

When browsing current alarms, a user finds that the U2000 has received multiple duplicate alarms with the same alarm source (IP NE) and alarm type.

Possible Causes

Alarm services of both inform and trap modes are configured in NE channel management. As a result, the U2000 receives multiple duplicate alarms. Deleting the configurations of the inform mode is recommended.

Procedure

Step 1 Select an alarm, right-click, and choose **Locate in Topology** from the shortcut menu.

Step 2 Locate the NE in the Main Topology, right-click the NE, and choose **NE Explorer** from the shortcut menu.

Step 3 In the NE Explorer, perform the following operations:

For a V5 NE:

1. Choose **System Management** > **NE Channel Management** > **Trap Service** from the navigation tree.
2. Select a record for which **Receiving Host IP Address** has been set to the U2000 server IP address and **Alarm Mode** has been set to **Inform**, right-click, and choose **Delete** from the shortcut menu.

- You can delete one record only when two records for which **Alarm Mode** is set to **Trap** and **Inform** and **Receiving Host IP Address** is set to the same IP address have been configured.

For a V8 NE:

1. In the **Function Tree**, choose **Channel Management** > **SNMP** > **Target Host**.

Copyright © Huawei Technologies Co., Ltd.

2. Select a record for which **Network Address** has been set to the U2000 server IP address and **Notice the Type of Information** has been set to **Inform** and click **Delete**.

NOTICE

- You can delete one record only when two records for which **Alarm Mode** is set to **Trap** and **Inform** and **Network Address** is set to the same IP address have been configured.

----End

11.1.4 FTP Test Failure

Fault Symptom

FTP test fails.

Fault Analysis

The FTP user root directory is incorrectly set.

Procedure

Step 1 The FTP user root directory is incorrectly set.

Add the FTP user and perform the FTP test again. For details, see **Working with the NMS** > **Topology Management** > **Setting Parameters for the Communication Between the U2000 and NEs** > **Configuring the xFTP Service** > **Testing FTP Services**.

NOTE

- On the Solaris or Linux OS, **Home directory** must be set to **/opt/backup/ftpboot**. **Home directory** on the Windows OS and the working directory of the xFTP user on the xFTP server OS must be the same. The default directory is **D:**, which can be changed as required.
- The FTP user can only be connected to the U2000 server using an FTP client. The Telnet or SSH connection is not supported.
- Do not modify the U2000's default user configurations.

----End

11.1.5 Excess Historical NE Alarms Are Displayed on the U2000

Fault Symptom

The U2000 displays NE historical alarms.

Fault Analysis

The displayed excess alarms are actually the historical alarms. When NEs are not managed by the U2000 or not connected to the U2000, the NE-generated alarms are cached and displayed on the U2000 after synchronization, causing that the time of alarm generation is the same as the server time.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **clear alarm active** command on the NE side to delete active alarm data.

Step 2 Delete related alarms on the U2000.

1. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style).
2. In the **Filter** dialog box, set filter criteria and click **OK**.
3. Select an alarm from the current alarms window, right-click, and then choose **Suppress NE Alarm**.
4. In the **Confirm** dialog box, click **Yes**.

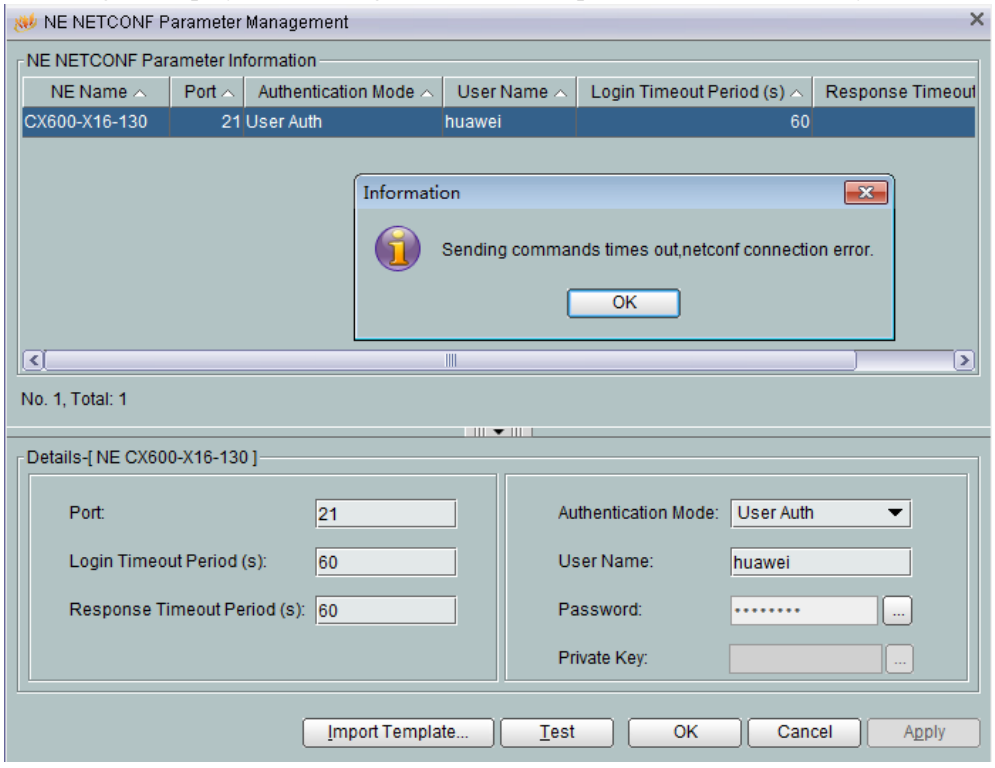
Step 3 Synchronize NE data.

----End

11.1.6 Incorrect NETCONF Parameter Setting

Symptom

A message is displayed indicating that NETCONF parameters are incorrectly set for a V8 NE.



Possible Causes

NETCONF parameters are not set on the U2000 or NE side, or NETCONF parameters set on the U2000 and NE sides are inconsistent.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set NETCONF parameters on the NE side using the following commands:

The following describes how to set the NETCONF user name to **huawei** and NETCONF password to **Changeme_123**.

1. Configure AAA.

```
sysname netconf-agent
aaa
local-user huawei password cipher Changeme_123
local-user huawei user-group manage-ug
local-user huawei level 15
local-user huawei service-type all
commit
```

2. Configure NETCONF connection.

```
netconf
max-sessions 5
commit
```

3. Configure a NETCONF user.

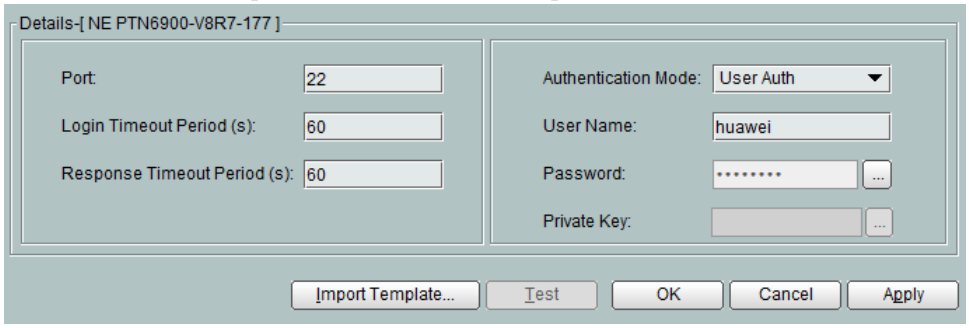
```
ssh user huawei authentication-type password
ssh user huawei service-type all
commit
```

4. Disable SNETCONF.

```
snetconf server enable
rsa local-key-pair create
1024
commit
quit
```

Step 2 Perform the following operations to set NETCONF parameters on the U2000:

1. Select a desired V8 NE in the Main Topology.
2. Choose **Administration** > **NE Communicate Parameter** > **NETCONF Parameter Template Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NETCONF Parameter Template Management** from the main menu (application style).
3. click **Create**. In the dialog box that is displayed, set **Template Name**, and click **OK**.
4. Select the created template. Then, set associated parameters in the **Details** area.

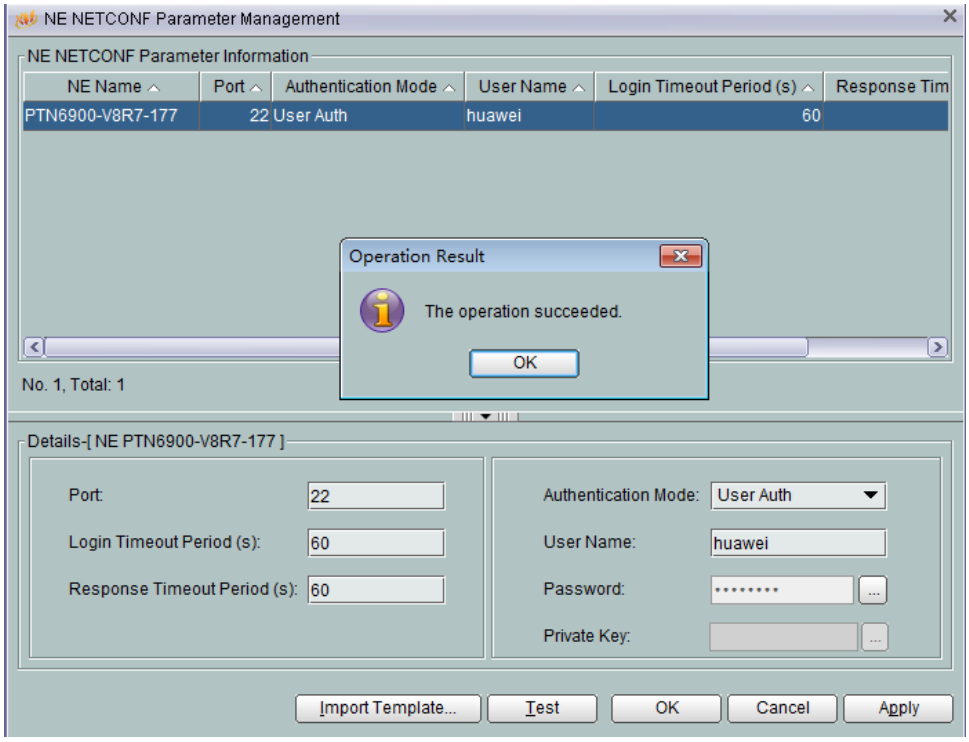


5. After setting all the parameters, click **OK**.

Step 3 Test whether NETCONF parameters set on the U2000 and NE sides are the same.

Copyright © Huawei Technologies Co., Ltd.

1. Select a desired V8 NE in the Main Topology.
2. Choose **Administration** > **NE Communicate Parameter** > **NE NETCONF Parameter Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE NETCONF Parameter Management** from the main menu (application style).
3. Click **Test** to check the test result.



----End

11.2 Data Synchronization Troubleshooting

This topic describes how to troubleshoot commonly seen data synchronization faults.

11.2.1 Failure to Synchronize Data and the Associated Error Message Displayed

Fault Symptom

Data synchronization fails and the system displays the associated error message.

Fault Analysis

- The privilege level and password on the U2000 are different from those on an NE.
- The network structure is complex and synchronizing other services results in the synchronization failure.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Ensure that the privilege level and password on the U2000 are the same as those on the NE.

1. Run the following command to view configurations on the NE: **display current-configuration**
2. Ensure that the parameters set on the U2000 are the same as those on the NE.

   For a V5 NE, the navigation path is as follows:

   On the U2000, set the same privilege level and password as those on the NE. In the **NE Explorer** of the NE, choose **System Management** > **NE Channel Management** > **VTY Service** and set the related parameters.

   For a V8 NE, the navigation path is as follows:

   In the NE Explorer of the NE, choose **Channel Management** > **VTY** > **VTY Configuration** from the Function Tree and set the related parameters.

   If the selected NE is a switch, perform the following operations:

   In the **NE Explorer**, choose **NE Channel Management** > **VTY Service** from the service tree.

Step 2 Data synchronization may fail if the structure of the live network is complex. Select the feature again and then synchronize data separately.

----End

11.2.2 A Message Is Displayed Indicating that Executing the SNMP Command Times Out During NE Synchronization

Fault Symptom

The U2000 displays the message indicating that executing the SNMP command times out during NE synchronization.

Fault Analysis

The timeout period and number of retries are improperly set for the SNMP command.

Procedure

Step 1 Set the timeout period and number of retry times for the SNMP command.

1. Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).
2. Double-click the corresponding SNMP record and set large valuesfor **Retries** and **Timeout Interval(s)**.

----End

Copyright © Huawei Technologies Co., Ltd.

11.2.3 A Message Is Displayed Indicating that the Length a Replied SNMP Packet Exceeds the Maximum Value During Data Synchronization

Symptom

Data synchronization fails, and the message "The length of the echo packet exceeds the maximum SNMP packet length" is displayed.

Cause Analysis

A user performs full synchronization or feature synchronization (such as OAM statistics and local MEP management) for a device. However, the device replies an SNMP packet whose length exceeds the maximum value.

Procedure

Step 1 Run the **snmp-agent packet max-size** command on the device to modify the maximum length for SNMP packets. It is recommended that the maximum length be set to the maximum value of the value range.

Step 2 Synchronize data again and check whether synchronization succeeds.

----End

11.3 QoS Management Troubleshooting

This describes how to rectify the common faults in QoS management.

11.3.1 Failed to Deploy the Applying Policy on the GE Interface

Fault Symptom

In the topology navigation tree, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.

For a V5 NE, perform the following operations:

In the service tree, expand **QoS Management**, and then click **Configure Interface QoS**. On the **Applying Policy** tab, deploy an applying policy on a GE interface. The system prompts operation failure.

For a V8 NE, perform the following operations:

Choose **QoS Management** > **QoS Management** > **Interface QOS** from the Function Tree. Then click **Create**. The **Interface QOS** dialog box is displayed. On the **Traffic Policy Application List** tab, deploy the applying policy on the GE interface. However, a message is displayed, indicating the operation failure.

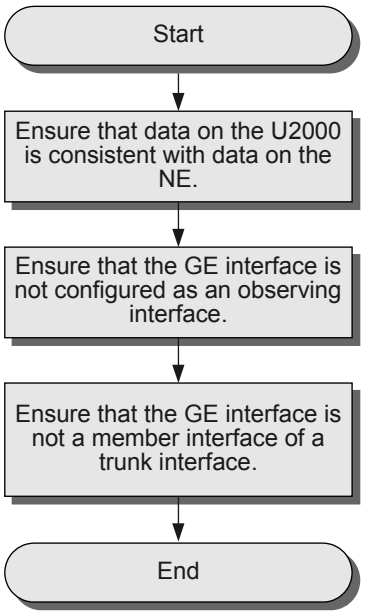
Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

- The data on the NE and U2000 is inconsistent.
- The GE interface is configured as an observing interface.
- The GE interface is a member interface of a trunk interface.

Troubleshooting Flowchart

Figure 11-1 Flowchart of troubleshooting the fault that the applying policy cannot be deployed on the GE interface



Procedure

Step 1 Make sure that the data on the NE and U2000 is consistent.

In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **Synchronize NE Data** on the shortcut menu.

Step 2 Make sure that the GE interface is not configured as an observing interface.

For a V5 NE, perform the following operations:

1. In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
2. In the service tree, expand **Security Management**, and then click **Configure Mirroring** > **Configure Observing Mirroring**.
3. On the **Configure Observing Mirroring** tab, click **Query**.
4. In the query result area, check whether the GE interface is configured as an observing interface.

   If so, delete the observing interface as required.

Copyright © Huawei Technologies Co., Ltd.

For a V8 NE, perform the following operations:

1. In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
2. Choose **Security Management** > **Network Monitor** > **Observing Interface** from the Function Tree.
3. In the **Observing Interface** window, click **Query**.
4. In the query result area, check whether the GE interface is configured as an observing interface.

   If so, delete the observing interface as required.

Step 3 Make sure that the GE interface is not a member interface of an Eth-Trunk interface.

For a V5 NE, perform the following operations:

1. In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
2. In the service tree, expand **Interface Management**, and then click **Interface Information**.
3. On the **Interface Information** tab, click **Query**.
4. In the query result area, click **Type** to display the interface list by interface type.
5. Select every record for which the value of **Type** is **Eth-Trunk**, and view the **Member Interface** tab. Check whether the GE interface is configured as an Eth-Trunk member interface.

   If so, delete the member interface as required.

For a V8 NE, perform the following operations:

1. In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
2. Choose **Interface Management** > **Trunk Interface** > **Trunk Interface** from the Function Tree.
3. In the **Trunk Interface** window, click **Query**.
4. 4. In the query result area, click **Trunk Interface Type** to display the interface list by interface type.
5. Select every record for which the value of **Trunk Interface Type** is **Eth-Trunk** and view the **Trunk Member Port** tab. Check whether the GE interface is configured as an Eth-Trunk member interface.

   If so, delete the member interface as required.

----End

11.3.2 Configurations Are Invalid Because of Problems with VTY Operation Rights

Fault Symptom

In QoS management, when you perform operations, such as creation and modification, that require delivering commands on devices, the system sometimes prompts "The Configuration is invalid."

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

- You do not have sufficient VTY operation rights.
- Your VTY operation rights need to be authenticated.

NOTE

The QoS module interacts with a device by delivering command lines through a VTY on the device. If a user does not have enough VTY operation rights to perform the related operation or fails to pass the authentication of VTY operation rights, the system prompts "The Configuration is invalid." If the VTYs are all used, wait several minutes and try again.

Procedure

Step 1 Check whether the VTY operation rights and authentication mode are correct.

In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then choose **Tool** > **Telnet** on the shortcut menu. Run the following command:

```
[Quidway] display user-interface
 Idx  Type     Tx/Rx      Modem Privi Auth
  0    CON 0    9600             3     N
* 1    VTY 0                     3     P
  2    VTY 1                     3     N
  3    VTY 2                     0     N
```

From the preceding information, you can see that the authority level of VTY 2 is **0**. In this case, if the U2000 uses this VTY to deliver QoS commands, the system will prompt "The Configuration is invalid."

The authentication mode of VTY 1 is **P**, indicating password authentication. If this authentication mode is not configured on the U2000, the system will also prompt "The Configuration is invalid" when the U2000 uses this VTY to deliver QoS commands.

Step 2 If the authority level is too low or the authentication mode is incorrect, modify the authority level or the authentication mode.

Run the following commands:

```
[Quidway] user-interface vty  0 4
[Quidway-ui-vty0-4] user privilege level 3
[Quidway-ui-vty0-4] authentication-mode none
```

NOTE

Because granting high authority levels may lead to security vulnerabilities, modify the authority level or the authentication mode according to the actual network security conditions.

----End

11.4 Troubleshooting LLDP Management

This describes how to rectify the common faults in LLDP management.

11.4.1 Failed to Synchronize LLDP Configurations

Fault Symptom

When you synchronize LLDP configurations, the system prompts the synchronization failure.

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

The MIB view is incorrectly configured on the device.

Procedure

Step 1 In the Main Topology, select the NE to be operated and right-click it. Then, choose **Tools** > **Telnet** from the shortcut menu.

Step 2 Run the following command to access the system view:

system-view

Step 3 Set NE-side parameters.

- If the NE uses SNMPv1/v2c, perform the following steps:
  1. Run the following command to start the SNMP Agent:

     snmp-agent
  2. Run the following command to set the SNMP version:

     snmp-agent sys-info version { { *v1* | *v2c* }* }
  3. Run the following command to set the name of the read community:

     snmp-agent community read *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*
  4. Run the following command to set the name of the write community:

     snmp-agent community write *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*
  5. Run the following command to add the ISO subtree to the view:

     snmp-agent mib-view included *view-name iso*
  6. Run the following command to enable the LLDP alarm function:

     snmp-agent trap enable feature-name LLDP

     NOTE

     After the LLDP alarm function is enabled, any of the following situation will trigger the equipment to send alarm information to the U2000:

     - The global LLDP function is disabled.
     - The LLDP management address is changed.
     - The neighbor information is changed. (No alarm information is generated on the local end if the neighbor management address is changed.)
- If the NE uses SNMPv3, perform the following steps:
  1. Run the following command to start the SNMP Agent:

     snmp-agent
  2. Run the following command to set the SNMP version:

     snmp-agent sys-info version *v3*
  3. Run the following command to set the SNMP version:

     snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]
  4. Run the following command to set the SNMP user group:

Copyright © Huawei Technologies Co., Ltd.

snmp-agent usm-user v3 *user-name* [**group** *group-name* | **acl** acl-name]

5. Run the following command to add a user to the SNMPv3 user group:

   snmp-agent mib-view included *view-name iso*

6. Run the following command to enable the LLDP alarm function:

   snmp-agent trap enable feature-name LLDP

   NOTE

   After the LLDP alarm function is enabled, any of the following situation will trigger the equipment to send alarm information to the U2000:

   - The global LLDP function is disabled.
   - The LLDP management address is changed.
   - The neighbor information is changed. (No alarm information is generated on the local end if the neighbor management address is changed.)

----End

11.5 Ethernet OAM Management Troubleshooting

This describes how to rectify the common faults in Ethernet OAM management.

11.5.1 When a User Performs the Ethernet Link OAM Loopback Test, the System Prompts That the Port Is in the Discovered State and the Loopback Test Cannot Be Started

Fault Symptom

Access the **Ethernet Link OAM** management module and perform the loopback test. The system prompts that the port is in the discovered state and the loopback test cannot be started. Check whether the peer EFM is enabled and whether the port is Up.

Fault Analysis

- EFM is not enabled on the peer device and the connected port.
- The local or peer port is Down.

Procedure

- If the connected peer device is a V5 router, service gateway, or switch, perform the following operations:
  1. In the Main Topology, right-click the peer device connecting to the local port and choose **NE Explorer** from the shortcut menu.
  2. Choose **Ethernet OAM Global Configuration** from the service tree.
     - Navigation path for a V5 router or service gateway:

       In the **NE Explorer**, choose **Reliability** > **OAM Management** > **Ethernet OAM Management** > **Global Ethernet OAM Configuration** from the service tree.
     - Navigation path for a switch:

Copyright © Huawei Technologies Co., Ltd.

In the **NE Explorer**, choose **Ethernet OAM Management** > **Global Ethernet OAM Configuration** from the service tree.

3. Check whether the **Enable EFM** check box is selected. If EFM is disabled, select the **Enable EFM** check box and click **Apply** to enable EFM on the device.

   NOTE

   After the enabling, perform the loopback test again. If the test cannot be performed, go to next steps.

4. Choose **Ethernet Link OAM** from the service tree.
   - Navigation path for a V5 router or service gateway:

     In the **NE Explorer**, choose **Reliability** > **OAM Management** > **Ethernet OAM Management** > **Ethernet Link OAM** > **Ethernet Link OAM** from the service tree.
   - Navigation path for a switch:

     In the **NE Explorer**, choose **Ethernet OAM Management** > **Ethernet Link OAM** from the service tree.
5. Check **EFM Protocol Enabling Status** of the port. If it is **Disable**, click **Set**.
6. In the **Set Port** dialog box, select **Enable Port EFM Protocol** and click **OK** to enable EFM on the port.
7. Click the **OAM Session** tab in the query result area. Then, click **Synchronize**. If the session status is **Detected**, the loopback test can be performed. If the session status is **Discovered**, go to step 8.
8. In the **NE Explorer**, choose **Interface Management** > **Interface Information** from the service tree. If the **Administrative Status** of the corresponding port is **Down**, right-click the port and choose **Up** from the shortcut menu. The **Administrative Status** of the port changes to **Up**.

- If the connected peer device is a V8 router, perform the following operations:
  1. In the Main Topology, right-click the peer device connecting to the local port and choose **NE Explorer** from the shortcut menu.
  2. In the **NE Explorer**, choose **Reliability Management** > **EFM** > **Global Attribute** from the function tree.
  3. Check whether **EFM Global Enable** is **true**. If not, select the record, right-click, and choose **true** from the shortcut menu. Then click **Apply** to enable EFM.

     NOTE

     After EFM is enabled, restart a loopback test. If the test fails, go to Step 4.
  4. In the **NE Explorer**, choose **Reliability Management** > **EFM** > **EFM Port Configuration** from the function tree.
  5. Check the port status. If the port status is Disable, select the record. In the **State** column, right-click and choose **Enable** from the shortcut menu, and click **Apply** to enable EFM on the port.
  6. Reselect the record. In the **Local FSM State** column, right-click and choose **Query Selected Record** from the shortcut menu. If the **Local FSM State** value is **Detect**, start the loopback test; otherwise, go to Step 7.
  7. In the **NE Explorer**, choose **Interface Management** > **Common Interface** > **Interface** from the function tree. If **Administrative Status** of the corresponding port

Copyright © Huawei Technologies Co., Ltd.

is **Administratively DOWN**, select the port, right-click, and choose **Administratively UP** from the shortcut menu to enable the port to go Up.

----End

11.5.2 During the Deletion of the MD, MA, Local MEP, or Remote MEP, the System Prompts That the Object to Be Deleted Does Not Exist

Fault Symptom

During the deletion of the MD, MA, local MEP, or remote MEP, the system prompts that the object to be deleted does not exist.

Fault Analysis

The data on the NMS side is inconsistent with that on the device side. The MD, MA, local MEP, or remote MEP does not exist on the device side. The following takes the deletion of the MD as an example. The deletion of other objects is the same as that of the MD.

Procedure

- For a V5 router, service gateway, or switch, perform the following operations:
  1. In the Main Topology, right-click the device to be operated and choose **NE Explorer** from the shortcut menu.
  2. Choose **MD Management** from the service tree.
     - Navigation path for a V5 router or service gateway:

       In the **NE Explorer**, choose **Reliability** > **OAM Management** > **Ethernet OAM Management** > **Ethernet Service OAM** > **MD Management** from the service tree.
     - Navigation path for a switch:

       In the **NE Explorer**, choose **Ethernet OAM Management** > **Ethernet Service OAM** > **MD Management** from the service tree.
  3. Right-click in the query result area and choose **Synchronize** from the shortcut menu.
  4. In the **Confirm** dialog box that is displayed, click **Yes**.
- For a V8 router, perform the following operations:

  In the Main Topology, right-click the device to be operated and choose **Synchronize NE Configuration Data** from the shortcut menu.

----End

11.6 MPLS-TP OAM Management Troubleshooting

This describes how to rectify the common faults in MPLS-TP OAM management.

Copyright © Huawei Technologies Co., Ltd.

11.6.1 Failed to send the SNMP message Is Displayed When MPLS-TP OAM Configurations Are Deployed

Fault Symptom

Failed to send the SNMP message is displayed when MPLS-TP OAM configurations are deployed. The cause needs to be identified.

Fault Analysis

- Though SNMP standard error codes are available, no standard for error reporting on NE configuration restriction is not available. The TPOAM module provides private error codes (extended error codes) for NEs of VRP V500R010C00.

  NOTE

  The procedure is applicable to NEs of VRP V500R010C00 and later versions and VRP V800R008C00 and later versions.

- If the MPLS-TP OAM configuration using Huawei NMS fails and **Failed to send the SNMP message** is displayed, enable the error code function to identify the cause.
- Using STelnet (if supported) to log in to the device is recommended. STelnet is more secure.

Procedure

Step 1 Log in to the NE that reports the error using Telnet/Stelnet.

Step 2 Run the **display snmp-agent extend error-code status** command to check whether the SNMP extended error code function is enabled.

If **enable** is displayed, this function is enabled. If **disable** is displayed, this function is disabled. Go to Step 3.

Step 3 Run the **system-view** command to access the system view.

Step 4 Run the **snmp-agent extend error-code enable** command to enable the SNMP extended error code function.

By default, NEs send SNMP standard error codes. SNMP sends extended error codes to the NMS only if the extended error code function is enabled.

Step 5 Reproduce the error reporting process to identify the cause. After the fault is rectified, perform the following operations to restore the configurations to prevent the NMS from another vendor from configuring Huawei devices using SNMP and enable the NMS to recognize the private error codes returned by Huawei devices.

1. Run the **system-view** command to access the system view.
2. Run the **undo snmp-agent extend error-code enable** command to disable the SNMP extended error code function.

----End

11.7 Change Audit Troubleshooting

This topic describes how to troubleshoot change audit.

Copyright © Huawei Technologies Co., Ltd.

11.7.1 In Change Audit, a User Cannot View and Compare the Configuration Files

Fault Symptom

In Solaris, when a user views and compares the configuration files in change audit, the system prompts that the transmission of SFTP files fails.

Fault Analysis

- The SFTP service is disabled on the NMS server side.
- The SFTP user is not created on the NMS server side, or the user directory is incorrect.
- The SFTP configurations are incorrect on the NMS client side.

Procedure

Step 1 Make sure that the SFTP service is enabled on the server side.

1. Run the **svcs -a |grep ssh** command to check whether the openssh process is running in the Solaris system.
   - If a message similar to online 10:50:00 svc:/network/ssh:default is returned, it indicates that the openssh process is in running state.
   - If the openssh process is not in running state, perform the following steps.
2. In the **/etc/ssh/sshd_config** file, change **PasswordAuthentication no** to **PasswordAuthentication yes**. In the same file, change **PermitRootLogin no** to **PermitRootLogin yes**.
3. Run the **svcadm refresh svc:/network/ssh:default** command.

Step 2 Make sure that the SFTP user is created on the server side and the user directory is correctly configured.

1. If the SFTP user is not created, run the following commands to create one:

   useradd -d *userhome username*

   passwd *username*

   NOTE

   All local UNIX accounts can access the Solaris system through SFTP.

   - **userhome** indicates the user directory. Normally, the default directory **/tftpboot** for the DC to store the configuration files is used as the user directory.
   - **username** indicates the user name.
2. If the SFTP user is created, you need to make sure that the user directory is correct, that is, the directory for the DC to store the configuration files can be accessed through SFTP.

Step 3 Make sure that the SFTP configurations on the client are correct.

1. Log in to the NMS client.
2. Choose **Administration** > **Settings** > **FTP Account Information Management** from the main menu (traditional style); alternatively, double-click **System Management** in

Copyright © Huawei Technologies Co., Ltd.

Application Center and choose **Settings** > **FTP Account Information Management** from the main menu (application style).

3. Set the parameters in the dialog box.

   NOTE

   To change the password for the xFTP user, select **Change password** and enter a new password in the text box provided.

4. Conduct either of the following test to verify the settings as required. If the verification fails, you must reset the parameters.
   - Click **Test FTP** to verify FTP-related settings.
   - Click **Test SFTP** to verify SFTP-related settings.
5. Click **OK**.
6. Return to the **Change Audit** tab. Check whether the operations of viewing and comparing the configuration files succeed.

----End

11.8 Link Troubleshooting

This topic describes the method of troubleshooting common link faults.

11.8.1 Links Displayed in Red on the U2000

Symptom

Links are displayed in red on the U2000.

Possible Causes

- Data on the U2000 side is inconsistent with data on the NE side.
- The device version does not match the U2000 version.

Procedure

Step 1 Ensure that data on the U2000 side is consistent with that on the NE side.

1. Set Telnet/STelnet parameters. For details, see Setting Telnet/STelnet Parameters with a Template and Manually Setting Telnet/STelnet Parameters.
2. Synchronize NE data.

   In the topology view or navigation tree, select the NE to be operated, right-click, and choose **Synchronize NE Configuration Data** from the shortcut menu.

Step 2 Ensure that the device version matches the U2000 version.

The port status displayed on the U2000 is **Down**, but the port status on the device is normal. The possible cause is that the device version does not match the U2000 version. Upgrade the device version to the latest one.

Step 3 If the problem persists, contact Huawei engineers.

----End

Copyright © Huawei Technologies Co., Ltd.

11.8.2 Failure to Automatically Discover Links Between Equipment

Symptom

The U2000 fails to automatically discover links between equipment.

Possible Causes

- The LLDP function is not enabled on equipment.
- NE data is not synchronized to the U2000.

NOTE

This case applies to routers and switches only.

Procedure

Step 1 Ensure that the equipment-side parameters are configured correctly.

- The related parameters must be set on the equipment.
- The data of the equipment must be synchronized to the U2000.
- The equipment must support the ability to configure LLDP globally.

Step 2 Configure LLDP Globally.

For a V5 NE, service gateway, S9300/S7700 switch, or S2300/S3300/S5300/S6300/S2700/S3700/S5700/S6700/CX200D switch, perform the following operations:

1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
2. Choose **LLDP Global Configuration** from the service tree.
   - Navigation path for V5 routers and multi-service gateway:

     In the NE Explorer, choose **System Management** > **LLDP Management** > **LLDP Global Configuration** from the service tree.
   - Navigation path for the S9300/S7700 series switch, S2300/S3300/S5300/S6300/S2700/S3700/S5700/S6700/CX200D series switch:

     In the NE Explorer, choose **LLDP Management** > **LLDP Global Configuration** from the service tree.
3. Set parameters such as **Management IP Address**, **Interval for Message Transmission**, and **Message Multiple**.
4. Click **Apply**.

For a V8 NE, perform the following operations:

1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
2. In the NE Explorer, choose **Function Tree** > **System Management** > **LLDP** > **Global Attribute**.
3. Set parameters such as **Management Address**, **LLDP Message Tx Interval(Second)**, and **LLDP Message Tx Hold Multiplier**.
4. Click **Apply**.

Step 3 Configure LLDP on Interfaces.

Copyright © Huawei Technologies Co., Ltd.

For a V5 NE, service gateway, S9300/S7700 switch, or S2300/S3300/S5300/S6300/S2700/S3700/S5700/S6700/CX200D switch, perform the following operations:

1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
2. Choose **LLDP Interface Configuration** from the service tree.
   - Navigation path for V5 routers and multi-service gateway:

     In the NE Explorer, choose **System Management** > **LLDP Management** > **LLDP Interface Configuration** from the service tree.
   - Navigation path for the S9300/S7700 series switch, S2300/S3300/S5300/S6300/S2700/S3700/S5700/S6700/CX200D series switch:

     In the NE Explorer, choose **LLDP Management** > **LLDP Interface Configuration** from the service tree.
3. On the **LLDP Interface Configuration** tab, click **Query**. The interfaces supporting LLDP are displayed in a list.
4. Right-click one or more interfaces that run LLDP and choose **Enable** or **Disable** from the shortcut menu to apply the interface configurations to the equipment.
   - If the status of the interfaces is **Enabled**, you can choose only **Disable** from the shortcut menu.
   - If the status of the interfaces is **Disabled**, you can choose only **Enable** from the shortcut menu.
   - If both **Enabled** and **Disabled** interfaces are selected, you can choose either **Enable** or **Disable** from the shortcut menu. Then, the status of all the interfaces becomes the same as the selected status.

For a V8 NE, perform the following operations:

1. Right-click the NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
2. In the NE Explorer, choose **Function Tree** > **System Management** > **LLDP** > **LLDP Interface**.
3. On the **LLDP Interface** tab, click **Query**. The interfaces supporting LLDP are displayed in a list.
4. Select one or more interfaces on which LLDP is to be configured, right-click, and choose **txAndRx**,**txOnly**,**rxOnly** or **disabled** from the shortcut menu to apply the LLDP interface configurations to the equipment.

Step 4 Perform synchronization on the U2000 client.

Right-click the NE icon on the Main Topology and choose **Synchronize NE Configuration Data** from the shortcut menu.

----End

Copyright © Huawei Technologies Co., Ltd.

11.9 Some Information Is Not Displayed in the U2000 NE Explorer and Data Is Not Correctly Displayed on the NE Panel

Symptom

- NE data is not synchronized; as a result, the device panel cannot be displayed on the U2000.
- Some interfaces of the NE are not displayed for selection during service configuration.
- The NE Panel on the U2000 cannot be viewed or the NE Panel fails to display newly registered boards.
- The U2000 cannot display the NE panel or the NE panel status is unknown.
- The NE panel cannot be opened on the U2000 and the error code 1107525648 is displayed.
- The NE Explorer becomes abnormal after a VRPv8-based NE is added.

Possible Causes

- Data on the U2000 side is inconsistent with data on the NE side.
- After NE panel data synchronization fails, a message is displayed indicating that SNMP communication times out.
- NAT mapping is not configured for the NAT network.
- One or more NEs are damaged.
- The Windows firewall is enabled but the FTP port 21 and SFTP 22 are disabled.
- FTP port 21 is filtered between the U2000 and NEs.
- The xFTP monitoring process is not running properly.

  NOTE

  This case applies only to V100R006C02 and earlier versions.
- Multiple network adapters cause the panel fault.
- NE data is not synchronized.
- Firewall blocking causes the panel display failure.
- NETCONF parameter settings on the U2000 side are inconsistent with those on the NE side.
- No operation set is added.
- The NE name has special characters.
- The router NE management process service is not started.
- The Netconf parameter is incorrectly displayed on the NE Panel because of incorrect parameter settings.
- Port 13154 on the VMF has been used, leading to a failure to start processes.

Procedure

Step 1 Ensure that data on the U2000 side is consistent with that on the NE side.

Copyright © Huawei Technologies Co., Ltd.

1. Set Telnet/STelnet parameters. For details, see Setting Telnet/STelnet Parameters with a Template and Manually Setting Telnet/STelnet Parameters.
2. Synchronize NE data.

   In the topology view or navigation tree, select the NE to be operated, right-click, and choose **Synchronize NE Configuration Data** from the shortcut menu.

Step 2 After NE panel data synchronization fails, a message is displayed indicating that SNMP communication times out.

1. Right-click the desired NE in the Main Topology and choose **NE Explorer** from the shortcut menu.
2. Choose **Device Management** > **NE Panel** from the navigation tree.
3. Click **Synchronize** to synchronize NE panel data to the U2000.

If a message is displayed indicating that SNMP communication times out after data synchronization fails, reset the SNMP timeout period and the number of retry times.

1. Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).
2. Double-click the corresponding SNMP record and set large values for **Retries** and **Timeout Interval**.

Step 3 NAT mapping is not configured for the NAT network.

Configure NAT mapping. For details, see **Router and Switch Network Management** > **Network Deployment** > **IP Network Commissioning** > **Optional Commissioning Items** > **Configuring NAT Mapping**.

Step 4 One or more NEs are damaged.

1. Delete a damaged NE.

   For details, see **Working with the NMS** > **Topology Management** > **Maintaining a Network Topology View** > **Deleting Topology Objects** > **Deleting NEs**.
2. Add the NE again.

   For details, see **Working with the NMS** > **Topology Management** > **Creating NEs** > **Creating a Single NE**.

Step 5 The Windows firewall is enabled but the FTP port 21 and SFTP 22 are disabled.

- Enable the Windows firewall and FTP port 21 and SFTP 22.

  For details, see **Installation and Commissioning** > **Single-Server System Software Installation Guide (Windows)** > **FAQs** > **Install the U2000 Software Exception Processing** > **Failure to Log In to the U2000 Server from a U2000 Client**.
- Disable the Windows firewall.

Step 6 FTP port 21 is filtered between the U2000 and NEs.

Enable FTP port 21.

For details about the operation, see **step 5**.

Copyright © Huawei Technologies Co., Ltd.

Step 7 The xFTP monitoring process is not running properly.

1. Log in to the U2000 System Monitor.
2. Click the **Process Monitor** tab and select **XftpDm**.
3. Select **Topology Process**, right-click, and then choose **Start Process** from the shortcut menu.

   NOTE

   The **Confirm** dialog box is displayed, showing the processes that rely on and will be started along with the selected process. To start the process, click **Yes**.

Step 8 Multiple network adapters cause the panel fault.

For details about the operation, see **step 3**.

Step 9 NE data is not synchronized.

For details, see **Router and Switch Network Management** > **Network Deployment** > **IP Network Commissioning** > **Synchronizing NE Data**.

If the panel is not displayed after NE data synchronization, restart the U2000 client.

Step 10 Firewall blocking causes the panel display failure.

Run the **ftp client-source -a** command on the device side to set the source address of the device that functions as the FTP client.

NOTE

Example:

Set the FTP client's source address to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the FTP client to 10.1.1.1.
```

Step 11 NETCONF parameter settings on the U2000 side are inconsistent with those on the NE side.

1. Configure NETCONF parameters on the NE side. For details, see the following commands.

Copyright © Huawei Technologies Co., Ltd.

```
#
sysname netconf-agent
#
aaa
 local-user client001 password cipher %$%$U|,(X4rFC)8izE%,QHz:$(|s%$%$
 local-user client001 service-type ssh
 local-user client001 user-group manage-ug
#
interface GigabitEthernet0/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.255
#
snetconf server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type snetconf
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

2. Configure NETCONF parameters on the U2000 side.

   For details, see **Router and Switch Network Management** > **Network Deployment** > **IP Network Commissioning** > **Configuring the Communication Between the U2000 and NEs** in the U2000 Help.

3. Synchronize NE data.

   In the topology view or navigation tree, select the target NE, right-click, and choose **Synchronize NE Configuration Data** from the shortcut menu.

Step 12 Add an operation set.

For details, see **Working with the NMS** > **Security Management** > **Managing User Rights** > **Getting to know Operation Rights Management** > **Operation and Operation Set** in the U2000 Help.

Step 13 The NE name has special characters.

1. In the Main Topology, select the VRPv8-based NE, right-click, and choose **Properties** from the shortcut menu.
2. In the **Properties** dialog box, modify **Name**.
3. Click **OK**.

Step 14 The router NE management process service is not started.

Log in to the System Monitor and start the router NE management process.

1. Log in to the System Monitor.
2. In the System Monitor window, click the **Service Monitor** tab.
3. Select the router NE management service, right-click, and choose **Start the Service** from the shortcut menu.

Copyright © Huawei Technologies Co., Ltd.

Step 15 The Netconf parameter is incorrectly displayed on the NE Panel because of incorrect parameter settings.

For details about how to set the Netconf parameter, see **Router and Switch Network Management** > **Network Deployment** > **IP Network Commissioning** > **Configuring the Communication Between the U2000 and NEs**.

Step 16 Port 13154 on the VMF has been used, leading to a failure to start processes.

Stop the processes that use port 13154.

1. Run the following command to view the processes that use port 13154:
   netstat -an | grep 13154
2. Run the following command to view qualified processes:
   lsof -i UDP@**:13154**
3. Run the following command to stop the process that uses port 13154:
   kill - 9 [PID]

----End

11.10 Failed to Telnet to an NE by Right-clicking the NE Icon on the Main Topology

Symptom

Select an NE in the Main Topology, right-click, and choose **Tools** > **Telnet** from the shortcut menu.

- The Telnet window disappears immediately after being displayed.
- The message "Proxy errors: SOCKS proxy did not accept our authentication" is displayed.

Possible Causes

- The proxy service access control list (ACL) was not configured.
- The interface is unavailable.

Procedure

Step 1 Ensure that the proxy service ACL has been configured.

1. Choose **Administration** > **NMS Security** > **Proxy Service ACL** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **Settings** > **Proxy Service ACL** from the main menu (application style).
2. In the dialog box that is displayed, click **Add**.
3. In the dialog box that is displayed, set **IP address or network segment** to the IP address of the client and **Operation** to **Accept**.
4. Click **OK**.
5. Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Ensure that interfaces are available.

Run the **netstat -ano|findstr:** *interface number* command in the CLI. If interfaces are unavailable, contact Huawei technical personnel.

Step 3 If the problem persists, contact Huawei engineers.

----End

11.11 An NE5000E Is Displayed Abormally After Being Upgraded from a Single Chassis to a Cluster

Symptom

After an NE5000E is upgraded from a single chassis to a cluster, the U2000 reports a cluster problem.

Possible Causes

After the NE5000E is upgraded from a single chassis to a cluster, the original single chassis information is not deleted from the U2000.

Procedure

Step 1 Delete the NE5000E from the U2000 and then re-add it to the U2000.

----End

11.12 Failed to Change an NE Interface Description

Symptom

Failed to change an NE interface description.

Possible Causes

The SNMP parameters on the NE are inconsistent with those on the U2000.

Procedure

Step 1 Choose **Service** > **PWE3 Service** > **Manage PWE3 Service** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **PWE3 Service** > **Manage PWE3 Service** from the main menu (application style).

Step 2 Click **Reset**.

Copyright © Huawei Technologies Co., Ltd.

Step 3 On the **SNMPv2 Parameters** tab of the **Default Access Protocol Parameters** dialog box, double-click in the **Set Community** field to change the community name. Ensure that the community name on the NE is the same as that on the U2000.

----End

11.13 Failure to Create a Test Case on the NE Side

Symptom

The U2000 displays an error message indicating a failure to create a test case on the NE side.

Possible Causes

The SNMP write community name on the U2000 side is different from that on the NE side.

Procedure

Step 1 Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).Check the settings of the SNMP parameters of the NE on the U2000.

Step 2 Log in to the NE and run the **display snmp-agent community read/write**command to check whether the read community and write community of the SNMP protocol (SNMPv1, SNMPv2c, and SNMPv3) on the NE are the same as those on the U2000.

