Maintaining and Troubleshooting Avaya Aura™ Session Manager

03-603325, Issue 1.5
Release 5.2
November 2011

© 2010 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

For full hardware support, please see the document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya support web site, http://www.avaya.com/support.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura™ is a registered trademark of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Chapter 1: Maintenance and Troubleshooting

This guide describes how to identify and troubleshoot problems for Avaya Aura™ Session Manager. It describes how to run maintenance tests, replace hardware, how to set up and view SIP tracing, how to monitor system components, and how to troubleshoot errors and alarms.

Required troubleshooting equipment

For maintenance and troubleshooting activities, you will need:

- A laptop
- SIP Protocol Analyzer
- xming or other virtual desktop tool
- DVD burner
- USB keyboard and mouse
- SVGA monitor
- Network sniffer such as wireshark

Session Manager software version

The Session Manager version string has the format **w.x.y.z.#** where

w = Major release number

x = Minor release number

y = Service pack number

z = Patch number

= Build number

For example: 5.2.1.0.521019

To view the software version number, select **Session Manager** > **System Status** > **System State Administration** on the System Manager console.

Customer account commands

The following is the list of commands which can be executed using the cust or craft login. The commands are executed from the shell of the Session Manager server.

- `/home/cust/SMnetSetup`
- `/home/cust/upgradeSM`
- `/opt/Avaya/bin/start`
- `/opt/Avaya/bin/restart`
- `/opt/Avaya/bin/statapp`
- `/opt/Avaya/bin/swversion`
- `/opt/Avaya/bin/initTM`
- `/opt/Avaya/bin/changeMgmtIP`
- `/opt/Avaya/bin/smconfig`
- `/opt/Avaya/bin/shutdownSM`
- `/opt/Avaya/bin/rebootSM`

Chapter 2: Safety information

General safety information

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the system units during and after maintenance.
  - Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the system unit.
  - Keep your tool case away from walk areas so that other people do not trip over it.
- When lifting any heavy object:
  a. Verify that you can stand safely without slipping.
  b. Distribute the weight of the object equally between your feet.
  c. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  d. Lift by standing or by pushing up with your leg muscles. This action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 16 kg (35 lb.) or objects that you think are too heavy for you.
- Do not perform any action that causes hazards to the customer, or that makes the equipment unsafe.
- Before you start the system unit, ensure that other technical support staff and customer personnel are not in a hazardous position.
- Do not wear loose clothing that can be trapped in moving parts. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 cm (3 inches) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing. Metal objects are good electrical conductors.
- Remove items from your shirt pocket, such as pens and pencils, that could fall into the server as you lean over it.
- Wear safety glasses when you are working in any conditions that might be hazardous to your eyes.

- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws, into the server.
- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
- Reinstall all covers correctly before returning the server to service.

Warning:

To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance with international radiated emissions requirements, tighten all captive screws securely so they cannot be loosened without the use of a tool.

Safety Inspection

Use this list to identify potentially unsafe conditions related to the server. Each server, as it was designed and built, had required safety items installed to protect users and technical support staff from injury. If any unsafe conditions are present, determine how serious the apparent hazard is and whether you can safely continue without first correcting the problem.

Consider these conditions and the safety hazards they present:

- Electrical hazards, especially primary power. Primary voltage on the frame can cause serious or fatal electrical shock.
- Explosive hazards, such as a damaged monitor face or bulging capacitor.
- Mechanical hazards, such as loose or missing hardware.

Perform the following safety checks when servicing this unit:

1. Check exterior covers for damage such as loose, broken, or sharp edges.
2. Shutdown the system and unplug the AC power cords.
3. Check the power cord:
   - Verify that the third-ground connector is in good condition. Use an ohmmeter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and frame ground.
   - Verify that the power cord is the appropriate type.
   - Verify that insulation is not frayed or worn.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquids, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Verify that the power-supply cover fasteners, such as screws or rivets, have not been removed or tampered with.
7. If you notice any damage, replace the appropriate system components.

Electrical safety rules

Electrical current from power, telephone, and communication cables can be hazardous. To avoid any shock hazard, you must disconnect all power cords and cables.

Observer the following rules when working on electrical equipment.

- Find the room emergency power-off (EPO) switch, disconnecting switch, or electrical outlet. If an electrical accident occurs, you can then operate the switch or unplug the power cord quickly.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Doing a mechanical inspection
  - Working near power supplies
  - Removing or installing servers
- Before you start to work on the server, unplug the power cord. If you cannot unplug it, ask the customer to switch off the wall box that supplies power to the server. Afterwards, lock the wall box in the off position.
- If you must work on a server that has exposed electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you. Another person must be there to switch off the power if necessary.
  - Stand on suitable rubber mats to insulate you from grounds such as metal floor strips and system unit frames. Obtain the mats locally, if necessary.
  - When using testers, set the controls correctly and use the approved probe leads and accessories for that tester.
  - Use only one hand when working with powered-on electrical equipment. Keep the other hand in your pocket or behind your back. This precaution can prevent a current from passing through your body.
- Regularly inspect and maintain your electrical hand tools for safe operational condition. Do not use worn or broken tools and testers.
- Never assume that power was disconnected from a circuit. First, verify that the unit is turned off.
- Always look carefully for possible hazards in your work area. Examples of hazards are moist floors, non-grounded power extension cables, power surges, and missing safety grounds.
- Do not touch live electrical circuits with the reflective surface of a plastic dental mirror. The surface is conductive. Touching a live circuit can cause personal injury and damage to the server.

- Use only approved tools and test equipment. Some hand tools have handles covered with a soft material that does not insulate you when working with live electrical currents.
- Many customers have, near their equipment, rubber floor mats that contain small conductive fibers to decrease electrostatic discharges. Do *not* use this type of mat to protect yourself from electrical shock.

If an electrical accident occurs:

- Use caution. Do not become a victim yourself.
- Turn off power.
- Send another person to get medical aid.

Protecting against ESD damage

Any system component that contains transistors or integrated circuits is sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge. The server, the part, the work mat, and the person handling the part must all be at the same charge.

Packaging materials that contain ESD-sensitive components are usually marked with a yellow and black warning symbol.

Caution:

You must observe proper grounding techniques to prevent the discharge of static electricity from your body into ESD-sensitive components.

To avoid damaging ESD-sensitive components:

- Limit your movement. Movement can cause static electricity to build up around you.
- Keep the parts in protective packages until you are ready to install them into the server. If it is necessary to set down a part, put it back into its static-protective package. Do not place the part on the server cover or on a metal surface.
- Place parts on a grounded surface before removing them from their containers.
- Handle the components only after attaching a wrist strap to your bare wrist. Attach the other end of the wrist strap to a ground that terminates at the system ground, such as any unpainted metallic chassis surface.
- Handle a circuit board by the faceplate or side edges only. Avoid touching pins, leads, or circuitry. Hold devices such as a hard disk drive in the same manner. The ESD-sensitive area of these components is located on the bottom surface.

  Caution:

  Make sure that the unprotected part of your hand is not in contact with the non-component side of the board.

- Keep components away from plastics and other synthetic materials such as polyester clothing. Most clothing is insulative and retains a charge even when you are wearing a wrist strap.
- Do not hand components to another person unless that person is grounded at the same potential level. In general, avoid contact with other people.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.
- Verify that the ESD protective devices you use are ISO 9000 certified as fully effective.

Chapter 3: Access to Session Manager

Access to Session Manager is not needed except for installations and upgrades.

Using the Session Manager services ports for local access

About this task

Local access is provided through each server's services ports for installation of the Session Manager and upgrades.

Procedure

1. Connect a USB keyboard to one of the two services ports on the front panel of the server.
2. Connect a USB mouse to the other services port on the front panel of the server.
3. Connect the SVGA monitor to the video connector on the front panel of the server.

Remote access

Remote access to Session Manager is provided by using one of the following access methods:

- RSIG
- SAC/SAC Lite/SSG/SIG
- SSLVPN
- Secure Access Link (SAL) to access System and Session Manager
- Web Conferencing using Meeting Exchange
- Secure Access Link (SAL) Gateway for access to System Manager and Session Manager

A secure shell (ssh) connection between System Manager and any Session Manager is required for shell access.