NOTE

Using SNMPv3 is recommended because of its higher security than SNMPv1 and SNMPv2c.

Step 3 Change the parameter settings to ensure that the SNMP parameter settings on the NE and the U2000 are the same.

----End

11.14 IP E2E Troubleshooting

This topic describes how to troubleshoot commonly seen IP E2E faults.

11.14.1 Services Created by a User Cannot Be Viewed by Other Users After the U2000 Is Upgraded

Problem Description

User A could not view the services created by user B after the U2000 was upgraded.

Possible Cause

This problem occurs because the service authorization function is enabled. If user A wants to view services created by user B after this function is enabled, you must log in to the system as

Copyright © Huawei Technologies Co., Ltd.

the admin user to authorize services for user A. If the service authorization function needs to be disabled, a formal license is required.

The confirmation with the field engineers shows that a temporary license is used after the U2000 is upgraded. The service authorization function is enabled by default and cannot be disabled. This problem can be addressed by applying for a formal license.

Procedure

Apply for a formal license and update the license used on the U2000.

11.14.2 Unavailability of Importing/Exporting Service Options

Problem Description

- A user chooses **Service** > **PWE3 Service** > **Manage PWE3 Service** from the main menu. In the window that is displayed, the user selects one or multiple services, right-clicks, and attempts to choose **Save** > **Export Service** from the shortcut menu, but the **Export Service** option is greyed out.
- A user chooses **Service** > **Tunnel** > **Manage Tunnel** from the main menu. In the window that is displayed, the user selects one or multiple services, right-clicks, and attempts to choose **Save** > **Export Service** from the shortcut menu, but the **Export Service** option is greyed out.
- When a user attempts to choose **Service** > **Import Service** > **Import Packet Service** from the main menu, the user finds that the **Import Packet Service** option is greyed out.

Possible Cause

- The function control item for **Import/Export IP Service** is unavailable in the U2000 license file.
- The prerequisites for importing/exporting services are not met.
- The selected NE or service does not support service exporting.

Procedure

1. Apply for a formal license and update the existing license.
2. Check whether the prerequisites for importing/exporting services are met.
   - Prerequisites for importing/exporting services: The Excel macro can be used when the exported file is with the version of Office 2007 or later. You must disable Excel macro if the exported file is with the version earlier than Office 2007. If an error message is displayed when opening an Excel file, you can close the dialog box and then modify the Excel file. Macro cannot be used after an error message is displayed.
   - Prerequisites for importing services:
     - Importing services requires that you are an NMS user with "Maintenance Group" rights or higher.
     - If the data about tunnel protection groups needs to be imported, ensure that the related tunnels exist, the tunnel names are unique, and the tunnels are not used by other protection groups. If any of the preceding requirements is not met, errors are reported on the U2000.

Copyright © Huawei Technologies Co., Ltd.

- Prerequisites for exporting tunnel protection groups: Associated tunnel protection information is exported only if all the tunnels in the protection group are selected and configured with OAM.

3. Check whether the selected NE or service supports service exporting.
   - NEs and services supporting the exporting of tunnel services and tunnel protection groups:
     - Only tunnels for which **Signaling Type** is **Static CR** or **RSVP TE** are supported.
     - Type of NEs supporting service exporting: Routers and PTN NEs support the exporting of RSVP TE tunnel services. Routers, PTN NEs, RTN NEs, and hybrid MSTP NEs support the exporting of static CR tunnel services.
     - The data about unterminated services cannot be imported.
   - NEs and services supporting the exporting of PWE3 services:
     - Only the ATM, CES, and Ethernet services can be exported on the NMS.
     - The data about PWE3 services for which switching nodes are configured cannot be imported .
     - Supported NEs include PTN, RTN, hybrid MSTP NEs.

11.14.3 The Create PWE3 Service Window Flickers

Problem Description

In the left pane of the Create PWE3 Service window, scroll boxes keep appearing and then disappearing, making the window flicker.

Possible Cause

The separator has been dragged to the left too much. In some resolution, the window cannot be adapted correctly for display.

Procedure

Drag the separator to the right until the window stops flickering.

11.14.4 A Label Allocation Conflict Occurs During the Creation of a Tunnel and a PWE3 Service

Symptom

The incoming label automatically allocated by the U2000 conflicts with the outgoing label automatically allocated by the U2000 during the creation of a tunnel and a PWE3 service.

Possible Causes

The NE data is inconsistent with that on the U2000.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Upload NE data.

1. Right-click an NE in the Main Topology and choose **Upload** from the shortcut menu.
2. For NEs whose **Logged in** is **Yes**. The **NE Configuration Data Management** window is displayed, and a **Confirm** dialog box is displayed.

   NOTE

   For NEs whose **Logged in** is **No**. Choose **Administration** > **NE Security Management** > **NE Login Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **NE Login Management** from the main menu (application style). In the window that is displayed, log in to the NEs.
3. Click **OK** in the **Confirm** dialog box.
4. Click **Close** in the **Operation Result** dialog box.

Step 2 Re-create the tunnel and PWE3 service after uploading NE data.

----End

11.14.5 A PWE3 Service Automatically Discovered by the U2000 Is in the Discrete State

Symptom

A PWE3 service automatically discovered by the U2000 is in the discrete state.

Possible Causes

The PWE3 service has duplicate LSR IDs.

Procedure

Step 1 On the NE Explorer, choose **MPLS Management** > **MPLS Configuration** > **Global MPLS Configuration** from the Service Tree.

Step 2 In the **Global MPLS Configuration** window, clear the **Enable MPLS** check box.

Step 3 Modify the **LSR ID** value.

Step 4 Perform automatic service discovery again.

----End

11.14.6 How to Delete a PWE3 Service from an Offline NE

Symptom

The U2000 cannot delete a PWE3 service from an NE.

Possible Causes

The NE is offline.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Service** > **PWE3 Service** > **Manage PWE3 Service** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **PWE3 Service** > **Manage PWE3 Service** from the main menu (application style).

Step 2 In the **Manage PWE3 Service** window, select the PWE3 service to be deleted, right-click, and choose **Deploy and Enable** > **Undeploy** from the shortcut menu. The PWE3 service is undeployed.

Step 3 In the **High Risk** dialog box that is displayed, select **I have read the prompt and have a good idea of the affection for the service caused by this operation.** and click **Yes**.

Step 4 Select the PWE3 service again, right-click, and choose **Delete Service** > **Delete from Network Side** from the shortcut menu. The PWE3 service is deleted from the network side.

Step 5 Select the offline NE's peer NE and access its NE Explorer.

Step 6 In the Service Tree of the NE Explorer, choose **VPN Management** > **PWE3 Management** > **PW Management**.

Step 7 In the **PW Management** window, select the PWE3 service, right-click, and choose **Delete** from the shortcut menu.

Step 8 In the **Confirm** dialog box that is displayed, click **Yes**.

----End

11.14.7 The U2000 Fails to Query Service Access Interfaces

Symptom

The U2000 fails to query service access interfaces.

Possible Causes

Data is inconsistent between the U2000 and NE sides.

Procedure

Step 1 Choose **Service** > **L3VPN Service** > **Manage L3VPN Service** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **L3VPN Service** > **Manage L3VPN Service** from the main menu (application style).

Step 2 In the **Manage L3VPN Service** window, select a service, right-click, and choose **Delete Service** > **Delete from Network Side** from the shortcut menu. The service is deleted from the network side.

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

Step 4 Choose **Service** > **Search for Service** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Service** > **Search for Service** from the main menu (application style).

Copyright © Huawei Technologies Co., Ltd.

Step 5 In the **Search for Service** dialog box, select the L3VPN service type in the **Discover Service** area and click **Start**.

Step 6 On the **Add Service** tab of the **Discovery Result** tab, click **Jump Service**. Then, query service access interfaces again.

----End

Copyright © Huawei Technologies Co., Ltd.

12 Troubleshooting for the Access Domain

About This Chapter

This topic describes how to locate and troubleshoot common faults for access NEs managed by the U2000 as well as providing some typical cases.

12.1 Failure to Make Added MDUs Online
This topic describes how to troubleshoot the fault wherein the newly added MDUs cannot go online.

12.2 Failure to Add NEs
This topic describes how to locate and troubleshoot the fault wherein NEs fail to be added to the U2000 as well as providing some typical cases.

12.3 Failure to Display NE Alarms After an Active/Standby Switchover in a Veritas High Availability System

12.4 Message "NE license authority failed" Displayed During NE Creation

Copyright © Huawei Technologies Co., Ltd.

12.1 Failure to Make Added MDUs Online

This topic describes how to troubleshoot the fault wherein the newly added MDUs cannot go online.

Fault Description

The newly added MDUs cannot go online properly. Icons of the MDUs in the Layer 2 topology do not turn green.

Fault Location

This fault occurs because no service virtual port is configured on the OLT to which the MDUs are connected.

Troubleshooting

Prerequisites

- The VLAN to which the service virtual port will be added is available.
- The VLAN has been configured with an upstream port.
- The MEF IP traffic template has been configured properly.

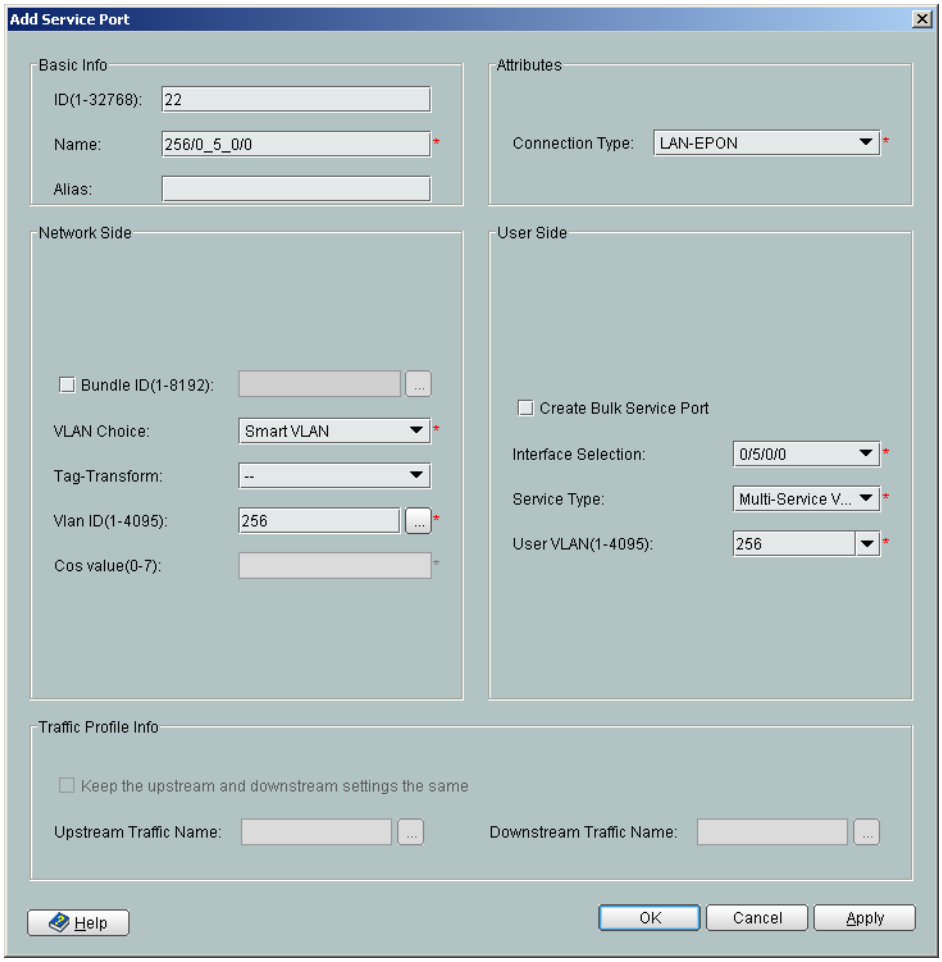
Procedure

NOTE

The following configurations use the EPON as an example.

1. In the Main Topology, double-click the required NE in the navigation tree, or right-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **EPON** > **EPON Management** from the navigation tree.
3. On the **EPON ONU** tab page, specify the filter criteria or click **Find** to display required EPON ONUs.
4. In the EPON ONU list, select an offline MDU.
5. In the lower pane, click **>>** to display the hidden tab pages.
6. Click the **ServicePort Info.** tab. Right-click and choose **Add** from the shortcut menu
7. In the dialog box that is displayed, configure the service virtual port.

Copyright © Huawei Technologies Co., Ltd.



8. Click **OK**.

12.2 Failure to Add NEs

This topic describes how to locate and troubleshoot the fault wherein NEs fail to be added to the U2000 as well as providing some typical cases.

12.2.1 Fault Location for a Failure to Add NEs

This topic describes how to locate the fault wherein NEs fail to be added to the U2000.

Fault Location

1. Check whether the U2000 processes are in the normal state.
2. Check whether the network functions properly.
3. Check whether the SNMP protocol parameter settings on the U2000 and NEs are consistent.
4. Reproduce the fault and obtain packet headers. Check whether NEs return response messages in SNMP packets. If response messages are returned, check for what operations (successful or failed) these messages are returned.
5. Collect message logs of processes.

Copyright © Huawei Technologies Co., Ltd.

6. Collect run logs of processes.
7. Collect NE information in databases.
8. Restore the level of run logs in the log component configuration file.

12.2.2 Troubleshooting for a Failure to Add NEs

This topic describes how to troubleshoot the fault wherein NEs fail to be added to the U2000.

Context

This topic uses the Solaris server as an example.

Procedure

Step 1 Record when the fault occurs, on which GUI, what error message is displayed, and in what sequence the operations are performed.

Step 2 Record the U2000 version, NE version, and NE IP address.

Step 3 Modify the level of run logs in the log component configuration file.

1. Run the following commands to view the log level:

   #**cd /opt/U2000/server/cbb/frame/conf/**

   #**more logconfig.cfg**

   The following information is displayed:

   ```
   ......
   DevLogLevel = 4
   ......
   ```

   NOTE

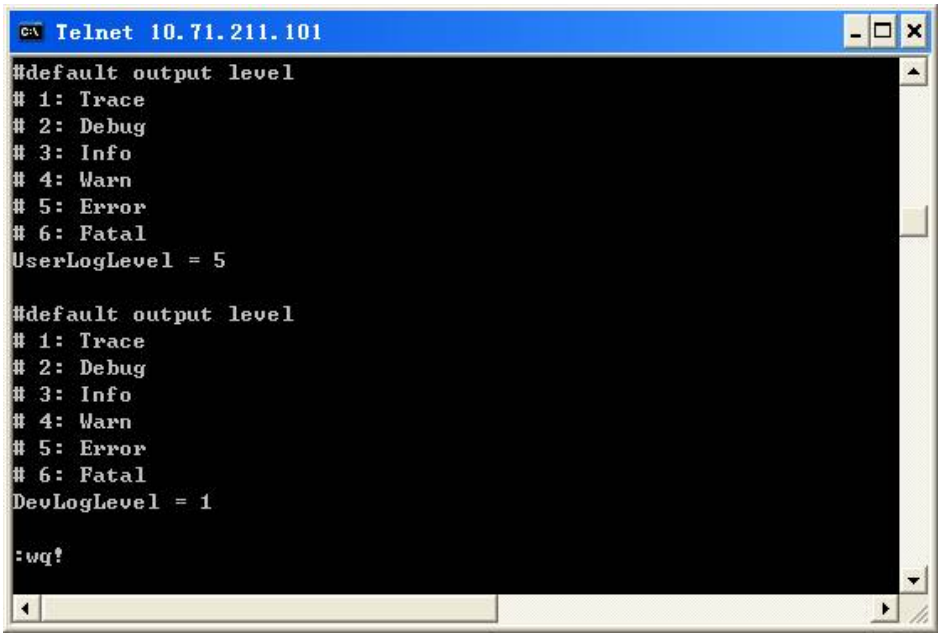
   Press **Ctrl+C** to exit.

2. Run the following command to modify the log level:

   #**vi logconfig.cfg**

3. **DevLogLevel = 4** is displayed. Select **4** in **DevLogLevel = 4**, press **x** and **A**, enter **1**, and then press **Esc**. Then, enter **:wq!** and press **Enter**, as shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.



4. Run the following command to verify the modification:

   #**more logconfig.cfg**

   The following information is displayed if the log level is successfully modified:

   ```
   ......
   DevLogLevel = 1
   ......
   ```

   NOTE

   Press **Ctrl+C** to exit.

Step 4 Reproduce the fault and obtain packet headers.

The following is an example describing how to obtain packet headers.

Run the following command to obtain packet headers transmitted between the U2000 server and the NE whose IP address is 10.71.212.13:

#**snoop -o /export/From13.cap -v ip 10.71.212.13**

NOTE

Press **Ctrl+C** to stop packet headers capture after capturing sufficient packet headers.

Step 5 Collect message logs of processes.

- Process logs: /opt/U2000/server/var/logs/mrblog/iMAPBase_p30*.*
- mdp logs: /opt/U2000/server/var/logs/mrblog/iMAPMrb_p2_*.*
- dam logs: /opt/U2000/server/var/logs/mrblog/iMAPMrb_p3000_*.*
- topo logs: /opt/U2000/server/var/logs/mrblog/iMAPMrb_p51_*.*
- topo log: /opt/U2000/server/var/logs/iMAP.eam_agent.trace

Step 6 Collect run logs of processes.

- /opt/U2000/server/log/Develop/BmsGdm_*/BootLog_*.log
- /opt/U2000/server/log/Develop/BmsGdm_*/BootLog_*.log

Copyright © Huawei Technologies Co., Ltd.

Step 7 Collect NE information in databases.

The following is an example describing how to collect NE information in the **bms_gdm_DeviceTab**, **TSNode**, and **tbl_ne** database tables on a U2000 running Solaris.

Run the following commands to collect the required information:

#**. /opt/U2000/server/svc_profile.sh**

isql -SDBSVR -Usa

NOTE

Enter the database administrator user password as prompted.

In order to enhance the security of the database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

1>**select * from BMSDB..bms_gdm_DeviceTab**

2>**go >/opt/U2000/bms_gdm_DeviceTab.txt**

NOTE

In the entered command, there is a space between go and >.

3>**select * from imaptmdb..TSNode**

4>**go >/opt/U2000/TSNode.txt**

NOTE

In the entered command, there is a space between go and >.

5>**select * from imapeamdb..tbl_ne**

6>**go > /opt/U2000/tbl_ne.txt**

NOTE

In the entered command, there is a space between go and >.

7>**quit**

Run the following commands to view the required information:

#**pwd**

```
/opt/U2000
```

#**ls**

```
bms_gdm_DeviceTab.txt TSNode.txt tbl_ne.txt
```

Step 8 Restore the level of run logs in the log component configuration file.

1. Run the following commands to view the log level:

   #**cd /opt/U2000/server/cbb/frame/conf/**

   #**more logconfig.cfg**

   The following information is displayed:

   ```
   ......
   DevLogLevel = 1
   ......
   ```


Copyright © Huawei Technologies Co., Ltd.

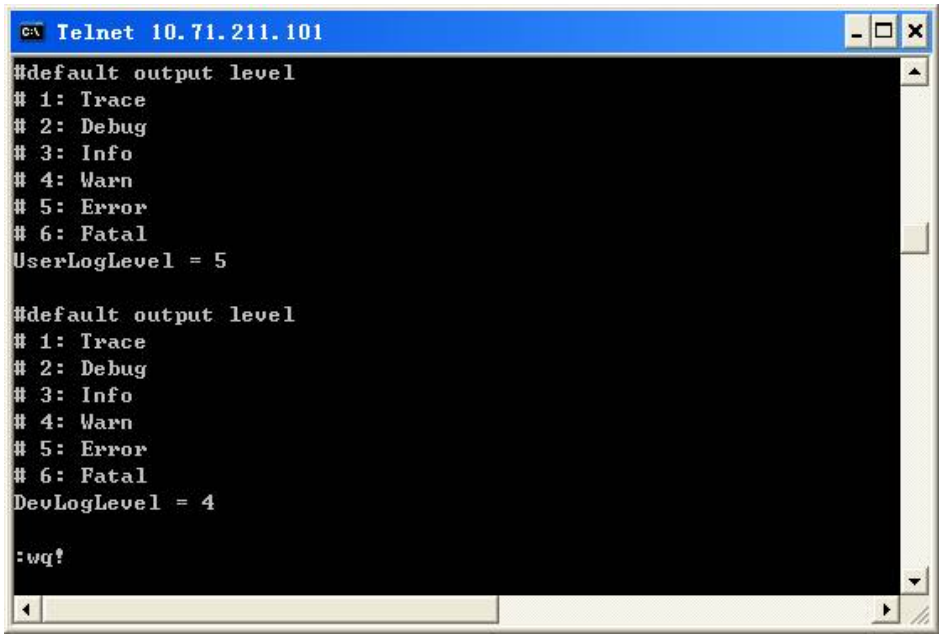
NOTE

Press **Ctrl+C** to exit.

2. Run the following command to restore the log level:

   #**vi logconfig.cfg**

3. **DevLogLevel = 1** is displayed. Select **1** in **DevLogLevel = 1**, press **x** and **A**, enter **4**, and then press **Esc**. Then, enter **:wq!** and press **Enter**, as shown in the following figure.



4. Run the following command to verify the restoration:

   #**more logconfig.cfg**

   The following information is displayed if the log level is successfully restored:

```
......
DevLogLevel = 4
......
```

   NOTE

   Press **Ctrl+C** to exit.

----End

12.2.3 Analysis on Typical Cases

This topic analyzes some typical cases for a failure to add NEs and provides the associated solutions.

NE Already Exists

Symptom

When a user attempts to add an NE to the U2000, the U2000 displays the error message "Device already exists."

Copyright © Huawei Technologies Co., Ltd.

Analysis

1. The NE really exists on the U2000, but the login user cannot see the existing NE in the Main Topology due to the lack of administration rights.
2. The NE actually does not exist on the U2000. Due to database errors, the user fails to add the NE although the user has administration rights.

   The possible causes are:

   - During addition or deletion of an NE, exceptions occur on the U2000 processes, such as restart, core dumps, and message transmission or response timeouts.
   - In NE upgrade scenarios, the possible cause is that redundant data exists in the U2000 database.

Solution

1. If the problem arises due to the first cause, contact the U2000 administrator to obtain the required administration rights for the NE.
2. If the problem arises due to the second cause, collect NE information in databases, contact R&D engineers for fault diagnosis, and delete redundant data.

   NOTE

   For details on how to collect NE information in databases, see step 7 in **12.2.2 Troubleshooting for a Failure to Add NEs**.

Suggestion and Summary

1. Back up all databases after the U2000 installation or upgrade. The MSuite can be used as a backup tool to back up databases regularly.
2. After the U2000 is started or restarted, add or delete NEs only when the automatically started processes are running stably.
3. Stop the operation of adding or deleting NEs immediately if this fault arises. This is to avoid the generation of more redundant data.

NE Timeout

Symptom

When a user attempts to add an NE to the U2000, the error message "Device timeout" is displayed.

Analysis

The possible causes are as follows:

- SNMP protocol parameters are set incorrectly.
- The communication between the U2000 and the NE is interrupted.
- The network connect is time out.
- The NE is busy (high CPU usage).
- The NE is offline.

Copyright © Huawei Technologies Co., Ltd.

Solution

1. Check whether the SNMP parameter settings on the U2000 and the NE are consistent.
   a. Check whether the read and write community names of SNMPv1 and SNMPv2 in the SNMP protocol template used by the U2000 are the same as those on the NE.
   b. Check whether the SNMPv3 user name, encryption protocol, authentication protocol, and password in the SNMP protocol template used by the U2000 are the same as those on the NE. Check whether the SNMPv3 user is assigned a user group. If yes, check whether the user group is configured properly in the MIB.
2. Check the connectivity between the U2000 and NE.
   a. Ping the NE on the U2000 server. If the NE cannot be pinged, create a route from the U2000 server to the NE.
   b. Telnet to the NE and ping the U2000 server on the NE. If the U2000 server cannot be pinged, create a route from the NE to the U2000 server.
   c. If the NE or U2000 enables a firewall, disable the firewall or configure an IP address for the NE or U2000 to pass through the firewall.
3. Ping the NE on the U2000 server to check whether timeouts or packet loss occurs.
4. Add the NE after the CPU usage drops.
5. The NE is offline when it is:
   - powered off.
   - being restarted.

Suggestion and Summary

Obtaining packet headers to locate the fault is the most effective method.

Network Transmission Timeout

Symptom

When a user attempts to add an NE to the U2000, a network transmission timeout message is displayed asking the user to retry later.

Analysis

The possible cause for the network transmission timeout is that the trap receiver process is not started.

Solution

Start the trap receiver process, that is, trapr_agent.

Suggestion and Summary

Ensure that all dependent processes are running before adding NEs to the U2000. The **Table 12-1** shows the dependent processes for adding NEs.

Copyright © Huawei Technologies Co., Ltd.

Table 12-1 Dependent processes for adding NEs

Service	Process
Access Device Manager_*	BmsAccess_*
Access Device Common Service	BmsCommon
Trap Dispatcher	trapdispatcher
Trap Receiver Process	trapr_agent
Security Process	sm_agent
License Process	lic_agent
Topology Process	eam_agent
EAM Process	eam_agent
Fault Process	ifms_agent
Desktop Service Process	ds_889_agent
United Manager	UniteUitlDM
Distribution Manager	mc
Device Access Manager	dam
xFtpWatcher Process	XftpDm

12.3 Failure to Display NE Alarms After an Active/Standby Switchover in a Veritas High Availability System

Symptom

The U2000 can receive alarms reported by NEs before an active/standby switchover in a Veritas high availability system. After the active/standby switchover, however, the U2000 cannot receive alarms reported by NEs.

Analysis

The server IP address changes after an active/standby switchover in the Veritas HA system. The IP addresses configured for devices to report traps, however, are not changed. As a result, the NMS cannot receive alarms reported by NEs.

Solution

Assume that the server IP address is **10.71.214.91** before an active/standby switchover in the Veritas high availability system and **10.71.214.92** after the active/standby switchover.

1. Log in to the server at **10.71.214.91** as the **root** user.

Copyright © Huawei Technologies Co., Ltd.

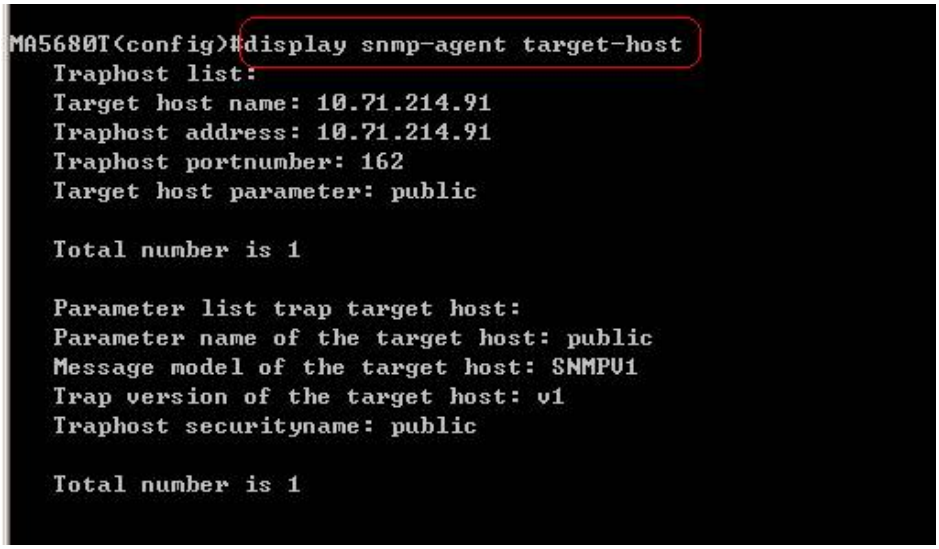
2. Run the following commands to verify the IP address set for the device to send traps:

   enable

   config

   display snmp-agent target-host

   Only **10.71.214.91** is displayed, as shown in the following figure.

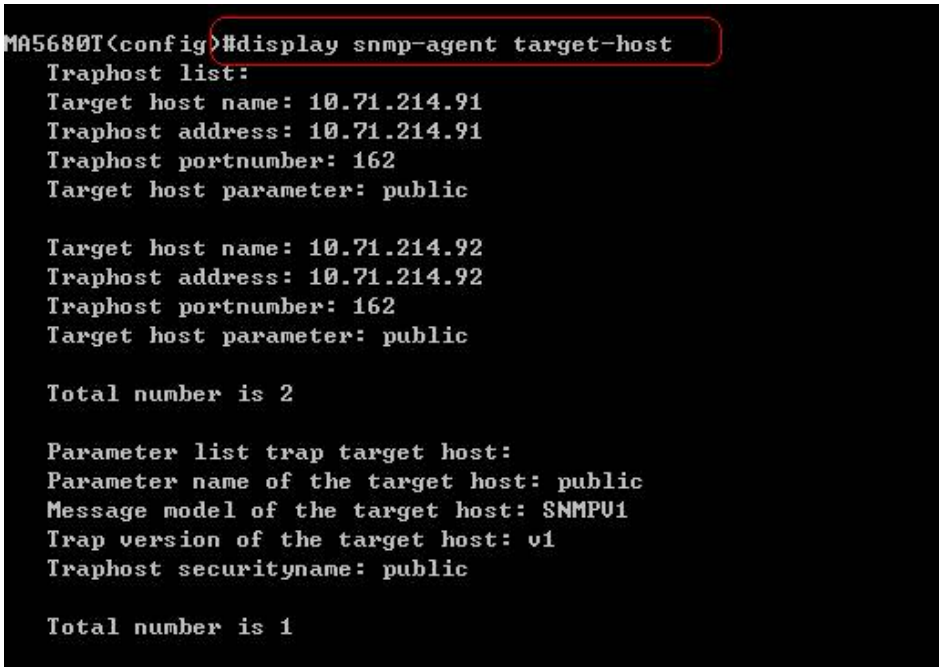


3. Run the following command to set **10.71.214.92**:

   snmp-agent target-host trap-hostname 10.71.214.92 address 10.71.214.92 trap-paramsname public

4. Repeat Step 1 to check the IP address set for the NE to send traps. The IP address **10.71.214.92** is displayed, as shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.



5. Run the following command to enable traps:

   snmp-agent trap enable standard

Suggestion and Summary

Pre-set the IP addresses of active and standby NMS servers on NEs so that the U2000 can receive alarms reported by the NEs even after an active/standby switchover in the Veritas high availability system.

12.4 Message "NE license authority failed" Displayed During NE Creation

Symptom

The message "NE license authority failed" is displayed during creation of an NE on the U2000.

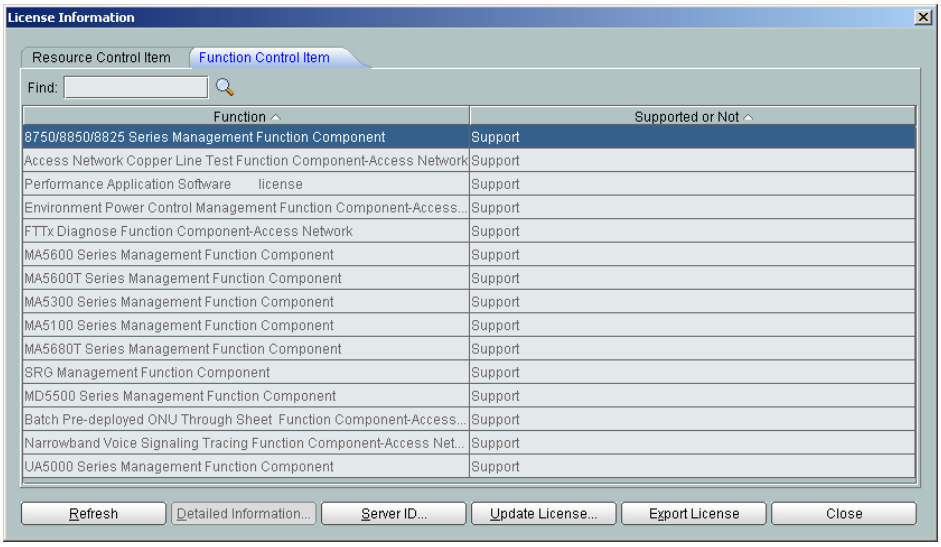
Analysis

The license file does not meet U2000 requirements. Specifically, license-controlled components are not authorized for the NE type in the license file.

Solution

1. Choose **Help** > **License Management** > **License Information** from the main menu.
2. In the **License Information** window, click the **Function Control Item** tab.

Copyright © Huawei Technologies Co., Ltd.



3. See **Table 12-2** to verify that the license-controlled components are authorized for the type of the created NE in the license file on the **Function Control Item** tab page. If the components are not authorized in the license file, apply for the license for this NE type.

Table 12-2 Mapping between NE types and license-controlled components

NE Type	License-controlled Component
ESRV005	8750/8850/8825 Series Management Function Component
ESRV500R005	8750/8850/8825 Series Management Function Component
ISN8850V5R2	8750/8850/8825 Series Management Function Component
radium8750	8750/8850/8825 Series Management Function Component
MD5500V1	MD5500 Series Management Function Component
UA5000(APM/ IPM)	UA5000 Series Management Function Component
UA5000(PVMV1)	UA5000 Series Management Function Component
UA5000(PVU)	UA5000 Series Management Function Component
UA5000(IPMB)	UA5000 Series Management Function Component
MA5105	MA5100 Series Management Function Component
MA5100V1	MA5100 Series Management Function Component
MA5100V2	MA5100 Series Management Function Component
MA5100V3	MA5100 Series Management Function Component
MA5103	MA5100 Series Management Function Component
MA5300V1	MA5300 Series Management Function Component
MA5303	MA5300 Series Management Function Component

Copyright © Huawei Technologies Co., Ltd.

NE Type	License-controlled Component
MA5605	MA5600 Series Management Function Component
MA5615	MA5600 Series Management Function Component
MA5600V3	MA5600 Series Management Function Component
MA5603	MA5600 Series Management Function Component
MA5600T	MA5600T Series Management Function Component
MA5603T	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5680T	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5683T	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5606T	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5626E	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5620E	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5620G	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5626G	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5620	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5626	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5651	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5651G	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5652G	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5610	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5612	MA5600T Series Management Function Component|MA5680T Series Management Function Component

Copyright © Huawei Technologies Co., Ltd.

NE Type	License-controlled Component
MA5616	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5603U	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5662	MA5600T Series Management Function Component|MA5680T Series Management Function Component
MA5628	MA5600T Series Management Function Component|MA5680T Series Management Function Component
SRG2200	SRG Series Management Function Component-Access Network
SRG3200	SRG Series Management Function Component-Access Network

Copyright © Huawei Technologies Co., Ltd.

13 Security NE Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot the commonly seen faults on security NE management.

13.1 Security VPN Service
This topic describes how to troubleshoot the commonly seen faults on security VPN service.

13.2 Centralized Policy Configuration Troubleshooting
This topic describes how to troubleshoot the commonly seen faults on centralized policy configuration.

13.3 Single-Point Web Configuration Troubleshooting
This topic describes how to troubleshoot the commonly seen faults on single-point web configuration.

Copyright © Huawei Technologies Co., Ltd.

13.1 Security VPN Service

This topic describes how to troubleshoot the commonly seen faults on security VPN service.

13.1.1 IPSec VPN Service Type Discovery Is Incorrect

Symptom Description

IPSec is enabled on the live network. After IPSec services and security VPN service discovery are enabled, IPSec Service is discovered as IPSec Service Interconnection on the U2000.

Assume that there are three devices: A, B, and C and that C is a third-party device. The service between A and B is IPSec service and that between A and C is IPSec service Interconnection. On the U2000, choose **Service** > **Security VPN Service** > **Discover Security VPN Service**. Select device A, and select **IPSec Service Interconnection** under **Service Type**. Click **OK**. Then, the system discovers that the services between A and C and between A and B are both IPSec Service Interconnection. Select device A and select **IPSec Service** under **Service Type**. The result is empty. If then device B and **IPSec Service Interconnection** are selected, the system still discovers that the service between B and A is **IPSec Service Interconnection**.

Cause Analysis

The two types of services cannot be both discovered. If IPSec Service Interconnection is discovered first, IPSec service will be discovered as IPSec Service Interconnection. As a result, the IPSec service fails to be discovered.

Handling Procedure

Delete the IPSec service interconnection discovered on the U2000 and set the **Service Type** to **IPSec Service**. Then, discover the IPSec service.

Suggestion and Summary

- To correctly discover IPSec Service, it is recommended that you discover the IPSec service before discovering IPSec service interconnection. Otherwise, the IPSec service may not be discovered.
- If you discover IPSec service interconnection of a device first, all services will be displayed as IPSec service interconnection, regardless of whether the service on the device is IPSec service interconnection or IPSec service.

13.1.2 Failed to Deploy IPSec VPN Services

Symptom Description

If you need to deploy IPSec VPN services between two USG5360 through U2000 software, configure various IPSec parameters in the security VPN service manager. But when you choose **Deploy** after configuration, U2000 client prompts you with the deployment failure.

Copyright © Huawei Technologies Co., Ltd.

Cause Analysis

- The service process is not started.
- The Telnet/Stelnet parameters are inconsistent with the U2000.
- The NE data is not synchronized.
- If IPSec VPN is not included in the NE License function control items, the NE does not support the configuration of the IPSec VPN.

Fault Diagnosis

1. Log in to the system monitoring client, and click the **Process Monitor** tab to check whether the **Security VPN Manager** process is started.
2. Log in to the clients on the NE and the U2000 respectively to check whether the Telnet/STelnet parameters on the NE are configured correctly, and the configurations on the NE and the U2000 are consistent.
3. Synchronize the NE data to the U2000.
4. Log in to the NE, and check whether the NE supports IPSec VPN or not.

After the previous steps, it is noticed that the IPSec VPN is not found in USG5360 licence function control item, and the relevant IPSec VPN configuration commands delivered from the U2000 cannot be indentified. Therefore, the deployment of the services failed.

Handling Procedure

Re-apply for the USG5360 NE License, update the NE licence, and deploy an IPSec VPN.

Suggestion and Summary

Before the U2000 related services being configured, ensure that the U2000 server can log in to the devices, and the NE support the configurations of the relevant services that has been included in the License function control list.

13.2 Centralized Policy Configuration Troubleshooting

This topic describes how to troubleshoot the commonly seen faults on centralized policy configuration.

13.2.1 Failure to Discover or Display NE Configurations on the U2000

Symptom

After the U2000 performs policy discovery, a message is displayed indicating successful policy discovery, whereas configuration data on an NE is not discovered or displayed on the U2000.

Possible Causes

NE data is not synchronized to the U2000.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to a U2000 client.

Step 2 Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.

Step 3 Double-click the policy package of the NE, or choose the policy package and click **Open** to access the **Centralized Configuration** window.

Step 4 Right-click the NE under the **Single NE Configuration** node in the navigation tree and choose **Synchronize NE Data** from the shortcut menu.

Step 5 Perform policy discovery.

- If configuration data on the NE is discovered and displayed on the U2000, the fault is rectified.
- If the fault persists, contact Huawei technical support engineers.

----End

13.2.2 Failure to Discover Policies, with "TimeRange [time1] no found, make sure it is created or synchronize the NE please." Displayed

Symptom

Policy discovery fails and the message "TimeRange [time1] no found, make sure it is created or synchronize the NE please." is displayed.

NOTE

The time range **time1** is used as an example.

Possible Causes

The possible causes are as follows:

- A failure in undeploying some applications from the U2000 may lead to inconsistency between data in the U2000 database and data on the NE. The U2000, however, does not synchronize data.
- ACL rules configured on the NE use **time1** that does not exist.

Procedure

Step 1 If the fault occurs due to the first cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.
3. Double-click the policy package of the NE, or choose the policy package and click **Open** to access the **Centralized Configuration** window.
4. Right-click the NE under the **Single NE Configuration** node in the navigation tree and choose **Synchronize NE Data** from the shortcut menu.
5. Discover policies.

Copyright © Huawei Technologies Co., Ltd.

- If a message is displayed indicating successful policy discovery, the fault is rectified.
- If the fault persists, perform **Step 2**.

Step 2 If the fault occurs due to the second cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **View** > **Main Topology** from the main menu.
3. Right-click in the Main Topology and choose **Find** from the shortcut menu.
4. In the **Search** dialog box, set **Search Mode** to **IP** and enter the IP address of the NE in the **Keyword** text box.
5. In the query result area, right-click the NE and choose **Locate to Topo** from the shortcut menu.
6. In the Main Topology, right-click the NE and choose **Tool** > **Telnet** from the shortcut menu. Then, enter a user name and password to log in the NE by means of Telnet.
7. Run the related commands to set **time1**.

   For example:

   a. Run the **system-view** command to access the system view.

   b. Run the **time-range time1** *x* command to set **time1**.

   Here, *x* indicates the user-defined time range. For example, 08:00 to 12:00 Mon.

   NOTE

   The following example uses Eudemon8000E. The commands vary according to device types and versions. Obtain the correct commands based on actual conditions. For more information, see the corresponding command reference.
8. Perform data synchronization again to synchronize data on the NE to the U2000.
9. Perform policy discovery again.
   - If a message is displayed indicating successful policy discovery, the fault is rectified.
   - If the fault persists, contact technical support engineers.

----End

13.2.3 Failed to Verify, Deploy, or Audit a Policy, with "The ZONE is not found. Please check the NE configuration or synchronize the NE, and make sure zone [zone1] of priority set up." Displayed

Symptom

Verifying, deploy, or auditing a policy fails and the "The ZONE is not found. Please check the NE configuration or synchronize the NE, and make sure zone [zone1] of priority set up." message is displayed.

NOTE

The security zone **zone1** is used as an example.

Possible Causes

The possible causes are as follows:

Copyright © Huawei Technologies Co., Ltd.

- NE data is not synchronized to the U2000.
- No priority is set for the security zone defined in the policy package.

Procedure

Step 1 If the fault occurs due to the first cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.
3. Double-click the policy package of the NE, or choose the policy package and click **Open** to access the **Centralized Configuration** window.
4. Right-click the NE under the **Single NE Configuration** node in the navigation tree and choose **Synchronize NE Data** from the shortcut menu.
5. Verify, deploy, or audit the policy.
   - If a message is displayed indicating successful policy verification, deployment, or audit, the fault is rectified.
   - If the fault persists, perform **Step 2**.

Step 2 If the fault occurs due to the second cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **View** > **Main Topology** from the main menu.
3. Right-click in the Main Topology and choose **Find** from the shortcut menu.
4. In the **Search** dialog box, set **Search Mode** to **IP** and enter the IP address of the NE in the **Keyword** text box.
5. In the query result area, right-click the NE and choose **Locate to Topo** from the shortcut menu.
6. In the Main Topology, right-click the NE and choose **Tool** > **Telnet** from the shortcut menu. Then, enter a user name and password to log in the NE by means of Telnet.
7. Run the associated commands to set a priority for **zone1**.

   NOTE

   The following example uses Eudemon8000E. The commands vary according to device types and versions. Obtain the correct commands based on actual conditions. For more information, see the corresponding command reference.

   For example:

   a. Run the **system-view** command to access the system view.
   b. Run the **firewall zone zone1** commands to access **zone1**.
   c. Run the **display this** command check whether any priority has been set for **zone1**.

      If no priority has been set, set a priority. For example, run the **set priority** *security-priority* command. Here, *security-priority* indicates the priority.

      NOTE

      If a priority has been set, **set priority x** is displayed in the output of the **display this** command. **x** indicates the priority that has been set for **zone1**.
8. Perform data synchronization again to synchronize data on the NE to the U2000.
9. Verify, deploy, or audit the policy again.

Copyright © Huawei Technologies Co., Ltd.

- If a message is displayed indicating successful policy verification, deployment, or audit, the fault is rectified.
- If the fault persists, contact technical support engineers.

----End

13.2.4 Failure to Deploy a Policy, with "Conflict with current NE configuration of Interzone Packet-Filter" Displayed

Symptom

Deploying a policy fails and the "Conflict with current NE configuration of Interzone Packet-Filter" message is displayed.

Possible Causes

Interzone packet filtering is configured on an NE in CLI mode. A packet filtering policy is configured on the same interzone and deployed, without data synchronization and policy discovery on the U2000.

Procedure

Step 1 Log in to a U2000 client.

Step 2 Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.

Step 3 Double-click the policy package to be deployed, or choose the policy package and click **Open**. The **Centralized Configuration** window is displayed.

Step 4 Right-click the NE for which policy deployment fails under the **Single NE Configuration** node in the navigation tree and choose **Synchronize NE Data** from the shortcut menu.

Step 5 Right-click the NE and choose **Discover Policy** from the shortcut menu.

NOTICE

Policy discovery may change current policy configurations. To ensure consistent policy configurations, you must configure the policy again.

Step 6 Deploy the policy again.

- If a message is displayed indicating successful policy deployment, the fault is rectified.
- If the fault persists, collect policy deployment information and contact Huawei technical support engineers.

----End

Suggestion and Summary

Data synchronization and policy discovery must be performed before policy configuration.

Copyright © Huawei Technologies Co., Ltd.

13.2.5 Failure to Undeploy a Policy, with "Fail to undeploy" Displayed

Symptom

Undeploying a policy fails and the "Fail to undeploy" message is displayed.

Possible Causes

The possible causes are as follows:

- The NE goes offline because of a power failure or another reason.
- The U2000 does not synchronize data of the NE.
- The U2000 does not discover policies.

Procedure

Step 1 If the fault occurs due to the first cause, perform the following steps:

Check network connectivity, that is, whether the route between the U2000 and the NE is reachable.

1. Log in to a U2000 client.
2. Choose **View** > **Main Topology** from the main menu.
3. Right-click in the Main Topology and choose **Find** from the shortcut menu.
4. In the **Search** dialog box, set **Search Mode** to **IP** and enter the IP address of the NE in the **Keyword** text box.
5. In the query result area, right-click the NE and choose **Locate to Topo** from the shortcut menu.
6. In the Main Topology, right-click the NE and choose **Tool** > **Ping** from the shortcut menu.
7. In the **Ping** dialog box, click the **Ping** option button and click **Start** to check the network connectivity and packet loss ratio between the U2000 and the NE.
   - If no information is displayed in the **Result** area, the NE is offline. In this case, rectify the disconnection fault and then undeploy the policy.
     - If a message is displayed indicating successful policy undeployment, the fault is rectified.
     - If the fault persists, perform **Step 2**.
   - If any information is displayed in the **Result** area, the route between the U2000 and the NE is reachable. In this case, perform **Step 2**.

Step 2 If the fault occurs due to the second cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.
3. Double-click the policy package of the NE, or choose the policy package and click **Open** to access the **Centralized Configuration** window.
4. Right-click the NE under the **Single NE Configuration** node in the navigation tree and choose **Synchronize NE Data** from the shortcut menu.

Copyright © Huawei Technologies Co., Ltd.

5. Undeploy the policy.
   - If a message is displayed indicating successful policy undeployment, the fault is rectified.
   - If the fault persists, perform **Step 3**.

Step 3 If the fault occurs due to the third cause, perform the following steps:

1. Log in to a U2000 client.
2. Choose **Configuration** > **Network Security** > **Policy Management** from the main menu.
3. Double-click the policy package of the NE, or choose the policy package and click **Open** to access the **Centralized Configuration** window.
4. Right-click the NE under the **Single NE Configuration** node in the navigation tree and choose **Discover Policy** from the shortcut menu to discover policies.

NOTICE

Policy discovery may change current policy configurations. To ensure consistent policy configurations, you must configure the policy again.

Step 4 Undeploy the policy.

- If a message is displayed indicating successful policy undeployment, the fault is rectified.
- If the fault persists, contact technical support engineers.

----End

13.3 Single-Point Web Configuration Troubleshooting

This topic describes how to troubleshoot the commonly seen faults on single-point web configuration.

13.3.1 Attempt to Log in to the Web Interface Fails and a Message Is Displayed Indicating that the Authentication Fails or Expires

Symptom Description

On the main topology map of the U2000, right-click an NE and choose **Login Web** from the shortcut menu. A message is displayed indicating that the authentication fails or expires.

Cause Analysis

No Web interface user accounts are created on the NE, or the login password has been changed.

Handling Procedure

1. On the main topology map of the U2000, right-click the NE and choose **Repair Web User** to repair the Web interface user.

Copyright © Huawei Technologies Co., Ltd.

2. In the **Repair Web User** dialog box that is displayed, set the mode of repairing Web user accounts and click **OK**.
   - **Create user automatically**: The U2000 automatically creates account **nms_user_super** whose password is randomly generated on the NE.
   - **Use given user**: The user logs in to the Web page of the NE by using an existing Web user account.
3. When the **web user create success.** message is displayed, click **OK**, the user account is successfully created or the password is successfully initiated. Then, the user can log in to the Web interface.

   Run the following command to Telnet or STelnet to the NE.
   - **telnet** *NE IP address*
   - **stelnet** *NE IP address*

   NOTE

   Using STelnet (if supported) to log in to the device is recommended. STelnet is more secure.

   Enter AAA view. Run the **display this** command to display the current configuration in AAA view, as shown in the following output.

```
aaa

 local-user nms_user_super password simple 1279633c5M
 local-user nms_user_super service-type web
 local-user nms_user_super level 3
```

4. If the problem persists, contact Huawei technical support engineers.

13.3.2 Failure to Repair the Web User Account, with "Failed to insert the user" Displayed

Symptom

Repairing the Web user account of an NE fails and the "Repair web user failed. Reason: failed to insert the user." message is displayed.

Possible Cause

The number of local users configured on the NE has reached the maximum value.

Procedure

1. Right-click the NE in the Main Topology and choose **Tools** > **Telnet** from the shortcut menu to log in to the NE.
2. Access the AAA view and run the **display local-user** command to view the local user list.

   NOTE

   The following example uses Eudemon8000E. The commands vary according to device types and versions. Obtain the correct commands based on actual conditions. For more information, see the corresponding command reference.
3. Run the **undo local-user** ***username*** command to delete invalid local user accounts.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The following example uses Eudemon8000E. The commands vary according to device types and versions. Obtain the correct commands based on actual conditions. For more information, see the corresponding command reference.

4. Right-click the NE in the Main Topology and choose **Repair Web User** from the shortcut menu to repair the Web user account.

   If **web user create success.** is displayed, the Web user account is repaired successfully and you can log in the Web configuration window of the NE by using the U2000.

Copyright © Huawei Technologies Co., Ltd.

14 Common Faults and Solutions for the HedEx Helper

About This Chapter

This topic describes how to remove common faults when you use the HedEx Helper.

14.1 When You Access the HedEx Helper Through the Internet Explorer, initialize the progress bar has been at 0% or with Confused Styles

14.2 Blank Window Does Not Close When You Attempt to View Help Information by Pressing F1

14.3 Libraries Fail to Be Uploaded in IE8.0

14.4 The System Prompts "Retrieving verify code failed" When You Register with the HedEx Helper or Log In to the HedEx Helper with a User Name

14.5 A Blank Window Appears in the Firefox When You Press F1 on the EMS Interface

14.6 An Exception Occurs when You Export All the Remarks

14.7 Failed to Launch the U2000 Online Help on Solaris OS

14.8 "Firefox is already running, but is no responding" Is Displayed When a User Presses F1 on Solaris-based U2000

14.9 Online Help Cannot Be Launched on the System Monitor Client

14.10 Help Is Not Displayed After F1 Is Pressed

14.11 The "The page cannot be displayed" Message Is Displayed Upon an Attempt to Visit the HedEx Helper

14.12 U2000 Help Invoked by F1 Is Displayed Unstably

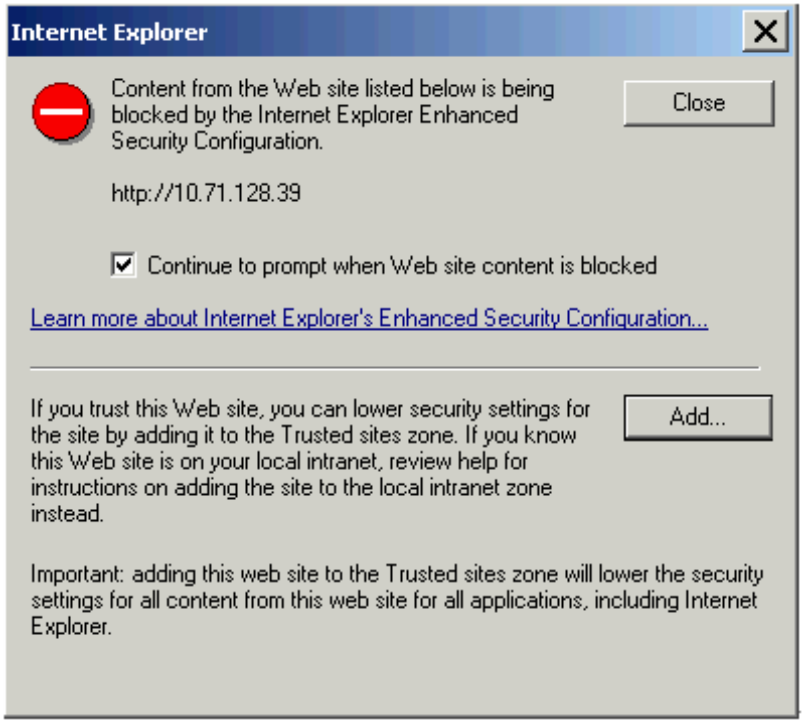
Copyright © Huawei Technologies Co., Ltd.

14.1 When You Access the HedEx Helper Through the Internet Explorer, initialize the progress bar has been at 0% or with Confused Styles

Fault Description

When You Access the HedEx Helper Through the Internet Explorer on a Windows 2008 Server, the HedEx Helper interface is blank or with confused styles.

Figure 14-1 Internet Explorer



Fault Analysis

This fault is because that the Web service address is not trusted by the browser. The IP address of the HedEx Helper service is not added to the trusted sites of the Internet Explorer, and thus the browser forbids the access to the HedEx Helper.

Add the IP address of the HedEx Helper service to the trusted sites of the Internet Explorer.

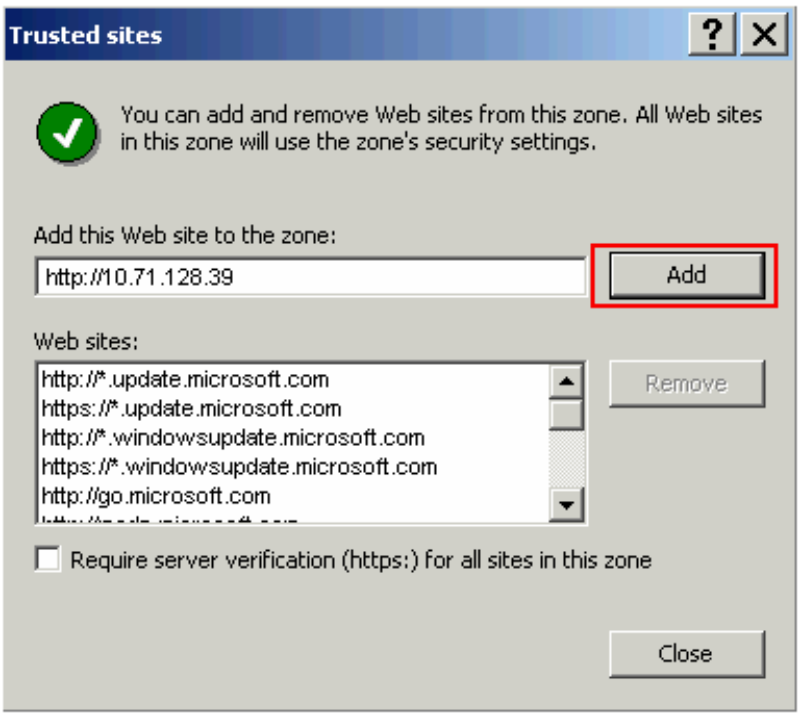
Procedure

1. Run the Internet Explorer, choose **Tools** > **Internet Options** to open the **Internet Options** dialog box.

Copyright © Huawei Technologies Co., Ltd.

2. In the **Internet Options** dialog box, click the **Security** tab and then select **Trusted sites**. Then click **Sites**.
3. In the displayed **Trusted sites** dialog box, click **Add** to add IP address of the HedEx Helper service to the trusted sites of the Internet Explorer. See **Figure 14-2**.

Figure 14-2 Trusted sites

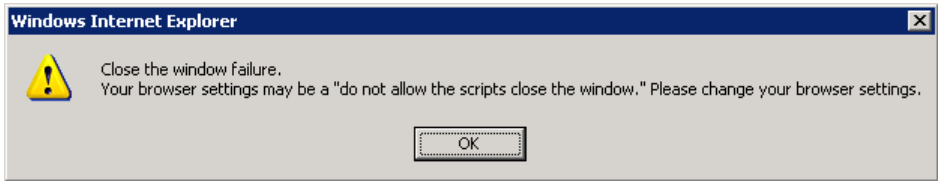


14.2 Blank Window Does Not Close When You Attempt to View Help Information by Pressing F1

Fault Description

When you press **F1** on the network management system (NMS) UI, a blank window is displayed, not the Help information. **Figure 14-3** shows the error page.

Figure 14-3 Error page



Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

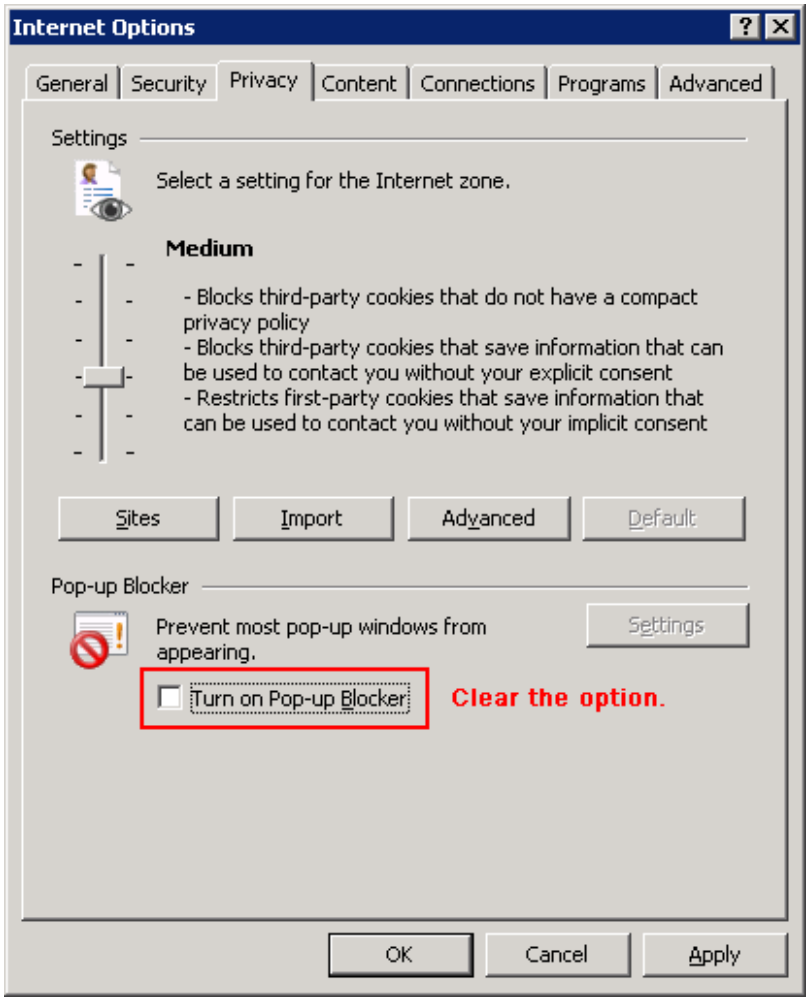
The browser blocks pop-up windows. You must enable the browser to allow pop-up windows; otherwise the blank window cannot be closed.

Procedure

The following is an example using Internet Explorer 7.0.

1. Open Internet Explorer 7.0, and choose **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed.
2. On the **Privacy** tab page, clear the **Turn on Pop-up Blocker** option, and click **OK**. See **Figure 14-4**.

Figure 14-4 Privacy page



3. Press **F1** to view Help information on the NMS UI.

Copyright © Huawei Technologies Co., Ltd.

14.3 Libraries Fail to Be Uploaded in IE8.0

Description

Libraries fail to be uploaded in Microsoft Internet Explorer 8.0, and the system prompts "No file found".

Fault Analysis

In Microsoft Internet Explorer 8.0, **Include local directory path when uploading files to a server** is set to **Disable** by default. Therefore, the browser automatically changes the file path to C:\fakepath\filename when uploading files.

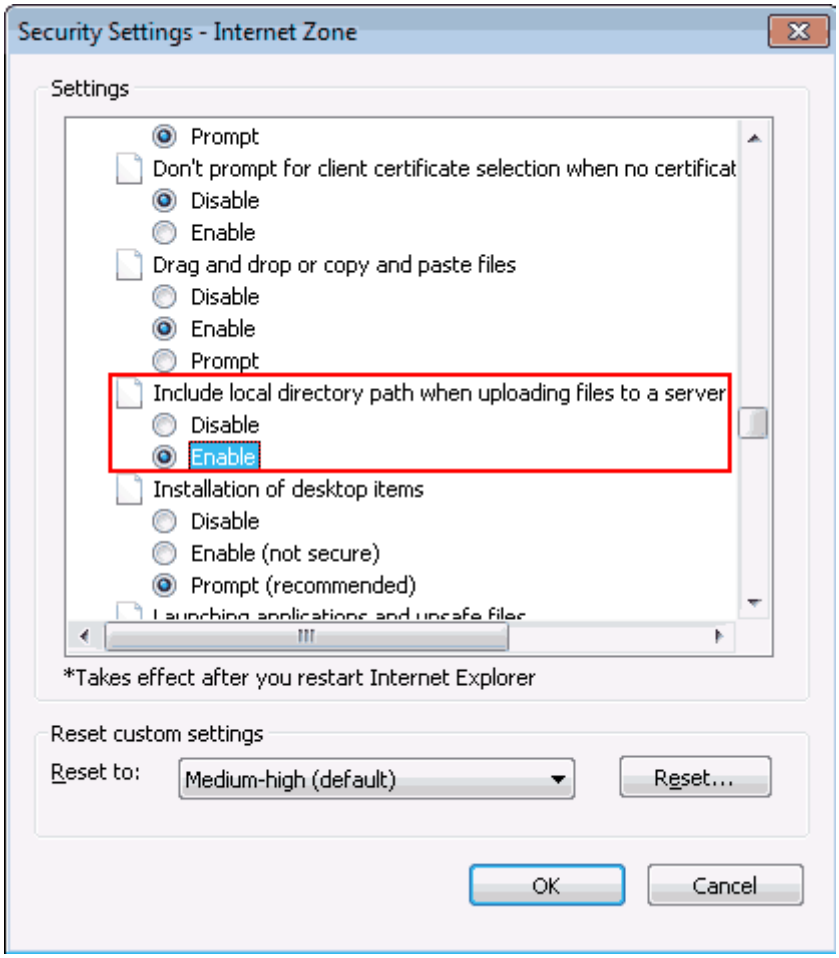
Procedure

To rectify the fault, do as follows:

1. In Internet Explorer, choose **Tools** > **Internet Options** to open the **Internet Options** dialog box.
2. In the **Internet Options** dialog box, click the **Security** tab and then click **Custom Level**.
3. In the **Security settings** dialog box, set **Include local directory path when uploading files to a server** to **Enable**.See **Figure 14-5**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-5 Security settings



4. Click **OK**.

14.4 The System Prompts "`Retrieving verify code failed`" When You Register with the HedEx Helper or Log In to the HedEx Helper with a User Name

Fault Description

The system prompts "`Retrieving verify code failed`" when you register with the HedEx Helper or log in to the HedEx Helper with a user name. See **Figure 14-6**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-6 `Retrieving verify code failed` prompt

Fault Analysis

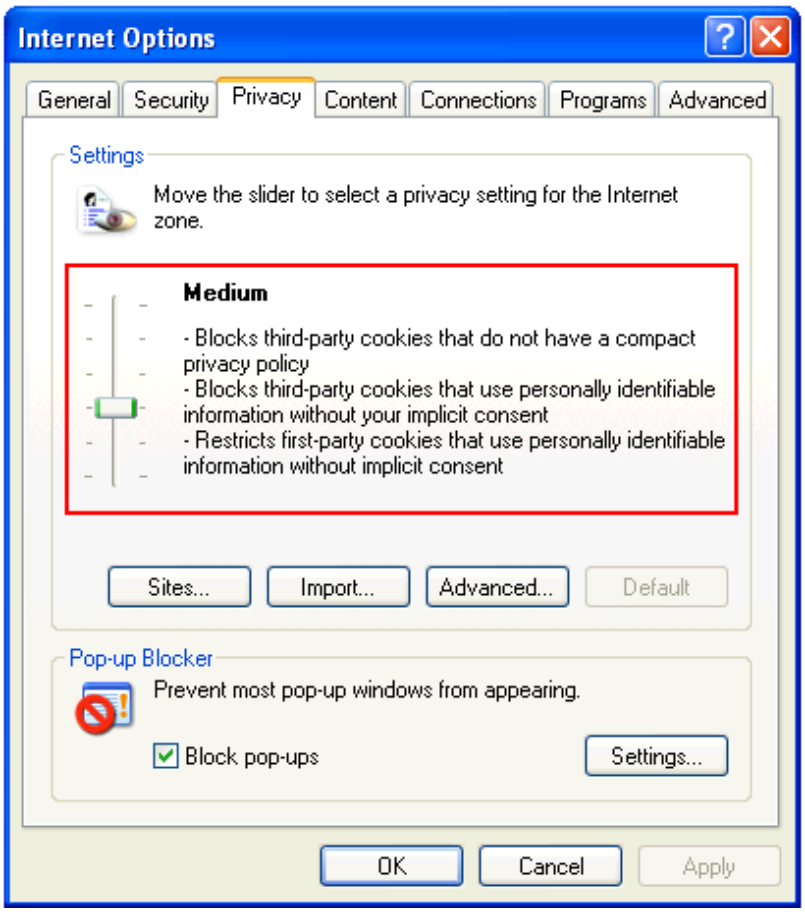
After the HedEx Helper verify code is generated, you need to save it to the client. The browser might disable the cookie, and thus the verify code cannot be saved to the browser. To solve this problem, you can set the cookie for receiving the site in the browser.

Procedure

1. To set the cookie for receiving the site in the browser, do as follows:
   - In Microsoft Internet Explorer,
     a. In the Internet Explorer, choose **Tools** > **Internet Options** to open the **Internet Options** dialog box.
     b. In the **Internet Options** dialog box, click the **Privacy** tab, and then set the parameters as shown in **Figure 14-7**.

Copyright © Huawei Technologies Co., Ltd.

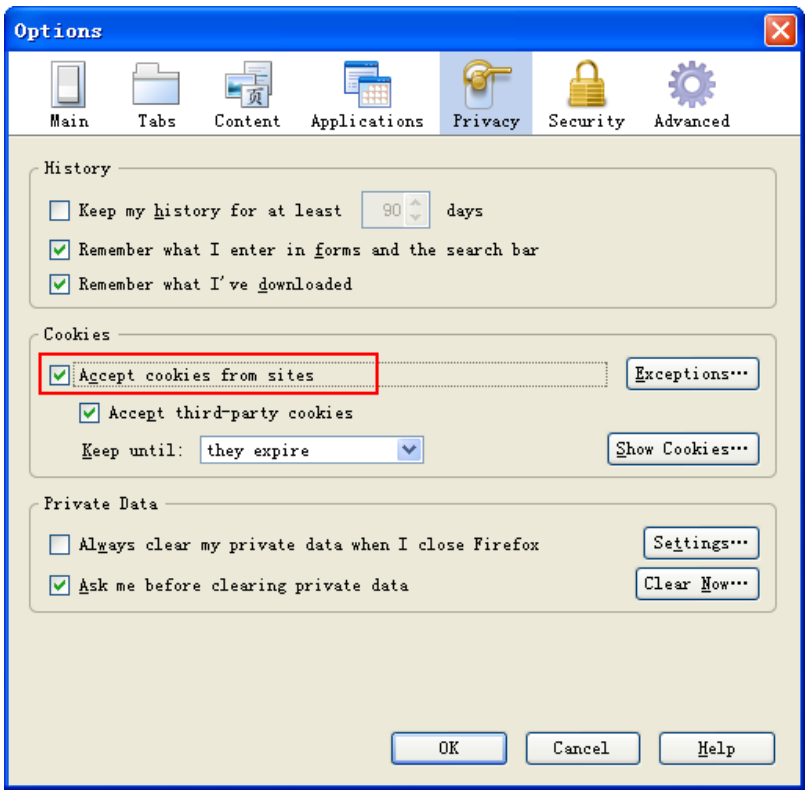
Figure 14-7 Setting the cookie in the Internet Explorer



- In the Firefox,
  a. In the Firefox, choose **Tools** > **Options** to open the **Options** dialog box.
  b. In the **Options** dialog box, click the **Privacy** tab, and then select **Accept cookies from sites** under **Cookies**. See **Figure 14-8**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-8 Setting the cookie in the Firefox



2. Continue with the registration or login with a new verify code.

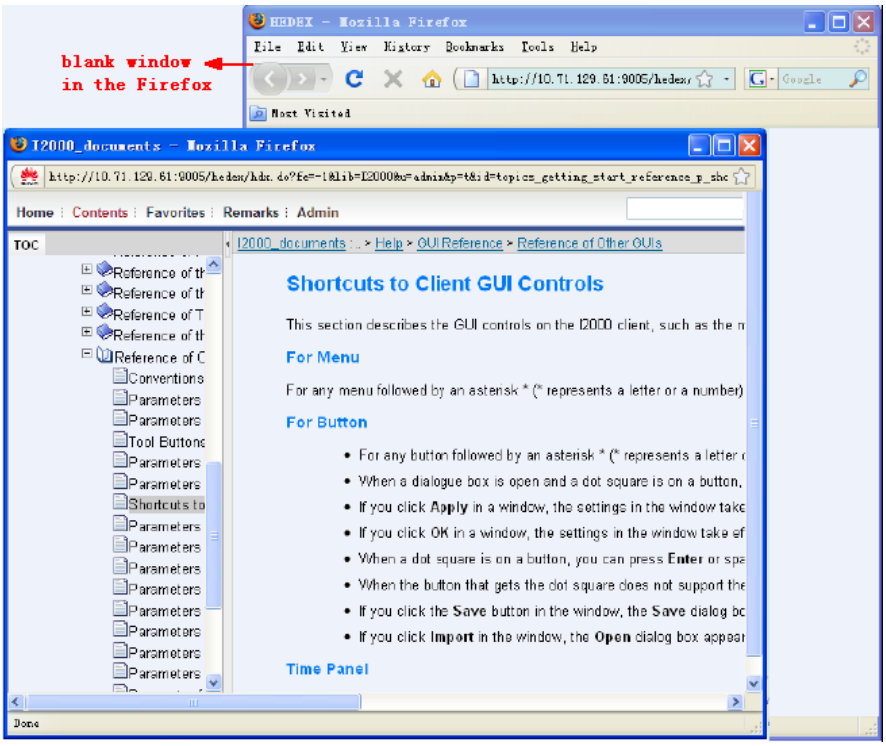
14.5 A Blank Window Appears in the Firefox When You Press F1 on the EMS Interface

Fault Description

On the EMS interface, if you press **F1** to view the Help, a blank window in the Firefox appears. See **Figure 14-9**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-9 Blank window in the Firefox



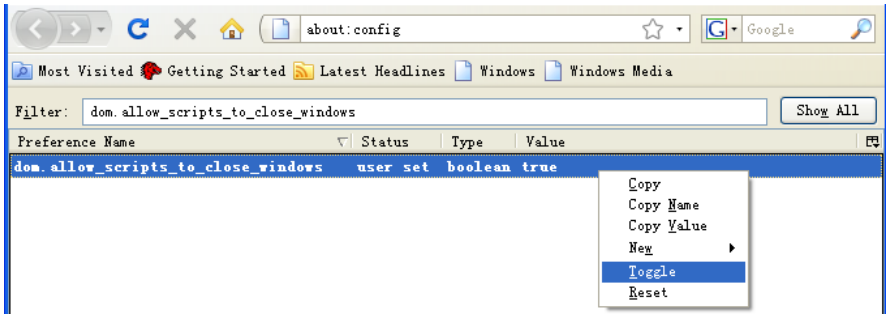
Fault Analysis

Before viewing the Help of the EMS, the HedEX closes certain temporary windows of the browser in daemon mode, but the Firefox forbids closing windows by default. Therefore, a blank window appears.

Procedure

1. Run the Firefox. Enter **about:config** in the address bar and then press **Enter**.
2. In the **Filter** text box, enter **dom.allow_scripts_to_close_windows**. In the lower part of the displayed interface, right-click **dom.allow_scripts_to_close_windows** and choose **Toggle** (that is, change the value of **dom.allow_scripts_to_close_windows** from **false** to **true**). See **Figure 14-10**.

Figure 14-10 Changing the default settings of the Firefox



Copyright © Huawei Technologies Co., Ltd.

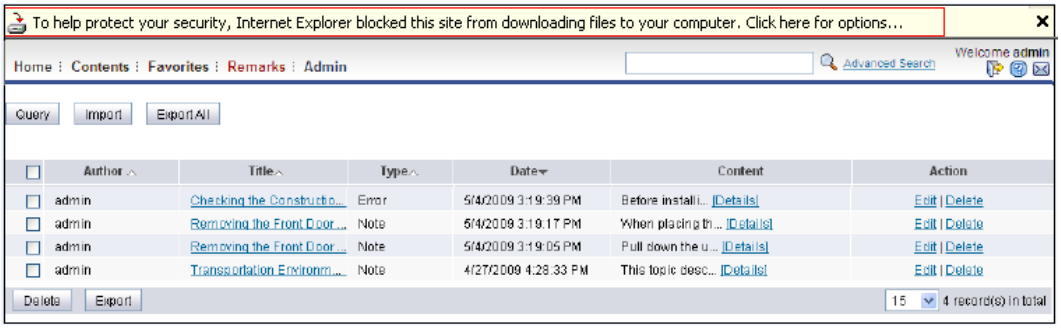
3. Close the Firefox. Then press **F1** on the EMS interface. No blank window appears.

14.6 An Exception Occurs when You Export All the Remarks

Fault Description

On the **Remarks** tab of the HedEx Helper, click **Export All** to export all the remarks. If an interface as shown in **Figure 14-11** is displayed, it indicates that the remarks cannot be exported.

Figure 14-11 Remarks failing to be exported



Procedure

1. Run the Internet Explorer, and then choose **Tools** > **Internet Options** to open the **Internet Options** interface.
2. On the **Internet Options** interface, click the **Security** tab, and then click **Custom Level** to open the **Security Settings** interface.
3. On the **Security Settings** tab, configure the parameter **Automatic prompting for ActiveX controls** of **ActiveX controls and plug-ins** and the parameter **Automatic prompting for file downloads** of **Downloads**to **Enable**.
4. On the **Remarks** tab, click **Export All**. All the remarks can be exported.

14.7 Failed to Launch the U2000 Online Help on Solaris OS

Symptom

On the U2000 client, I cannot launch the Online Help in any of the following ways:

- 1. Choose **Help** > **> Help Topics** from the main menu.
- 2. Click the Online Help icon .
- 3. Press **F1**.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The Firefox Web browser equipped with Solaris OS is 2.0.0.19 or an earlier version. On the U2000, the transport NE management process is deployed. This process uses the Mozilla Web browser that conflicts with the earlier Firefox Web browser. As a result, the Firefox Web browser cannot be started and the U2000 Online Help cannot be launched.

Procedure

- Manually start the Firefox Web browser to launch Online Help.
  1. Manually start the Firefox Web browser and keep it open.
  2. Launch the U2000 Online Help.

     NOTE

     When closing the U2000 Online Help, close the current page rather than the Firefox Web browser.
- Install a later version of the Firefox Web browser.

  NOTE

  On the Solaris OS, the U2000 Online Help can be launched through Firefox 3.0, Firefox 3.5 and Firefox 3.6. Two formats (**Tarball**and **Pkgadd**) of Firefox installation packages are available, and **Tarball** is recommended. You can obtain the Firefox installation package in either of the following way: Log in to **http://releases.mozilla.org/pub/mozilla.org/firefox/releases**, the official website of Mozilla.

  1. Use SFTP or FTP to send the Firefox installation package to the U2000 client as user **root**. Using SFTP is recommended to ensure transmission security.

     Assume that the Firefox installation package is stored in the **opt/export/home** directory and the package name is **firefox-3.6.18.en-US.solaris-10-fcs-sparc.tar.bz2**.
  2. Log in to the Solaris graphic user interface (GUI) as user **root**, open the terminal, and run the following command to go to **opt/export/home**:

     # **cd /opt/export/home**
  3. Run the following command to decompress the Firefox installation package to the current directory:

     # **bzip2 -dc firefox-3.6.18.en-US.solaris-10-fcs-sparc.tar.bz2 | tar -xf -**

     The **firefox** folder is generated in **/opt/export/home**.

     NOTE

     It is not recommended to install the Firefox Web browser by replacing the original **firefox** folder. Therefore, ensure that the **firefox** folder does not exist before decompressing the installation package.
  4. Run the following commands to enter the installation directory of Firefox Web browser and rename the existing **firefox** folder **firefox_backup**:

     # **cd /usr/lib**

     # **mv firefox firefox_backup**
  5. Run the following commands to copy the **firefox** folder of the target version to the installation directory and assign the execution permission to user **ossuser**:

     # **mv /opt/export/home/firefox /usr/lib/firefox**

     # **chown -R ossuser:ossgroup /usr/lib/firefox**

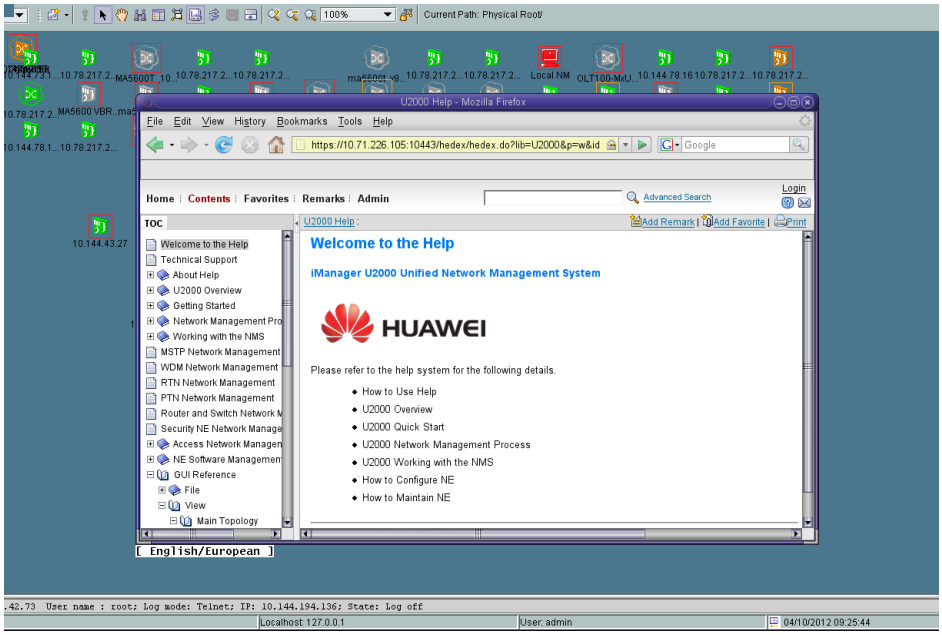
Copyright © Huawei Technologies Co., Ltd.

 # chown -R 775 /usr/lib/firefox

NOTE

Assigning the permission ensures that user ossuser has sufficient rights for the Firefox Web browser.

6. Log in to the Solaris OS, log in to the U2000 client, and launch Online Help.



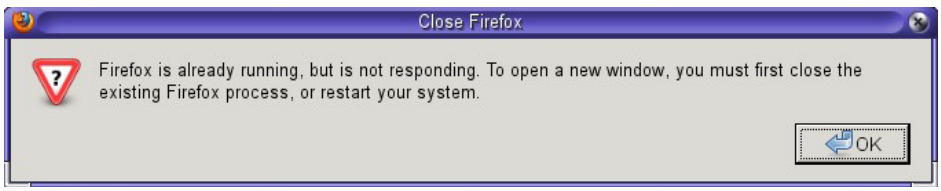
----End

14.8 "Firefox is already running, but is no responding" Is Displayed When a User Presses F1 on Solaris-based U2000

Symptom

The second time I press **F1** on the U2000 that runs on Solaris OS, the U2000 displays the error message in **Figure 14-12**. Then I run the **kill** command to end Firefox processes and retry. The Online Help is launched successfully only after the first retry; the U2000 displays the error message again after subsequent retries.

Figure 14-12 Error message



Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The Firefox browser is faulty, and Firefox processes are still running after the Online Help is closed. As a result, the Firefox processes cannot be started next time you attempt to launch the Online Help.

Procedure

- Install a stable Firefox browser.

  NOTE

  The U2000 Online Help can be launched on Firefox 3.0, Firefox 3.5, and Firefox 3.6. The Firefox software package has two formats: **Tarball** and **Pkgadd**. **Tarball** is recommended. You can obtain a Firefox software package by visiting the Mozilla website **http://releases.mozilla.org/pub/mozilla.org/firefox/releases**.

  1. Log in to the Solaris OS as user **root** and run the following command to check Firefox processes:

     ```
     # ps -ef | grep firefox
     ```

     A message similar to the following is displayed:

     ```
     root 18338  4605   0 12:13:53 pts/2       0:00 grep firefox
     ossuser 18058  5733   0 12:13:04 ?          0:13 /usr/lib/firefox/firefox-
     bin https://10.78.216.97:10443/hedex/hedex.do?k=13291063
     ossuser 18765  2879   0 12:13:44 ?          0:13 /usr/lib/firefox/firefox-
     bin https://10.78.216.97:10443/hedex/hedex.do?k=13291063
     ```

  2. Run the **kill** command to end Firefox processes except **grep firefox**. For example, run the following command to end process 18058:

     ```
     # kill -9 18058
     ```

  3. Use SFTP or FTP to send the Firefox software package to the U2000 client as user **root**. Using SFTP is recommended to ensure transmission security.

     Assume that the Firefox software package is stored in **export/home** and named **firefox-3.6.18.en-US.solaris-10-fcs-sparc.tar.bz2**.

  4. Log in to the Solaris OS as user **root** and run the following command to open the **export/home** directory:

     # **cd /export/home**

  5. Run the following command to decompress the Firefox software package to the current directory:

     # **bzip2 -dc firefox-3.6.18.en-US.solaris-10-fcs-sparc.tar.bz2 | tar -xf -**

     After this operation, a **firefox** folder is generated in **export/home**.

     NOTE

     Before decompressing the Firefox software package, ensure that there is no **firefox** folder in **export/home**. Overwriting the original **firefox** folder is not recommended.

  6. Run the following command to open the default Firefox directory provided by the Solaris OS and rename the **firefox** folder **firefox_backup**:

     # **cd /usr/lib**

     # **mv firefox firefox_backup**

Copyright © Huawei Technologies Co., Ltd.

7. Run the following commands to copy the **firefox** folder generated in step 5 to the default Firefox directory and assign the execute permission for this folder to user **ossuser**:

   # **mv /export/home/firefox /usr/lib/firefox**

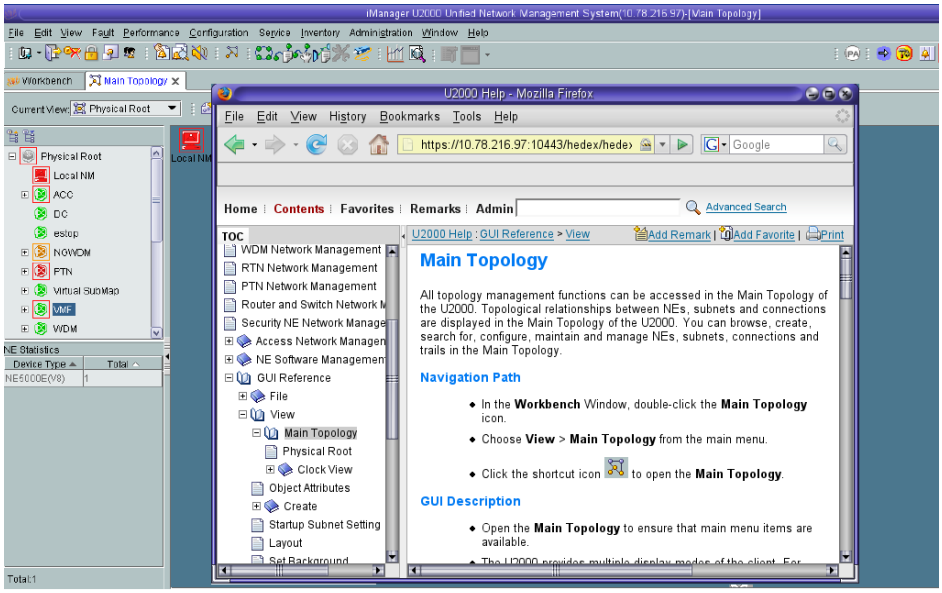
   # **chown -R ossuser:ossgroup /usr/lib/firefox**

   # **chown -R 775 /usr/lib/firefox**

   NOTE

   If you skip this step, you may fail to start the Firefox browser after logging in to the U2000 as user **ossuser**.

8. Log in to the Solaris OS as user **ossuser**. Then log in to the U2000 and press **F1**. The Online Help is launched successfully.



----End

14.9 Online Help Cannot Be Launched on the System Monitor Client

Symptom

Online Help cannot be launched on the System Monitor client by pressing **F1**.

Possible Causes

The U2000 server starts up in SSL mode while the System Monitor client logs in to the U2000 server in common mode. As a result, the Online Help address is invalid.

Procedure

- Change the login mode of the System Monitor client to SSL.

Copyright © Huawei Technologies Co., Ltd.

1. Exit the System Monitor client.
2. Choose **Start** > **Programs** > **Network Management System** > **U2000 System Monitor**. Alternatively, double-click the shortcut icon **U2000 System Monitor** on the desktop.
3. Click next to **Server**. In the dialog box that is displayed, select a U2000 server and click **Modify**.
4. In the dialog box that is displayed, set **Mode** to **Security(SSL)**.
5. Click **OK**. The login mode of the System Monitor client is changed to SSL.

----End

14.10 Help Is Not Displayed After F1 Is Pressed

Fault Description

After a user presses **F1**, the U2000 Help is not displayed and **Internet Explorer cannot display the webpage** is displayed.

After a user chooses **Help** > **Help Topics** from the main menu of the U2000, the U2000 Help is not displayed.

Fault Analysis

The System Monitor client shows that the Tomcat process has been started. The fault persists after the Tomcat process is restarted.

A possible cause is port conflict. If the report server and the U2000 are installed on the same server, port conflict occurs because both the Help and report processes use port 8080.

Procedure

1. Start the report server.
   - On Windows, double-click the icon on the taskbar.
   - On Solaris, run the following commands:

     #**cd iWebReportServer/bin**

     #**./ServiceManager.sh**
2. In the **iWeb Report Server Manager** dialog box, click **System**.
3. Set **Primary Port** to an available port and click **Test**.

   If **Test Successful** is displayed, the port for the report system can be used.

   If **Report Server Port is already in use** is displayed, modify the port for the report system.
4. After the test succeeds, click **OK**.

Copyright © Huawei Technologies Co., Ltd.

14.11 The "The page cannot be displayed" Message Is Displayed Upon an Attempt to Visit the HedEx Helper

Fault Description

When a user uses the Internet Explorer 6.0 to visit HedEx Helper, an error message is displayed and the user cannot view the Online Help.

Fault Analysis

Do not supports to uses the Internet Explorer 6.0 to visit HedEx Helper.

Procedure

If the customer uses IE6, upgrading to IE7 is recommended.

14.12 U2000 Help Invoked by F1 Is Displayed Unstably

Fault Description

After a user presses F1 on the U2000 to invoke Help, the U2000 displays an IE window, which zooms in or out and then shows the Help content. The customer considers that this symptom is caused by a U2000 problem.