Chapter 4: Alarming

The alarming service provides access to alarms generated by the components of a Session Manager system. The following operations can be performed:

- Viewing alarms
- Changing alarm status
- Exporting alarms to a comma separated values (csv) file

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation and identify the system component which generates the alarm.

System Manager can be configured to forward alarms to Avaya Services. It can also be configured to send SNMP traps to a customer Network Management System (NMS).

Alarm events

There are three types of alarm event logging:

- **ALARM:** Software recovery actions have failed to correct the problem.
- **WARN:** Indicates that something is not quite right. This is not an alarm, but repeated instances may generate an alarm.
- **CLEAR:** The problem has been fixed and the alarm has been cleared.

Alarm severities

CRITICAL alarms indicate that the system or certain system components are unusable. The default color for these alarms is red.

INDETERMINATE alarms indicate a log event is missing the severity but still matches one of the established alarm rules. This alarm is displayed in blue.

MAJOR alarms identify failures that cause a critical degradation of service. These alarms require immediate attention. These alarms are displayed in orange.

MINOR alarms identify failures that cause some service degradation but do not cause the system to be inoperable. Minor alarms require attention and typically affect only a few trunks, stations, or a single feature. These alarms are displayed in yellow.

WARNING alarms identify failures that cause no significant degradation of service or equipment failures external to the switch. These failures are not reported to a services organization. These alarms are displayed in purple.

The colors of the severities can be changed.

Changing alarm severity colors

Procedure

1. Select **Settings** > **Service Profile Management** > **System Manager 5.2** > **Alarming UI** on the System Manager console.
2. Change the color for a particular alarm as desired.
3. Click the **Commit** button when finished.

Forwarding alarms to Avaya Services

About this task

System Manager can be configured to forward alarms to Avaya Services.

Procedure

1. Click **Settings** > **Service Profile Management** > **SPIRIT 1.0** > **DataTransportConfig** on the System Manager console.
2. Enter information in the fields as described in the DataTransportConfig field descriptions on page 16 table.
3. Click the **Commit** button when finished.

DataTransportConfig field descriptions

The following table contains a list of the fields on the DataTransportConfig screen which need to be administered for forwarding alarms to Avaya Services.

Name	Description
Connection.AvayaProduction.UseProxy	Use proxies for this platform (true or false)
OrganizationFQDN	A Fully Qualified Domain Name to uniquely identify the business organization that the SM100 platform resides in.
ProxyAddress	The domain name or IP address of the proxy to use.
ProxyPass	The password to use with the proxy.
ProxyPort	The port of the proxy to use.
ProxyType	The type of proxy to use (HTTP or SOCKS).
ProxyUseAuthentication	Whether to use username/password authentication with this proxy (true or false).
ProxyUser	The user name to use with the proxy.

Forwarding alarms to NMS

About this task

System Manager can be configured to send SNMP traps to a customer Network Management System (NMS).

Procedure

1. Select **Settings** > **Service Profile Management** > **AlarmManagementService 1.0** > **AlarmMgmt** on the System Manager console.
2. Click the **Edit** button.
3. Enter the appropriate information in the fields as described in the table for AlarmMgmt field descriptions on page 18.
4. Click the **Commit** button when finished.
5. Restart the JBoss in order for changes to take effect:
   a. Log in as root on the System Manager.
   b. Enter the command **service jboss restart**

Caution:

This command affects service on the System Manager server. Any current web session to the System Manager will be disconnected, and alarm processing will be down for approximately a minute during the restart.

AlarmMgmt field descriptions

The following table contains a list of the fields on the AlarmMgmt screen and a description of the field.