Fault Analysis

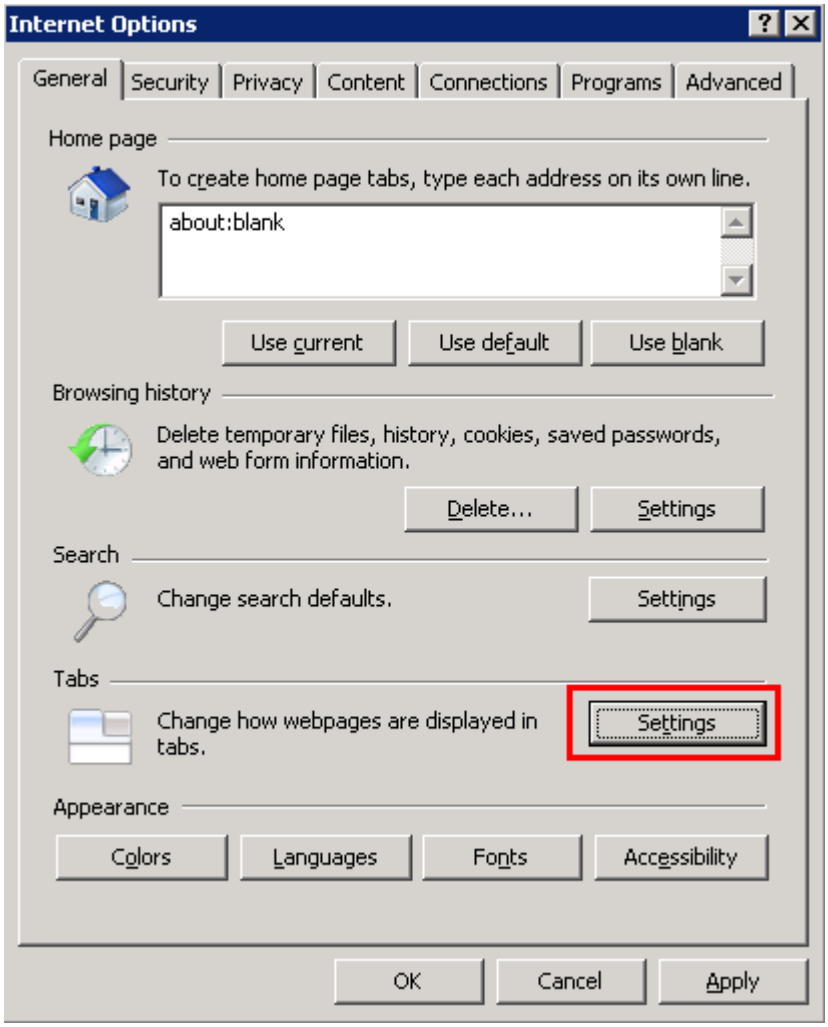
The U2000 uses the IE bearing HedEx to display Help. If the IE window is larger or smaller than the HedEx window, the IE window will zoom in or out to fit the HedEx window. This problem can be handled by setting IE parameters.

Procedure

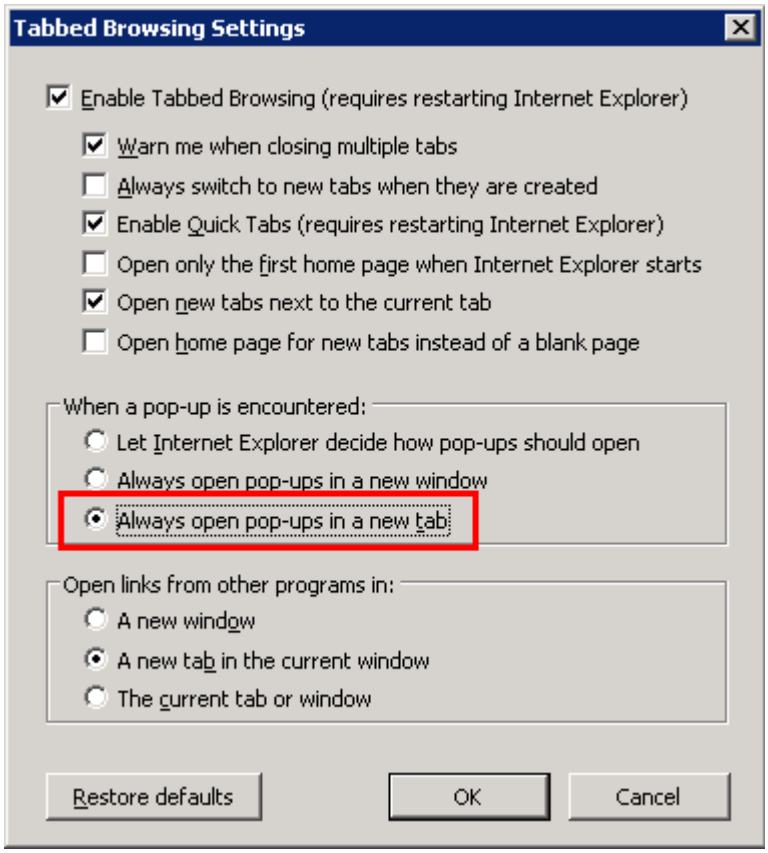
Currently, the HedEx supports IE7 and IE8. If the customer uses IE6, upgrading to IE7 is recommended. After the IE web browser is upgraded to IE7 or later, set the web browser as described in the next paragraph.

If the customer uses IE7 or later, choose **ToolsInternet Options** from the main menu of the IE and click the **General** tab. In the **Tabs** area, click **Settings**. In the **Tabbed Browsing Settings** dialog box, select **Always open pop-ups in a new tab** in the **When a pop-up is encountered:** area. Then click **OK**.

Copyright © Huawei Technologies Co., Ltd.



Copyright © Huawei Technologies Co., Ltd.



Copyright © Huawei Technologies Co., Ltd.

A NMS Alarm Reference

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

A.1 NE_COMMU_BREAK

A.2 NE_NOT_LOGIN

A.3 ALARM_PERFORM_LOG_SIZE_CROSS_THRESHOLD

A.4 GNE_CONNECT_FAIL

A.5 The Device Is Offline

A.6 COMMU_BREAK_BTWN_NE_AND_BAKGNE

A.7 GNE_MGR_LIMIT_OVER

A.8 DB_ERR_AUTO_CLEAR_FRAGMENT_DATA

A.9 MGR_LIMIT_OVER

A.10 EMS_SERVER_STARTUP

A.11 SERVICE_OUTAGE

A.12 PROTECT_DEGRADED

A.13 GNE_NUM_LIMIT_OVER

A.14 XC_LICENSE_OVERFLOW

A.15 XC_LICENSE_UNEXPECTED

A.16 NE_COMMU_GNE_SWITCH

A.17 PROTECT_LOSS

A.18 LOOP_ALM

A.19 CLOSETO_MAX_CAPACITY

A.20 OVERFLOW_MAX_CAPACITY

A.21 NE_DATA_INCONSISTENCY

Copyright © Huawei Technologies Co., Ltd.

A.22 CLOSETO_AIR_LICENSE_LIMIT

A.23 OVERFLOW_AIR_LICENSE_LIMIT

A.24 ALM-33 The Server Is Disconnected from the Database

A.25 ALM-34 The Disk Usage Is Too High (Warning)

A.26 ALM-35 The Disk Usage Is Too High (Minor)

A.27 ALM-36 The Disk Usage Is Too High (Major)

A.28 ALM-38 The database process is abnormal

A.29 ALM-39 The database had exception logs

A.30 ALM-40 The ESN of the server does not match that in the License file

A.31 ALM-42 The Database Usage Is Too High (Warning)

A.32 ALM-43 The Database Usage Is Too High (Minor)

A.33 ALM-44 The Database Usage Is Too High (Major)

A.34 ALM-47 Memory Usage of Service Is Too High

A.35 ALM-50 Task execution failure alarm

A.36 ALM-51 The temporary Feature field of the OSS License file expires

A.37 ALM-52 The temporary Feature field of the OSS License file enters to the default state

A.38 ALM-53 High log space usage for the database

A.39 ALM-54 The swap Usage Is High

A.40 Communication with the Device Failed

A.41 ALM-100 The CPU Usage Is High

A.42 ALM-101 The Disk Usage Is Too High (Critical)

A.43 ALM-102 The Memory Usage Is Too High

A.44 ALM-103 The Database Usage Is Too High (Critical)

A.45 ALM-106 The OSS Service Is Terminated Abnormally

A.46 MAC Address Conflict

A.47 OMC license not exist

A.48 ALM-114 The Number of Login Attempts Reaches the Maximum

A.49 ALM-116 The Master Server Cannot Communicate with the Slave Server

A.50 ALM-117 Avalanche alarm

A.51 ALM-120 The number of records in the database table has reached the threshold

A.52 Predeploy device type no match

A.53 ALM-121 Sending Remote Notification Message Failed

Copyright © Huawei Technologies Co., Ltd.

A.54 ALM-123 The Digital Certificate Is to Expire

A.55 ALM-124 The Digital Certificate Has Expired

A.56 ALM-119 Alarm of the Switchover to the Standby Syslog Server

A.57 ALM-118 Alarm of the Failure to Connect the Master and Standby Syslog Servers

A.58 ALM-130 The Alarm Report Buffering Blocked

A.59 ALM-294 Expired OSS License File

A.60 ALM-295 OSS License File in Default State

A.61 ALM-296 The NE Capacity Reached the Threshold Alarm

A.62 ALM-297 The OSS License Expired

A.63 ALM-298 The User in the SMManagers Group Changes a User's Password

A.64 ALM-299 An OSS User Is Added to the Administrators, SMManagers or Sub Domain User Group

A.65 The status of the interface configured with IPSec services turns to Down

A.66 ALM-801 OSS License Beyond Limitation

A.67 OceanStor Storage System Alarm

A.68 ALM-1100 CPU abnormal

A.69 ALM-1101 Memory abnormal

A.70 ALM-1102 Environment abnormal

A.71 ALM-1103 HD abnormal

A.72 ALM-1119 Network interface status changed

A.73 Power Failure

A.74 Fan Failure

A.75 Hard Disk Failure

A.76 The Network Cable Is Disconnected

A.77 NIC in Half-Duplex Mode

A.78 Power Threshold Alarm

A.79 Database Size exceeds the threshold

A.80 The size of Sybase logs exceeds the threshold

A.81 The usage of the paged kernel memory on Windows exceeds the alarm threshold

A.82 The usage of the non-paged kernel memory on Windows exceeds the alarm threshold

A.83 The virtual memory of Windows is insufficient

A.84 The disk space for the virtual memory of Windows is insufficient

Copyright © Huawei Technologies Co., Ltd.

A.85 The swap space is insufficient

A.86 Database needs to be maintenanced

A.87 Database needs to be maintenanced

A.88 Database needs to be maintenanced

A.89 NE SSH Fingerprint Mismatch

A.90 Failure to Connect to an Integration Server

A.91 Failure to Connect to All Integration Servers

A.92 Abnormal Integration Information

A.93 OCH_TRAIL_POWER_ABNORMAL

A.94 Communication Failure of Alarm Reporting Channel

A.95 Buffer Overflow of Alarm Reporting Channel

A.96 A Member System in the Maintenance State

A.97 PSEUDOWIRE_OUTAGE

A.98 Trap numbers of NEs exceeded the threshold of NMS

A.99 NE Management by Multiple U2000s

A.100 Data Inconsistency

A.101 tmp Occupies Much Space

A.102 Veritas Resources Are Faulty

A.103 Veritas replication buffer exceeds the threshold

A.104 Manual Restoration Is Required After Primary-Primary Veritas Status

A.105 Veritas Heartbeat Is Interrupted

A.106 The Veritas data replication is interrupted

A.107 Veritas Resource Group Is Frozen

A.108 Veritas License Is a Temporary One

A.109 Veritas Process Is Faulty

A.110 Automatic Backup Operation Failed

A.111 Automatic Save Operation Failed

A.112 Automatic Recover Operation Failed

A.113 ALM-52003 Host cpu usage

A.114 ALM-52004 Host memory usage

A.115 ALM-52005 Virtual machine cpu usage

A.116 ALM-52006 Virtual machine memory usage

Copyright © Huawei Technologies Co., Ltd.

A.117 ALM-52008 Unable connect to vCenter Server

A.118 ALM-52009 Datastore usage on disk

A.119 FIBER_POWER_DEG

A.120 Database Backup

A.121 Unified Management Engine License Alarm

A.122 A Fault Occurs on the FTP or SFTP Server That Is Used to Execute ONT Loading Tasks

A.123 CLOCK_LINK_LOOP

A.124 The device is unwonted

A.125 NE type change

Copyright © Huawei Technologies Co., Ltd.

A.1 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

There is no alarm parameter.

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 A-1**. 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.

Copyright © Huawei Technologies Co., Ltd.

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 A-1 Indicator description of the SCC board

Indicator	Name	Status	Description
STAT	Board Hardware Indicator	On (green)	The board works normally.
		On (red)	A critical alarm occurs on the board.
		On (yellow)	A minor alarm occurs on the board.
		Off	The board is not powered on.

Copyright © Huawei Technologies Co., Ltd.

Indicator	Name	Status	Description
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.
		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)	A critical or major alarm occurs in the service.
		On (yellow)	A minor or remote alarm occurs in the 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.

Copyright © Huawei Technologies Co., Ltd.

A.2 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

There is no alarm parameter.

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

There is no related information.

Copyright © Huawei Technologies Co., Ltd.

A.3 ALARM_PERFORM_LOG_SIZE_CROSS_THRESHOLD

Description

The ALARM_PERFORM_LOG_SIZE_CROSS_THRESHOLD alarm is generated when the number of records of alarms, performance events, and abnormal events exceeds the upper threshold of the log capacity.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3	Warning	Environment

Parameters

None.

Impact on the System

The system operation is not affected. If the database table that records alarms, performance events, or abnormal events is too large, it affects the response time of the U2000.

Possible Causes

The possible causes of the ALARM_PERFORM_LOG_SIZE_CROSS_THRESHOLD alarm are as follows:

- Cause 1: The value of the capacity alarm threshold is small, and thus the U2000 reports the alarm frequently.
- Cause 2: The number of records in the database exceeds the capacity alarm threshold.

Procedure

- Method 1: Reset the capacity alarm threshold.
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
  2. Set the dump for the threshold-crossing events. That is, set the parameters in the **Overflow Dump**, **Enable Dumping Periodically**, **Dump Settings**, **Automatic Deletion of Dump Files**, **Dumping when Overflow**, **Dumping in Schedule**, and **Dump To (Path)** areas.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Different parameters can be set for various threshold-crossing events. Therefore, a user needs to set the specific parameters of a threshold-crossing event.

3. Click **OK**.

NOTE

The default values are recommended when the U2000 database dump is set.

Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style). View the current situation of the alarm on the U2000. The alarm stops.

- Method 2: Dump the database table that records excessive alarms, performance events, or abnormal events to a file.
  1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
  2. **Optional:** Click **Query** to query the number of records of alarms, performance events, or abnormal events that can be dumped.
  3. Set the dump for the threshold-crossing events, including the **File**, **File type**, **Start time**, **End time**, and **Deadline** parameters.

     NOTE

     Different parameters can be set for various threshold-crossing events. Therefore, a user needs to set the specific parameters of a threshold-crossing event.

  4. Click **Dump** to wait for the U2000 to perform the overflow dump automatically.

  Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style). View the current situation of the alarm on the U2000. The alarm stops.

----End

Related Information

None.

A.4 GNE_CONNECT_FAIL

Description

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

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4	Critical	Communication

Parameters

There is no alarm parameter.

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

Step 1 Cause 1: The parameter settings about DCN communication of the gateway NE are incorrect.

1. Choose **Administration** > **DCN Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **DCN Management** from the main menu (application style). 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.

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

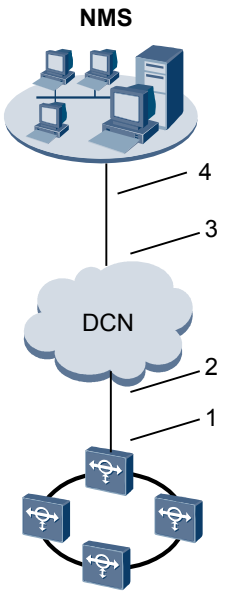
1. In NE Explorer, select the non-gateway NE and choose **Communication** > **Communication Parameters** from Function Tree.

Copyright © Huawei Technologies Co., Ltd.

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.

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.

Step 4 If the alarm persists, contact a Huawei engineer.

----End

Copyright © Huawei Technologies Co., Ltd.

Related Information

There is no related information.

A.5 The Device Is Offline

Description

Device discontinuity.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7	Critical	Equipment

Impact on the System

There is no impact on the system.

Possible Causes

- The device is offline.
- The NMS server cannot be connected to the device through ICMP/SNMP.

Procedure

Step 1 Check whether the device is offline.

Step 2 Check whether the route between the NMS server and the device is reachable.

----End

Related Information

There is no related information.

A.6 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.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7	Major	Communication

Parameters

There is no alarm parameter.

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

Step 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.

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** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **Physical Inventory** from the main menu (application style). Choose **NE** from the **Physical Inventory Type** navigation tree. 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.

Copyright © Huawei Technologies Co., Ltd.

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.

Step 3 If the alarm persists, contact a Huawei engineer.

----End

Related Information

There is no related information.

A.7 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	Major	Service

Parameters

There is no alarm parameter.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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

Step 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 **A.4 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.

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 **A.1 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.

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 (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **DCN Management** from the main menu (application style). Re-assign a gateway NE for each NE to ensure that the number of NEs connected to each gateway NE does not exceed 50.

Step 4 If the alarm persists, contact a Huawei engineer.

----End

Related Information

There is no related information.

A.8 DB_ERR_AUTO_CLEAR_FRAGMENT_DATA

Description

The DB_ERR_AUTO_CLEAR_FRAGMENT_DATA alarm is generated when the database fragments are automatically cleared. It indicates that the U2000 server has already cleared the management information tree (MIT) data that loses association with the parent node from the database.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
10	Critical	Environment

Parameters

None.

Impact on the System

- This alarm indicates that the data in the MIT is incorrectly associated during last period when the U2000 is running. The incorrectly associated data may cause unpredictable errors, such as a data repetition or EMS anomaly.
- When starting up, the system checks for data loss. If any data is lost, the system generates this alarm and clears all the data related to the lost data from the database to avoid an EMS startup failure or disorder of the user service data.
- The memory data loss may turn the data that is associated with the lost memory data in the database into junk data. When the U2000 continues running, the junk data may result in a disorder of service logic of the system. To avoid this type of faults, the system checks for such junk data during startup. If any junk data is detected, the system clears the data, and displays a prompt, indicating the necessity of networkwide data upload.

Possible Causes

This alarm is generated when the process memory data to be saved to the database is lost, or an error occurs during data saving. This alarm is generated when certain data that has been saved to the database becomes junk data because the process memory data that needs to be saved to the database is lost or an error occurs when the data is saved. When the U2000 clears the junk data, this alarm is reported.

Procedure

Step 1 Check whether the database server works normally.

1. Log in to the U2000 client. Right-click the **OSS** icon on the Main Topology and choose **Browse Current Alarms**.
2. View the current U2000 alarms to check for the alarms about the U2000 database or network communication. Such alarms include **A.4 GNE_CONNECT_FAIL** and **A.1 NE_COMMU_BREAK**.
3. In case of any alarm about the U2000 database or network communication, rectify the fault according to the handling procedure for the alarm.

Step 2 Upgrade the networkwide data. For details, see Uploading NE Configuration Data.

NOTE

If the NM data, such as the customized information of fibers and trails, is lost, you need to restore the data from the backup data, and then upload and search for trails.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Re-start the U2000 server and client, and then check whether the DB_ERR_AUTO_CLEAR_FRAGMENT_DATA alarm stops.

Step 4 If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

A.9 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

There is no alarm parameter.

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

Step 1 Method 1: Delete unnecessary NEs. For details, see Deleting NEs.

Step 2 Method 2: 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.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Method 3: When upgrading the NMS, contact a Huawei engineer and ask the engineer to apply for a license of larger management capability of the NMS.

Step 4 If the alarm persists, contact a Huawei engineer.

----End

Related Information

There is no related information.

A.10 EMS_SERVER_STARTUP

Description

An EMS_SERVER_STARTUP alarm is reported to the OSS after the U2000 server is restarted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
12	Warning	Communication

Parameters

None.

Impact on the System

None.

Possible Causes

The U2000 server is restarted.

Procedure

- No measure is required.

----End

Related Information

None.

Copyright © Huawei Technologies Co., Ltd.

A.11 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 ID	Alarm Severity	Alarm Type
20	Major	Service

Parameters

There is no alarm parameter.

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

Step 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.

Copyright © Huawei Technologies Co., Ltd.

Step 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.

Step 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

There is no related information.

A.12 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

Step 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.

Step 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.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Handle the current alarms that affect the service.

----End

A.13 GNE_NUM_LIMIT_OVER

Description

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

Attribute

Alarm ID	Alarm Severity	Alarm Type
22	Major	Service

Parameters

There is no alarm parameter.

Impact on the System

In case of the GNE_NUM_LIMIT_OVER alarm, the number of gateway 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 managed by the NE explorer exceeds the limit.

Procedure

Step 1 Choose **Administration** > **Settings** > **NE Partition** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **Settings** > **NE Partition** from the main menu (application style). Migrate certain gateway NEs to a similar NE explorer with the number of managed gateway NEs under the limit. For details, see Expanding the Capacity of the Transport NE Management Process, Balancing Load of an NE Explorer.

Step 2 If the alarm persists, contact a Huawei engineer.

----End

Related Information

There is no related information.

Copyright © Huawei Technologies Co., Ltd.

A.14 XC_LICENSE_OVERFLOW

Description

The XC_LICENSE_OVERFLOW alarm is generated when the number of subracks configured with certain service 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

There is no alarm parameter.

Impact on the System

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

Possible Causes

- The number of subracks that are configured with certain service type or cross-connect capacity and managed by the U2000 exceeds the license limit.
- A hybrid service type is used for an NG WDM NE. As a result, the number of occupied resources exceeds the license limit.

Procedure

- Locate the fault according to the alarm.
  1. Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).
  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.
- **Optional:** Apply for and update the license file to increase the number of subracks configured with certain cross-connect type or cross-connect capacity.
- **Optional:** Delete unused subracks.
  1. Choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu

Copyright © Huawei Technologies Co., Ltd.

(application style). 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**.

- **Optional:** Modify the subrack service type of the NE.
  1. Choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu (application style). 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. On the NE Panel, right-click the subrack and choose **Modify Shelf Attribute** from the shortcut menu.
  4. In the **Modify Shelf Attribute** dialog box, set **Service Type** to a non-hybrid type.
  5. Click **OK**.
- 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

There is no related information.

A.15 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

There is no alarm parameter.

Copyright © Huawei Technologies Co., Ltd.

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

- This alarm is reported for a subrack when the subrack has no cross-connection configured and its cross-connect type and cross-connect capacity have not been set. To clear this alarm, set **Cross-connect Type** to **None** and **Cross-connect Capacity** to **0G** if the subrack has no cross-connection configured.
- View the license information.
  1. Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Licenes Information** from the main menu (application style).
  2. Select the **Resource Control Item** tab in the displayed dialog box to view the license information.
- **Optional:** 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 (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu (application style). 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.

Copyright © Huawei Technologies Co., Ltd.

- 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

There is no related information.

A.16 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

There is no alarm parameter.

Impact on the System

There is no impact on the system.

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.
  1. Choose **Administration** > **DCN Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **DCN Management** from the main menu (application style).
  2. In the **Filter** dialog box, set the filter criteria and click **OK**.
  3. Select the NE that reported this alarm, right-click in the **Active GNE** column and choose **Switch to Primary GNE1** from the shortcut menu.
  4. In the **Operation Result** dialog box, click **Close**.

Copyright © Huawei Technologies Co., Ltd.

- If the fault persists, contact Huawei engineers.

----End

Related Information

There is no related information.

A.17 PROTECT_LOSS

Description

The PROTECT_LOSS is an alarm indicating that a trail is out of protection.

Attribute

Alarm ID	Alarm Severity	Alarm Type
26	Major	Service

Parameters

None.

Impact on the System

When this alarm occurs, the trail is out of protection.

Possible Causes

The trail is protected but its protection route or protected working route is interrupted.

Procedure

Step 1 Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, select **Alarm name** and enter **PROTECT_LOSS** in the text box to filter PROTECT_LOSS alarms.

Step 2 Right-click an alarm and choose **Alarm Affect Object** > **Link** from the shortcut menu.

Step 3 In the trail management window, right-click a desired trail or multiple trails and choose **Service Fault Analysis** from the shortcut menu. In the window that is displayed, check **Connectivity Status** of the trail or trails.

Step 4 Select a desired trail and click **Next**. On the **Fault Point Analysis** tab in the **Alarm Information** area, view alarm details.

Step 5 Select a desired alarm and click **Next**. In the **Troubleshooting Suggestion** area, view the troubleshooting suggestion and clear the alarm accordingly.

Copyright © Huawei Technologies Co., Ltd.

Step 6 If the fault persists, contact Huawei engineers for a solution.

----End

Related Information

None.

A.18 LOOP_ALM

Description

A LOOP_ALM alarm is reported after loopback is configured.

Attribute

Alarm ID	Alarm Severity	Alarm Type
27	Critical	Service

Parameters

None.

Impact on the System

This alarm indicates that loopback is configured for the optical port or channel of an NE line board or tributary board. The loopback setting may affect the receipt and transmission of services, thereby interrupting services.

Possible Causes

Out of test or maintenance needs, loopback is configured to loop a cross-connection back to its source or sink.

Procedure

Step 1 Set the loopback status of the cross-connection for which the alarm is reported to **Non-Loopback**.

1. Click the network-wide maintenance status icon on the toolbar.
2. In the **Networkwide Maintenance Status** dialog box, click the **Cross-Connection Loopback** tab.
3. In the object tree, select the NE that appears in the alarm location information and click to view the loopback status of channels.
4. Click **Query** to query the loopback status from the NE.

Copyright © Huawei Technologies Co., Ltd.

5. Set **Loopback Status** to **Non-Loopback** and click **Apply**. After a message is displayed indicating that the operation is successful, click **Close**.

----End

Related Information

None.

A.19 CLOSETO_MAX_CAPACITY

Description

The CLOSETO_MAX_CAPACITY alarm shows that the number of equivalent NEs managed by the current NE Explorer is close to the maximum capacity.

NOTE

For the transmit domain NE, the number of equivalent NEs managed by each NE Explorer is no more than 2,000.

Attribute

Alarm ID	Alarm Severity	Alarm Type
28	Critical	Security

Impact on the System

The U2000 performance or running efficiency may be degraded.

If you reduce the equivalent NE quantity to less than 95% of the maximum capacity, this alarm will be cleared. If you continue to create NEs, this alarm will not be reported again, but the **OVERFLOW_MAX_CAPACITY** alarm will be reported when the NE quantity exceeds the maximum capacity.

Possible Causes

The equivalent NEs that managed by the current NE Explorer exceed 95% of the maximum capacity.

Procedure

- Method 1: Delete unnecessary NEs. For details, see Deleting NEs.
- Method 2: Move some NEs to other NE Explorers.
  1. Add NE Explorers to expand the management capacity of the U2000. For details, see Expanding the Capacity of the Transport NE Management Process.
  2. Move some NEs to other NE Explorers. For details, see Balancing Load of an NE Explorer.

Copyright © Huawei Technologies Co., Ltd.

- If the alarm persists, contact a Huawei engineer.

----End

A.20 OVERFLOW_MAX_CAPACITY

Description

The OVERFLOW_MAX_CAPACITY alarm shows that the number of equivalent NEs managed by the current NE Explorer has exceeded the maximum capacity.

NOTE

For the transmit domain NE, the number of equivalent NEs managed by each NE Explorer is no more than 2,000.

Attribute

Alarm ID	Alarm Severity	Alarm Type
29	Critical	Security

Impact on the System

The U2000 performance or running efficiency may deteriorate.

Possible Causes

The equivalent NEs that managed by the current NE Explorer exceeds the maximum capacity.

Procedure

- Method 1: Delete unnecessary NEs. For details, see Deleting NEs.
- Method 2: Move some NEs to other NE Explorers.
  1. Add NE Explorers to expand the management capacity of the U2000. For details, see Expanding the Capacity of the Transport NE Management Process.
  2. Move some NEs to other NE Explorers. For details, see Balancing Load of an NE Explorer.
- If the alarm persists, contact a Huawei engineer.

----End

A.21 NE_DATA_INCONSISTENCY

Description

The NE_DATA_INCONSISTENCY alarm indicates that the data on the NE that reports alarms is inconsistent with the data on the U2000.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
30	Minor	Process

Impact on the System

Data on the NE that reports alarms may be inconsistent with that on the U2000. Therefore, operations on the U2000 may be invalid.

NOTE

When the U2000 detects data inconsistency between NEs and the U2000, it reports the alarm. When data inconsistency occurs, it causes the following results:

The synchronized data reported from NEs changes

The U2000 regularly detects that the final synchronization serial numbers (SNs) are inconsistent.

Manually querying the synchronization data triggers the detecting of the final synchronization SNs.

The alarm is cleared when the data synchronization is performed. Data synchronization operations include uploading, synchronizing, and downloading NE data.

Possible Causes

- Data inconsistency between NEs and the U2000 may be caused by the modification on NE configuration with command line tools.
- Assume that an NE is managed by multiple NMSs. After data is modified on one NMS, data on the NE is inconsistent with data on another NMS. As a result, the NMS report this alarm.

Procedure

- Method 1: Perform the uploading operation. For details, see Uploading NE Configuration Data.
- Method 2: Perform NE data synchronization. For details, see Synchronizing NE Configuration Data.
- Method 3: Perform the downloading operation. For details, see Downloading NE Configuration Data.
- Contact Huawei R&D engineers if the fault still exists.

----End

A.22 CLOSETO_AIR_LICENSE_LIMIT

Description

The CLOSETO_AIR_LICENSE_LIMIT is an alarm indicating that the consumption of network-wide microwave air-interface capacity is close to the license limit.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
31	Major	Security

Parameters

None.

Impact on the System

- When this alarm occurs, the consumption of network-wide microwave air-interface capacity exceeds the specified alarm threshold and is close to the license limit. In this case, you need to reduce the capacity consumption or apply for a license that permits larger capacity consumption.
- This alarm prompts you only to take actions in a timely manner and does not affect the network or services.

Possible Causes

The consumption of network-wide microwave air-interface capacity exceeds the specified alarm threshold and is close to the license limit.

Procedure

Step 1 Use the **Microwave Air Interface Capacity License Report** function to generate a report. Then, check the license-permitted consumption, actual consumption, and alarm threshold of network-wide microwave air-interface capacity.

NOTE

Choose **Inventory** > **Microwave Report** > **Microwave Air Interface Capacity License Report** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **Microwave Report** > **Microwave Air Interface Capacity License Report** from the main menu (application style).

Step 2 If the capacity consumption exceeds the alarm threshold, reduce the capacity consumption or apply for a license that permits larger capacity consumption.

----End

Related Information

None.

A.23 OVERFLOW_AIR_LICENSE_LIMIT

Description

The OVERFLOW_AIR_LICENSE_LIMIT is an alarm indicating that the consumption of network-wide microwave air-interface capacity exceeds the license limit.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
32	Critical	Security

Parameters

None.

Impact on the System

- When this alarm occurs, the consumption of network-wide microwave air-interface capacity exceeds the license limit. In this case, you need to reduce the capacity consumption or apply for a license that permits larger capacity consumption.
- When this alarm occurs, take timely actions. If the grace period expires, some microwave functions will be unavailable.

Possible Causes

The consumption of network-wide microwave air-interface capacity exceeds the license limit.

Procedure

Step 1 Use the **Microwave Air Interface Capacity License Report** function to generate a report. Then, check the license-permitted consumption and actual consumption of network-wide microwave air-interface capacity.

NOTE

Choose **Inventory** > **Microwave Report** > **Microwave Air Interface Capacity License Report** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **Microwave Report** > **Microwave Air Interface Capacity License Report** from the main menu (application style).

Step 2 If the capacity consumption exceeds the license limit, reduce the capacity consumption or apply for a license that permits larger capacity consumption.

----End

Related Information

None.

A.24 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 that the connection is recovered, the alarm is cleared.

Copyright © Huawei Technologies Co., Ltd.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

This alarm cannot be automatically cleared in the following situations:

- The name of the server that generates this alarm is changed.
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
33	Major	Processing error

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Database service name of the server.
Database	Database name.

Impact on the System

- Database-involved operations fail.
- The U2000 functions are unavailable.

System Actions

None.

Possible Causes

- The database service is abnormal.
- The Sybase or SQL Server database password is incorrect.
- The Sybase or SQL Server database password has expired.
- The Sybase or SQL Server database account is locked.
- The U2000 frequently accesses the database, and the database cannot respond to new connection requests in a timely manner due to insufficient system resources or the busy database.

Procedure

Step 1 Attempt to log in to the database.

For the Sybase database, set Sybase database environment variables and run the **isql -Usa -SDBSVR** command as the **dbuser** user to log in to the database.

Copyright © Huawei Technologies Co., Ltd.

For the SQL Server database, run the **isql -Usa -SDBSVR** command as the **dbuser** user to log in to the database.

- If the login is successful, go to **Step 2**.
- If the login fails, the database service may be abnormal, the database password may be incorrect, the database password may have expired, or the database account may be locked. Visit the official website of the database and query the help information and troubleshooting method based on the error message provided by the database.

NOTE

Official websites of various databases:

- Sybase database: **http://infocenter.sybase.com**
- SQL Server database: **http://www.microsoft.com**

Step 2 Log in to the U2000 client. Choose **System** > **System Monitor** > **Settings** from the main menu (application style) from the main menu. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab and view the value of **Database usage sampling interval**, which indicates the database monitoring interval.

Step 3 Wait for a database monitoring interval and check whether the alarm is automatically cleared.

- If the alarm is automatically cleared, and you do not care or you have known the operations that the U2000 performs when the alarm is reported, the procedure ends.
- If the alarm is automatically cleared, and you want to know the operations that the U2000 performs when the alarm is reported, go to **Step 4**.
- If the alarm is not cleared, the database cannot respond to new connection requests in a timely manner probably because the database is busy. Go to **Step 4**.

Step 4 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.25 ALM-34 The Disk Usage Is Too High (Warning)

Description

When the disk or partition (volume) usage is greater than or equal to the threshold for generating a warning alarm for high disk usage, the U2000 generates this alarm. When the disk or partition (volume) usage falls below the threshold for clearing a warning alarm for high disk usage, the alarm is cleared.

NOTE

To set the threshold for generating a high disk usage alarm, log in to the U2000 system monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Hard Disk Monitor** tab. Then set the threshold on the **Hard Disk Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, these alarms need to be cleared manually.

Copyright © Huawei Technologies Co., Ltd.

- The name of the server that generates this alarm is changed.
- The mount point of the disk that generates this alarm is changed.
- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
34	Warning	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server that generates an alarm.
Disk	Disk path of the server that generates an alarm.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
Capacity	Disk capacity.
Usage	Disk usage.

Impact on the System

The U2000 service may fail to write data to the disk, and database exceptions may occur.

System Actions

None.

Possible Causes

- The disk contains many unnecessary files.
  - The recycle bin is not emptied.
  - The U2000 server has received a large amount of data, including NE alarms, events, and logs. All the data is exported from the database to the disk in a short time.
  - Many temporary data files and backup files are stored.
- The threshold for generating a high disk usage alarm is small.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Delete unnecessary files from the disk.

- If the server runs on Windows OS, perform the following operations:

  1. Empty the recycle bin.
  2. Delete unnecessary U2000 files from the disk.

     NOTE

     If you are not sure whether a file can be deleted, contact Huawei technical support engineers.

     Use **Explore** to delete unnecessary files, such as historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files.

     Table A-2 lists the U2000 files that can be deleted.

     Table A-2 U2000 files that can be deleted on Windows OS

Directory	File to Be Deleted	Method
D:\oss\server\var\logs	Core files (whose names start with core)	Use FileZilla to back up the files to another disk and run the **del** command to delete them from the current disk. For details about how to use the FileZilla tool, see How Do I Use FileZilla to Transfer Files?.
D:\oss\server\var\logs\traceback	Trace backup files	Run the **del** command to delete excessive backup trace files.
D:\oss\server\var\logs\mrblog	Dumped MRB log files	Run the **del** command to delete excessive .gz files.

  3. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
     - If yes, no further operation needs to be taken.

Copyright © Huawei Technologies Co., Ltd.

- If no, go to **Step 2**.

- If the server runs on Solaris or SUSE Linux OS, perform the following operations:

  1. Empty the recycle bin.

     Log in to the U2000 server on Xwindows and perform the following operations in the graphical user interface (GUI):

  2. Run the **df -k** command to identify the disks whose disk usage is high.

     If other disks also have high disk usage besides the **Disk** in the alarm parameter but no alarm has been generated, free up some space for all these disks.

  3. Run the **cd** command to open the directory that occupies much disk space. Then run the **LC_ALL=en_US du -k | LC_ALL=en_US sort -nr >** */tmp/du_k.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **du_k.txt**.

  4. Run the **more** */tmp/du_k.txt* command to view **du_k.txt** and find the subdirectory that causes high disk usage.

  5. Run the **cd** command to open the subdirectory that causes high disk usage. Then run the **ls -l >** */tmp/ls_l.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **ls_l.txt**.

  6. Run the **more** */tmp/ls_l.txt* command 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 delete these files. You are advised to delete the historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files. **Table A-3** lists the U2000 and database files that can be deleted.

     NOTE

     If you are not sure whether a file can be deleted, contact the system administrator or Huawei technical support engineers.

Table A-3 U2000 and database files that can be deleted on Solaris or SUSE Linux OS

Directory	File to Be Deleted	Method
/opt/oss/server/var/logs	Core files (whose names start with **core**)	Use FTP to back up the files to another disk and run the **rm** command to delete them from the current disk.
/opt/oss/server/var/logs/tracebak	Trace backup files	Run the **rm** command to delete excessive backup trace files.
/opt/oss/server/var/logs/mrblog	Dumped MRB log files	Run the **rm** command to delete excessive .gz files.

Copyright © Huawei Technologies Co., Ltd.

Directory	File to Be Deleted	Method
/opt/sybase/ASE-15_0/install (Solaris)	Sybase database logs. **NOTE** Check whether oversized Sybased database log files exist. If a log file is oversized, delete it. (A Sybase database log file is named in *Database instance name*.log format, for example, **DBSVR.log**.)	Run the following commands to delete the oversized Sybase database log file, for example, **DBSVR.log**: $ **cd** */opt/sybase/ASE-15_0/install* $ **rm** *DBSVR.log*

7. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

Step 2 Check whether the threshold for generating a warning alarm for high disk usage of the U2000 server is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a warning alarm for high disk usage is greater than or equal to 60% (the default value).
   - If yes, go to **Step 3**.
   - If no, increase the threshold for generating a warning alarm for high disk usage to 60% and increase the alarm clearance threshold to 55% (the default value). Then go to **Step 2.2**.
2. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.26 ALM-35 The Disk Usage Is Too High (Minor)

Description

When the disk or partition (volume) usage is greater than or equal to the threshold for generating a minor alarm for high disk usage, the U2000 generates this alarm. When the disk or partition (volume) usage falls below the threshold for clearing a minor alarm for high disk usage, the alarm is cleared.

NOTE

To set the threshold for generating a high disk usage alarm, log in to the U2000 system monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Hard Disk Monitor** tab. Then set the threshold on the **Hard Disk Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, these alarms need to be cleared manually.

- The name of the server that generates this alarm is changed.
- The mount point of the disk that generates this alarm is changed.
- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
35	Minor	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Disk	Disk for whom the server generates an alarm.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
Capacity	Disk capacity.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Usage	Disk usage.

Impact on the System

The U2000 service may fail to write data to the disk, and database exceptions may occur.

System Actions

None.

Possible Causes

- The disk contains many unnecessary files.
  - The recycle bin is not emptied.
  - The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to the disk in a short time.
  - Many temporary data files and backup files are stored.
- The threshold for generating a minor alarm for high disk usage is small.

Procedure

Step 1 Delete unnecessary files from the disk.

- If the server runs on Windows OS, perform the following operations:
  1. Empty the recycle bin.
  2. Delete unnecessary U2000 files from the disk.

     NOTE

     If you are not sure whether a file can be deleted, contact Huawei technical support engineers.

     Use **Explore** to delete unnecessary files, such as historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files.

     Table A-4 lists the U2000 files that can be deleted.

Copyright © Huawei Technologies Co., Ltd.

Table A-4 U2000 files that can be deleted on Windows OS

Directory	File to Be Deleted	Method
D:\oss\server\var\logs	Core files (whose names start with core)	Use FileZilla to back up the files to another disk and run the **del** command to delete them from the current disk. For details about how to use the FileZilla tool, see How Do I Use FileZilla to Transfer Files?.
D:\oss\server\var\logs\traceback	Trace backup files	Run the **del** command to delete excessive backup trace files.
D:\oss\server\var\logs\mrblog	Dumped MRB log files	Run the **del** command to delete excessive .gz files.

3. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

- If the server runs on Solaris or SUSE Linux OS, perform the following operations:

  1. Empty the recycle bin.

     Log in to the U2000 server on Xwindows and perform the following operations in the graphical user interface (GUI):

  2. Run the **df -k** command to identify the disks whose disk usage is high.

     If other disks also have high disk usage besides the **Disk** in the alarm parameter but no alarm has been generated, free up some space for all these disks.

  3. Run the **cd** command to open the directory that occupies much disk space. Then run the **LC_ALL=en_US du -k | LC_ALL=en_US sort -nr >** */tmp/du_k.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **du_k.txt**.

Copyright © Huawei Technologies Co., Ltd.

4. Run the **more** */tmp/du_k.txt* command to view **du_k.txt** and find the subdirectory that causes high disk usage.
5. Run the **cd** command to open the subdirectory that causes high disk usage. Then run the **ls -l >** */tmp/ls_l.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **ls_l.txt**.
6. Run the **more** */tmp/ls_l.txt* command 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 delete these files. You are advised to delete the historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files. **Table A-5** lists the U2000 and database files that can be deleted.

   NOTE

   If you are not sure whether a file can be deleted, contact the system administrator or Huawei technical support engineers.

Table A-5 U2000 and database files that can be deleted on Solaris or SUSE Linux OS

Directory	File to Be Deleted	Method
/opt/oss/server/var/logs	Core files (whose names start with **core**)	Use FTP to back up the files to another disk and run the **rm** command to delete them from the current disk.
/opt/oss/server/var/logs/tracebak	Trace backup files	Run the **rm** command to delete excessive backup trace files.
/opt/oss/server/var/logs/mrblog	Dumped MRB log files	Run the **rm** command to delete excessive .gz files.
/opt/sybase/ASE-15_0/install (Solaris)	Sybase database logs. **NOTE** Check whether oversized Sybased database log files exist. If a log file is oversized, delete it. (A Sybase database log file is named in *Database instance name*.log format, for example, **DBSVR.log**.)	Run the following commands to delete the oversized Sybase database log file, for example, **DBSVR.log**: $ **cd** */opt/sybase/ASE-15_0/install* $ **rm** *DBSVR.log*

7. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current**

Copyright © Huawei Technologies Co., Ltd.

Alarm from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If yes, no further operation needs to be taken.
- If no, go to **Step 2**.

Step 2 Check whether the threshold for generating a minor alarm for high disk usage of the U2000 server is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a minor alarm for high disk usage is greater than or equal to 70% (the default value).
   - If yes, go to **Step 3**.
   - If no, increase the threshold to 70% and increase the alarm clearance threshold to 65% (the default value). Then go to **Step 2.2**.
2. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.27 ALM-36 The Disk Usage Is Too High (Major)

Description

When the disk or partition (volume) usage is greater than or equal to the threshold for generating a major alarm for high disk usage, the U2000 generates this alarm. When the disk or partition (volume) usage falls below the threshold for clearing a major alarm for high disk usage, the alarm is cleared.

NOTE

To set the threshold for generating a high disk usage alarm, log in to the U2000 system monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Hard Disk Monitor** tab. Then set the threshold on the **Hard Disk Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, these alarms need to be cleared manually.

- The name of the server that generates this alarm is changed.
- The mount point of the disk that generates this alarm is changed.

Copyright © Huawei Technologies Co., Ltd.

- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
36	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Disk	Disk for whom the server generates an alarm.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
Capacity	Disk capacity.
Usage	Disk usage.

Impact on the System

The U2000 service may fail to write data to the disk, and database exceptions may occur.

System Actions

None.

Possible Causes

- The disk contains many unnecessary files.
  - The recycle bin is not emptied.
  - The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to the disk in a short time.
  - Many temporary data files and backup files are stored.
- The threshold for generating a major alarm for high disk usage is small.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Delete unnecessary files from the disk.

- If the server runs on Windows OS, perform the following operations:

  1. Empty the recycle bin.
  2. Delete unnecessary U2000 files from the disk.

     NOTE

     If you are not sure whether a file can be deleted, contact Huawei technical support engineers.

     Use **Explore** to delete unnecessary files, such as historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files.

     Table A-6 lists the U2000 files that can be deleted.

     Table A-6 U2000 files that can be deleted on Windows OS

Directory	File to Be Deleted	Method
D:\oss\server\var\logs	Core files (whose names start with core)	Use FileZilla to back up the files to another disk and run the **del** command to delete them from the current disk. For details about how to use the FileZilla tool, see How Do I Use FileZilla to Transfer Files?.
D:\oss\server\var\logs\traceback	Trace backup files	Run the **del** command to delete excessive backup trace files.
D:\oss\server\var\logs\mrblog	Dumped MRB log files	Run the **del** command to delete excessive .gz files.

  3. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
     - If yes, no further operation needs to be taken.

Copyright © Huawei Technologies Co., Ltd.

- If no, go to **Step 2**.

- If the server runs on Solaris or SUSE Linux OS, perform the following operations:

  1. Empty the recycle bin.

     Log in to the U2000 server on Xwindows and perform the following operations in the graphical user interface (GUI):

  2. Run the **df -k** command to identify the disks whose disk usage is high.

     If other disks also have high disk usage besides the **Disk** in the alarm parameter but no alarm has been generated, free up some space for all these disks.

  3. Run the **cd** command to open the directory that occupies much disk space. Then run the **LC_ALL=en_US du -k | LC_ALL=en_US sort -nr >** */tmp/du_k.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **du_k.txt**.

  4. Run the **more** */tmp/du_k.txt* command to view **du_k.txt** and find the subdirectory that causes high disk usage.

  5. Run the **cd** command to open the subdirectory that causes high disk usage. Then run the **ls -l >** */tmp/ls_l.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **ls_l.txt**.

  6. Run the **more** */tmp/ls_l.txt* command 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 delete these files. You are advised to delete the historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files. **Table A-7** lists the U2000 and database files that can be deleted.

     NOTE

     If you are not sure whether a file can be deleted, contact the system administrator or Huawei technical support engineers.

Table A-7 U2000 and database files that can be deleted on Solaris or SUSE Linux OS

Directory	File to Be Deleted	Method
/opt/oss/server/var/logs	Core files (whose names start with **core**)	Use FTP to back up the files to another disk and run the **rm** command to delete them from the current disk.
/opt/oss/server/var/logs/tracebak	Trace backup files	Run the **rm** command to delete excessive backup trace files.
/opt/oss/server/var/logs/mrblog	Dumped MRB log files	Run the **rm** command to delete excessive .gz files.

Copyright © Huawei Technologies Co., Ltd.

Directory	File to Be Deleted	Method
/opt/sybase/ASE-15_0/install (Solaris)	Sybase database logs. NOTE Check whether oversized Sybased database log files exist. If a log file is oversized, delete it. (A Sybase database log file is named in *Database instance name*.log format, for example, **DBSVR.log**.)	Run the following commands to delete the oversized Sybase database log file, for example, **DBSVR.log**: $ **cd** */opt/sybase/ASE-15_0/install* $ **rm** *DBSVR.log*

7. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

Step 2 The threshold for generating a major alarm for high disk usage of the U2000 server is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a major alarm for high disk usage is greater than or equal to 80% (the default value).
   - If yes, go to **Step 3**.
   - If no, increase the threshold to 80% and increase the alarm clearance threshold to 75% (the default value). Then go to **Step 2.2**.
2. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.28 ALM-38 The database process is abnormal

Description

On Solaris or SUSE Linux OS, if the service process of the Sybase database does not exist, this alarm is generated. If the service process of the Sybase database appears again, the alarm is cleared.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared.

- The name of the server that generates this alarm is changed.
- The server that generates this alarm runs on Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
38	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Database service	Sybase database service name.

Impact on the System

The U2000 services fail to access the database. The fault and security menus that need to read data from the database are unavailable. Only the topology menu items are available. If the fault lasts for a long time, alarm information will be lost or the U2000 functions are unavailable.

System Actions

None.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The server is powered off, ending the Sybase database process.
- Sybase database process is ended manually.

Procedure

Step 1 For details about how to rectify Sybase database faults, see **The Sybase Database Process Is Abnormal**.

If the Sybase database process is abnormal, perform the following operations:

1. Use the PuTTY to log in to the U2000 server as user **ossuser** in SSH mode.
2. Run the following command to switch to dbuser:

   $ **su - dbuser**

   Password: ***Password of dbuser***
3. Run the following commands to start the Sybase database, such as Sybase database 15.0 (the directory varies according to database versions):

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

   $ **./startserver -f** *./RUN_DBSVR*

   $ **nohup ./startserver -f** *./RUN_DBSVR_back*

   DBSVR and **DBSVR_back** are the names of the database instance and the backup database instance respectively.

   - If the Sybase database is started and the alarm is cleared, go to **1.4** to identify the fault cause.
   - If the Sybase database fails to be started, go to **1.4**.
4. Run the following commands to view the database log files, such as **DBSVR.log** (the file name is the same as the database instance name):

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

   $ **more -100** *DBSVR.log*

   NOTE

   - Each error log contains the time when the error occurred. Query the error logs around the time when this alarm was generated.
   - Check the log files for "Error" and find the error codes. For example, error 926 is recorded as follows:

     ```
     Error: 926,Severity: 14,State: 1 00:00000:00001:2007/09/14 15:36:26.65
     server Database 'FaultDB' cannot be opened.
     ```

   - If no error is found, go to **1.5**.
   - If an error is found, go to **1.6**.
5. Run the following commands to check whether the database is normal:

   $ **.** */opt/sybase/SYBASE.sh*

   $ **isql -S***DBSVR* **-U***sa*

   Password: ***Password of sa***

   NOTE

   In order to enhance the security of the Sybase database after the U2000 is installed, the **sa** user may be manually disabled and replaced with a customized administrator name, such as **dbadmin**.

Copyright © Huawei Technologies Co., Ltd.

If **1>** is displayed, the database is running properly. If **1>** is not displayed, check that the **sa** password is correct.

Run the following command to check whether the database status is **offline**:

1>**sp_helpdb**

2>**go**

- If yes, go to **Step 2**.
- If no, the database has been recovered, and no further operation needs to be taken.

6. Recover the database based on the error code. For example, if error 926 is found, run the following commands to recover the FaultDB database:

1>**sp_configure "allow updates"** *1*

2>**go**

1>**update sysdatabases set status=32768 where name="FaultDB"**

2>**go**

1>**shutdown SYB_BACKUP**

2>**go**

1>**shutdown**

2>**go**

After the database is recovered, restart the Sybase database by following the instructions described in **1.3** and log in to the Sybase database as user **sa**.

1>**update sysdatabases set status=0 where name="FaultDB"**

2>**go**

1>**sp_configure "allow updates"** *0*

2>**go**

1>**shutdown SYB_BACKUP**

2>**go**

1>**shutdown**

2>**go**

- After you rectify the fault and start the database, the alarm is cleared. The alarm processing is complete.
- If you cannot start the database, go to **Step 2**.

Step 2 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.29 ALM-39 The database had exception logs

Description

If the Sybase database generates an exception log at level 19 or higher, this alarm is generated. This alarm cannot be automatically cleared and must be manually cleared.

Copyright © Huawei Technologies Co., Ltd.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared .

- The name of the server that generates this alarm is changed.
- The server that generates this alarm runs on Solaris or SUSE Linux. The OS is upgraded or an OS patch is installed after the alarm is generated.
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
39	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Database service	Sybase database service name.

Impact on the System

The database is faulty, and the U2000 functions may be unavailable.

System Actions

None.

Possible Causes

The operation on the Sybase database is abnormal.

Procedure

Step 1 For details about how to rectify Sybase database faults, see **The Sybase Database Log Is Abnormal**.

If the Sybase database generates abnormal logs, perform the following operations:

1. Use the PuTTY to log in to the U2000 server as user **ossuser** in SSH mode.
2. View the database log files and identify the abnormal operations performed on the Sybase database.

Copyright © Huawei Technologies Co., Ltd.

The log files of the Sybase database are stored in **/opt/sybase/ASE-15_0/install**.(Sybase 15.0 is used as an example. The directory varies according to database versions.) The log file name of the primary database is ***Service name of the primary database*.log**. You can run the **more** command to view the log file.

- Identify abnormal operations and rectify the fault on the Sybase database. The alarm processing is complete.
- If you cannot identify abnormal operations or rectify the fault on the Sybase database, go to **Step 2**.

Step 2 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.30 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 generates an alarm.

Impact on the System

The services or functions controlled by the License are unavailable after the grace period.

System Actions

None.

Possible Causes

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

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Apply for another License or contact Huawei technical support engineers.

----End

A.31 ALM-42 The Database Usage Is Too High (Warning)

Description

When the database usage is greater than or equal to the threshold for generating a warning alarm for high database usage, the U2000 generates this alarm. When the database usage falls below the threshold, the alarm is cleared.

NOTE

To set the threshold for generating a warning alarm for high database usage, log in to the U2000 System Monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Then set the threshold on the **Database Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared.

- The name of the server that generates this alarm is changed.
- After the alarm is generated for a database, the value of **Threshold** is changed to **Disabled Monitoring** for the database related to the alarm. (Change method: In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. In the **Property** column, expand the nodes under **Custom** until the name of the database related to the alarm is displayed, and then click the cell in the **Threshold** column corresponding to the database name and select **Disabled Monitoring** from the drop-down list.)
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
42	Warning	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Database service name.
Database	Database name.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Size	Database capacity.
Threshold	Threshold for generating an alarm.
Usage	Database usage.

Impact on the System

If the database usage is too high, database-involved operations on the U2000 database may fail. For example, alarm information may fail to be saved to the database.

This alarm may not bring advertise impact soon.

System Actions

None.

Possible Causes

- The U2000 receives a large number of alarms or events within a short period of time.
- The U2000 records a large number of logs within a short period of time.
- The threshold for generating a warning alarm for high database usage is small.
- The period of U2000 data export or dump or other parameters are set incorrectly, leading to high usage of the alarm database.
- Small space has been allocated to the U2000 database.

Procedure

Step 1 Check whether a large number of alarms or events are reported within a short period of time.

1. Check whether **Database** in the alarm information is the alarm database **fmdb**.
   - If yes, go to **Step 1.2**.
   - If no, go to **Step 2**.
2. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported within a short period of time. Choose **Fault** > **Browse Event Logs** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Query Event Logs** from the main menu (application style). In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported within a short period of time.
   - If a large number of alarms or events are reported within a short period of time, go to **Step 1.3**.

Copyright © Huawei Technologies Co., Ltd.

- If a small number of alarms or events are reported within a short period of time, go to **Step 3**.

3. Handle these alarms or events reported within a short period of time.

   Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, run the scheduled task of dumping alarms or events immediately and identify the causes for these alarms or events.

4. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 2 Check whether a large number of logs are reported within a short period of time.

1. Check whether **Database** in the alarm information is the log database **logdb**.
   - If yes, go to **Step 2.2**.
   - If no, go to **Step 3**.
2. (Generally, only system logs are recorded in large quantities within a short period of time.) Log in to the U2000 client. Choose **Administration** > **Log Management** > **Query System Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query System Logs** from the main menu (application style). In the **Query System Logs** window, check whether a large number of system logs are reported (more than 300 logs per second) are reporded.
   - If yes, go to **Step 2.3**.
   - If no, go to **Step 3**.
3. Handle these logs reported within a short period of time.

   In the **Task Management** window, run the scheduled task for system log dump immediately, and identify the cause for system log generation.

4. Log in to the U2000 client, and choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Check whether the threshold for generating a warning alarm for high database usage is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Check whether the threshold for generating a warning alarm for high database usage is greater than or equal to 85% (the default value).
   - If yes, go to **Step 4**.
   - If no, increase the threshold to 85% and go to **Step 3.2**.

Copyright © Huawei Technologies Co., Ltd.

2. After **Database usage sampling interval** elapses, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 4**.

Step 4 Check whether the period of U2000 data export or dump or other parameters are set incorrectly.

1. Log in to the U2000 client.Choose **Fault** > **Query Alarm Log Statistics** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Alarm Log Statistics** from the main menu (application style).
2. In the **Filter** dialog box, click the **Basic Settings** tab. In **Occurred** area, change the value of **Previous** to **90**, and click **OK** to collect statistics on the historical alarm records generated in recent 90 days.
3. In the **Confirm** dialog box, click **Yes**.
   - If there are a large number of historical alarm records, the data export or dump period or other parameters may be set incorrectly. As a result, the amount of data written to the database is larger than the amount of data dumped within a short period of time. In this case, go to **Step 4.4**.
   - If the number of historical alarm records is not large, go to **Step 5**.
4. Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style). In the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump** from the navigation tree. In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Run Now** from the shortcut menu.
5. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Attributes** from the shortcut menu. In the **Attributes** dialog box, click the **Extended Parameters** tab. Change the value of **Storage period in database(days)** to a smaller value, for example, 30 days.
6. After **Database usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.32 ALM-43 The Database Usage Is Too High (Minor)

Description

When the database usage is greater than or equal to the threshold for generating a minor alarm for high database usage, the U2000 generates this alarm. When the database usage falls below the threshold, the alarm is cleared.

NOTE

To set the threshold for a minor alarm for high database usage, log in to the U2000 System Monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Then set the threshold on the **Database Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared.

- The name of the server that generates this alarm is changed.
- After the alarm is generated for a database, the value of **Threshold** is changed to **Disabled Monitoring** for the database related to the alarm. (Change method: In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. In the **Property** column, expand the nodes under **Custom** until the name of the database related to the alarm is displayed, and then click the cell in the **Threshold** column corresponding to the database name and select **Disabled Monitoring** from the drop-down list.)
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
43	Minor	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Database service name.
Database	Database name.
Size	Database capacity.
Threshold	Threshold for generating an alarm.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Usage	Database usage.

Impact on the System

If the database usage is too high, database-involved operations on the U2000 database may fail. For example, alarm information may fail to be saved to the database.

This alarm may not bring advertise impact soon. However, you need to check whether the database usage is increased continuously.

System Actions

None.

Possible Causes

- The U2000 receives a large number of alarms or events within a short period of time.
- The U2000 records a large number of logs within a short period of time.
- The threshold for generating a minor alarm for high database usage is small.
- The period of U2000 data export or dump or other parameters are set incorrectly, leading to high usage of the alarm database.
- Small space has been allocated to the U2000 database.

Procedure

Step 1 Check whether a large number of alarms or events are reported within a short period of time.

1. Check whether **Database** in the alarm information is the alarm database **fmdb**.
   - If yes, go to **Step 1.2**.
   - If no, go to **Step 2**.
2. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported within a short period of time. Choose **Fault** > **Browse Event Logs** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Query Event Logs** from the main menu (application style). In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported within a short period of time.
   - If a large number of alarms or events are reported within a short period of time, go to **Step 1.3**.
   - If a small number of alarms or events are reported within a short period of time, go to **Step 3**.
3. Handle these large number of alarms or events that an NE has reported within a short period of time.

Copyright © Huawei Technologies Co., Ltd.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, run the scheduled task of dumping alarms or events immediately, and identify the causes for these alarms or events.

4. Wait for 10 minutes after masking alarms or events that have been reported in a short period of time and log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 2 Check whether a large number of logs are reported within a short period of time.

1. Check whether **Database** in the alarm information is the log database **logdb**.
   - If yes, go to **Step 2.2**.
   - If no, go to **Step 3**.
2. Generally, only system logs are recorded in large quantities within a short period of time. Log in to the U2000 client. Choose **Administration** > **Log Management** > **Query System Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query System Logs** from the main menu (application style). In the **Query System Logs** window, check whether a large number of system logs (more than 300 logs per second) are recorded.
   - If yes, go to **Step 2.3**.
   - If no, go to **Step 3**.
3. Handle these logs reported within a short period of time.

   In the **Task Management** window, run the scheduled tasks for system log dump immediately, and identify the causes for system log generation.
4. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Check whether the threshold for generating a minor alarm for high database usage is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Check whether the threshold for generating a minor alarm for high database usage is greater than or equal to 90% (the default value).
   - If yes, go to **Step 4**.
   - If no, increase the threshold to 90% and go to **Step 3.2**.
2. After the **Database usage sampling interval** elapses, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box,

Copyright © Huawei Technologies Co., Ltd.

click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If yes, no further operation needs to be taken.
- If no, go to **Step 4**.

Step 4 Check whether the period of U2000 data export or dump or other parameters are set incorrectly.

1. Log in to the U2000 client. Choose **Fault** > **Query Alarm Log Statistics** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Alarm Log Statistics** from the main menu (application style).
2. In the **Filter** window, click the **Basic Settings** tab. In **Occurred** area, change the value of **Previous** to **90**, and click **OK** to collect statistics on the historical alarm records generated in recent 90 days.
3. In the **Confirm** dialog box, click **Yes**.
   - If there are a large number of historical alarm records, the data export or dump period or other parameters may be set incorrectly. As a result, the amount of data written to the database is larger than the amount of data dumped within a short period of time. In this case, go to **Step 4.4**.
   - If the number of historical alarm records is not large, go to **Step 5**.
4. Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style). In the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump** from the navigation tree. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Run Now** from the shortcut menu.
5. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Attributes** from the shortcut menu. In the **Attributes** dialog box, click the **Extended Parameters** tab. Change the value of **Storage period in database(days)** to a smaller value, for example, 30 days.
6. After **Database usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** window, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.33 ALM-44 The Database Usage Is Too High (Major)

Description

When the database usage is greater than or equal to the threshold for generating a major alarm for high database usage, the U2000 generates this alarm. When the database usage falls below the threshold, the alarm is cleared.

NOTE

To set the threshold for a major alarm for high database usage, log in to the U2000 System Monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Then set the threshold on the **Database Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared.

- The name of the server that generates this alarm is changed.
- After the alarm is generated for a database, the value of **Threshold** is changed to **Disabled Monitoring** for the database related to the alarm. (Change method: In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. In the **Property** column, expand the nodes under **Custom** until the name of the database related to the alarm is displayed, and then click the cell in the **Threshold** column corresponding to the database name and select **Disabled Monitoring** from the drop-down list.)
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
44	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Database service name.
Database	Database name.
Size	Database capacity.
Threshold	Threshold for generating an alarm.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Usage	Database usage.

Impact on the System

If the database usage is too high, database-involved operations on the U2000 may fail. For example, alarm information may fail to be saved to the database.

This alarm poses risks of exceptions and may even interrupt the U2000. Therefore, you are advised to handle the alarm immediately.

System Actions

None.

Possible Causes

- The U2000 receives a large number of alarms or events within a short period of time.
- The U2000 records a large number of logs within a short period of time.
- The threshold for generating a major alarm for high database usage is small.
- The period of U2000 data export or dump or other parameters are set incorrectly, leading to high usage of the alarm database.
- Small space has been allocated to the U2000 database.

Procedure

Step 1 Check whether a large number of alarms or events are reported within a short period of time.

1. Check whether **Database** in the alarm information is the alarm database **fmdb**.
   - If yes, go to **Step 1.2**.
   - If no, go to **Step 2**.
2. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported within a short period of time. Choose **Fault** > **Browse Event Logs** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Query Event Logs** from the main menu (application style). In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported within a short period of time.
   - If a large number of alarms or events are reported within a short period of time, go to **Step 1.3**.
   - If a small number of alarms or events are reported within a short period of time, go to **Step 3**.
3. Handle a large number of alarms or events that an NE has reported within a short period of time.

Copyright © Huawei Technologies Co., Ltd.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, run the scheduled task of dumping alarms or events immediately, 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 (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 2 Check whether a large number of logs are reported within a short period of time.

1. Check whether **Database** in the alarm information is the log database **logdb**.
   - If yes, go to **Step 2.2**.
   - If no, go to **Step 3**.
2. Generally, nly system logs are recorded in large quantities within a short period of time. Log in to the U2000 client. Choose **Administration** > **Log Management** > **Query System Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query System Logs** from the main menu (application style). In the **Query System Logs** window, check whether a large number of system logs (more than 300 logs per second) are recorded.
   - If yes, go to **Step 2.3**.
   - If yes, go to **Step 3**.
3. Handle these logs reported within a short period of time.

   In the **Task Management** window, run scheduled tasks for system log dump, and identify the cause for system log generation.
4. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Check whether the threshold for generating a major alarm for high database usage is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Check whether the threshold for generating a major alarm for high database usage is greater than or equal to 95% (the default value).
   - If yes, go to **Step 4**.
   - If no, increase the threshold to 95% and go to **Step 3.2**.
2. After **Database usage sampling interval** elapses, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box,

Copyright © Huawei Technologies Co., Ltd.

click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If yes, no further operation needs to be taken.
- If no, go to **Step 4**.

Step 4 Check whether the period of U2000 data export or dump or other parameters are set incorrectly.

1. Log in to the U2000 client. Choose **Fault** > **Query Alarm Log Statistics** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Alarm Log Statistics** from the main menu (application style).
2. In the **Filter** dialog box, click the **Basic Settings** tab. In **Occurred** area, change the value of **Previous** to **90**, and then click **OK** to collect statistics on the historical alarm records generated in recent 90 days.
3. In the **Confirm** dialog box, click **Yes**.
   - If there are a large number of historical alarm records, the data export or dump period or other parameters may be set incorrectly. As a result, the amount of data written to the database is larger than the amount of data dumped within a short period of time. In this case, go to **Step 4.4**.
   - If the number of historical alarm records is not large, go to **Step 5**.
4. Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style). In the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump** from the navigation tree. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Run Now** from the shortcut menu.
5. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Attributes** from the shortcut menu. In the **Attributes** dialog box, click the **Extended Parameters** tab. Change the value of **Storage period in database(days)** to a smaller value, for example, 30 days.
6. After **Database usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.34 ALM-47 Memory Usage of Service Is Too High

Description

If the memory usage of a service is greater than or equal to the preset threshold, the U2000 generates this alarm. If the memory usage of the service falls below the preset threshold, the alarm is cleared.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared .

- The name of the server that generates this alarm is changed.
- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
47	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Service	Service name of the host that generated the alarm.
Threshold	Threshold for generating an alarm. An alarm is generated when **Usage** is greater than or equal to **Threshold**.
Usage	Memory usage occupied by the service.

Impact on the System

The U2000 server responds slowly.

System Actions

None.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The U2000 is busy in processing services; therefore, the memory usage increases.
- The threshold for generating a high memory usage alarm is small.
- A program error occurs.

Procedure

Step 1 Check whether memory usage increases due to busy service processing.

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

- If the memory usage of service decreases, the alarm is cleared and no further operation needs to be taken.
- If the memory usage of service does not decrease, go to **Step 2**.

Step 2 For SUSE Linux or Solaris OS, after service processing is complete, the memory resources of the service are not recycled if the memory is sufficient. Therefore, the alarm is not cleared. In this case, perform the following operations to check whether the memory usage is increased continuously:

1. In **Details** of the alarm, check **Service name** to find the service whose memory usage is high.
2. Log in to the U2000 System Monitor client. On the **Service Monitor** tab, find this service and query its process name. On the **Process Monitor** tab, check whether the memory usage of the service process is increased continuously.

- If no, no further operation needs to be taken.
- If yes, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Related Information

A.41 ALM-100 The CPU Usage Is High

A.43 ALM-102 The Memory Usage Is Too High

A.35 ALM-50 Task execution failure alarm

Description

A task failed to be executed in the **Task Management** window.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
50	Minor	Service

Parameters

Name	Meaning
Task name	Name of the task failing to be executed.
Execution result	Task execution result.

Impact on the System

The scheduled task does not work.

System Actions

None.

Possible Causes

The service of the task is abnormal.

Procedure

Step 1 If the task cannot be started, log in to the U2000 System Monitor client.Check whether the service of the task is running properly 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 of the task is not running, right-click it and choose **Start the Service** from the shortcut menu.

Step 2 Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style). In the **Task Management** window on the U2000 client, right-click the failed task and choose **Run Now** from the shortcut menu.

- If the task is successfully executed, no further operation needs to be taken.
- If the task fails to be executed, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.36 ALM-51 The temporary Feature field of the OSS License file expires

Description

This alarm is generated on the next day after the temporary **Feature** field contained in the permanent commercial plus fixed-period License file expires. This alarm is cleared when the updated License file does not have the temporary **Feature** field or the expiration date of the temporary **Feature** field in this License file is later than the date of the current OSS.

Attribute

Alarm ID	Alarm Severity	Alarm Type
51	Critical	Processing error

Parameters

Name	Meaning
ProductName	Product to which the License file belongs.

Impact on the System

None.

System Actions

When the retention period of the temporary **Feature** field expires, this alarm is cleared and reported to the **A.37 ALM-52 The temporary Feature field of the OSS License file enters to the default state** .

For example, the expiration date of a temporary **Feature** field is Dec 30, 2011, and the retention period is 90 days, the U2000 generates this alarm on Dec 31, 2011. After this alarm is generated, the temporary **Feature** field can still be used for 90 days. This alarm is cleared after 90 days and is reported to the **A.37 ALM-52 The temporary Feature field of the OSS License file enters to the default state** . Then, the License item in the temporary **Feature** field is unavailable.

Possible Causes

The temporary **Feature** field contained in the permanent commercial plus fixed-period License file expires and enters the retention period.

Procedure

Step 1 Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose

Copyright © Huawei Technologies Co., Ltd.

License Management > **License Information** from the main menu (application style). On the **Resource Control Item** or **Function Control Item** tab page of the **License Information** dialog box, check whether **Authorization Expiration Time** of the License item expires.

Step 2 Contact Huawei technical support engineers to apply for a License that contains the temporary **Feature** field based on **Authorization Expiration Time** of the specified License items.

Step 3 Update the License file.

----End

A.37 ALM-52 The temporary Feature field of the OSS License file enters to the default state

Description

This alarm is generated when the temporary **Feature** field contained in the permanent commercial plus fixed-period License file expires and exceeds the retention period. In default state, the License item in the temporary **Feature** field is unavailable.

This alarm is cleared when the updated License file meets one of the following conditions:

- The updated License file does not contain the temporary **Feature** field.
- The date when the retention period expires in the updated License file is later than the date when the retention period expires in the current License file.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52	Critical	Processing error

Parameters

Name	Meaning
ProductName	Product to which the License file belongs.

Impact on the System

The functions of the License item in the temporary **Feature** field are unavailable.

System Actions

None.

Possible Causes

The temporary **Feature** field contained in the permanent commercial plus fixed-period License file exceeds the retention period and enters the default state.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Contact Huawei technical support engineers to apply for a new OSS License.

----End

A.38 ALM-53 High log space usage for the database

Description

When the usage of the Sybase log space is greater than or equal to the alarm generation threshold (85% by default), the U2000 generates this alarm. When the log space usage falls below the alarm clearance threshold (85% by default), the alarm is cleared.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the server that generates this alarm is changed.
- The server that generates this alarm runs on SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.
- After this alarm is generated for a database, the value of **Threshold** is changed to **Disabled Monitoring** for the database related to the alarm. (Change method: Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. In the **Property** column, expand the nodes under **Custom** until the name of the database related to the alarm is displayed, and then click the cell in the **Threshold** column corresponding to the database name and select **Disabled Monitoring** from the drop-down list.)
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
53	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Name of the database service on the server that generates an alarm, for example, DBSVR.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Database	Name of the Sybase database that generates an alarm. For example, eamdb and logdb.
Size	Size of the log space in the Sybase database that generates the alarm.
Threshold	Threshold of the alarm. The alarm is generated when the value of **Usage** is equal to or greater than the value of **Threshold**.
Usage	Log space usage of the Sybase database that generates the alarm.

Impact on the System

High usage of the Sybase database log space may cause abnormal running of the U2000 services.

This alarm may cause U2000 failures at any time; therefore, you need to clear it in a timely manner.

Possible Causes

- The U2000 is performing time-consuming operations that involve a large amount of data in the database.
- The log space in the database is small.

Procedure

Step 1 Check whether the U2000 is performing time-consuming operations that involve a large amount of data in the database.

Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). Check the occurrence time of the alarm.

NOTE

If the alarm occurred not long ago, the U2000 may be performing operations involving a large amount of data. The alarm will be automatically cleared after the operations are complete. No measure needs to be taken.

Assume that a time-consuming operation takes 30 minutes.

- If the alarm occurred within the past 30 minutes, note this alarm after several minutes. No further operation needs to be taken.
- If the alarm occurs 30 minutes ago, go to **Step 2**.

Step 2 Contact Huawei technical support engineers.

----End

Copyright © Huawei Technologies Co., Ltd.

A.39 ALM-54 The swap Usage Is High

Description

When the swap memory usage of the server that runs Solaris or SUSE Linux OS is greater than or equal to the generation threshold, the U2000 generates this alarm. When the swap memory usage falls below the alarm clearance threshold, the alarm is cleared.

NOTE

- To set the thresholds for generating and clearing a high swap memory usage alarm, log in to the U2000System Monitor client, choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Server Monitor** tab. Then set the thresholds on the **Server Monitor** tab.
- In an HA system, the U2000 monitors swap memory usage of each server.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

You must manually clear the alarm in the following situations because the alarm cannot be automatically cleared:

- The name of the server that generates the alarm is changed.
- The OS of the server that generates this alarm is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
54	Critical	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
Swap Memory Usage	Swap memory usage of a server that generates an alarm.

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

- The available swap space of the system is decreased. The U2000 responds slowly, and operations are delayed.
- U2000 performance deteriorates. Real-time information reporting from the NBI, performance module, and fault module is delayed, and information cannot be collected in a timely manner.
- 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 **/tmp** is high (on Solaris OS).
- The threshold for generating a high swap memory usage alarm on the U2000 server is small.
- A small swap space has been allocated to the U2000 server.
- Non-U2000 services (for example, the database) occupy many U2000 system resources.

Procedure

Step 1 Identify the OS of the U2000 server.

- If the U2000 server runs on Solaris OS, go to **Step 2**.
- If the U2000 server runs on SUSE Linux OS, go to **Step 3**.

Step 2 Check whether the disk usage of **/tmp** is high.

1. Use the PuTTY to log in to the U2000 server as user **ossuser** in SSH mode.
2. Run the following command to switch to user **root**.

   $ **su - root**

   Password:***Password of root***

3. Run the **df -k** command. Locate the record in which **Mounted on** is set to **/tmp** and **Filesystem** is set to **swap**. Check whether the disk usage of **/tmp** exceeds 50%.

   - If the disk usage of **/tmp** exceeds 50%, **/tmp** may store many unnecessary files. Run the **cd /tmp** command to open **/tmp** and the **ls -l** command to query files in it. If unnecessary temporary files exist in **/tmp**, run the **rm** command to delete them. Then go to **Step 2.4**.
   - If the disk usage of **/tmp** is below 50%, go to **Step 3**.

   NOTE

   If you are not sure whether a file can be deleted, contact Huawei technical support engineers.

4. After a sampling period, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high swap memory usage alarm is cleared.

Copyright © Huawei Technologies Co., Ltd.

- If yes, no further operation needs to be taken.
- If no, go to **Step 3**.

Step 3 Check whether the threshold for generating a high swap memory usage alarm on the U2000 server is small.

1. Log in to the U2000System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Server Monitor** tab. Then check whether the threshold for generating a high swap memory usage alarm is greater than or equal to 95% (the default value).
   - If no, and the system responds properly, the threshold has been specified to a small value. Go to **Step 3.2**.
   - If yes, go to **Step 4**.
2. On the **Server Monitor** tab of the **System Monitor Settings** dialog box, increase the threshold for generating a high swap memory usage alarm to **95%** and increase the alarm clearance threshold to **85%** (the default value).
3. After a sampling period, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style).In the **Browse Current Alarm** window, check whether the high swap memory usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 4**.

Step 4 Check whether a small swap space has been allocated to the U2000 server.

On the **Server Monitor** tab, check whether the swap space is less than 16 GB (check whether the swap space is less than the memory space when the memory space is less than 16 GB).

- If yes, a small swap space has been allocated to the U2000 server. Contact Huawei technical support engineers for a solution.
- If no, go to **Step 5**.

Step 5 Check whether the high swap memory usage is caused by non-U2000 applications.

On Solaris OS, run the **prstat** command and view the swap memory usage of processes in the **SIZE** column.

On SUSE Linux OS, run the **top** command and view swap memory usage of processes in the **VIRT** column.

- If the swap memory usage of a few non-U2000 processes is high, contact the system administrator for a solution. The procedure ends.
- If the swap memory usage of non-U2000 processes is not high, go to **Step 6**.

Step 6 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Related Information

A.43 ALM-102 The Memory Usage Is Too High

Copyright © Huawei Technologies Co., Ltd.

A.40 Communication with the Device Failed

Description

The alarm is generated when the communication between the U2000 and fails to communicate with an NE fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
100	Critical	Equipment

Impact on the System

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

Possible Causes

- Cause 1: The NE is powered off.
- Cause 2: The NE is restarted.
- Cause 3: The SNMP protocol parameters configured on the NE and the U2000 are different.
- Cause 4: The firewall is enabled on the NE or the computer that runs the U2000.
- Cause 5: The network delay is long or the U2000 is pinging the device.

Procedure

Step 1 Check whether the NE is powered off as follows:

1. Check the power supply status of the NE. If the power connector is connected in poor contact, reconnect the power lines. If the power supply unit is faulty, replace it.
2. Then check whether the alarm is cleared.
   - If the alarm is cleared, no further action is required.
   - If the alarm is not cleared, go to Step 2.

Step 2 Check whether the NE is restarted.

If so, wait a while and then check whether the alarm is cleared.

- If the alarm is cleared, no further action is required.
- If the alarm is not cleared, go to Step 3.

Step 3 Check whether the SNMP protocol parameters configured on the NE and the U2000 are different as follows:

1. Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE**

Copyright © Huawei Technologies Co., Ltd.

Communicate Parameter > **NE Access Protocol Parameters** from the main menu (application style). Check the settings of the SNMP parameters of the NE on the U2000.

2. Log in to the NE and run the **display snmp-agent community read/write** command to check whether the read community and write community of the SNMP protocol (SNMPv1, SNMPv2c, and SNMPv3) on the NE are the same as those on the U2000.

   NOTE

   Using SNMPv3 is recommended because of its higher security than SNMPv1 and SNMPv2c.

3. Change the parameter settings to ensure that the SNMP parameter settings on the NE and the U2000 are the same.
4. Then check whether the alarm is cleared.
   - If the alarm is cleared, no further action is required.
   - If the alarm is not cleared, go to Step 4.

Step 4 Check whether the firewall is enabled.

1. If the firewall is enabled, view the configuration of the firewall policy based on the list of ports that are used by the U2000.
2. Then check whether the alarm is cleared.
   - If the alarm is cleared, no further action is required.
   - If the alarm is not cleared, go to Step 5.

Step 5 Check whether the network delay is long or the U2000 is pinging the device.

1. retry later.
2. Then check whether the alarm is cleared.
   - If the alarm is cleared, no further action is required.
   - If the alarm is not cleared, go to Step 6.

Step 6 Collect the information about alarm handling, and contact Huawei technical support engineers.

----End

A.41 ALM-100 The CPU Usage Is High

Description

The U2000 consecutively samples the CPU usage. In a sampling period (max. consecutive CPU overloads for alarm x server usage sampling interval), 600s by default, if the CPU usage is greater than or equal to the generating threshold for generating a high CPU usage alarm each time, the U2000 generates this alarm. When the CPU usage falls below the clearance threshold each time, the alarm is cleared.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- To set the max. consecutive CPU overloads for alarm, server usage sampling interval, and thresholds for generating and clearing a high CPU usage alarm, log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click **Server Monitor** tab . Then set these items on the **Server Monitor** tab.
- If the server has more than one CPU, the U2000 continuously samples the usage of each CPU.
- In a dual-node system or a distributed system, the U2000 continuously samples the CPU usage of each U2000 server.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the server that generates this alarm is changed.
- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
100	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server that generated an alarm.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
CPU Usage	CPU usage.

Impact on the System

- The U2000 responds slowly, and operations are delayed.
- Real-time information reporting from the NBI, performance module, and fault module is delayed, and information cannot be collected in a timely manner.
- The system processes services slowly. As a result, messages may be accumulated, and the system may crash.

Copyright © Huawei Technologies Co., Ltd.

System Actions

None.

Possible Causes

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

Procedure

Step 1 Check whether the U2000 is busy temporarily.

1. Log in to the U2000 client.
2. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style).
3. In the **Filter** dialog box, click **OK**.
4. In the **Browse Current Alarm** window, view **First Occurred** of the alarm.

Check whether any of the following situations exist:

- The alarm is not consecutively generated and is automatically cleared in 10 minutes. In addition, the alarm is seldom generated. It is generated once each day at most.
- The alarm affects the system functions (including the NBI, performance collection, 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 not more than 10 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 (not mandatory).

Solution:

- If any of these situations exist, the system is busy temporarily. You do not need to handle the alarm. If many alarms or events alarm (more than 100 alarms or events per second) are reported when the high CPU usage alarm is generated, you need to handle these alarms or events as soon as possible. No further operation needs to be taken.
- If none of these situations exists, go to **Step 2**.

Step 2 Check whether the CPU usage of the U2000 application is high.

Log in to the U2000 System Monitor client. In the **System Monitor Settings** dialog box, click On the **Process Monitor** tab. Then check whether the CPU usage of the U2000 processes is high.

For details about the processes, see the U2000 administrator guide.

- If the memory usage of the U2000 processes is high (exceeds 90%), the CPU resources are exhausted due to the U2000 applications. The alarm is cleared automatically after the related

Copyright © Huawei Technologies Co., Ltd.

process services are processed. If you need to clear the alarm before the service processing is complete, go to **Step 6**.

- If the CPU usage of the U2000 processes is not high, go to **Step 3**.

Step 3 Check whether the CPU usage of non-U2000 application is high.

On Solaris OS, run the **prstat** command to check the CPU usage of processes in the **CPU** column.

On SUSE Linux OS, run the **top** command to check the CPU usage of processes in the **CPU** column.

On Windows OS, click the **Process** tab in **Windows Task Manager** and check the CPU usage of processes in the **CPU** column.

- If the CPU usage of non-U2000 processes is high (exceeds 90%), contact the system administrator. The operation is complete.
- If the CPU usage of non-U2000 processes is not high, go to **Step 4**.

Step 4 Check whether the threshold for generating a high CPU usage alarm of the U2000 server is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Server Monitor** tab. Then check whether the threshold for generating a high CPU usage alarm is appropriate.

   Check whether the following situations exist:

   - The threshold for generating a high CPU usage alarm is changed from 90% (the default value) to a smaller value and the alarm is generated but the system runs efficiently.
   - The alarm is generated more than once each day.

   Solution:

   - If these situations exist, 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 alarm clearance threshold to 70% (the default value). Then go to **Step 4.2**.
   - If these situations do not exist, go to **Step 5**.
2. After a sampling period, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high CPU usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 5**.

Step 5 Check whether the server hardware meets the requirements of the U2000.

Symptoms of poor server hardware performance:

- The hardware configurations required by the management scale of the U2000 are beyond the actual hardware capabilities of the server.
- The alarm is generated consecutively or frequently.

Go to **Step 6**.

Copyright © Huawei Technologies Co., Ltd.

Step 6 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.42 ALM-101 The Disk Usage Is Too High (Critical)

Description

When the disk or partition (volume) usage is greater than or equal to the threshold for generating a critical alarm for high disk usage, the U2000 generates this alarm. When the disk or partition (volume) usage falls below the threshold for clearing a critical alarm, the alarm is cleared.

NOTE

To set the threshold for generating a high disk usage alarm, log in to the U2000 system monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Hard Disk Monitor** tab. Then set the threshold on the **Hard Disk Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, these alarms need to be cleared manually.

- The name of the server that generates this alarm is changed.
- The mount point of the disk that generates this alarm is changed.
- The server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
101	Critical	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Disk	Disk for whom the server generates an alarm.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Capacity	Disk capacity.
Usage	Disk usage.

Impact on the System

The U2000 service may fail to write data to the disk, and database exceptions may occur.

System Actions

None.

Possible Causes

- The disk contains many unnecessary files.
  - The recycle bin is not emptied.
  - The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to the disk in a short time.
  - Many temporary data files and backup files.
- The threshold for generating a critical alarm for high disk usage is small.

Procedure

Step 1 Delete unnecessary files from the disk.

- If the server runs on Windows OS, perform the following operations:
  1. Empty the recycle bin.
  2. Delete unnecessary U2000 files from the disk.

     NOTE

     If you are not sure whether a file can be deleted, contact Huawei technical support engineers.

     Use **Explore** to delete unnecessary files, such as historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files.

     Table A-8 lists the U2000 files that can be deleted.

Copyright © Huawei Technologies Co., Ltd.

Table A-8 U2000 files that can be deleted on Windows OS

Directory	File to Be Deleted	Method
D:\oss\server\var\logs	Core files (whose names start with core)	Use FileZilla to back up the files to another disk and run the **del** command to delete them from the current disk. For details about how to use the FileZilla tool, see How Do I Use FileZilla to Transfer Files?.
D:\oss\server\var\logs\traceback	Trace backup files	Run the **del** command to delete excessive backup trace files.
D:\oss\server\var\logs\mrblog	Dumped MRB log files	Run the **del** command to delete excessive .gz files.

3. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

- If the server runs on Solaris or SUSE Linux OS, perform the following operations:

  1. Empty the recycle bin.

     Log in to the U2000 server on Xwindows and perform the following operations in the graphical user interface (GUI):

  2. Run the **df -k** command to identify the disks whose disk usage is high.

     If other disks also have high disk usage besides the **Disk** in the alarm parameter but no alarm has been generated, free up some space for all these disks.

  3. Run the **cd** command to open the directory that occupies much disk space. Then run the **LC_ALL=en_US du -k | LC_ALL=en_US sort -nr >** */tmp/du_k.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **du_k.txt**.

Copyright © Huawei Technologies Co., Ltd.

4. Run the **more** */tmp/du_k.txt* command to view **du_k.txt** and find the subdirectory that causes high disk usage.
5. Run the **cd** command to open the subdirectory that causes high disk usage. Then run the **ls -l >** */tmp/ls_l.txt* command to query the size of all files and subdirectories in it, sort the files and subdirectories, and write them into **ls_l.txt**.
6. Run the **more** */tmp/ls_l.txt* command 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 delete these files. You are advised to delete the historical backups of installation packages, patch packages, installation packages for the adaptation layer, backup files during installation, and core files. **Table A-9** lists the U2000 and database files that can be deleted.

   NOTE

   If you are not sure whether a file can be deleted, contact the system administrator or Huawei technical support engineers.

Table A-9 U2000 and database files that can be deleted on Solaris or SUSE Linux OS

Directory	File to Be Deleted	Method
/opt/oss/server/var/logs	Core files (whose names start with **core**)	Use FTP to back up the files to another disk and run the **rm** command to delete them from the current disk.
/opt/oss/server/var/logs/tracebak	Trace backup files	Run the **rm** command to delete excessive backup trace files.
/opt/oss/server/var/logs/mrblog	Dumped MRB log files	Run the **rm** command to delete excessive .gz files.
/opt/sybase/ASE-15_0/install (Solaris)	Sybase database logs. **NOTE** Check whether oversized Sybased database log files exist. If a log file is oversized, delete it. (A Sybase database log file is named in *Database instance name*.log format, for example, **DBSVR.log**.)	Run the following commands to delete the oversized Sybase database log file, for example, **DBSVR.log**: $ **cd** */opt/sybase/ASE-15_0/install* $ **rm** *DBSVR.log*

7. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current**

Copyright © Huawei Technologies Co., Ltd.

Alarm from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If yes, no further operation needs to be taken.
- If no, go to **Step 2**.

Step 2 Check whether the threshold for generating a critical alarm for high disk usage alarm of the U2000 server is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a critical alarm for high disk usage is greater than or equal to 90% (the default value).
   - If yes, go to **Step 3**.
   - If no, increase the threshold to 90% and increase the alarm clearance threshold to 85% (the default value). Then go to **Step 2.2**.
2. After the **Hard disk usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.43 ALM-102 The Memory Usage Is Too High

Description

When the **memory usage** of the server that runs on Windows OS is greater than or equal to the threshold for generating a high memory usage alarm, this alarm is generated. When the memory usage falls below the alarm clearance threshold, the alarm is cleared.

NOTE

- Memory Usage = (1 - **Commit Charge Limit**/**Commit Charge Available**) x 100%.
- To set the thresholds for generating and clearing a high memory usage alarm, log in to the U2000System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Server Monitor**. Then set the thresholds on the **Server Monitor** tab.
- In an HA system, the U2000 monitors the memory usage of each server.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared .

- The name of the server that generates this alarm is changed.

Copyright © Huawei Technologies Co., Ltd.

- The server that generates this alarm runs on Windows OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
102	Major	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Operating System	OS of the server.
Threshold	Threshold for generating an alarm.
Clearance threshold	Threshold for clearing an alarm.
Memory Usage	Memory usage of a server that generates an alarm.

Impact on the System

- The available memory space is decreased. The U2000 responds slowly, and operations are delayed.
- The U2000 performance deteriorates. Real-time information reporting from the NBI, performance module, and fault module is delayed, and information cannot be collected in a timely manner.
- 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 threshold for generating a high memory usage alarm on the U2000 server is small.
- The U2000 server is performing an operation that occupies many system resources.
- The hardware performance of the U2000 server is poor. Therefore, the U2000 cannot run properly.