Name	Description
email.fromAddress	Email address of the Alarm Manager
email.host	Address of the host server
Addressesemail.to	Address to send email to
email.userid	Userid of the email sender
federation.member.platform.name	
nms.forward	Enables/disables Network Management System forwarding. The default is **false** (disable NMS forwarding).
nms.urls	A comma-separated list of NMS URLs. For example: `[123.456.78.90:9162]` **Note:** The [ ] must surround the destination IP address and port.
spirit.ui.url	
trouble.ticket.url	

Alarming field descriptions

The Alarming page has two sections; Upper and Lower. The upper section has buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms , and set filters to view specific alarms. The lower section displays alarms in a table.

The table provides information about the status of the alarms along with their severity. You can click a column title to sort the information in the table in ascending or descending order.

Field	Description
Time Stamp	Date and time when the alarm is generated.
Severity	Severity of the alarm.
Status	Current status of the alarms.
Host Name	The name of the host computer that generated the alarm.
Message	A short description of the problem that generated the alarm.
Identifier	Unique identifier for an alarm.
Agent Reference	The reference number of the agent who has reported the alarm.
M/E Ref Number	A unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • Acknowledged • Clear
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. This is a toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file, which can be viewed with Wordpad or Excel.
More Actions > **Export All**	Exports all the alarms to to a CSV file, which can be viewed with Wordpad or Excel.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays the logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the upper right corner of page.

Name	Description
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down list. Select the operator from the second drop-down field. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Time Stamp: Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM. • Severity: Searches all of the alarms that match the specified severity level. • Status: Searches all of the alarms that match the specified status. • Host Name: Searches all of the alarms that are generated from the specified host. • Identifier: Searches all of the alarms that match the specified identifier.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>

Message: Searches all of the alarms that match the specified message.
M/E Ref Number: Searches all of the alarms that match the specified M/E Ref Number.

The operators available are based on the search criterion that you select in the first drop-down field. The following table list the operators that are available for a search criterion:
<table>
<tr><th>Criterion</th><th>Operators</th></tr>
<tr><td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr>
<tr><td>Severity</td><td>Equals, Not Equals</td></tr>
<tr><td>Status</td><td>Equals, Not Equals</td></tr>
<tr><td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr>
<tr><td>Message</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
</table>
When you select Begin Date and End Date from the first drop-down list, you are prompted to enter the date in the third field.
</td></tr>
</table>

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.
Close/Advanced Search	Hides the search fields.

Button	Description
+	Adds a search condition.
-	Deletes a search condition.

Viewing alarms

Procedure

1. On the System Manager console, select **Monitoring** > **Alarms**
2. Select an alarm to view. You can also select multiple alarms.
3. Click **View**.

Filtering alarms

The criteria for filtering the alarms are status, M/E Reference Number, Agent Reference, or severity. You can use more than one filter criterion on the selected alarms.

Procedure

1. On the System Console, select **Monitoring** > **Alarms**
2. On the Alarming page, select the alarms you want to filter.
3. Click **Filter: Enable** at the top right corner of the alarm log table.
4. Select the filter criteria you want to apply to the selected alarms.
   The **Status** and **Severity** fields have drop-down menus.
5. Click **Filter: Apply**.

Note:

A message will be displayed if no records are found which match the specified filter criteria.

Result

The page displays the alarms matching the filter criteria on the Alarm viewer.

Changing status of an alarm

The status of an alarm can be:

- Acknowledged – Maintenance support must manually set the alarm to this state, indicating the alarm is under investigation.
- Cleared – Maintenance support must manually set the alarm to this state, indicating that the error condition has been resolved.

Procedure

1. On the System Manager console, select **Monitoring** > **Alarms**
2. On the Alarming page, select an alarm and click **Change Status**.
   You can select multiple alarms.
3. Click on the status that you want to apply to the selected alarms.

Exporting alarms

Alarms can be exported to a Comma Separated Values (csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Excel.

Procedure

1. On the System Manager console, click **Monitoring** > **Alarms** in the left navigation pane.
2. On the Alarming page, perform one of the following steps:
   - To export a selected alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export all the alarms to a CSV file, click **More Actions** > **Export All**.
3. Click **Save** to save the exported file to the local disk.

Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only those alarms which satisfy the search conditions. Multiple search conditions can be specified.