Procedure

Step 1 Check whether the threshold for generating a high memory usage alarm on the U2000 server is small.

Copyright © Huawei Technologies Co., Ltd.

1. Log in to the U2000system monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Server Monitor** tab. Then check whether the threshold for generating a high memory usage alarm has been properly set.
   - If the threshold is below the default value **95%** and the system responds properly, the threshold has been specified to a small value. Go to **Step 1.2**.
   - If the threshold is above **95%**, go to **Step 2**.
2. On the **Server Monitor** tab of the **System Monitor Settings** dialog box, increase the threshold for generating a high memory usage alarm to **95%** and increase the alarm clearance threshold to **85%** (the default value). Then go to **Step 1.3**.
3. After a sampling period, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high memory usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

Step 2 Check whether the high memory usage is caused by U2000 applications.

On the **Process Monitor** tab, check the memory usage of U2000 processes.

- If the memory usage of a few U2000 processes is high, the memory resources are exhausted due to the U2000 applications. The alarm is automatically cleared after the related services are processed. If you need to clear the alarm before the service processing is complete, go to **Step 5**.
- If memory usage of U2000 processes is not high, go to **Step 3**.

Step 3 Check whether the high memory usage is caused by non-U2000 applications.

Click the **Process** tab in **Windows Task Manager** and check the memory usage of processes in the **Memory** column.

- If memory usage of a few non-U2000 processes is high, contact the system administrator for a solution. The procedure ends.
- If memory usage of non-U2000 processes is not high, go to **Step 4**.

Step 4 Check whether the hardware performance of the server is poor and the hardware does not support proper U2000 running.

If the hardware performance is poor, go to **Step 5**.

NOTE

Symptoms of poor server hardware performance:

- The hardware configurations required by the management scale of the U2000 are beyond the actual hardware capabilities of the server.
- The alarm is generated consecutively or frequently.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

Related Information

A.39 ALM-54 The swap Usage Is High

A.44 ALM-103 The Database Usage Is Too High (Critical)

Description

When the database usage is greater than or equal to the threshold for generating a critical alarm for high database usage, the U2000 generates this alarm. When the database usage falls below the threshold, the alarm is cleared.

NOTE

To set the threshold for a critical alarm for high database usage, log in to the U2000 System Monitor client and choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Then set the threshold on the **Database Monitor** tab.

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

The following situations cause failures in automatically clearing alarms. Instead, they need to be manually cleared.

- The name of the server that generates this alarm is changed.
- After the alarm is generated for a database, the value of **Threshold** is changed to **Disabled Monitoring** for the database related to the alarm. (Change method: In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. In the **Property** column, expand the nodes under **Custom** until the name of the database related to the alarm is displayed, and then click the cell in the **Threshold** column corresponding to the database name and select **Disabled Monitoring** from the drop-down list.)
- The database that generates this alarm is deleted after the U2000 is stopped.

Attribute

Alarm ID	Alarm Severity	Alarm Type
103	Critical	Service

Parameters

Name	Meaning
Host	Name of the server that generates an alarm.
Database service	Database service name.
Database	Database name.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Size	Database capacity.
Threshold	Threshold for generating an alarm.
Usage	Database usage.

Impact on the System

If the database usage is too high, database-involved operations on the U2000 may fail. For example, alarm information may fail to be saved to the database.

This alarm may cause U2000 failures at any time. Therefore, you need to clear it immediately.

System Actions

None.

Possible Causes

- The U2000 receives a large number of alarms or events within a short period of time.
- The U2000 records a large number of logs within a short period of time.
- The threshold for generating a critical alarm for high database usage of the U2000 is small.
- The period of U2000 data export or dump or other parameters are set incorrectly, leading to high usage of the alarm database.
- Small space has been allocated to the U2000 database.

Procedure

Step 1 Check whether a large number of alarms or events are reported within a short period of time.

1. Check whether **Database** in the alarm information is the alarm database **fmdb**.
   - If yes, go to **Step 1.2**.
   - If no, go to **Step 2**.
2. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported within a short period of time. Choose **Fault** > **Browse Event Logs** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Query Event Logs** from the main menu (application style). In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported within a short period of time.
   - If a large number of alarms or events are reported within a short period of time, go to **Step 1.3**.

Copyright © Huawei Technologies Co., Ltd.

- If a small number of alarms or events are reported within a short period of time, go to **Step 3**.

3. Handle the large number of alarms or events that an NE has reported within a short period of time.

   Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, run the scheduled task of dumping alarms or events immediately and identify the causes for these alarms or events.

4. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 2 Check whether a large number of logs are reported within a short period of time.

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

   - If yes, go to **Step 2.2**.
   - If no, go to **Step 3**.

2. Generally, only system logs are recorded in large quantities within a short period of time. Log in to the U2000 client. Choose **Administration** > **Log Management** > **Query System Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query System Logs** from the main menu (application style). In the **Query System Logs** window, check whether a large number of system logs (more than 300 logs per second) are reporded.

   - If yes, go to **Step 2.3**.
   - If no, go to **Step 3**.

3. Handle these logs reported within a short period of time.

   In the **Task Management** window, run scheduled tasks for system log dump immediately, and identify the cause for system log generation.

4. Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Check whether the threshold for generating a critical alarm for high database usage of the U2000 is small.

1. Log in to the U2000 System Monitor client. Choose **Administration** > **Settings**. In the **System Monitor Settings** dialog box, click the **Database Monitor** tab. Check whether the threshold for generating a critical alarm for high database usage is greater than or equal to 98% (the default value).

   - If yes, go to **Step 4**.

Copyright © Huawei Technologies Co., Ltd.

- If no, increase the threshold to 98% and go to **Step 3.2**.

2. After **Database usage sampling interval** elapse, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 4**.

Step 4 Check whether the period of U2000 data export or dump or other parameters are set incorrectly.

1. Log in to the U2000 client. Choose **Fault** > **Query Alarm Log Statistics** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Alarm Log Statistics** from the main menu (application style).
2. In the **Filter** dialog box, click the **Basic Settings** tab. In **Occurred** area, change the value of **Previous** to **90** and click **OK** to collect statistics on the historical alarm records generated in recent 90 days.
3. In the **Confirm** dialog box, click **Yes**.
   - If there are a large number of historical alarm records, the data export or dump period or other parameters may be set incorrectly. As a result, the amount of data written to the database is larger than the amount of data dumped within a short period of time. In this case, go to **Step 4.4**.
   - If there are not a large number of historical alarm records, go to **Step 5**.
4. Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style). In the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump** from the navigation tree. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Run Now** from the shortcut menu.
5. In the **Task Management** window, right-click the **Alarm/Event Log Dump** task in the task list and choose **Attributes** from the shortcut menu. In the **Attributes** dialog box, click the **Extended Parameters** tab. Change the value of **Storage period in database(days)** to a smaller value, for example, 30 days.
6. After **Database usage sampling interval** elapses, choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Filter** dialog box, click **OK**. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.
   - If yes, no further operation needs to be taken.
   - If no, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

A.45 ALM-106 The OSS Service Is Terminated Abnormally

Description

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

If a switchover occurs between the active and standby servers, this alarm may not be automatically cleared and therefore needs to be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
106	Major	Processing error

Parameters

Name	Meaning
Server name	Name of the server that generates an alarm.
SvcAgent	Process name of the service that exits abnormally.
SvcName	Name of the service that exits abnormally.

Impact on the System

The functions provided by this service are unavailable, and other services that depend on this service also exit.

System Actions

None.

Possible Causes

- The service is terminated manually. For example, a user forcible ends a process.
- The database password is changed abnormally.
- Another exception occurs. For example, database connections are not enough or the tempdb database is full.

Procedure

Step 1 Check whether the U2000 service provided in the alarm details is running properly.

Copyright © Huawei Technologies Co., Ltd.

1. Log in to the U2000 server as user ossuser.
2. Set the environment variable.
   - On Solaris or SuSE Linux OS, run the following commands:

     $ **cd** */opt/oss/server*

     $**. ./svc_profile.sh**
   - On Windows OS, the environment variable of the U2000 automatically takes effect.
3. Run the following command to check the service status:

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

Step 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 **Step 3** to ensure that the alarm is cleared.
- If the service fails to be started, collect fault information. For details about how to collect fault information, see the U2000 administrator guide. Then go to **Step 4**.

Step 3 Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the abnormal service exit alarm of the U2000 service is cleared.

- If no, go to **Step 4**.
- If yes, no further operation needs to be taken.

Step 4 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.46 MAC Address Conflict

Description

The MAC addresses of two NEs conflict with each other.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
106	Major	Equipment

Impact on the System

One of the NEs goes offline on the U2000 when the other one goes online.

Possible Causes

- The IP address of an NE is changed, and the NE is added to the U2000 again.
- The MAC address of a newly added NE is the same as that of an existing NE on the U2000.

Procedure

Step 1 Delete the NE that uses the original IP address from the U2000.

Step 2 Delete one of the two NEs that use the same MAC address from the U2000.

----End

Related Information

None

A.47 OMC license not exist

Description

The license file does not contain this control item and therefore service provisioning and maintenance will be affected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
131	Critical	Process

Impact on the System

Service provisioning and maintenance are affected.

NOTE

This alarm cannot be masked. Handle it as soon as possible. Purchase a new license within 60 days after this alarm is reported; otherwise, services on the NE will be affected.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

The control item is not purchased.

Procedure

Step 1 Contact Huawei engineers to apply for a new license.

----End

A.48 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, and the number of login attempts reaches the upper limit.
- The user logged in is inactive on the U2000, and the number of login attempts reaches the upper limit.
- The password is incorrect, and the number of login attempts reaches the upper limit.
- The user logged in enters an incorrect password when unlocking the client, and the number of login attempts reaches the upper limit.

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

NOTE

To set the account policy, you can choose **Administration** > **NMS Security** > **Security Policy** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **Security Policy** from the main menu (application style). In the **Security Policy** dialog box, click the **Account Policy** tab.

Attribute

Alarm ID	Alarm Severity	Alarm Type
114	Critical	Security

Parameters

Name	Meaning
User Name	Name of the user who attempts to log in to the system.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
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 Name)	Client that the user attempts to connect to the U2000 server. Clients are represented by IP addresses or host names.

Impact on the System

The user account is locked. The user has to wait 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 or unlock the client for consecutive times.

Procedure

Step 1 The alarm does not need to be handled.

----End

A.49 ALM-116 The Master Server Cannot Communicate with the Slave Server

Description

The master server cannot communicate with a slave server. The master server fails to detect the slave server.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- A switchover occurs between the slave and backup servers.
- The slave server that generates this alarm runs on Windows, Solaris or SUSE Linux OS. The OS is upgraded or an OS patch is installed after the alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
116	Critical	Communication

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
Host	Name of the slave server that generates an alarm.
Operating System	OS of the slave server.

Impact on the System

The master server cannot monitor the resources on the slave server.

System Actions

None.

Possible Causes

- The ResourceMonitor process of the slave server is not running.
- The network is faulty.

Procedure

Step 1 Check whether the ResourceMonitor process is running on the slave server.

1. In the alarm location information, identify the slave server that fails to connect to the master server.
2. Log in to the slave server as user **ossuser** and run the following command to check whether the ResourceMonitor process is running:

   $ **daem_ps | grep** *ResourceMonitor*

   If the ResourceMonitor process is running, information about the ResourceMonitor process is displayed.

   ```
   ossuser 23296     1   0   Sep 27 ?          17:48 ResourceMonitor -cmd start
   ```

   - If the process is displayed, go to **Step 2**.
   - If the process is not displayed, the ResourceMonitor process is not running or has exited abnormally. Go to **Step 1.3**.
3. Run the following commands to start the ResourceMonitor process and check whether it is started successfully.

   $ **start_daem**

   $ **daem_ps | grep** *ResourceMonitor*

   - If the ResourceMonitor process is started successfully and the alarm is cleared, no further operation needs to be taken.
   - If the ResourceMonitor process is started successfully but the alarm is not cleared, go to **Step 2**.
   - If the ResourceMonitor process fails to be started, go to **Step 3**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether the network is faulty.

1. Log in to the master server as user ossuser and run the following command to check the connection between the master server and the slave server:

   $ **ping** *IP address of the slave server*

   - If the command is executed successfully, the cause for the alarm may be that the ResourceMonitor process is faulty. Go to **Step 3**.
   - If the command fails to be executed, the cause for the alarm may be that the network is faulty. Go to **Step 2.2**.
2. Verify that hardware is working properly. For example, the network cable is properly connected or the switch is working properly.
3. Run the following command to recheck the connection between the master server and the slave server:

   $ **ping** *IP address of the slave server*

   - If the alarm is not cleared, go to **Step 3**.
   - If the alarm is cleared, no further operation needs to be taken.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.50 ALM-117 Avalanche alarm

Description

According to the alarm or event frequency analysis rule, when the number of occurrence times of an alarm or event within the specified **Time period** is greater than **Generated alarm count**, this alarm is generated. When the number of occurrence times of an alarm or event within the specified **Time period** is less than **Cleared alarm count**, the alarm is cleared.

NOTE

To add an alarm or event frequency analysis rule, choose **Fault** > **Settings** > **Correlation** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Correlation** from the main menu (application style). Click the **Alarm/Event Frequency Analysis** tab, click **Add**, and set parameters such as the alarm or event name and time period.

Attribute

Alarm ID	Alarm Severity	Alarm Type
117	Major	Processing error

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
Alarm name	Name of the alarm that causes an avalanche alarm.
Alarm source	Source of the alarm that causes an avalanche alarm.
Location information	Location information of the alarm that causes an avalanche alarm.
NE address	IP address of the alarm source.
DN	Distinguished name of the alarm source.

Impact on the System

The alarm processing efficiency of the U2000 server is affected.

System Actions

None.

Possible Causes

- The ratio of **Generated alarm count** to **Time period** is small in the alarm frequency analysis rule.
- Some NEs are abnormal and report a large number of alarms in a short period.

Procedure

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

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

- If the avalanche alarm is generated before the fault service is started, select this alarm among the current alarm and click **Clear**. No further operation needs to be taken.
- If the avalanche alarm is generated after the fault service is started, go to **Step 2**.

Step 2 Check whether the ratio of **Generated alarm count** to **Time period** is small in the alarm frequency analysis rule.

Log in to the U2000 client. Choose **Fault** > **Settings** > **Correlation** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Correlation** from the main menu (application style). On the **Alarm/Event Frequency Analysis** tab, view **Generated alarm count** and **Time period** in the trigger conditions of the rule for the avalanche alarm.

Copyright © Huawei Technologies Co., Ltd.

- If the ratio of **Generated alarm count** to **Time period** is small (for example, 10 alarms per second), change time period and generated alarm count to proper values. No further operation needs to be taken.
- If the ratio of **Generated alarm count** to **Time period** is appropriate, go to **Step 3**.

Step 3 Check whether the NE is in the commissioning state.

- If the NE is in the commissioning state, check whether the avalanche alarm is cleared automatically when the commissioning ends. If the alarm is cleared automatically, the procedure ends. If the alarm is not cleared automatically, go to **Step 4**.
- If the NE is not in the commissioning state, go to **Step 4**.

Step 4 Check whether the NE is in the normal state.

- If no, rectify the fault. The procedure ends.
- If yes, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.51 ALM-120 The number of records in the database table has reached the threshold

Description

When the usage of a table in the database is greater than or equal to the preset threshold, this alarm is generated. When the usage of a table in the database is smaller than the preset threshold, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
120	Minor	Service

Parameters

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

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
Max capacity	Maximum number of historical alarm or event logs that can be stored in the database.
Threshold	Triggering condition of a dump task. If the number of historical alarms or event logs in the database is greater than or equal to the product of **Max capacity** and **Threshold**, the U2000 dumps logs and generates ALM-120 The number of records in the database table has reached the threshold.
Current capacity	Number of historical alarms or event logs currently stored in the database.

Impact on the System

None.

System Actions

The U2000 automatically dumps data.

Possible Causes

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

Procedure

Step 1 Check the gap between the alarm occurrence time and the current time.

1. Log in to the U2000 client.
2. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style).
3. In the **Browse Current Alarm** window, view **Last Occurred** of the alarm. Calculate the gap between the last occurrence time and the current time.
   - The U2000 automatically rectifies this fault every 10 minutes. If the gap is shorter than 10 minutes, this alarm does not need to be handled.
   - If the gap is longer than 10 minutes and the alarm is cleared, the U2000 has rectified this fault. No further operation needs to be taken.
   - Otherwise, go to **Step 2**.

Step 2 In the **Browse Current Alarm** window, check whether **Location Information** of this alarm contains the table names in **Table A-10**.

- If yes, find the tasks to be executed and go to **Step 3**.
- If no, go to **Step 4**.

Copyright © Huawei Technologies Co., Ltd.

Table A-10 Relationships between the tables and tasks to be executed

Table	Task to Be Executed
tbl_alm_log	Alarm overflow dump
tbl_event_log	Event overflow dump
tbl_SysLog	System log overflow dump
tbl_Security	Security log overflow dump
tbl_Audit	Operation log overflow dump

Step 3 Change the threshold of the overflow dump task.

1. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
2. In the **Task Management** window, right-click a task that is found in **Step 2** and choose **Attributes** from the shortcut menu.
3. In the **Attributes** dialog box, click the **Extended Parameters** tab.
   - If the value of **Max. records** multiplied by **Record threshold-crossing value(%)** is less than 40% of **Max. records**, set the two parameters to larger values and click **OK**. For example, if the value of **Max. records** is **500000**, the value of **Record threshold-crossing value(%)** is **60**%, and the maximum value of **Max. records** is **2000000**. As 500000 multiplied by 60% is less than 2000000 multiplied by 40%, you need to set **Max. records** and **Record threshold-crossing value(%)** to larger values. You can set **Max. records** to **1000000** and **Record threshold-crossing value(%)** to **80%**. Then right-click the task and choose **Run Now** from the shortcut menu. No further operation needs to be taken.
   - Otherwise, go to **Step 4**.

Step 4 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.52 Predeploy device type no match

Description

The type of the NE to be predeployed cannot be matched.

Attribute

Alarm ID	Alarm Severity	Alarm Type
120	Critical	Equipment

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

The NE fails to be predeployed.

Possible Causes

The type of the NE to be predeployed is inconsistent with the planned NE type.

Procedure

Step 1 Check whether the planned NE type is correct. If incorrect, change it to the actual NE type and predeploy the NE again.

----End

Related Information

None

A.53 ALM-121 Sending Remote Notification Message Failed

Description

When remote notification short messages fail to be sent, this alarm is generated. The alarm must be manually cleared.

NOTE

The location information of the alarm contains the text (255 characters at most) in remote notifications.

Attribute

Alarm ID	Alarm Severity	Alarm Type
121	Major	Processing error

Impact on the System

The specified user fails to receive remote notifications.

System Actions

None.

Possible Causes

The communication parameters are set incorrectly.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 1. Log in to the U2000 client. Choose **Fault** > **Settings** > **Remote Notification** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Remote Notification** from the main menu (application style). In the **Remote Notification** window, check whether the remote notification rule is set and enabled.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 In the **Remote Notification** window, check whether the phone number is correct in the remote notification rule.

- If no, change it to the correct number. Then go to **Step 3**.
- If yes, go to **Step 3**.

Step 3 In the **Remote Notification** window, click **Settings** in the lower left corner and choose **Communication Device**. Then check whether communication parameters of the SMS type have been set.

- If yes, go to **Step 5**.
- If no, go to **Step 4**.

Step 4 Click **Add**. Set the communication parameters and select **Enable**.

Step 5 Select an enabled SMS communication parameter and click **Properties**. In the **Modify Communication Device** window, click the **Communication Device** tab. Click **Test on Server**.

- If the test succeeds, go to **Step 6**.
- If the test fails, go to **Step 7**.

Step 6 Choose **Fault** > **Browse Current Alarms** from the main menu. Right-click an alarm and choose **Send Notification** > **Short Message** from the shortcut menu to send a remote notification. Check whether ALM-121 Sending Remote Notification Message Failed is reported.

- If yes, go to **Step 7**.
- If no, the procedure ends.

Step 7 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.54 ALM-123 The Digital Certificate Is to Expire

Description

If the number of remaining validity days of a digital certificate is smaller than the threshold (the default value is 30) for generating digital certificate validity alarms, the alarm that the digital certificate is to expire is generated once each day. This alarm only indicates that the current digital certificate is to expire and the user needs to apply for a new one to replace it. This alarm is automatically cleared after the new certificate is used.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
123	Minor	Processing error

Parameters

Name	Meaning
Type of certificate	Type of the digital certificate. The value is device certificate, trust certificate, or cross certificate.
Certificate file	Name of the digital certificate file.
Common Name	Name of the entity who uses the certificate.
Issuer	Certificate authority name that issued the certificate.
Serial Number	Serial number of the certificate file.
Days about to expire	Number of days before the digital certificate expires.

Impact on the System

The system displays a message indicating that the current digital certificate is to expire and the user needs to replace it with a new one. If a digital certificate has expired, the SSL communication re-handshake fails. As a result, the device communications are interrupted.

System Actions

None.

Possible Causes

The digital certificate is to expire.

Procedure

Step 1 Apply for a digital certificate.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **Step 2**.

Step 2 Contact Huawei technical support engineers to resolve the problem.

----End

Copyright © Huawei Technologies Co., Ltd.

A.55 ALM-124 The Digital Certificate Has Expired

Description

When a digital certificate expires, an alarm is generated, indicating that the digital certificate becomes invalid and the user needs to apply for a new one. This alarm is automatically cleared after the new certificate is used.

Attribute

Alarm ID	Alarm Severity	Alarm Type
124	Major	Processing error

Parameters

Name	Meaning
Type of certificate	Type of the digital certificate. The value is device certificate, trust certificate, or cross certificate.
Certificate file	Name of the digital certificate file.
Common Name	Name of the entity who uses the certificate.
Issuer	Certificate authority name that issued the certificate.
Serial Number	Serial number of the certificate file.
Expired days	Number of days after the digital certificate expires.

Impact on the System

If a digital certificate has expired, the SSL communication re-handshake fails. As a result, the device communications are interrupted.

System Actions

None.

Possible Causes

The digital certificate has expired, and the user needs to replace it with a new one.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Apply for a digital certificate.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **Step 2**.

Step 2 Contact Huawei technical support engineers to resolve the problem.

----End

A.56 ALM-119 Alarm of the Switchover to the Standby Syslog Server

Description

When services are switched to the standby syslog server because the U2000 fails to connect to the master syslog server, this alarm is generated. If services are switched back to the master syslog server after the connection to the master syslog server recovers, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
119	Major	Environment

Parameters

Name	Meaning
Master Server IP	IP address of the master syslog server.
Master Server Port	Port of the master syslog server.
Standby Server IP	IP address of the standby syslog server.
Standby Server Port	Port of the standby syslog server.

Impact on the System

Logs delivered through the Syslog protocol are then forwarded to the standby 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 standby syslog server.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

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

Procedure

Step 1 Check whether the master syslog server is running.

- If no, start it. No further operation needs to be taken.
- If yes, go to **Step 2**.

NOTE

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

Step 2 Check whether the network connection of the master syslog server is correct.

- If no, rectify the network fault. No further operation needs to be taken.
- If yes, go to **Step 3**.

Step 3 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.57 ALM-118 Alarm of the Failure to Connect the Master and Standby Syslog Servers

Description

When the U2000 fails to connect to the master and standby syslog servers, this alarm is generated. If the connection to the master or standby syslog server recovers, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
118	Major	Environment

Parameters

Name	Meaning
Master Server IP	IP address of the master syslog server.
Master Server Port	Port of the master syslog server.
Standby Server IP	IP address of the standby syslog server.
Standby Server Port	Port of the standby syslog server.

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

Logs cannot be forwarded to the master or standby syslog servers, and the number of logs to be forwarded keeps increasing. When the number of logs accumulated in the database reaches the upper limit 20,000, subsequent logs are discarded.

System Actions

None.

Possible Causes

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

Procedure

Step 1 Check whether the master and standby syslog servers are running.

- If no, start them. No further operation needs to be taken.
- If yes, go to **Step 2**.

NOTE

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

Step 2 If **Protocol** used for the communication between the U2000 server and the Syslog server is set to **TLS**, run the following command to check whether the identity certificate of the log forwarding service matches the private key of the service. If **Protocol** is not set to **TLS**, go to **Step 3**. For details about how to query the value of **Protocol**, see Setting the Interconnection Between the U2000 and the Syslog Server.

$ **ssl_adm -cmd verify -app** *syslog*

Enter the identity certificate password of the log forwarding service as prompted.

NOTE

- The identity certificate password is specified when certificates are deployed for the log forwarding service. For details, see U2000 administrator guide.
- In the command, *syslog* indicates the folder that stores the log forwarding service certificates under **/opt/oss/server/etc/ssl**, In the entire procedure, it is assumed that certificates are stored in **/opt/oss/server/etc/ssl/syslog**.

- If information similar to the following is displayed, the identity certificate matches the private key. Go to **Step 3**.
  ```
  Successfully verify certificates and configuration.
  ```
- If information similar to the following is displayed, the identity certificate does not match the private key. Deploy the certificates again by following the procedure provided in U2000 administrator guide.
  ```
  Verify Failed.
  ```

Step 3 Check whether the network connections of the master and standby syslog servers are correct.

- If no, rectify the network fault. No further operation needs to be taken.
- If yes, go to **Step 4**.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.58 ALM-130 The Alarm Report Buffering Blocked

Description

When the size of the alarm buffer is greater than 80% of the capacity, the alarm buffering is blocked, and this alarm is generated. When the buffer size is less than 30% of the capacity, the alarm buffering is unblocked, and this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
130	Major	Service

Parameters

Name	Meaning
Service name	Service name of the server that generates an alarm.

Impact on the System

Alarm reporting is delayed. Some alarms cannot be displayed on the client or the OSS in a timely manner.

System Actions

None.

Possible Causes

- Some NEs are abnormal and report a large number of alarms in a short period.
- Many correlation rules are set, which slows down the system analysis.

Procedure

Step 1 Log in to the U2000 client. Choose **Fault** > **Settings** > **Correlation** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Correlation** from the main menu (application style). In the **Correlation** window, check whether alarm correlation rules have been set and enabled.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). Then, choose **Fault** > **Browse Event Logs** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Query Event Logs** from the main menu (application style). Check whether an NE reports alarms or events frequently in each displayed window.

- If yes, go to **Step 4**.
- If no, go to **Step 6**.

Step 3 In the **Correlation** window, disable the existing correlation rules. Then go to **Step 5**.

Step 4 Choose **Fault** > **Settings** > **Mask Rules** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Alarm Settings** > **Mask Rules** from the main menu (application style). In the **Mask Rules** window, set mask rules for the NE that reports alarms or events frequently. Then go to **Step 5**.

Step 5 Wait for 30 minutes. After that, check whether the alarm is cleared.

- If yes, the fault is rectified successfully and the procedure ends.
- If no, go to **Step 6**.

Step 6 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.59 ALM-294 Expired OSS License File

Description

When the permanent commercial and fixed-period License files of a product are simultaneously used on the OSS and the fixed-period License file expires and enters the grace period, this alarm is generated. This alarm is automatically cleared when **A.60 ALM-295 OSS License File in Default State** is generated for the fixed-period License file.

Attribute

Alarm ID	Alarm Severity	Alarm Type
294	Critical	Processing error

Parameters

Name	Meaning
Product	Product to which the License file belongs.
LicenseSN	Identity of the License file for which an alarm is generated.

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

None

System Actions

The OSS clears **A.59 ALM-294 Expired OSS License File** when **A.60 ALM-295 OSS License File in Default State** is generated for the fixed-period License file.

Assume that the permanent commercial and fixed-period License files of the U2000 are simultaneously used on the OSS, and the fixed-period License file expired on December 30, 2011, with a grace period of 90 days. On December 31, 2011, the OSS generated **A.59 ALM-294 Expired OSS License File**. After that, the License file still could be used for 90 days. On March 29, 2012, **A.59 ALM-294 Expired OSS License File** was cleared, **A.60 ALM-295 OSS License File in Default State** was generated, and the License file became invalid.

Possible Causes

The permanent commercial and fixed-period License files of a product are simultaneously used on the OSS and the fixed-period License file expires and enters the grace period.

Procedure

Step 1 Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **License Information** from the main menu (application style). In the **License Information** dialog box, click the **Resource Control Item** or **Function Control Item** tab. Then check whether **Authorization Expiration Time** of the License item is due.

Step 2 If **Authorization Expiration Time** is due, ask Huawei technical support engineers to apply for a new License.

Step 3 Update the License file.

----End

A.60 ALM-295 OSS License File in Default State

Description

When the permanent commercial and fixed-period License files of a product are simultaneously used on the OSS and the fixed-period License file enters the default state, this alarm is generated. When the License is updated, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
295	Critical	Processing error

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
Product	Product to which the License file belongs.
LicenseSN	Identity of the License file for which an alarm is generated.

Impact on the System

The functions controlled by the License file that has entered the default state are unavailable.

System Actions

A.60 ALM-295 OSS License File in Default State is generated when the permanent commercial and fixed-period License files of a product are simultaneously used on the OSS and the fixed-period License file enters the default state. Then, the License file in the default state is removed.

Assume that the permanent commercial and fixed-period License files of the U2000 are simultaneously used on the OSS, and the fixed-period License file expired on December 30, 2011, with a grace period of 90 days. On March 30, 2012, the U2000 generated **A.60 ALM-295 OSS License File in Default State**. After that, the expired License file could not be used.

Possible Causes

The permanent commercial and fixed-period License files of a product are simultaneously used on the OSS, and the fixed-period License file enters the default state at the end of the grace period.

Procedure

Step 1 Ask Huawei technical support engineers to apply for a new License file.

----End

A.61 ALM-296 The NE Capacity Reached the Threshold Alarm

Description

When the total capacity of NEs connected to the U2000 reaches the preset threshold, this alarm is generated. When the total capacity falls below the threshold, the alarm is cleared.

NOTE

To set the NE capacity threshold, choose **Help** > **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (application style), set **Threshold**.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
296	Critical	Processing error

Parameters

Name	Meaning
Threshold	The NE capacity threshold for the U2000 License.
CurrentPercent	The total capacity of NEs connected to the U2000.

Impact on the System

A message is displayed, indicating that the NE capacity has reached the threshold and that users must 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 low.
- The NE capacity specified in License is small.

Procedure

Step 1 Choose **Help** > **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **Alarm Configuration for License Resource Item Capacity** from the main menu (application style). Check whether the NE capacity threshold is too low.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **License Information** from the main menu (application style). Check whether the NE capacity in the License is sufficient.

- If yes, no further operation needs to be taken.
- If no, apply for a new License to increase the NE capacity. Then go to **Step 5**.

Step 3 Specify another NE capacity threshold (90% is recommended) in the License.

- If the alarm is cleared, no further operation needs to be taken.

Copyright © Huawei Technologies Co., Ltd.

- If the alarm is not cleared, go to **Step 5**.

Step 4 Reduce the number of NEs controlled in the U2000.

- If the alarm is cleared, no further operation needs to be taken.
- If the alarm is not cleared, go to **Step 5**.

Step 5 Collect the above-mentioned alarm information and contact Huawei technical support engineers for a solution.

----End

A.62 ALM-297 The OSS License Expired

Description

When the OSS License expires, this alarm is generated. When the License is updated, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
297	Critical	Processing error

Parameters

Name	Meaning
ProductName	Product to which the License file belongs.

Impact on the System

When the License expires, the U2000 periodically displays a message, asking users to update the License. The frequency of displaying this message increases with time. It is recommended that users promptly ask Huawei technical support engineers to apply for a new License.

NOTE

After the dialog box indicating that the License expires is displayed, OSS functions are not affected during the grace period. To ensure that OSS functions can be properly used in the future, users are advised to apply for a new License.

System Actions

None.

Possible Causes

The U2000 License expires.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Ask Huawei technical support engineers to apply for a new U2000 License.

----End

A.63 ALM-298 The User in the SMManagers Group Changes a User's Password

Description

When a user in the **SMManagers** group changes the password of another user, this alarm is generated. This alarm needs to be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
298	Critical	Security

Parameters

Name	Meaning
User Name	Name of the user whose password is changed.
Timestamp	Time when a user password is changed.

Impact on the System

This alarm is critical. The user whose password is changed cannot log in to the U2000 using the old password.

System Actions

None.

Procedure

Step 1 The alarm does not need to be handled.

----End

Copyright © Huawei Technologies Co., Ltd.

A.64 ALM-299 An OSS User Is Added to the Administrators, SMManagers or Sub Domain User Group

Description

When an U2000 user is added to the user group **Administrators**, **SMManagers**, or **Subdomain Security Administrator Group**, this alarm is generated. This alarm needs to be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
299	Critical	Security

Parameters

Name	Meaning
User Name	Name of a new user.

Impact on the System

This alarm is critical. A user with high rights is added.

System Actions

None.

Procedure

Step 1 The alarm does not need to be handled.

----End

A.65 The status of the interface configured with IPSec services turns to Down

Description

The status of the interface configured with IPSec services changes from **Up** to **Down**.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
663	Major	Service

Impact on the System

IPSec services will be interrupted.

Possible Causes

The interface configured with IPSec services is shut down or the cable is disconnected.

Procedure

Step 1 Telnet to the device. Run the **display ip interface brief** command to check the current status of the interface.

- If the interface is Down, Run the **undo shutdown** command to enable the interface.
- If the interface is Up, go to **Step 2**.

Step 2 Contact technical support personnel.

----End

Related Information

None.

A.66 ALM-801 OSS License Beyond Limitation

Description

When the consumed capacity exceeds the License capacity, this alarm is generated. When the consumed capacity falls below the License capacity, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
801	Critical	Processing error

Parameters

Name	Meaning
LicenseID	ID of a License authorization item.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
LicenseName	Name of a License authorization items.
LicenseCapacity	Maximum number of NEs and maximum number of client connections in a License.
LicenseConsumption	Consumed capacity.
BeyondTime	Time when the consumed capacity exceeds the License capacity.

Impact on the System

- If the total consumed capacity of NEs managed by the U2000 exceeds the License capacity, no more NE can be added to the U2000.
- If the number of clients connected to the U2000 exceeds the License capacity, no more client can connect to the U2000.

System Actions

None

Possible Causes

- The total consumed capacity of NEs managed by the U2000 exceeds the License capacity.
- The number of clients connected to the U2000 exceeds the License capacity.
- The number of other resources managed by the current U2000 exceeds the License capacity.

Procedure

Step 1 Log in to the U2000 client.

Step 2 Choose **Help** > **License Management** > **License Information** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **License Management** > **License Information** from the main menu (application style). In the **License Information** dialog box, check the license capacity on the **Resource Control Item** tab.

Step 3 Reduce the number of consumed resources that have exceeded the capacity specified in the License, or ask Huawei technical support engineers to apply for a new U2000 License.

----End

A.67 OceanStor Storage System Alarm

Description

This alarm is generated when the server OceanStor storage system does not function properly.

Copyright © Huawei Technologies Co., Ltd.

Alarm ID **1043** specifies the alarm of the OceanStor S2600 disk array. Alarm ID **1049** specifies the alarm of the OceanStor S3900 disk array.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1043	Critical	Environment
1049	Critical	Environment

Impact on the System

The disk array may not function properly or data may be lost.

Possible Causes

- The member disks (hard disks constituting a RAID group in the OceanStor system) are faulty or removed.
- The disk is faulty or reading the capacity fails.
- The disk is not connected to the loop.
- The disks are not working properly.
- The SMART information of disks are illegal.
- The disk is isolated.
- The disk capacity is too small.
- The disk types are different.
- The expander subrack power fails.
- The types of coffer disks are inconsistent.
- The disk is faulty or removed.
- No available free disk is found.
- Only single controller identifies the disk subrack.
- The expander port is faulty.
- The expander port link down.
- Only single controller registers with the coffer disks successfully.
- The SES firmware (internal storage chip) fails to register.

Copyright © Huawei Technologies Co., Ltd.

- The version synchronization of the SES firmware fails.
- The voltage of the host port module is too low.
- The temperature of the disk exceeds the maximum value.
- The SES firmware fails to communicate with other devices or the temperature sensor on the air intake vent fails.
- The controller subrack temperature exceeds the maximum value and services stop.
- The temperature of checkpoint 2 exceeds the maximum value.
- Two fans are idling.
- Two fans are faulty.
- The fan is absent.
- No output from the power supply is available.
- The PEM is not present.
- The BBU(Backup Battery Unit) is in the abnormal status.
- The BBU exceeds the service period.
- No battery (UPS/BBU) is attached.
- The DE4 port component on the controller fails.
- The actual working specifications of the optical module are not in the normal range of the working specifications.
- The SAS (internal storage chip) host port module is faulty.
- An expander module is removed.
- An failure occurs in the controller or the expander module.
- Only single controller is running in the system.
- The system is in the safe mode.
- 1068E is faulty. This controller will reset.
- Fail to recover the coffer disk.
- The coffer log works improperly. No information is recorded in the log.
- The OS coffer fails to be reconstructed.
- The OS coffer fails to be recovered on the peer end.
- The Boot Device (flash card) of Controller is Corrupt.
- Failed to clear the controller power failure.
- Failed to clear the battery or PEM failure.
- Failed to clear the PEM failure.
- Failed to clear the mirroring link failure.
- Failed to handle the recover of the mirroring link failure.
- Failed to switch over the controllers.
- Failed to power on the storage system.
- Failed to restart the storage system.
- Failed to remove the over temperature fault of the controller subrack.
- Failed to clear the disk subrack power failure.

Copyright © Huawei Technologies Co., Ltd.

- Failed to read DBs.
- Failed to clear the alarm that the peer controller is not powered on.
- The hot-spare disk is insufficient.
- The speed of SFP mismatches the speed of port.
- The capacity of the hard disk is not supported in this version. The access to the hard disk is forbidden.
- Expander port PHY disable.
- Disk faulty sector recovery failed.
- LUN medium error.
- Error codes occur on the front-end FC port.
- Disk response is slow.
- Power module version is too old, cannot support BBU.

Procedure

Step 1 This document provides troubleshooting methods for the fault occurred because of different causes, as shown in the following table.

Table A-11 Troubleshooting methods

Possible Cause	Troubleshooting Method
The disk is not functioning properly or is removed.	Insert the disk again or replace the disk.
The disk is faulty or reading the capacity fails.	Insert the disk again or replace the disk.
The disk is not connected to the loop.	Insert the disk again or replace the disk.
The SMART information of disks are illegal.	Back up data and check the disk status.
The disks are invalid.	Replace the disks with new disks that have been approved.
The disk is isolated.	Replace the disk.
The disk capacity is lower than the minimum value.	Replace the disk.
The disk types are different.	Replace the disk.
The expander subrack power supply fails.	● Check whether the expander subrack is powered on. ● Check whether cascading cables are connected properly.
The coffer disk types are different.	Replace the coffer disk that causes inconsistency.

Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Troubleshooting Method
A member disk becomes invalid or is removed during copyback.	Replace the disk.
A member disk becomes invalid or is removed during reconstruction.	Replace the disk.
A member disk becomes invalid or is removed during LUN formatting.	Locate the disk and contact technical support engineers.
A member disk becomes invalid or is removed.	Locate the disk and contact technical support engineers.
The hot space disk becomes invalid or is removed during pre-copy.	Check whether an alarm about a invalid disk is generated and replace or insert the disk.
The hot spare disk becomes invalid and a proper idle disk is unavailable currently.	Replace the disk.
Only one controller identifies the disk subrack.	Check whether the FC cables or power cables of the disk subrack are properly connected.
The expander port is faulty.	Replace the expander port.
The expander port link is down.	Check whether the expander port is functioning properly or cascading cables are connected properly.
Registration of the coffer disk fails.	Replace the coffer disk and restart the disk array.
Registration of the SES firmware fails.	● Check whether cascading cables are connected properly. ● Power on the control subrack or expander subrack again.
The version synchronization of the SES firmware fails.	Power on the control subrack or expander subrack again. If problem persists, change the controller or cascading module.
The voltage of the host port module is lower than the minimum value.	Check the voltage and take proper measures to stabilize the voltage.
The temperature of the disk exceeds the maximum value.	Check whether the fan is running properly.
The SES firmware fails to communicate with other devices or the temperature sensor on the air intake vent fails.	Check whether the related blade is functioning properly.

Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Troubleshooting Method
The controller subrack temperature exceeds the maximum value and services stop.	Check the controller subrack temperature.
The temperature of the monitoring points exceeds the maximum value.	Lower the room temperature or replace the faulty fan.
Two fans are idling.	Replace fans with new ones.
Two fans are not functioning properly.	Replace fans with new ones.
The fan is unavailable.	Insert a fan module.
No output from the power supply is available.	Check the power input or replace the power supply.
The PEM is not available.	Install a PEM or replace the faulty PEM.
The BBU is not functioning properly.	Check the status of the BBU or replace the BBU.
The BBU exceeds the service period.	Replace the BBU.
No battery (UPS/BBU) is attached.	Attach the battery (UPS/BBU).
The DE4 port component on the controller fails.	Replace the host port module or the controller.
The actual working specifications of the optical module are not in the normal range.	Replace the optical module.
The SAS host port module is not functioning properly.	Restart the controller to rectify this fault. If the fault is not rectified, replace the SAS host port module.
An expander module is removed.	Insert a expander module.
A failure occurs on the controller or the expander module.	Replace the I2C component.
Only one controller is running in the system.	Install another controller.
The system is in safe mode.	Clear the database and power on the storage system again.
The controller 1068E is faulty and will be reset.	Replace the controller.

Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Troubleshooting Method
Failed to recover the coffer disk.	When the system fails to recover the coffer disk, check whether information about the coffer disk is correct.
The coffer log does not work properly. No information is recorded in the log file.	Contact technical support engineers.
The OS coffer fails to be reconstructed.	Replace the coffer disk.
The OS coffer fails to be recovered on the peer end.	Replace the coffer disk.
The boot device (flash card) of the controller is corrupted.	Replace the boot device (flash card).
Failed to handle with the controller power failure.	Power on the storage array again.
Failed to handle with the battery or PEM failure.	Check the battery status or PEM status.
Failed to handle with the PEM failure.	Contact technical support engineers.
Fail to clear the mirroring link failure	Restart the storage array.
Failed to handle the recover of the mirroring link failure.	Restart the storage array.
Failed to switch over the controllers.	Restart the storage array.
Failed to power on the storage system.	Power on the storage system again.
Failed to restart the storage system.	Check whether the hardware is faulty.
Failed to rectify the over-temperature fault on the controller subrack.	Check whether the temperature in the telecommunications room is proper and whether the fan module is functioning properly and restart the storage array.
Failed to clear the disk subrack power failure.	● Check whether the expander subrack is powered on. ● Check whether cascading cables are properly connected and restart the storage array.
Failed to read DBs.	Check whether the coffer works properly and whether the system version is consistent with the DB.
Failed to clear the alarm that the peer controller is not powered on.	Locate and rectify the fault and power on the controller again.

Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Troubleshooting Method
The hot-spare disk is insufficient.	Add a hot-spare disk.
The speed of SFP mismatches the speed of port.	Replace the SFP with a speed of 4 Gbit/s.
The capacity of the hard disk is not supported in this version. The access to the hard disk is forbidden.	Upgrade the version to support the capacity.
Expander port PHY is disabled.	The error code of expander port PHY is too large. Check the faulty board and contact technical support engineers to manually recover the alarm.
Disk faulty sector recovery fails.	Replace the hard disk and recover the alarm manually.
A LUN medium error occurs.	Contact technical support engineers.
Error codes occur on the front-end FC port.	Make sure that the optical fiber is properly connected and no fault alarm about optical transceiver is displayed. Remove the fault or contact technical support engineers.
Disk response is slow.	Contact technical support engineers.
Power module version is too old and cannot support BBU.	Contact engineer for technical support to replace power module.

----End

A.68 ALM-1100 CPU abnormal

Description

An error occurs in the CPU hardware. The alarm must be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1100	Major	Hardware system

Parameters

Name	Meaning
AlmName	Alarm name.

Copyright © Huawei Technologies Co., Ltd.

Name	Meaning
AlmDesc	Alarm description.

Impact on the System

An error occurs in the hardware. Services may be interrupted.

System Actions

None.

Procedure

Step 1 Check whether you can rectify the fault based on alarm location information, additional information, and logs.

- If yes, clear the alarm.
- If no, go to **Step 2**.

Step 2 Start the dedicated hardware monitoring program (IBM Director, HP WEBES, and DELL OpenManager) to check running status of system hardware.

- If the hardware is running properly, clear the alarm.
- If you cannot identify the fault cause or rectify the fault, go to **Step 3**.