Procedure

1. On the System Manager console, click **Monitoring** > **Alarms** in the left navigation pane.
2. On the Alarming page, click **Advanced Search**.
3. In the Click to Search to find alarms for the given search conditions section, select the search criterion from each of the drop-down fields.
4. If you want to add another search condition, click the **+** button.

   Note:

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
5. Select the AND or OR from the drop-down field.

   This option appears when you add a search condition using the + button.
6. Click **Search** to find alarms for the given search conditions.

Troubleshooting alarms

About this task

Alarms are not automatically acknowledged or cleared. Some alarms, such as OS or platform alarms, do not have a clear event code.

The steps for troubleshooting an alarm when it appears on the Alarm Viewer screen involve:

- Acknowledging the alarm.
- Checking the log event list to see if the alarm has an associated clear event code.
- Troubleshooting the alarm if further investigation is required.
- Clearing the alarm.

Procedure

1. Select **Monitoring** > **Alarming** on the System Manager console
2. Select the appropriate alarm(s).
3. Click on the **Change Status** button.
4. Select **Acknowledged** from the drop-down menu.
5. Select **Monitoring** > **Logging** on the System Manager console.
6. Using the **Display filter** option, enter the Event ID or part of the Event ID (OP_MMTC) in the filter field for Event ID.
7. If the alarm has an associated clear event ID, change the status of the alarm(s) to **Cleared**:
   a. Select **Monitoring** > **Alarming** on the System Manager console.
   b. Select the appropriate alarm(s).
   c. Click on the **Change Status** button.
   d. Select **Cleared** from the drop-down menu.
8. If the alarm does not have an associated clear event ID, look for the alarm code in the **Log and Alarm Event ID Table** and investigate how to troubleshoot the problem using the link in the Log Message/Alarm Description column.
9. If the problem has been fixed, clear the alarm using the steps listed in step 7.

Alarm Event Codes

The table for Alarm Event Codes, descriptions, and troubleshooting actions is found in Appendix A: Log and Alarm Event IDs on page 144.

Chapter 5: Logging

The logging service provides an interface for viewing logs and their details generated by System Manager or other components. The System Manager console allows you to:

- monitor log messages
- view the details of a log
- search for a log
- filter specific logs

Log details include information about the event which generated the log and the severity level of the log. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Viewing log details

Procedure

1. On the System Manager console, select **Monitoring** > **Logs**
2. On the Logging page, select a log.
3. Click **View**

Searching for logs

Use the Advanced Search function to find logs based on certain specified conditions. The system displays only those logs which satisfy the search conditions. Multiple search conditions can be specified.

Procedure

1. On the System Manager console, select **Monitoring** > **Logs**
2. On the Logging page, click **Advanced Search**.
3. In the *Criteria* section, from the first and second drop-down fields, select the search criterion and the operator.

4. Select or enter the search value in the third field.
5. If you want to add another search condition, click **+** and repeat the steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
6. Select the AND or OR operator from the drop-down field.

   This page displays this drop-down field when you specify more than one search condition.
7. Click **Search** to find the logs for the given search conditions.

Filtering logs

You can filter and view logs that meet the specified filter criteria. Applying the filters requires you to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

Procedure

1. On the System Manager console, select **Monitoring** > **Logs**
2. On the Logging page, click **Filter: Enable**.

   You can find this button on the top right corner in the table displaying logs.
3. Enter or select the filter criteria.
4. Click **Filter: Apply**.

Note:

If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

Result

The page displays the logs that matches the specified filter criteria.

Logging field descriptions

The Logging page has two sections. The upper section contains buttons that allow you to view the details of the selected logs, search for logs, and set filters. The lower section displays logs

in a table. The table provides information about the logs. You can click the title of the column to sort the data of the column in ascending or descending order.

Name	Description
Select check box	Use this check box to select a log.
Log ID	Unique identification number that identifies the log.
Time Stamp	Date and time of the log generation.
Host Name	Name of the system from which the log is generated.
Product Type	A code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.
Severity	Severity level of the log. The following are the type of severities: • Emergency : System is unusable • Alert : Action must be taken immediately • Critical : Critical conditions • Error : Error conditions • Warning : Warning conditions • Notice: Normal but significant condition • Informational : Informational messages • Debug: Debug-level messages **Note:** The colors of severities do not indicate logging severities.
Event ID	Unique identification number assigned to the event that has generated the log.
Message	Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	Process on the device that has generated the message. This is usually the process name and process ID.