Step 3 Contact Huawei technical support engineers for a solution or submit a fault report at **http://icare.huawei.com**.

----End

Clearing

After the fault is rectified, you need to manually clear the alarm on the U2000 client.

A.69 ALM-1101 Memory abnormal

Description

An error occurs in the memory hardware. The alarm must be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1101	Major	Hardware system

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
AlmName	Alarm name.
AlmDesc	Alarm description.

Impact on the System

An error occurs in the hardware. Services may be interrupted.

System Actions

None.

Procedure

Step 1 Check whether you can rectify the fault based on alarm location information, additional information, and logs.

- If yes, clear the alarm.
- If no, go to **Step 2**.

Step 2 Start the dedicated hardware monitoring program (such as IBM Director, HP WEBES, and DELL OpenManager) to check running status of system hardware.

- If the hardware is running properly, clear the alarm.
- If you cannot identify the fault cause or rectify the fault, go to **Step 3**.

Step 3 Contact Huawei technical support engineers for a solution or submit a fault report at **http://icare.huawei.com**.

----End

Clearing

After the fault is rectified, you need to manually clear the alarm on the U2000 client.

A.70 ALM-1102 Environment abnormal

Description

An error occurs in the power supply or fans. The alarm must be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1102	Major	Hardware system

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
AlmName	Alarm name.
AlmDesc	Alarm description.

Impact on the System

An error occurs in the hardware. Services may be interrupted.

System Actions

None.

Procedure

Step 1 Check whether you can rectify the fault based on alarm location information, additional information, and logs.

- If yes, clear the alarm.
- If no, go to **Step 2**.

Step 2 Start the dedicated hardware monitoring program (IBM Director, HP WEBES, and DELL OpenManager) to check the running status of system hardware.

- If the hardware is running properly, clear the alarm.
- If you cannot identify the fault cause or rectify the fault, go to **Step 3**.

Step 3 Contact Huawei technical support engineers for a solution or submit a fault report at **http://icare.huawei.com**.

----End

Clearing

After the fault is rectified, you need to manually clear the alarm on the U2000 client.

A.71 ALM-1103 HD abnormal

Description

An error occurs in a hard disk. The alarm must be manually cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1103	Major	Hardware system

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
AlmName	Alarm name.
AlmDesc	Alarm description.

Impact on the System

An error occurs in the hardware. Services may be interrupted.

System Actions

None.

Procedure

Step 1 Check whether you can rectify the fault based on alarm location information, additional information, and logs.

- If yes, clear the alarm.
- If no, go to **Step 2**.

Step 2 Start the dedicated hardware monitoring program (IBM Director, HP WEBES, and DELL OpenManager) to check the running status of purchased hardware.

- If the hardware is running properly, clear the alarm.
- If you cannot identify the fault cause or rectify the fault, go to **Step 3**.

Step 3 Contact Huawei technical support engineers for a solution or submit a fault report at **http://icare.huawei.com**.

----End

Clearing

After the fault is rectified, you need to manually clear the alarm on the U2000 client.

A.72 ALM-1119 Network interface status changed

Description

When an exception occurs in the communication of a network adapter on the U2000 server, this alarm is generated. When the network adapter communication is recovered, the alarm is cleared.

NOTE

Only HP servers report this alarm.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1119	Major	Hardware system

Parameters

Name	Meaning
NetCard	ID of the network adapter that reports an alarm.
AlmCause	Alarm cause.
AlmDesc	Alarm description.
AlmAction	Handling suggestion.

Impact on the System

A network adapter on the U2000 server works improperly.

System Actions

None.

Possible Causes

- The network adapter is not started.
- The network cable is disconnected.
- A hardware fault occurs.
- The peer device is faulty.

Procedure

Step 1 Check whether the network adapter is started.

1. Use the PuTTY to log in to the U2000 server as user **ossuser** in SSH mode.
2. Run the following command to switch to user **root**:

   $ **su - root**

   Password:***Password of root***
3. Run the following command to check the network adapter status:

   NOTE

   You can locate the network adapter where the alarm is generated from the alarm information. This procedure assumes that the network adapter is lan0.

   # **lanscan**

Copyright © Huawei Technologies Co., Ltd.

```
Hardware Station        Crd Hdw   Net-Interface  NM  MAC       HP-DLPI DLPI
Path     Address        In# State NamePPA        ID  Type      Support Mjr#
0/0/0/0  0x6A9BFD165596 0   DOWN    lan0 snap0     1   ETHER     Yes     119
0/0/2/0  0xBED87D502DEE 1   UP    lan1 snap1     2   ETHER     Yes     119
0/0/4/0  0x9642E1C1E7F7 2   UP    lan2 snap2     3   ETHER     Yes     119
0/0/5/0  0x321C9A83147B 3   UP    lan3 snap3     4   ETHER     Yes     119
LinkAgg0 0x000000000000 900 DOWN  lan900 snap900 6   ETHER     Yes     119
LinkAgg1 0x000000000000 901 DOWN  lan901 snap901 7   ETHER     Yes     119
LinkAgg2 0x000000000000 902 DOWN  lan902 snap902 8   ETHER     Yes     119
LinkAgg3 0x000000000000 903 DOWN  lan903 snap903 9   ETHER     Yes     119
LinkAgg4 0x000000000000 904 DOWN  lan904 snap904 10  ETHER     Yes     119
```

- In the command output, if the value of **Hdw State** is **DOWN**, the network adapter is not started. Then go to **1.4**.
- In the command output, if the value of **Hdw State** is **UP**, go to **Step 2**.

4. Run the following command to start the network adapter:

   # **ifconfig lan0 up**

   Run the following command to check the network adapter status:

   # **lanscan**

   - If the network adapter is started, go to **1.5**.
   - If the network adapter is not started, go to **Step 4**.

5. Check whether the alarm is cleared on the U2000.

   After the preceding steps, wait for 10 minutes. Then log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the alarm is cleared.

   - If yes, no further operation needs to be taken.
   - If no, go to **Step 2**.

Step 2 Check whether the network cable is disconnected.

1. Run the following command to check the network connection status:

   # **ifconfig lan0**

   - The following information indicates that the network connection is proper. Then go to **Step 4**.

     ```
     lan0: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
             inet 10.71.169.104 netmask fffffe00 broadcast 10.71.169.255
     ```

   - The following information indicates that the network connection is faulty. Then go to **2.2**.

     ```
     lan0: flags=1843<BROADCAST,RUNNING,MULTICAST,CKO>
             inet 10.71.169.104 netmask fffffe00 broadcast 10.71.169.255
     ```

2. Check whether the network cable is disconnected from the network adapter.
   - If yes, reconnect the network cable. When the network connection is proper, go to **2.4**.
   - If no, go to **2.3**.
3. Check whether the network cable is disconnected from the peer device.
   - If yes, reconnect the network cable. When the network connection is proper, go to **2.4**.

Copyright © Huawei Technologies Co., Ltd.

- If no, go to **Step 3**.

4. Check whether the alarm is cleared on the U2000.

   After the preceding steps, wait for 10 minutes. Then log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the alarm is cleared.

   - If yes, no further operation needs to be taken.
   - If no, go to **Step 3**.

Step 3 Check whether a hardware fault occurs.

1. Connect the network cable to the standby network port if the server has a standby network port. Then check whether the network connection is proper.
   - If yes, a hardware fault occurs on the network adapter. Ask the server supplier to replace the faulty network adapter. Then go to **3.4**.
   - If no, go to **3.2**.
2. Replace the network cable and check whether the network connection is proper.
   - If yes, go to **3.4**.
   - If no, go to **3.3**.
3. Ask the peer device maintenance engineer to check whether the peer device is faulty.
   - If yes, rectify the fault on the peer device. Then go to **3.4**.
   - If no, go to **Step 4**.
4. Check whether the alarm is cleared on the U2000.

   After the preceding steps, wait for 10 minutes. Then log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarms** > **Browse Current Alarm** from the main menu (application style). In the **Browse Current Alarm** window, check whether the alarm is cleared.

   - If yes, no further operation needs to be taken.
   - If no, go to **Step 4**.

Step 4 Collect alarm information.

If the alarm persists, collect the following information and contact Huawei technical support engineers:

- Alarm details displayed on the U2000 client
- Command output in steps **Step 1** to **Step 3**
- Physical device types
- Network diagram

----End

Clearing

After the fault is rectified, the U2000 will automatically clear the alarm.

Copyright © Huawei Technologies Co., Ltd.

A.73 Power Failure

Description

This alarm is generated when the server power supply does not function properly.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1200	Critical	Environment

Impact on the System

The server power supply may be insufficient; as a result, the U2000 stops running.

Possible Causes

- The PEM is not present.
- No output from the power supply.

Procedure

- You need to install a PEM or replace the faulty PEM.
- Check the power input or replace the power supply.

----End

A.74 Fan Failure

Description

This alarm is generated when the server fan does not function properly.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.

Copyright © Huawei Technologies Co., Ltd.

- The host that generates the alarm runs on Solaris. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1201	Critical	Environment

Impact on the System

The server dissipation may be insufficient and the equipment temperature is too high; as a result, the U2000 stops running.

Possible Causes

- The fan is absent.
- The fan is faulty.

Procedure

- Check the fan input.
- You need to replace the fan with a new one.

----End

A.75 Hard Disk Failure

Description

This alarm is generated when the server hard disk does not function properly.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1203	Critical	Equipment

Impact on the System

The U2000 may stop running.

Possible Causes

The disk is faulty or reading the capacity fails.

Procedure

Step 1 You need to reinsert the disk or replace the disk.

----End

A.76 The Network Cable Is Disconnected

Description

This alarm is generated when server network cables do not function properly.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1211	Major	Equipment

Impact on the System

Client fail to be properly connected to the U2000.

Possible Causes

The link is down.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the link is down. If the link is down, replace it.

----End

A.77 NIC in Half-Duplex Mode

Description

On Solaris 10, the NIC is in half-duplex mode.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5221	Warning	Environment

Impact on the System

Data replication between the primary and secondary sites is slow.

Possible Causes

The duplex mode of the NIC has been changed or the switch is in half-duplex mode.

Procedure

Step 1 Run the following command as the **root** user to go to the **rc3.d** directory:

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

Step 2 Run the following commands to create and edit the **S99set*bge*** file:

```
# 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
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Meanings of these commands:

```
ndd -set /dev/bge0 adv_1000fdx_cap 0      (This command disables the 1000M full-duplex mode.)
ndd -set /dev/bge0 adv_1000hdx_cap 0     (This command disables the 1000M half-duplex mode.)
ndd -set /dev/bge0 adv_100fdx_cap 1      (This command enables the 100M full-duplex mode.)
ndd -set /dev/bge0 adv_100hdx_cap 0     (This command disables the 100M half-duplex mode.)
ndd -set /dev/bge0 adv_10fdx_cap 0       (This command disables the 10M full-duplex mode.)
ndd -set /dev/bge0 adv_10hdx_cap 0       (This command disables the 10M half-duplex mode.)
ndd -set /dev/bge0 adv_autoneg_cap 0     (This command disables the autonegotiation mode.)
```

NOTICE

In the preceding commands, *bge0* is the NIC name. In practice, replace it with the actual name.

Step 3 Run the following commands to modify the properties of the **S99setbge** file:

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

Step 4 Run the following command to verify the properties of the **S99setbge** file:

```
# ls -l S99setbge
```

Step 5 Run the following commands to restart the U2000 for the NIC settings to take effect:

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

Step 6 Run the following command to check the duplex mode of the NIC:

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

The bge0 NIC has been successfully set to the 100M full-duplex mode if the following information is displayed:

```
......
bge:0:parameters:link_duplex    2
......
bge:0:parameters:link_speed     100
......
```

link_duplex indicates the duplex mode and may take one of the following values:

- **0**: down
- **1**: half-duplex
- **2**: full-duplex

----End

Copyright © Huawei Technologies Co., Ltd.

A.78 Power Threshold Alarm

Description

An alarm is generated when the remaining capacity of the storage battery is lower than the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4001	Major	Communication

Parameters

Parameter Name	Description
Parameter 1	EMU ID
Parameter 2	Storage battery power threshold
Parameter 3	Remaining power

Impact on the System

The remaining capacity of the storage battery is lower than the threshold. If the storage battery is exhausted, NEs will malfunction.

Possible Causes

If the AC power is interrupted, a storage battery supplies power to NEs. If the remaining capacity of the storage battery is lower than the threshold, the alarm occurs.

Procedure

- Check whether the AC power supply is functioning properly.
- Check whether the storage battery is aged. If it is aged, replace it in a timely manner.

----End

Related Information

There is no related information.

Copyright © Huawei Technologies Co., Ltd.

A.79 Database Size exceeds the threshold

Description

The performance database PMDataDB is full.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4233	Critical	Equipment

Parameters

None.

Impact on the System

Impact on the system: The newly collected performance data cannot be stored, resulting in data loss.

Possible Causes

- Cause 1: The life cycle of performance data is too long.
- Cause 2: The size of the performance database PMDataDB is too small.

Procedure

Step 1 For cause 1: adjust the life cycle of performance data. For details, see **Lifecycle Configuration for Auto Dump** of *U2000 User Guide for PMS-(version)*.

Step 2 For cause 2: expand capacity for the performance data PMDataDB.

1. Calculating the size of the performance database. For details, see **Planning of Performance Database Size** of *U2000 User Guide for PMS-(version)*

   NOTE

   If the size of the current performance database is larger than the size of the calculated performance database, contact Huawei technical support engineers.

2. Log in to the OS as user **root** and run the following commands to execute the **$OSS_ROOT/server/tools/expandDB/expandDB.py** script for manually expanding the database:

```
# . /opt/oss/server/svc_profile.sh
# cd $OSS_ROOT/server/tools/expandDB
# python expandDB.py
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Enter the following information as prompted:

- Password for the database **sa** user.
- Name of the database to be expanded.
- New database size required (The unit is MB and only a number needs to be entered.)

----End

Related Information

None.

A.80 The size of Sybase logs exceeds the threshold

Description

This alarm is generated when the size of Sybase logs exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5002	Critical	Environment

Impact on the System

This problem results in abnormal running of the database.

Possible Causes

The Sybase database is not functioning properly; as a result, the size of Sybase logs exceeds the threshold, 800 MB.

Procedure

Step 1 Contact Huawei technical support engineers to obtain key logs.

Step 2 Back up logs for the Sybase database.

Step 3 Run the following command to delete Sybase logs:

```
# echo ''>/opt/sybase/ASE-*/install/DBSVR.log
```

----End

Copyright © Huawei Technologies Co., Ltd.

A.81 The usage of the paged kernel memory on Windows exceeds the alarm threshold

Description

This alarm is generated when the usage of the paged kernel memory on Windows exceeds the alarm threshold (300 MB).

NOTE

This alarm applies only to 32-bit Windows OS.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5003	Critical	Environment

Impact on the System

The upper limit of the paged kernel memory space is 360 MB. If a little space remains in the paged kernel memory, the Windows OS and application software will function inappropriately.

Possible Causes

- The server hardware drive is incorrect.
- The server OS is infected with viruses.
- The application software has a paged kernel memory leak.

Procedure

Step 1 Check the drive program of the server. If the drive program is incorrect, update it.

Step 2 Check whether the server OS is infected with viruses. If yes, use the Trend Micro antivirus software to remove viruses.

Step 3 Check whether the value of **Paged Pool** of the application software is increasing. If yes, update or stop using the application software.

Step 4 If the fault persists, contact Huawei technical support engineers for a solution.

----End

Related Information

The kernel memory recovers automatically: When the paged kernel memory space occupied reaches the upper limit (360 MB), the U2000 will collapse. To ensure security, the U2000 detects the paged kernel memory every 3 minutes. If more than 340 MB space is occupied, the U2000 automatically restarts the process that occupies the largest memory space among each type of the following processes:

Copyright © Huawei Technologies Co., Ltd.

1. Processes with more than 20,000 handles
2. Processes occupying more than 2 MB space in the paged kernel memory
3. Processes occupying more than 2 MB space in the non-paged kernel memory

In addition, the U2000 reports the event **The kernel memory recovers automatically**.

A.82 The usage of the non-paged kernel memory on Windows exceeds the alarm threshold

Description

This alarm is generated when the non-paged kernel memory on Windows exceeds the threshold (170 MB).

NOTE

This alarm applies only to 32-bit Windows OS.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5004	Critical	Environment

Impact on the System

The upper limit of the non-paged kernel memory space is 256 MB. If a little space remains in the non-paged kernel memory, the Windows OS and application software will function inappropriately.

Possible Causes

- The server hardware drive is incorrect.
- The server OS is infected with viruses.
- The application software has a non-paged kernel memory leak.

Procedure

Step 1 Check the drive program of the server. If the drive program is incorrect, update it.

Step 2 Check whether the server OS is infected with viruses. If yes, use the Trend Micro antivirus software to remove viruses.

Step 3 Check whether the value of **Non-paged pool** of the application software is increasing. If yes, update or stop using the application software.

Step 4 Restart the server and update the operating system patch.

Step 5 If the fault persists, contact Huawei technical support engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

Related Information

The kernel memory recovers automatically: When the non-paged kernel memory space occupied reaches the upper limit (256 MB), the U2000 will collapse. To ensure security, the U2000 detects the non-paged kernel memory every 3 minutes. If more than 236 MB space is occupied, the U2000 automatically restarts the process that occupies the largest memory space among each type of the following processes:

1. Processes with more than 20,000 handles
2. Processes occupying more than 2 MB space in the paged kernel memory
3. Processes occupying more than 2 MB space in the non-paged kernel memory

In addition, the U2000 reports the event **The kernel memory recovers automatically**.

A.83 The virtual memory of Windows is insufficient

Description

This alarm is generated when the virtual memory on Windows is insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5005	Critical	Environment

Impact on the System

If the virtual memory on Windows is insufficient, the system fails to work properly. If the virtual memory in Windows exceeds the lower limit, there are risks in running the U2000.

Possible Causes

- The virtual memory is not set properly.
- There is a memory leakage issue.

Procedure

Step 1 Check whether the virtual memory is set properly.

1. Right-click **Computer** and choose **Properties** from the shortcut menu.
2. Click the **Advanced system settings** tab.
3. Click the **Advanced** tab and click **Settings** in the **Performance** area.
4. Click the **Advanced** tab to view the size of the virtual memory.

Step 2 Check whether the lower limit of the virtual memory equals the physical memory and the upper limit of the virtual memory is twice the physical memory.

- If the virtual memory is not set within a proper range, correct the size of the virtual memory.

Copyright © Huawei Technologies Co., Ltd.

- If the virtual memory is set within a proper range, contact Huawei technical support engineers.

----End

A.84 The disk space for the virtual memory of Windows is insufficient

Description

This alarm is generated when the disk space for the virtual memory on Windows is insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5006	Critical	Environment

Impact on the System

If the virtual memory for the involved disk reaches the upper limit, the remaining space for the disk will be insufficient.

Possible Causes

- The virtual memory is not set properly.
- The remaining space for the disk in which the **pagefile** file is located is insufficient.

Procedure

Step 1 Check whether the virtual memory is configured properly.

1. Right-click **Computer** and choose **Properties** from the shortcut menu.
2. Click the **Advanced system settings** tab.
3. Click the **Advanced** tab. Then click **Settings** in the **Performance** area.
4. Click the **Advanced** tab to view the size of the virtual memory.

Step 2 Check whether the lower limit of the virtual memory equals the physical memory and the upper limit of the virtual memory is twice the physical memory.

- If the virtual memory is not set within a proper range, correct the size of the virtual memory.
- If the virtual memory is set within a proper range, clean up the involved disk, for example, deleting useless disk files and emptying the recycle bin.

----End

Copyright © Huawei Technologies Co., Ltd.

A.85 The swap space is insufficient

Description

This alarm is generated when the swap space is insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5007	Critical	Environment

Impact on the System

If the swap space is insufficient, the system fails to work properly. If the remaining space of the swap space is lower than 30% of the configuration, there are risks in running the U2000.

Possible Causes

- The swap space is insufficient.
- There is a memory leakage issue.

Procedure

Step 1 Contact Huawei technical support engineers.

----End

A.86 Database needs to be maintenanced

Description

This alarm is generated when database statistics are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5100	Major	Equipment

Impact on the System

Statistics on some database tables are invalid, which may lead to U2000 performance deterioration.

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

Statistics on some database tables are changed frequently, which causes invalid statistics.

Procedure

Step 1 Obtain a separate operation time window for updating statistics because this operation and other database operations are exclusive. Setting the time window to 1 hour is recommended because the statistics updating ranges from several minutes to 1 hour depending on data volumes.

Step 2 Shut down the U2000 services.

Step 3 Log in to OS as user **root** and run the following commands to execute the **$OSS_ROOT/server/tools/dbmontool/updatestat.py** script for updating the statistics:

```
# . /opt/oss/server/svc_profile.sh
# cd $OSS_ROOT/server/tools/dbmontool
# python updatestat.py
```

NOTE

Enter the following information as prompted:

- U2000 installation path, for example, **/opt/oss**.
- Username for the database administrator user.
- Password for the database administrator user.

Step 4 Restart the U2000.

----End

A.87 Database needs to be maintenanced

Description

This alarm is generated when database indexes are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5101	Major	Equipment

Impact on the System

Indexes of some database tables are invalid, which may lead to U2000 performance deterioration.

Possible Causes

The Sybase database is unstable.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Obtain a separate operation time window for recreating indexes because this operation and other database operations are exclusive. Setting the time window to 1 hour is recommended because the index recreation ranges from several minutes to 1 hour depending on data volumes.

Step 2 Shut down the U2000 services.

Step 3 Log in to OS as user **root** and run the following commands to execute the **$OSS_ROOT/server/tools/dbmontool/reindex.py** script for recreating the indexes:

```
# . /opt/oss/server/svc_profile.sh
# cd $OSS_ROOT/server/tools/dbmontool
# python reindex.py
```

NOTE

Enter the following information as prompted:

- U2000 installation path, for example, **/opt/oss**.
- Username for the database administrator user.
- Password for the database administrator user.

Step 4 Restart the U2000.

----End

A.88 Database needs to be maintenanced

Description

This alarm is generated when automatic database growth fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5102	Major	Equipment

Impact on the System

Automatic database growth fails, which may cause database space used up.

Possible Causes

The Sybase database is unstable.

Procedure

Step 1 Manually expanding the database is allowed when the U2000 is running.

Step 2 Log in to the OS as user **root** and run the following commands to execute the **$OSS_ROOT/server/tools/expandDB/expandDB.py** script for manually expanding the database:

```
# . /opt/oss/server/svc_profile.sh
```


Copyright © Huawei Technologies Co., Ltd.

```
# cd $OSS_ROOT/server/tools/expandDB
# python expandDB.py
```

NOTE

Enter the following information as prompted:

- Username for the database administrator user.
- Password for the database administrator user.
- Name of the database to be expanded.
- Extra database size required (The unit is MB and only a number needs to be entered.)

Step 3 After the database is expanded, the alarm is not automatically cleared. Log in to a U2000 client and manually clear this alarm.

----End

A.89 NE SSH Fingerprint Mismatch

Description

The SSH fingerprint of an NE does not match.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5103	Critical	Security

Impact on the System

The U2000 cannot use Secure Shell (SSH) to log in to NE, and services may be interrupted.

Possible Causes

- The public and private keys have been changed on the NE.
- The previously confirmed public key fingerprint is different from the actual public key fingerprint on the NE.
- SSH man-in-the-middle (MITM) attacks are initiated on the network.

Procedure

Step 1 Check whether the public and private keys have been changed on the NE.

If they have been changed, Choose **Administration** > **NE Communicate Parameter** > **Set NE SSH Fingerprint** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **Set NE SSH Fingerprint** from the main menu (application style).. Confirm the fingerprint again.

Step 2 Check whether the fingerprint saved on the U2000 is the same as the SSH fingerprint on the NE. If they are different, change them to the same value.

Copyright © Huawei Technologies Co., Ltd.

Step 3 If SSH MITM attacks have been initiated on the network, eliminate fake devices from the network.

----End

A.90 Failure to Connect to an Integration Server

Description

The U2000 server cannot establish communication with an integration server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5111	Major	Communication

Impact on the System

The U2000 server fails to connect to an integration server or the integration server is abnormal.

- If a standby integration server is available, system running is not affected.
- If both integration servers fail to connect to the U2000 server, the **A.91 Failure to Connect to All Integration Servers** alarm is generated.

After the alarm is generated, the U2000 continues to reconnect to the integration server. If the connection is established, the alarm is automatically cleared and its **Clearance Status** is changed to **Cleared**.

Possible Causes

- The integration server does not respond; the U2000 server fails to connect to the integration server; or the communication port is disabled on a firewall.
- An incorrect integration server IP address or port number is configured on the U2000 server.
- The integration service on the integration server does not run.
- An incorrect U2000 server IP address is registered on the integration server. Therefore, the connection request is rejected.
- An incorrect SSL certificate is configured for the U2000 server or integration server.

Procedure

Step 1 Check whether the integration server responds, whether the network between the U2000 and integration servers is normal, and whether the communication port is enabled on the firewall.

On SUSE Linux, run the following command to check the network between the U2000 and integration servers:

ping -s *integration server IP address*

1. If the integration server and network are normal, go to **Step 2**.

Copyright © Huawei Technologies Co., Ltd.

2. If they are abnormal, restore them. Wait 2 minutes after the network becomes normal. If the alarm is automatically cleared, no further operation needs to be taken. If the alarm is not cleared, go to **Step 2**.
3. If the network fault persists, contact Huawei engineers for a solution.

Step 2 Check whether the is_ip value of the U2000 server are consistent with the IP address of the integration server.

The integration information of the U2000 server is recorded in **server\etc\oss_cfg\frame\isinfo.cfg**.

1. If they are consistent, go to **Step 3**.
1. If they are inconsistent, perform the following operations:
   a. Run the integration information setting script as the **ossuser** user. On SUSE Linux, the script is **server/tools/integrate/setis.sh**.
   b. Restart the U2000 service.
      1) In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **stopnms.bat** file to stop the U2000 processes.
      2) In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **startnms.bat** file to start the U2000 processes.
   c. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, go to **Step 3**.

Step 3 Log in to the integration server and check whether the integration service runs properly.

NOTE

Open a Web browser and enter **https://*primary IS server's IP address*/ui/login** in the address box. If the page is displayed and shows registered member systems, the integration service runs properly.

1. If the integration service does not run, start it and wait 2 minutes. If the alarm is automatically cleared, no further operation needs to be taken. If the alarm is not cleared, go to **Step 4**.
2. If the integration service runs but the alarm is not cleared, go to **Step 4**.
3. If the integration service does not run, contact Huawei engineers for a solution.

Step 4 Check whether the U2000 server IP address registered on the integration server is correct.

NOTE

Log in to the integration server. Open a Web browser and enter **https://*primary IS server's IP address*/ui/login** in the address box. Check whether the U2000 server IP address is correct.

1. If the U2000 server IP address is correct, go to **Step 5**.
2. If the U2000 server IP address is incorrect, correct it. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, go to **Step 5**.

Step 5 Check whether the SSL certificates of the U2000 and integration servers are incorrectly configured.

1. If they are incorrect, correct them.
2. If they are correct, restart the U2000 service. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, contact Huawei engineers for a solution.

----End

Copyright © Huawei Technologies Co., Ltd.

Related Information

None

A.91 Failure to Connect to All Integration Servers

Description

The U2000 server cannot establish communication with both integration servers.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5112	Major	Communication

Parameters

None

Impact on the System

The U2000 server fails to connect to the active and standby integration servers.

- The U2000 server can only use the locally cached integration data. If the data is outdated, the U2000 server will fail to communicate with the operations support system (OSS) or other U2000 servers.
- Single sign-on (SSO) users are also affected. Only the users that have successfully logged in to the U2000 server before can log in.

After the alarm is generated, the U2000 continues to reconnect to the integration server. If the connection is established, the alarm is automatically cleared and its **Clearance Status** is changed to **Cleared**.

Possible Causes

- The integration server does not respond; the U2000 server fails to connect to the integration server; or the communication port is disabled on a firewall.
- An incorrect integration server IP address or port number is configured on the U2000 server.
- The integration service on the integration server does not run.
- An incorrect U2000 server IP address is registered on the integration server. Therefore, the connection request is rejected.
- An incorrect SSL certificate is configured for the U2000 server or integration server.

Procedure

Step 1 Check whether the integration server responds, whether the network between the U2000 and integration servers is normal, and whether the communication port is enabled on the firewall.

Copyright © Huawei Technologies Co., Ltd.

On SUSE Linux, run the following command to check the network between the U2000 and integration servers:

ping -s *integration server IP address*

1. If the integration server and network are normal, go to **Step 2**.
2. If they are abnormal, restore them. Wait 2 minutes after the network becomes normal. If the alarm is automatically cleared, no further operation needs to be taken. If the alarm is not cleared, go to **Step 2**.
3. If the network fault persists, contact Huawei engineers for a solution.

Step 2 Check whether the is_ip value of the U2000 server are consistent with the IP address of the integration server.

The integration information of the U2000 server is recorded in **server\etc\oss_cfg\frame\isinfo.cfg**.

1. If they are consistent, go to **Step 3**.
1. If they are inconsistent, perform the following operations:
   a. Run the integration information setting script as the **ossuser** user. On SUSE Linux, the script is **server/tools/integrate/setis.sh**.
   b. Restart the U2000 service.
      1) In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **stopnms.bat** file to stop the U2000 processes.
      2) In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **startnms.bat** file to start the U2000 processes.
   c. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, go to **Step 3**.

Step 3 Log in to the integration server and check whether the integration service runs properly.

NOTE

Open a Web browser and enter **https://*primary IS server's IP address*/ui/login** in the address box. If the page is displayed and shows registered member systems, the integration service runs properly.

1. If the integration service does not run, start it and wait 2 minutes. If the alarm is automatically cleared, no further operation needs to be taken. If the alarm is not cleared, go to **Step 4**.
2. If the integration service runs but the alarm is not cleared, go to **Step 4**.
3. If the integration service does not run, contact Huawei engineers for a solution.

Step 4 Check whether the U2000 server IP address registered on the integration server is correct.

NOTE

Log in to the integration server. Open a Web browser and enter **https://*primary IS server's IP address*/ui/login** in the address box. Check whether the U2000 server IP address is correct.

1. If the U2000 server IP address is correct, go to **Step 5**.
2. If the U2000 server IP address is incorrect, correct it. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, go to **Step 5**.

Step 5 Check whether the SSL certificates of the U2000 and integration servers are incorrectly configured.

Copyright © Huawei Technologies Co., Ltd.

1. If they are incorrect, correct them.
2. If they are correct, restart the U2000 service. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, contact Huawei engineers for a solution.

----End

Related Information

None

A.92 Abnormal Integration Information

Description

Integration information on the U2000 server is inconsistent with that registered on the integration server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5113	Critical	Communication

Impact on the System

The U2000 server fails to communicate with the operations support system (OSS) or other U2000 servers.

Possible Causes

- An incorrect U2000 server IP address is registered on the integration server.
- The integration information setting script is not executed on the U2000 server after the U2000 server is added to the integration server.

Procedure

Step 1 Check whether the U2000 server IP address is correct.

NOTE

Log in to the integration server. Open a Web browser and enter **https://*primary IS server's IP address*/ui/login** in the address box. On the page that is displayed, check whether the U2000 server IP address is correct.

1. If the U2000 server IP address is correct, go to **Step 2**.
2. If the U2000 server IP address is incorrect, correct it. If the alarm is automatically cleared, no further operation needs to be taken. If the alarm is not cleared, go to **Step 2**.

Step 2 Log in to the U2000 server and run the integration information setting script **server/tools/integrate/setis.sh** as the **ossuser** user.

Copyright © Huawei Technologies Co., Ltd.

1. Enter information as prompted, including the U2000 server name, integration server IP address, and the port of the integration server.
2. Restart the U2000 service.
   a. In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **stopnms.bat** file to stop the U2000 processes.
   b. In the U2000 installation directory, for example, **D:\oss\server\platform\bin**, run the **startnms.bat** file to start the U2000 processes.
3. If the alarm is automatically cleared in 2 minutes, no further operation needs to be taken. If the alarm is not cleared, contact Huawei engineers for a solution.

----End

A.93 OCH_TRAIL_POWER_ABNORMAL

Description

The U2000 implements online scheduled monitoring on WDM optical power. When the U2000 detects the optical power exception of OCh trails, this alarm is generated. The exception may occur on transmit optical power, optical power flatness, and receive optical power on OTUs.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5200	Minor	Service

Impact on the System

Service performance and communication are affected.

Possible Causes

The optical power monitoring function detects an optical power exception on an OCh trail that needs optimizing.

Procedure

Step 1 Choose **Configuration** > **WDM Optical Management** > **Online Optimization Management**from the main menu (traditional style).

Step 2 Click **Refresh** to update information in **Trail to Be Optimized**.

Step 3 Select trails to be optimized and click **Optimize**.

Step 4 In the **Automatic Optical Power Commissioning (Link Optimization)** window, click **Start** to start link optimization commissioning.

Step 5 Two confirmation dialog boxes are displayed. Click **OK** to start link optimization commissioning.

Copyright © Huawei Technologies Co., Ltd.

Step 6 After the commissioning is complete, click **OK**.

Step 7 Collect the information about alarm handling, and contact Huawei technical support engineers.

----End

A.94 Communication Failure of Alarm Reporting Channel

Description

The alarm reporting channel encounters a communication failure, for example, the connection to the NM or an EM or between them is broken or unstable.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5201	Critical	Communication

Impact on the System

Alarms on the EM cannot be synchronized to the NM.

Possible Causes

- The connection between the NM and EM is broken or unstable.
- EM services have been stopped.
- Certificates have expired.

Procedure

Step 1 Check the connection between the NM and EM by pinging each other.

Step 2 Log in to the System Monitor client and verify that all EM services are running, especially the UniteUitlDM and FaultService services.

Step 3 Check the certificates of the NM and EM. If the certificates have expired, update them immediately.

- The certificate of the EM is stored in **server\etc\ssl\server**.
- The certificate of the NM is stored in **server\etc\ssl\server**.

----End

A.95 Buffer Overflow of Alarm Reporting Channel

Description

The alarm reporting channel encounters a buffer overflow.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5205	Critical	Communication

Impact on the System

After alarms received from a lower-layer EM cause a buffer overflow on the NM, some alarms cannot be synchronized to the NM.

Possible Causes

The lower-layer EM reports alarms in large amounts and at a fast speed, exceeding the buffer limit of the NM.

Procedure

Step 1 Check whether the EM reports alarms in large amounts or at a fast speed and take measures accordingly.

1. If a few devices are faulty and constantly report alarms, replace the devices.
2. If many devices report alarms in large amounts, check the condition of the U2000, analyze the root causes of the alarms, and take measures accordingly.

Step 2 Synchronize alarms from the EM.

1. Choose **Configuration** > **EM Management** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Configuration** > **EM Management** from the main menu (application style).
2. In the **EM Management** window, right-click the EM and choose **Synchronize Current Alarms** from the shortcut menu.

----End

A.96 A Member System in the Maintenance State

Description

In the distributed U2000 system, a member system has been set to the maintenance state.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5212	Major	Environment

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

The upload function is unavailable, and data cannot be synchronized between the NM and EMs. In addition, the NM cannot receive some configuration messages.

Possible Causes

A system maintenance engineer has changed the system status to maintenance in the **Distributed Systems Integration Tool**.

Procedure

Step 1 After system maintenance is finished, change the system status back to normal in the **Distributed Systems Integration Tool**. Then the alarm will be cleared automatically.

Step 2 Upload configuration data from EMs.

1. Choose **Configuration** > **EM Management** from the main menu (traditional style); alternatively, double-click **Bearer Network Service Configuration** in **Application Center** and choose **Configuration** > **EM Management** from the main menu (application style).
2. In the **EM Management** window, right-click an EM and choose **Upload** from the shortcut menu.

NOTE

If the alarm is reported by an EM, upload data only from that EM. If the alarm is reported by the NM, upload data from all the EMs managed by the NM.

----End

A.97 PSEUDOWIRE_OUTAGE

Description

After a critical or major device alarm is located to the specific path, the U2000 checks whether the associated service is interrupted. If yes, a service interruption alarm is reported.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5301	Major	Service

Impact on the System

The PW related to the VPLS service is interrupted, and the fault must be rectified immediately.

Possible Causes

The PW related to the VPLS service was interrupted. For example, the tunnel carrying the PW was torn down, and the tunnel generated an MPLS_TUNNEL_LOCV, MPLS_TUNNEL_FDI, or ETH_LOS alarm.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 In the **Browse Current Alarm** window, select the alarm, right-click, and choose **Alarm-affecting Object** > **VPLS** from the shortcut menu.

Step 2 Based on the PW ID in alarm details, locate the interrupted PW and view the tunnel carrying the PW.

Step 3 Handle the tunnel alarm, such as MPLS_TUNNEL_LOCV, MPLS_TUNNEL_FDI, or ETH_LOS, based on the alarm information about the tunnel.

----End

Related Information

None

A.98 Trap numbers of NEs exceeded the threshold of NMS

Description

The number of traps exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5403	Major	Equipment

Impact on the System

This alarm occurs when a process receives an excessively large number of traps or alarms. Subsequent traps or alarms may be discarded. As a result, the services that depend on the traps or alarms cannot be refreshed in real time. For example, if a board status change trap is discarded, the board status cannot be refreshed in real time.

Possible Causes

The number of traps sent from an NE exceeds the threshold.

Procedure

Step 1 Search the **Browse Event Logs** window for the "Traps of NE sended to NMS too much" event. If the event exists, check the running status of the NE based on the trap information in the event.

----End

Related Information

None

Copyright © Huawei Technologies Co., Ltd.

A.99 NE Management by Multiple U2000s

Description

An NE is being managed by multiple U2000s.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5406	Major	Equipment

Impact on the System

This alarm indicates that the same NE might be managed by multiple U2000s. If this alarm is generated, the NE data might be inconsistent with the U2000 data. If you operate the NE in this situation, service interruptions may occur.

Possible Causes

Multiple target hosts are configured or multiple U2000s are connected to the same NE, which may result in a configuration conflict.

Procedure

Step 1 Allow only one U2000 to manage the NE.

Step 2 Check whether multiple target hosts are configured. If yes, delete unwanted target hosts after determining that the hosts are not used by other U2000s.

----End

A.100 Data Inconsistency

Description

The data on the NE reporting this alarm is different from the NE data on the U2000.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5408	Major	Process

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

Data on the NE that reports alarms may be inconsistent with that on the U2000. Therefore, operations on the U2000 may be invalid.

NOTE

When the U2000 detects data inconsistency between NEs and the U2000 (due to NE command configuration changes), it reports the alarm.

The alarm is cleared when the data synchronization is performed. Data synchronization operations include uploading and synchronizing the NE data.

Possible Causes

NE data has ever been changed in CLI mode.

NOTE

If the NE data becomes inconsistent with the U2000 data because multiple U2000s manage an NE and a U2000 delivers changed configurations to the NE, the alarm is not reported.

Procedure

Step 1 Use any of the following methods to achieve data consistency between the NE and U2000s.

- Method 1: Upload NE data to the U2000. For details, see Uploading NE Configuration Data.
- Method 2: Synchronize NE data to the U2000. For details, see Synchronizing NE Configuration Data.

Step 2 Prevent the NE from being managed by multiple U2000s or operated in CLI mode.

Step 3 If the fault persists, contact Huawei technical support engineers.

----End

A.101 tmp Occupies Much Space

Description

The **/tmp** directory occupies much space.

Attribute

Alarm ID	Alarm Severity	Alarm Type
5440	Major	Environmental alarm

Impact on the System

Physical memory becomes insufficient, and processes fail to run properly.

Possible Causes

The **/tmp** directory stores some unnecessary core files or large log files.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Remove unnecessary core files or large log files.

----End

A.102 Veritas Resources Are Faulty

Description

The alarm is generated when Veritas resources on the server do not function properly.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6101	Critical	Security

Impact on the System

The U2000 on the site where the involved resource group is located does not function properly; as a result, a failover occurs on the high availability system.

Possible Causes

Generally, a registered resource is not functioning properly because the resource cannot be started within the specific period or the resource becomes offline abnormally.

Veritas resources include **NMSServer**, **NMSAgent**, **DataFilesystem**, **mountRes**, **APPBOND**, **appNIC**, **RVGPrimary**, **DatabaseServer**, **BackupServer**, **FloatIP**, **csgnic**, **datarvg**, **appNIC**, and **ntfr**.

Procedure

Step 1 Perform the following operations to rectify resource faults:

- **APPBOND** and **appNIC** resource failure

  The **APPBOND** and **appNIC** are NIC resources. The **appNIC** is the NIC resource of the Solaris high availability system, and the **APPBOND** is the NIC resource of the SUSE Linux high availability system. NIC resource faults are caused because the network cable is disconnected or the communication between the NIC and a gateway fails. The **APPBOND**

Copyright © Huawei Technologies Co., Ltd.

resource fault may occur because of a failure on the switch connected to the NIC. Check whether the network is normal and whether the switch connected to the NIC functions properly.

- **RVGPrimary** resource failure:

  The possible cause of a **RVGPrimary** resource failure is that the data is not synchronized between the primary and secondary sites.

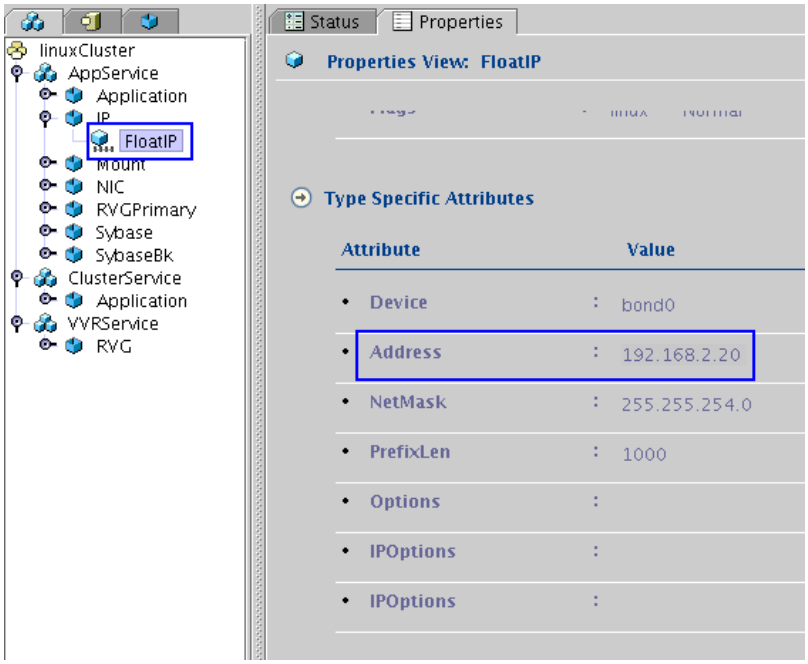
  1. Run the following command to check the replication status:
     ```
     # vradmin -g datadg repstatus datarvg
     ```
     Information similar to the following is displayed:
     ```
     Replicated Data Set: datarvg
     Primary:
       Host name:                    10.71.210.78
       RVG name:                     datarvg
       DG name:                      datadg
       RVG state:                    enabled for I/O
       Data volumes:                 4
       VSets:                        0
       SRL name:                     lv_srl
       SRL size:                     3.00 G
       Total secondaries:            1

     Secondary:
       Host name:                    10.71.210.76
       RVG name:                     datarvg
       DG name:                      datadg
       Data status:                  consistent, up-to-date
       Replication status:           replicating (connected)
       Current mode:                 asynchronous
       Logging to:                   SRL
       Timestamp Information:        behind by 0h 0m 0s
     ```
  2. Perform the following operations to rectify faults based on scenarios:
     - If **Replication status** is displayed as **resync in progress (autosync)**, **Data status** is displayed as **inconsistent**, and the value next to **Logging to** is decreasing, data between the primary and secondary sites is being replicated.
     - If **Replication status** is displayed as **replicating (connected)** and **Data status** is displayed as **consistent, up-to-date**, the data replication of the Veritas hot backup high availability system is complete.
     - If **Replication status** is displayed as **logging to DCM (needs dcm resynchronization)**, run the **vradmin -g datadg resync datarvg** command on the primary site as the **root** user and then perform manual synchronization.

- **FloatIP** resource failure:

  The **FloatIP** resource fault occurs only in the local SUSE Linux high availability system and generally occurs because of an IP address conflict. You can run the **ping** command to confirm the fault.

  1. Log in to the VCS and navigate to the following location to obtain the IP address. As shown in the following figure, the IP address is **192.168.2.20**.

Copyright © Huawei Technologies Co., Ltd.

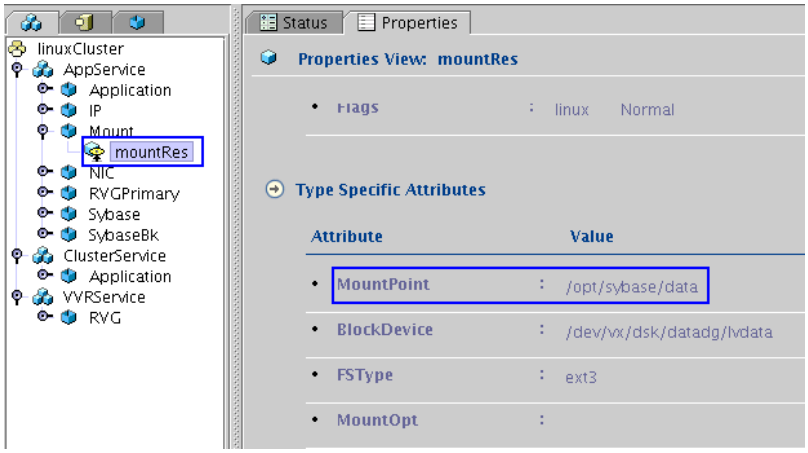


2. Check whether an IP address conflict occurs.
3. Rectify the fault after the IP address conflict problem is addressed.

- **DataFilesystem** and **mountRes** resource failure:

  The **DataFilesystem** and **mountRes** resources are mounting resources, with the **DataFilesystem** resource in the Solaris high availability system and the **mountRes** resource in the SUSE Linux high availability system. The possible cause of a mounting resource failure is that the mounting directory does not exist.

  1. Confirm the mounting directory. The default mounting directory is **/opt/sybase/data**. If the mounting directory is customized, navigate to the following path to obtain the mounting point:



  2. Generally, a mounting resource fault occurs because the mounting directory does not exist. Run the following command to check whether the mounting directory exists:
     ```
     # cd /opt/sybase/data
     ```
     If no command output is displayed, the mounting directory exists. If the following information is displayed, the mounting directory does not exist.
     ```
     cd: /opt/sybase/data: No such file or directory
     ```


Copyright © Huawei Technologies Co., Ltd.

3. If the mounting directory does not exist, run the following commands to create a mounting directory and change the owner:
   ```
   # mkdir -p /opt/sybase/data
   # chown -R dbuser:dbgroup /opt/sybase/data
   ```

- **NMSServer** resource failure:

  The common cause of an **NMSServer** resource failure is a startup failure of a key U2000 process. You can view the **monitor** file in the **/opt/OSSICMR/OSSApp/log** directory to confirm the fault. Locate the specific fault process based on the time the fault occurs. For example, the following log shows that the nemgr_otn_9973 process does not function properly.

  After the fault is located, manually start the fault process on the System Monitor. If the process still fails to be started, contact Huawei technical support engineers.

  ```
  12-05-23 15:31:27 || haMonitor:Success to get the process running status at
  2012-05-23_15:31:27.
  12-05-23 15:31:27 || haMonitor:The process nemgr_otn_9973 is restarted more than
  3 times, and the current status is not running!
  12-05-23 15:31:27 || haMonitor:The nms process nemgr_otn_9973 is fault!
  ```

Step 2 After the fault is rectified, log in to the VCS client. Then right-click the name of the resource that is in the **Faulted** state and choose **Clear Fault** from the shortcut menu to rectify the fault.

Step 3 Enable the **Online** resource.

- If active/standby switchover has not been triggered, right-click the resource where the fault has been rectified on the primary site and choose **Online** from the shortcut menu.
- If active/standby switchover has been triggered, manually performing switchover is recommended to ensure that the servers on the primary and secondary sites are in the normal state.

Step 4 If the fault persists, contact Huawei technical support engineers.

----End

A.103 Veritas replication buffer exceeds the threshold

Description

The alarm is generated when the data to be synchronized in the Veritas replication buffer exceeds the threshold.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6103	Major	Security
6117	Critical	Security

Impact on the System

If such an alarm is generated and the primary site does not function properly, the high availability system fails to perform switchover. This is because the data between the primary and secondary sites is inconsistent and the data to be synchronized fails to be replicated to the secondary site within the default timeout period (5 minutes).

Possible Causes

The amount of data in the Veritas replication buffer depends on the accumulated I/O data, available bandwidth for data replication, and replication network quality. The possible causes of this problem are as follows:

- The NMS applications read and write a large amount of data from and into the database in a short term, which results in long-time I/O data accumulation.
- The DCN is unstable. For example, the value of the packet loss ratio, jitter, or delay exceeds the threshold.
- The available bandwidth for data replication is insufficient.

If the amount of data in SRL is larger than or equal to 210 MB and smaller than 450 MB, a major alarm is generated. If the amount of data in SRL is larger than or equal to 450 MB, a critical alarm is generated.

Procedure

Step 1 Contact Huawei technical support engineers to troubleshoot the high availability system based on the analysis of the I/O data, replication buffer, network bandwidth usage, and network quality.

If the amount of data in SRL is smaller than 210 MB, clear the critical alarm. If the amount of data in SRL is smaller than 90 MB, clear the major alarms.

----End

A.104 Manual Restoration Is Required After Primary-Primary Veritas Status

Description

The alarm is generated when a Veritas high availability system enters the dual-host status and is waiting for manual data restoration.

Copyright © Huawei Technologies Co., Ltd.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6105	Critical	Security

Impact on the System

- By default, the U2000 on the primary site functions and the U2000 on the secondary site automatically stops. If data replication between the primary and secondary sites is interrupted and the primary site does not function properly, the secondary site is not capable of taking over U2000 services. Force the server where the U2000 resides functions properly and the recent data exists to function as the primary server. Forcing the server where is recently logged in to function as the primary server and reestablishing replication relationship on the server is recommended.
- If the U2000 on the primary site fails, this alarm is generated after the U2000 recovers. In this case, you must force the U2000 on the secondary site to function as the primary server.

Possible Causes

- The DCN between the primary and secondary sites is unstable or interrupted; as a result, the heartbeat connection and data replication time out for over 10 minutes. In such a situation, the U2000 on the primary site automatically starts. After the DCN restores, the system automatically enters the dual-host state and is waiting for manual data restoration.
- The U2000 on the primary site does not function for over 10 minutes and then recovers.

Procedure

Step 1 Force the server where the U2000 resides functions properly and the recent data exists to function as the primary server. Forcing the server where is recently logged in to function as the primary server is recommended. If this alarm is generated because the U2000 on the primary site does not function and then recovers, force the server on the secondary site to function as the primary server.

Step 2 On a computer where the MSuite client is installed, double-click the **U2000 NMS Maintenance Suite** shortcut icon on the desktop and then wait about one minute. The **Login** dialog box is displayed.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- In Solaris or SUSE Linux OS, log in to the Java desktop system as user **ossuser**. 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 **ossuser**. If you have logged in as the **root** user, relog in to the OS as user **ossuser**, you cannot run the **su - ossuser** command to switch to the **ossuser** user to run the following command.
  ```
  $ cd /opt/oss/client/engineering
  $ ./startclient.sh
  ```
- If a dialog box showing **The client and server versions are different. Upgrade the client using the CAU.** is displayed, the method of upgrading the U2000 client by using the CAU is as follow:
  1. Install the U2000 client software in network mode: Enter **https://*server_IP_address*/cau/** (more secure, recommended) or **http://*server_IP_address*/cau/** in the address box of the Internet Explorer, and press **Enter** to access the Web installation page. For details, see *U2000 Client Software Installation Guide* in the *U2000 Client Software Installation Guide*.
  2. If you upgrade the U2000 client software using the CAU, the MSuite client is also upgraded.

Step 3 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.

  NOTE

  The **Login** dialog box of the MSuite client has the function to keep the login list. Selecting an IP address from the **IP Address** drop-down list is recommended. If the desired IP address is not displayed in the drop-down list, enter an IP address.
- Port: 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 initial password of the **admin** user is **Changeme_123** (It is Admin_123 for a U2000 that comes preinstalled). The password must be changed during the first login to ensure system security. Keep the password confidential and change it regularly.

Step 4 Click **Login**.

NOTE

- When you log in to the MSuite client, a progress bar is displayed showing the progress of **Refresh Deployment Information**. 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.

Step 5 Choose **Deploy** > **Force Active of Local Site**.

Step 6 Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

A.105 Veritas Heartbeat Is Interrupted

Description

The alarm is generated when Veritas heartbeat is interrupted.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6107	Critical	Security

Impact on the System

If the heartbeat connection times out, the secondary site may take over U2000 services and the high availability system enters the dual-host state. By default, the timeout period is about 10 minutes.

Possible Causes

- Heartbeat NICs on the primary and secondary sites do not function properly.
- The DCN between the primary and secondary sites is interrupted.
- The heartbeat IP addresses of the primary and secondary sites are not reachable.

Procedure

Step 1 On the primary and secondary sites, run the following command to check whether the heartbeat IP addresses exist:

ifconfig -a

If the command output does not contain heartbeat IP addresses, use the commissioning tool to reset heartbeat IP addresses. For details, see **Commissioning System Parameters** in the commissioning guide for the specific installation solution.

Step 2 On the primary and secondary sites, run the following command to check whether the NICs where the heartbeat IP addresses are located are in marked **UP** and **RUNNING**, but not **DUPLICATED**:

ifconfig -a

Copyright © Huawei Technologies Co., Ltd.

- If the command output does not contain **UP**, run the **ifconfig** *NIC name* **up** command to make the NIC status **UP**.
- If the command output does not contain **RUNNING**, verify that NICs are properly connected.
- If the command output contains **DUPLICATED**, IP addresses may be occupied and you must reset IP addresses.

Step 3 On the primary and secondary sites, run the following command to check whether the heartbeat IP addresses of the primary and secondary sites are reachable:

ping *peer heartbeat IP address*

If the primary and secondary sites can ping through each other, the heartbeat IP addresses of the primary and secondary sites are reachable.

----End

A.106 The Veritas data replication is interrupted

Description

The alarm is generated when data replication between the primary and secondary sites is interrupted.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6109	Critical	Security

Impact on the System

Data on the primary site cannot be synchronized to the secondary site in time; as a result, the replication buffer overflows. In this case, the secondary site is not capable of taking over U2000 services.

Possible Causes

- Replication NICs on the primary and secondary sites do not function properly.
- The DCN between the primary and secondary sites is interrupted.

Copyright © Huawei Technologies Co., Ltd.

- The replication IP addresses of the primary and secondary sites are not reachable.
- The amount of I/O data on the primary site soars; as a result, the replication buffer overflows.

Procedure

Step 1 On the primary and secondary sites, run the following command to check whether the replication IP addresses exist:

ifconfig -a

If the command output does not contain replication IP addresses, use the commissioning tool to reset replication IP addresses. For details, see **Commissioning System Parameters** in the commissioning guide for the specific installation solution.

Step 2 On the primary and secondary sites, run the following command to check whether the NICs where the replication IP addresses are located are in marked **UP** and **RUNNING**, but not **DUPLICATED**:

ifconfig -a

- If the command output does not contain **UP**, run the **ifconfig** *NIC name* **up** command to make the NIC status **UP**.
- If the command output does not contain **RUNNING**, verify that NICs are properly connected.
- If the command output contains **DUPLICATED**, IP addresses may be occupied and you must reset IP addresses.

Step 3 On the primary and secondary sites, run the following command to check whether the replication IP addresses of the primary and secondary sites are reachable:

ping *remote replication IP address*

If the primary and secondary sites can ping through each other, the replication IP addresses of the primary and secondary sites are reachable.

Step 4 On the primary site, run the following command to check whether the replication buffer overflows:

vradmin -g datadg repstatus datarvg | grep "Logging to"

If the command output contains DCM information, the replication buffer overflows. To restore data replication, run the following command:

vradmin -g datadg resync datarvg

----End

A.107 Veritas Resource Group Is Frozen

Description

The alarm is generated when a Veritas resource group is in the Freeze state.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

Copyright © Huawei Technologies Co., Ltd.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6111	Critical	Security

Impact on the System

A failover does not occur on the resource group when a resource group is in the Freeze state and some resources in the resource group do not function properly.

Possible Causes

- The administrator has frozen the resource group but does not unfreeze it in time during the maintenance of the high availability system.
- When the MSuite is used, the high availability system automatically freezes and unfreezes resource groups. In this case, the alarm generated is automatically cleared after the deployment is complete.

Procedure

Step 1 Log in to the site where the frozen resource group is located as the **root** user.

Step 2 Run the following command to view the freezing mode of the resource group:

hagrp -display *resource group name* **| grep Frozen**

In the command output, if the value of the Frozen field is 1, the resource group is permanently frozen. If the value of the TFrozen field is 1, the resource group is permanently frozen. If the value is 0, the resource group is not frozen.

Step 3 Run the following commands to clear the Freeze state of the resource group:

- If the resource group is temporarily frozen, run the following command:

  # **hagrp -unfreeze** *resource group name*

- If the resource group is permanently frozen, run the following command:

  # **hagrp -unfreeze** *resource group name* **-persistent**

----End

Copyright © Huawei Technologies Co., Ltd.

A.108 Veritas License Is a Temporary One

Description

The alarm is generated when the current Veritas license is a temporary license or expires.

- If the validity period for Veritas 5.0 is a negative number, the Veritas license is a temporary one and has expired. If the validity period for Veritas 5.0 is a positive number, the Veritas license is a temporary one and has not yet expired.
- The license of Veritas 5.1 is a temporary one.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6113	Critical	Security

Impact on the System

- If the license of Veritas with the version of 5.0 or earlier expires, the operating system becomes unavailable after it is restarted and the official technical support from Symantec is unavailable.
- If the license of Veritas with the version of 5.1 or later is a temporary one, official technical support from Symantec is unavailable.
- This alarm cannot be masked. Handle it as soon as possible.

Possible Causes

The current Veritas license is a temporary license or expires.

Procedure

Step 1 Update the current Veritas license. For details, see chapter *Updating a Veritas License* in the *U2000 HA System Software Installation and Commissioning Guide (Solaris)*.

----End

Copyright © Huawei Technologies Co., Ltd.

A.109 Veritas Process Is Faulty

Description

The alarm is generated when a Veritas process is faulty.

The following situations cause failures in automatically clearing alarms. Instead, they need to be cleared manually.

- The name of the host that generates this alarm is changed.
- The host that generates the alarm runs on Solaris or SUSE Linux. The operating system is upgraded or operating system patches are installed after the alarm is generated.
- The local end is forcibly configured as the primary site to make the high availability system work in the normal state when the high availability system enters the Primary-primary status and is waiting for data restoration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
6115	Critical	Security

Impact on the System

The high availability system fails to work properly. The monitoring and data replication functions may be abnormal. Some alarms, such as the Veritas heartbeat interruption and data replication interruption alarms fail to be generated. You must locate the fault and manually rectify it.

Process	System Impact
/opt/VRTSvcs/bin/had	The Veritas cluster management function is unavailable.
/opt/VRTSvcs/bin/hashadow	The Veritas fails to monitor the **had** process. If the **had** process is faulty, the Veritas cannot restart it.
/usr/sbin/vxconfigd	The system fails to configure and maintain disks and disk groups.
/usr/sbin/vradmind	The volume management commands of the Veritas cannot be delivered.

Possible Causes

The Veritas core processes are not started or are abnormally stopped. The Veritas core processes are **had**, **hashadown**, **vxconfigd**, and **vradmind**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Handle the process abnormality by referring to the following table.

Process	Handling Method
/opt/VRTSvcs/bin/had	The **hashadow** process automatically starts the **had** process. If the **hashadow** process fails to automatically start the **had** process, contact Huawei technical support engineers.
/opt/VRTSvcs/bin/hashadow	The **had** process automatically starts the **hashadow** process. If the **had** process fails to automatically start the **hashadow** process, contact Huawei technical support engineers.
/usr/sbin/vxconfigd	Run the following command as the **root** user: # **/usr/sbin/vxconfigd -k** If the **vxconfigd** process fails to be started, contact Huawei technical support engineers.
/usr/sbin/vradmind	Run the following command as the **root** user: # **/usr/sbin/vradmind** If the **vradmind** process fails to be started, contact Huawei technical support engineers.

----End

A.110 Automatic Backup Operation Failed

Description

An alarm is generated if data fails to be automatically backed up using the NE software management.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7938	Minor	Equipment

Parameters

Parameter Name	Description
Parameter 1	NE name
Parameter 2	Operation

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

Automatic NE data backup fails so that NE data files fail to be backed up on the NMS server.

Possible Causes

- NEs are disconnected to the NMS.
- The FTP service is not started.
- NE communication parameters are not configured.

Procedure

- Check whether the FTP server is running properly.
- Check whether the disk space of the NMS server is sufficient.
- Check whether NE communication parameters are configured.

----End

Related Information

There is no related information.

A.111 Automatic Save Operation Failed

Description

An alarm is generated if NE data fails to be automatically saved using the NE software management.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7939	Minor	Equipment

Parameters

Parameter Name	Description
Parameter 1	NE name
Parameter 2	Operation

Copyright © Huawei Technologies Co., Ltd.

Impact on the System

Automatic NE data saving fails so that NE configuration information fails to be saved to the NE storage medium.

Possible Causes

- NEs are disconnected to the NMS.
- The FTP service is not started.
- NE communication parameters are not configured.

Procedure

- Check whether the FTP server is running properly.
- Check whether the disk space of the NMS server is sufficient.
- Check whether NE communication parameters are configured.

----End

Related Information

There is no related information.

A.112 Automatic Recover Operation Failed

Description

When a faulty MDU device is replaced, no software package whose version is consistent with the version of the control board of the replacement device is found in the MDU automatic upgrade policy, resulting in an MDU replacement failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7940	Minor	Equipment

Parameters

Parameter Name	Description
Parameter 1	NE name
Parameter 2	Operation

Impact on the System

This alarm indicates that when upgrading the replacement device, the NE Software Management module does not find software matching the control board of the replacement device in the MDU

Copyright © Huawei Technologies Co., Ltd.

upgrade policy, resulting in a device replacement failure. If the MDU automatic upgrade policy contains a software package whose version is consistent with the version of the control board of the replacement device, this alarm will not be generated.

This alarm cannot be self-handled and needs to be acknowledged manually.

Possible Causes

The MDU upgrade policy does not contain any software package whose version is consistent with the version of the control board of the replacement device.

Procedure

- Choose **Administration** > **NE Software Management** > **NE Software Library Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Software Library Management** from the main menu (application style)., and check whether a software package whose version is consistent with the version of the control board of the replacement device is imported.
- Choose **Configuration** > **FTTx Service Pre-Deployment** > **Configure MDU Upgrade Policy** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **FTTx Service Pre-Deployment** > **Configure MDU Upgrade Policy** from the main menu (application style)., view the MDU target version and software package, and determine whether the version of the software package is consistent with that of the control board of the replacement device based on the software package name.

----End

Related Information

There is no related information.

A.113 ALM-52003 Host cpu usage

Description

This alarm is generated when the CPU usage of the host is greater than or equal to the alarm generation threshold. It is cleared when the CPU usage is lower than the alarm clearance threshold.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52003	Major	Software

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.
Host Name	Name of the host on which an alarm is generated.

Impact on the System

- Service responds slowly and operations time out.
- The system processes services slowly. As a result, messages may be accumulated, and the system may crash.

System Actions

None

Possible Causes

- The host is busy temporarily.
- The threshold of the alarm is specified to a smaller value.
- The hardware performance of the host is low. Therefore, the service cannot run properly.

Procedure

Step 1 Check whether the threshold for generating a high CPU usage alarm of the host is specified as a smaller value.

1. Log in to the vCenter Server through the VMware client.
2. Check whether the alarm reporting threshold is specified properly.
   a. Click **Home** in the main toolbar.
   b. In **Inventory**, click the icon for the **Hosts and Clusters**.
   c. Select the **Alarms** tab, click the **Definitions** subtab and double-click this alarm in the list.
   d. In the displayed **Alarm Settings** dialog box, select the **Triggers** tab.

   Check whether the following conditions are met:

   - You have reset the threshold (by default, the threshold for generating a high CPU usage alarm is 85% in yellow and 90% in red) and the current value is lower than the default value. An alarm is generated but the system runs properly with fast response.
   - The threshold is set to a smaller value.

   Solution:

   - If the preceding conditions are met, set the yellow threshold to 85% and the red threshold to 90% in the vCenter alarming setting.

Copyright © Huawei Technologies Co., Ltd.

Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, perform **Step 2**.

- If the preceding conditions are not met, perform **Step 2**.

Step 2 Check whether the server system is temporarily busy.

1. Log in to the U2000 client.
2. Check the time when the alarm is first generated.

   Check whether the one of following conditions is met:

   - 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 10 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. The operation ends.
   - If not, go to **Step 3**.

Step 3 Collect the information about alarm handling, and contact Huawei technical engineers for support.

----End

Related Information

None

A.114 ALM-52004 Host memory usage

Description

This alarm is generated when the memory usage of the host is greater than or equal to the alarm generation threshold. It is cleared when the memory usage is lower than the alarm clearance threshold.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52004	Major	Software

Copyright © Huawei Technologies Co., Ltd.

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.
Virtual Machine Name	Name of the virtual machine on which an alarm is generated.

Impact on the System

- The available memory space of the system is insufficient. The service responds slowly and operations time out.
- 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 threshold of the alarm is specified to a smaller value.
- The hardware performance of the host is low. Therefore, the service cannot run properly.

Procedure

Step 1 Check whether the threshold for generating a high memory usage alarm of the host is specified as a smaller value.

1. Log in to the vCenter Server through the VMware client.
2. Check whether the alarm reporting threshold is specified properly.
   a. Click **Home** in the main toolbar.
   b. In **Inventory**, click the icon for the **Hosts and Clusters**.
   c. Select the **Alarms** tab, click the **Definitions** subtab and double-click this alarm in the list.
   d. In the displayed **Alarm Settings** dialog box, select the **Triggers** tab.

   Check whether the following conditions are met:

   - You have reset the threshold (by default, the threshold for generating a high memory usage of the host alarm is 75% in yellow and 90% in red) and the current value is lower than the default value. An alarm is generated but the system runs properly with fast response.
   - The threshold is set to a smaller value.

   Solution:

   - If the preceding conditions are met, set the yellow threshold to 75% and the red threshold to 90% in the vCenter alarming setting.

Copyright © Huawei Technologies Co., Ltd.

Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, perform **Step 2**.

- If the preceding conditions are not met, perform **Step 2**.

Step 2 Collect the information about alarm handling, and contact Huawei technical engineers for support.

----End

Related Information

None

A.115 ALM-52005 Virtual machine cpu usage

Description

This alarm is generated when the CPU usage of the virtual machine is greater than or equal to the alarm generation threshold. It is cleared when the CPU usage is lower than the alarm clearance threshold.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52005	Major	Software

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.
Virtual Machine Name	Name of the virtual machine on which an alarm is generated.

Impact on the System

- Service responds slowly and operations time out.
- The system processes services slowly. As a result, messages may be accumulated, and the system may crash.

System Actions

None

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The host is busy temporarily.
- The threshold of the alarm is specified to a smaller value.
- The hardware performance of the virtual machine is low. Therefore, the service cannot run properly.

Procedure

Step 1 Check whether the threshold for generating a high CPU usage alarm of the virtual machine is specified as a smaller value.

1. Log in to the vCenter Server through the VMware client.
2. Check whether the alarm reporting threshold is specified properly.
   a. Click **Home** in the main toolbar.
   b. In **Inventory**, click the icon for the **Hosts and Clusters**.
   c. Select the **Alarms** tab, click the **Definitions** subtab and double-click this alarm in the list.
   d. In the displayed **Alarm Settings** dialog box, select the **Triggers** tab.

   Check whether the following conditions are met:

   - You have reset the threshold (by default, the threshold for generating a high CPU usage alarm is 75% in yellow and 90% in red) and the current value is lower than the default value. An alarm is generated but the system runs properly with fast response.
   - The threshold is set to a smaller value.

   Solution:

   - If the preceding conditions are met, set the yellow threshold to 75% and the red threshold to 90% in the vCenter alarming setting.

     Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, go to **Step 3**.
   - If the preceding conditions are not met, perform **Step 3**.

Step 2 Check whether the virtual machine system is temporarily busy.

1. Log in to the U2000 client.
2. Check the time when the alarm is first generated.

   Check whether the one of following conditions is met:

   - 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 10 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:

Copyright © Huawei Technologies Co., Ltd.

- If so, it indicates that the system is busy temporarily. You do not need to process the alarm. The operation ends.
- If not, go to **Step 3**.

Step 3 Collect the information about alarm handling, and contact Huawei technical engineers for support..

----End

Related Information

None

A.116 ALM-52006 Virtual machine memory usage

Description

This alarm is generated when the memory usage of the virtual machine is greater than or equal to the alarm generation threshold. It is cleared when the memory usage is lower than the alarm clearance threshold.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52006	Major	Software

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.
Virtual Machine Name	Name of the virtual machine on which an alarm is generated.

Impact on the System

- The available memory space of the system is insufficient. The service responds slowly and operations time out.
- 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

Copyright © Huawei Technologies Co., Ltd.

Possible Causes

- The threshold of the alarm is specified to a smaller value.
- The hardware performance of the virtual machine is low. Therefore, the service cannot run properly.

Procedure

Step 1 Check whether the threshold for generating a high memory usage alarm of the virtual machine is specified as a smaller value.

1. Log in to the vCenter Server through the VMware client.
2. Check whether the alarm reporting threshold is specified properly.
   a. Click **Home** in the main toolbar.
   b. In **Inventory**, click the icon for the **Hosts and Clusters**.
   c. Select the **Alarms** tab, click the **Definitions** subtab and double-click this alarm in the list.
   d. In the displayed **Alarm Settings** dialog box, select the **Triggers** tab.

   Check whether the following conditions are met:

   - You have reset the threshold (by default, the threshold for generating a high memory usage of the virtual machine alarm is 75% in yellow and 90% in red) and the current value is lower than the default value. An alarm is generated but the system runs properly with fast response.
   - The threshold is set to a smaller value.

   Solution:

   - If the preceding conditions are met, set the yellow threshold to 75% and the red threshold to 90% in the vCenter alarming setting.

     Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, go to **Step 2**.
   - If the preceding conditions are not met, perform **Step 2**.

Step 2 Collect the information about alarm handling, and contact Huawei technical engineers for support.

----End

Related Information

None

A.117 ALM-52008 Unable connect to vCenter Server

Description

This alarm is generated when connecting to the vCenter fails three times. It is cleared when connecting to the vCenter is successful.

Copyright © Huawei Technologies Co., Ltd.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52008	Major	Software

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.

Impact on the System

Alarms generated on the vCenter cannot be queried and forwarded.

System Actions

None

Possible Causes

- The IP address is incorrect.
- The user name or password is incorrect.
- The vCenter services are not started.
- The network is faulty.

Procedure

Step 1 Check whether the user name, password, and IP address of the vCenter Server you have entered during the alarm service installation are correct.

For detailed operations, see *U2000 Distributed System User Guide*.

- If they are correct, perform **Step 2**.
- If they are incorrect, change them correctly by referring to *U2000 Distributed System User Guide*.

  Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, go to **Step 2**.

Step 2 Check whether the network is faulty.

Log in to the server where alarm services are installed as user **ossuser** and run the following command to check the network connection between the server and the vCenter Server.

$ **ping** *IP address of the vCenter on which an alarm is generated*

Copyright © Huawei Technologies Co., Ltd.

- If the IP address can be pinged, the network connection is normal. Then, perform **Step 3**.
- If the IP address cannot be pinged, the network connection is abnormal. Then, check and recover the network connection.

  Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, go to **Step 3**.

Step 3 Collect the information about alarm handling, and contact Huawei technical engineers for support..

----End

Related Information

None

A.118 ALM-52009 Datastore usage on disk

Description

This alarm is generated when the usage of a disk or a partition (volume) is greater than or equal to the alarm generation threshold. It is cleared when the usage of a disk or a partition (volume) is lower than the alarm clearance threshold.

The alarm results from a VMware alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
52009	Major	Software

Parameters

Name	Meaning
CMSType	Type of the cloud management platform.
IP Address	IP address of the vCenter on which an alarm is generated.
Virtual Machine Name	Name of the virtual machine on which an alarm is generated.
Data Store	Name of the data center.

Impact on the System

The write operation of the service may fail. Database exception may occur.

Copyright © Huawei Technologies Co., Ltd.

System Actions

None

Possible Causes

- The disk contains too many unnecessary files.
- The service has received a large amount of data. The data is exported from the database to disk files in a short time.
- The threshold of the alarm is specified to a smaller value.

Procedure

Step 1 Check whether the threshold for generating a high disk usage alarm of the virtual machine is specified as a smaller value.

1. Log in to the vCenter Server through the VMware client.
2. Check whether the alarm reporting threshold is specified properly.
   a. Click **Home** in the main toolbar.
   b. In **Inventory**, click the icon for the **Hosts and Clusters**.
   c. Select the **Alarms** tab, click the **Definitions** subtab and double-click this alarm in the list.
   d. In the displayed **Alarm Settings** dialog box, select the **Triggers** tab.

   Check whether the following conditions are met:

   - You have reset the threshold (by default, the threshold for generating a high disk usage alarm is 80% in yellow and 85% in red) and the current value is lower than the default value.
   - The threshold is set to a smaller value.

   Solution:

   - If the preceding conditions are met, set the yellow threshold to 80% and the red threshold to 85% in the vCenter alarming setting.

     Check whether the alarm has been cleared. If the alarm has been cleared, the operation ends. If the alarm has not been cleared, go to **Step 2**.
   - If the preceding conditions are not met, perform **Step 2**.

Step 2 Delete unnecessary files from the disk.

NOTICE

If you are not sure whether the file can be deleted, contact the system administrator or Huawei technical engineers.

1. Log in to the virtual machine and run the following command to check in which position the disk usage is over high:

Copyright © Huawei Technologies Co., Ltd.

df -k

2. Run **cd** command to open the directory with high disk usage. Then run **LC_ALL=en_US du -k | LC_ALL=en_US sort -nr > /tmp/du_k.txt** command to query the sizes of all files and subdirectories under this directory. Sort the files and subdirectories, and write them into **du_k.txt**.
3. Run **more /tmp/du_k.txt** command to view du_k.txt and find the subdirectory that causes high disk usage.
4. Run **cd** command to open the subdirectory that causes high disk usage. Then run **ls -l > /tmp/ls_l.txt** command to query the sizes of all files and subdirectories under this subdirectory. Sort the files and subdirectories, and write them into **ls_l.txt**.
5. 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.
6. Check whether the alarm has been cleared.
   - If the alarm has been cleared, the operation ends.
   - The alarm is not cleared. Perform **Step 3**.

Step 3 Collect the information about alarm handling, and contact Huawei technical engineers for support.

----End

Related Information

None

A.119 FIBER_POWER_DEG

Description

The performance system of the uTraffic provides optical power monitoring means for users to manually set the optical power change threshold. If the optical power loss of a fiber exceeds the threshold, the performance system automatically reports a FIBER_POWER_DEG alarm to the U2000.

NOTICE

- This alarm cannot be checked or synchronized.
- This alarm depends on performance data analysis conducted by the uTraffic. Therefore, it is reported to the U2000 with a delay.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
61001	Minor	Service

Parameters

Name	Meaning
Location Information	Indicates the full distinguished name (FDN) or name of the fiber.

Impact on the System

The quality of service transmission over this fiber deteriorates. This alarm must be handled immediately.

Possible Causes

The performance system of the uTraffic detects that the optical power loss of a fiber exceeds the threshold.

Procedure

Step 1 Check whether the fiber is faulty.

- If yes, replace the faulty fiber and check the RX and TX optical power values.
  - If the values are still incorrect, go to **Step 2**.
  - If the values are correct, no further operation needs to be taken.
- If no, go to **Step 2**.

Step 2 Check whether the pluggable optical modules are faulty.

- If yes, replace the faulty pluggable optical modules and check the RX and TX optical power values.
  - If the values are still incorrect, go to **Step 3**.
  - If the values are correct, no further operation needs to be taken.
- If no, go to **Step 3**.

Step 3 Check whether optical attenuators are faulty.

- If yes, replace the faulty optical attenuators and check the RX and TX optical power values.
  - If the values are still incorrect, go to **Step 4**.
  - If the values are correct, no further operation needs to be taken.
- If no, go to **Step 4**.

Step 4 Check whether boards are faulty.

Copyright © Huawei Technologies Co., Ltd.

- If yes, the fault may be caused by a cold reset or removal and insertion of the boards. Check the working status of the boards.
  - If the boards are not working properly, replace the boards with spare boards that have the same parameters as the faulty boards.
  - If the boards are working properly, no further operation needs to be taken.
- If no, no further operation needs to be taken.

Step 5 If the fault persists, contact Huawei technical support engineers for a solution.

----End

Related Information

There is no related information.

A.120 Database Backup

Description

The database fails to be backed up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70001	Major	Equipment

Parameters

Name	Meaning
Parameter 1	Primary IP Address.
Parameter 2	Function. For example, backing up the database periodically.

Impact on the System

None.

Possible Causes

- Cause 1: The database user does not have the write permission for the backup path.
- Cause 2: No file exists for backup.
- Cause 3: The server has insufficient disk space.
- Cause 4: In FTP or SFTP remote database backup mode, network connection is abnormal.
- Cause 5: In FTP or SFTP remote database backup mode, the user name, password, or server IP address is incorrect, or the backup path does not exist.

Copyright © Huawei Technologies Co., Ltd.

- Cause 6: Database processes are not started.
- Cause 7: A backup task is being performed on the U2000 client and MSuite at the same time.
- Cause 8: Third-party components are missing.
- Cause 9: Others.

Procedure

Step 1 Cause 1: The database user does not have the write permission for the backup path.

1. Check whether the database user has the write permission for the backup path. If the user does not have the write permission, grant one the user.

Step 2 Cause 2: No file exists for backup.

1. Check whether the files to be backed up exist.

Step 3 Cause 3: The server has insufficient disk space.

1. Generally, the available space of the local backup path is 1/3 greater than the size of the local database, and the available disk space of the remote backup path is 1/3 greater than that of the local database. Check whether the disk space of the backup path meets the requirement. If it does not meet the requirement, clean the disk in a timely manner.

Step 4 Cause 4: In FTP or SFTP remote database backup mode, network connection is abnormal.

1. Check whether the network connection between the current server and remote server is proper.

Step 5 Cause 5: In FTP or SFTP remote backup database mode, the user name, password, or server IP address is incorrect, or the backup path does not exist.

1. Log in to the U2000 client.
2. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Task Schedule** > **Task Management** from the main menu (application style).
3. In the **Task Management** window, choose **Task Type** > **Backup** > **DB Backup** from the navigation tree. In the right pane, right-click the created task and select **Attribute** from the shortcut menu.
4. In the dialog box that is displayed, check whether the parameters are set correctly.

Step 6 Cause 6: Database processes are not started.

1. Log in to the U2000 System Monitor client and check whether the database is running properly on the **Database Monitor** tab. If it is not running, go to the next step.
2. Start the database. For details, see "Starting the U2000 System" in the *U2000 Administrator Guide*.

Step 7 Cause 7: A backup task is being performed on the U2000 client and MSuite at the same time.

Perform a backup task on the U2000 client or MSuite first. Prevent a backup task from being performed on the U2000 client and MSuite at the same time.

Step 8 Cause 8 and cause 9.

Copyright © Huawei Technologies Co., Ltd.

Contact Huawei technical support engineers for help.

----End

Related Information

None.

A.121 Unified Management Engine License Alarm

Description

The U2000 manages NEs in two or three domains, but the unified management engine license has not been purchased.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70002	Warning	Equipment

Impact on the System

This alarm has no impact on functions or services. Users are advised to purchase the unified management engine license based on the NEs being managed.

Possible Causes

- Cause 1: The U2000 manages NEs in two domains, but has not purchased the unified management engine license for managing two or three domains.
- Cause 2: The U2000 manages NEs in the IP, access, and transport domains, but has not purchased the unified management engine license for managing three domains.

Procedure

Step 1 Contact Huawei technical support engineers to apply for a unified management engine license.

----End

Related Information

None.

Copyright © Huawei Technologies Co., Ltd.

A.122 A Fault Occurs on the FTP or SFTP Server That Is Used to Execute ONT Loading Tasks

Description

The U2000 cannot connect to the FTP or SFTP server that is used to execute ONT loading tasks.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70004	Critical	Equipment

Impact on the System

ONT loading tasks on the U2000 cannot be applied to NEs.

Possible Causes

- Cause 1: The FTP or SFTP server IP address is set incorrectly.
- Cause 2: A fault occurs on the FTP or SFTP server.
- Cause 3: The FTP or SFTP server may be a third-party server and cannot be connected by the U2000 due to network interruption.
- Cause 4: The ONT configuration files and program files do not need to be loaded through the U2000. Therefore, the FTP or SFTP server is stopped.

Procedure

- Perform the following operations to solve the problem occurred due to cause 1.
  1. Choose **Administration** > **Settings** > **FTP Account Information Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Settings** > **FTP Account Information Management** from the main menu (application style). In the **FTP Account Information Management** dialog box, check the FTP account used by the **ONT Load** application on the **Configure FTP Application** tab, click the **Configure FTP Account** tab and verify the server IP address, user name, and password of the FTP account.
  2. Modify the file server configurations if they are incorrect.
  3. Check whether the alarm is cleared.
     a. If yes, no further operation is required.
     b. If not, perform **2**.
- Perform the following operations to solve the problem occurred due to cause 2.
  1. Check whether a fault occurs on the FTP or SFTP server.
  2. Rectify the fault on the FTP or SFTP server if it occurs.

Copyright © Huawei Technologies Co., Ltd.

3. Choose **Administration** > **Settings** > **FTP Account Information Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Settings** > **FTP Account Information Management** from the main menu (application style). Click the **Configure FTP Application** tab and check the FTP account used by the **ONT Load** application. Click the **Configure FTP Account** tab, right-click the FTP account and choose **Test** from the shortcut menu to test the FTP server.
4. Check whether the alarm is cleared.
   a. If yes, no further operation is required.
   b. If not, perform **3**.

- Perform the following operations to solve the problem occurred due to cause 3.
  1. Ping the FTP or SFTP server IP address on the U2000 and check whether the network is normal.
  2. Rectify the FTP or SFTP network fault if it occurs.
  3. Choose **Administration** > **Settings** > **FTP Account Information Management** from the main menu (traditional style); alternatively, double-click **System Management** in **Application Center** and choose **Settings** > **FTP Account Information Management** from the main menu (application style). Click the **Configure FTP Application** tab and check the FTP account used by the **ONT Load** application. Click the **Configure FTP Account** tab, right-click the FTP account and choose **Test** from the shortcut menu to test the FTP server.
  4. d. Check whether the alarm is cleared.
     a. If yes, no further operation is required.
     b. If not, perform **5**. If the FTP or SFTP server does not need to be used, perform **4**.
- Perform the following operations to solve the problem occurred due to cause 4.
  1. Log in to the MSuite client.
  2. Choose **Tools** > **Config Manager** from the main menu.
  3. In the **Config Manager** dialog box, click **Filter** in the upper right corner. In the **Set Filter** dialog box, set **Config Name** to **XPON_CPEFTP_ALARMCHECK_TIME** and click **OK**.
  4. Double-click the configuration item. In the **Modify Config Value** dialog box, change **Config Value** to **0**, which indicates that the fault status of the FTP or SFTP server is no longer checked.
  5. Restart the BmsAccess process.
  6. Manually clear the alarm.
- Collect fault information and contact Huawei engineers for troubleshooting.

----End

A.123 CLOCK_LINK_LOOP

Description

One or more loops exist on a clock link.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70006	Critical	Communication

Parameters

None.

Impact on the System

A loop results in service interruption.

Possible Causes

Multiple loops exist on the clock link.

Procedure

Step 1 Check the clock loop.

1. Choose **View** > **Main Topology** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** (application style).
2. Select **Clock View** from the **Current View** drop-down list.
3. Right-click in the blank area of the **Clock View** and choose **Check for Clock Loop** from the shortcut menu.
4. In the **Clock Loop** dialog box, view loop information.

Step 2 Troubleshoot the NE whose configurations are incorrect in the loop list.

You can perform clock configruation check on NEs based on the NE and port information in the check result, analyze the incorrect part, and modify the clock tracing relationship.

Step 3 Perform clock loopback check again and ensure that no loop exists on the clock link.

----End

Related Information

None.

A.124 The device is unwonted

Description

The device is unwonted.

Copyright © Huawei Technologies Co., Ltd.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70007	Critical	Equipment

Impact on the System

The NE cannot be managed on the U2000.

Possible Causes

- Some data is kept on the U2000 after the NE is deleted.
- Data is inconsistent due to other causes.

Procedure

Step 1 If some data is kept on the U2000 after the NE is deleted, perform the following operation:

1. Delete the NE again.

Step 2 If data is inconsistent due to other causes, perform the following operations:

1. Check the NE information to ensure that it is a manageable NE.
2. Delete the NE and add it again.

----End

A.125 NE type change

Description

NE type is changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
70010	Major	Processing error

Impact on the System

None.

Possible Causes

- The original NE is faulty and is replaced with another type of NE.
- The NE type is modified in the NE CLI.
- The NE type is changed after the NE is restarted.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- If the original NE is faulty and is replaced with another type of NE, perform the following operation:
  1. Right-click the alarm and choose **Locate in Topology** from the shortcut menu to switch to the NE topology view.
  2. Right-click the NE and choose **Update NE Type** from the shortcut menu. In the confirmation dialog box, click **Yes**.
  3. Synchronize NE data and check whether the alarm is cleared. If yes, no further operation is required. If no or the operation cannot be completed, proceed to step **4**.
  4. Delete the NE and add it again.
- If the NE type is modified in the NE CLI, perform the following operations:
  1. Log in to the NE and run commands to restore the NE type to be consistent with that on the U2000 or perform operations by referring to steps in **Reason (1)**.
- If the NE type is changed after the NE is restarted, perform the following operations:
  1. Log in to the NE and run commands to restore the NE type to be consistent with that on the U2000 or perform operations by referring to steps in **Reason (1)**.

----End

Related Information

None.

Copyright © Huawei Technologies Co., Ltd.

B Obtaining Technical Support

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

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

NOTE

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

Copyright © Huawei Technologies Co., Ltd.

C Glossary and Abbreviations

A

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

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

B

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

C

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

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

D

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

E

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

Copyright © Huawei Technologies Co., Ltd.

F

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

G

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

H

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

Copyright © Huawei Technologies Co., Ltd.

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

I

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

Copyright © Huawei Technologies Co., Ltd.

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

J

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

K

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

Copyright © Huawei Technologies Co., Ltd.

L

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

M

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

Copyright © Huawei Technologies Co., Ltd.

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

N

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

O

OAM	See **operation, administration and maintenance**

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

P

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

R

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

Copyright © Huawei Technologies Co., Ltd.

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

S

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

Copyright © Huawei Technologies Co., Ltd.

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

Copyright © Huawei Technologies Co., Ltd.

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

T

TCP	See **Transmission Control Protocol**
TCP/IP	See **Transmission Control Protocol/Internet Protocol**
Telecommunication Management Network	The Telecommunications Management Network is a protocol model defined by ITU-T for managing open systems in a communications network.An architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks and services.
Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
TFTP	See **Trivial File Transfer Protocol**

Copyright © Huawei Technologies Co., Ltd.

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

U

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

V

VCS	See **Veritas Cluster Server**
Veritas Cluster Server	A High-availability cluster software, for Unix, Linux and Microsoft Windows computer systems, created by Veritas Software. It provides application cluster capabilities to systems running Databases, file sharing on a network, electronic commerce websites or other applications.
Veritas Volume Manager	A software product from veritas Inc.. The Veritas Volume Manager is used to manage disk storage.
Veritas Volume Replicator	A wide area network data replication solution offered by VERITAS for multiple operating systems. These include. AIX, HPUX and Solaris.
Virtual Local Area Network	A logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same IP network number. This is often associated with switched Ethernet.

Copyright © Huawei Technologies Co., Ltd.

Virtual Router Redundancy Protocol	A protocol used for multicast or multicast LANs such as an Ethernet. A group of routers (including an active router and several backup routers) in a LAN is regarded as a virtual router, which is called a backup group. The virtual router has its own IP address. The host in the network communicates with other networks through this virtual router. If the active router in the backup group fails, one of the backup routers become the active one and provides routing service for the host in the network.
VLAN	See **Virtual Local Area Network**
volume	A logical unit for disk virtualization management, and basic object for host applications.
VRRP	See **Virtual Router Redundancy Protocol**
VVM	See **Veritas Volume Manager**

W

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

Copyright © Huawei Technologies Co., Ltd.