Name	Description
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of a selected log.
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. This is a toggle button.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays logs in the previous page. This button is not available if you are on the first page.
Next	Displays logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the top right corner.

Name	Description
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down field. Select the operator from the second drop-down field. Enter the search value in the text field. Select following search criteria from the first drop-down field: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The second drop-down field displays operators. Based on the search criterion that you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains

Name	Description
	The operators for Time Stamp are: =, >, <, >=, <=, and !=. When you select Time Stamp from the first drop-down field, the page provides date and time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format . You can select the date from the calender. You need to enter the time in one of the following format: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and set it to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition

Chapter 6: Call Detail Recording (CDR)

CDR on Session Manager

The Call Detail Recording (CDR) feature records information on tandem calls. When CDR is enabled, the CDR records are saved in a special directory on the server's local hard drive.

The call record contains information regarding:

- time of the call
- duration of the call
- dialed number
- calling party
- terminating SIP entity
- originating SP entity

Each Session Manager can have CDR either disabled or enabled. If at least one of two Session Manager entities has CDR enabled, then CDR records will be created.

In route-through scenarios where one Session Manager routes directly to another Session Manager, CDR is recording only on the originating Session Manager if so administered, not the terminating Session Manager.

CDR record transfer

The CDR records are not transmitted over an IP connection to the CDR adjunct. CDR data is transferred in an encrypted manner from the Session Manager server to the CDR adjunct using a secure file transfer protocol such as SFTP. CDR records are stored and transferred in batches rather than one record at a time.

The CDR adjunct retrieves the CDR data files by logging into the server and copying the files to its own storage device. After all of the files are successfully copied, the CDR adjunct deletes the files from the server's hard drive and processes the CDR records.

CDR login and password

The CDR adjunct uses a special login, CDR_User. This login is restricted to accessing only the directory where the CDR records are stored. Passwords are set up for each Session Manager which has CDR enabled. The Session Manager administrator creates a password for the designated login CDR_User. The login and password need to be provided to the CDR adjunct administrator so that the adjunct can retrieve the CDR data files. The administrator should verify that this login and password work on each server on which CDR is administered.

CDR record deletion

There are three methods for removing CDR data files from the server, listed in order of preference:

- Once the CDR adjunct has successfully retrieved a data file from the server and verified that it contains valid data, the adjunct deletes the data file from the server.
- The server automatically removes any CDR data file stored on its local hard drive that is older than 5 days.
- The onsite or remote switch administrator/technician (with proper permissions) can delete unwanted CDR data files.

CDR security provisions

Due to the potentially sensitive nature of CDR records, a secure transport mechanism is used for all communications between the CDR adjunct and the server such as Secure File Transfer Protocol (SFTP). Periodically, the CDR adjunct must log on to each of the administered Session Manager servers and retrieve the CDR data files that are available.

If firewalls are implemented anywhere between the CDR adjunct and the various Session Manager servers, it may be necessary to “punch” pinholes in those firewalls to allow communication between the CDR adjunct and the servers. Please work with the network administrators to implement these pinholes if needed.

CDR alarms

Alarms are generated when CDR detects problems with recording on an entity for which CDR is enabled. These alarms indicate that call accounting for that entity is not available. During the outage, some or all calls will not be recorded in CDR.

Alarms need to be cleared manually by the administrator or maintenance support when the failure condition has been resolved.

An example of alarm text is: `There is a problem with the Call Detail Recording (CDR) system. Call accounting is not operational.`

An example of text when the alarm clears is: `Call Detail Recording (CDR) system is now operational. Call accounting is resumed.`

See CDR Not Operational on page 164 for more information.

Minimum requirements for CDR

In order to support the Session Manager CDR functionality, the following minimum requirements must be met:

- The Session Manager server must be running the Session Manager first release or a subsequent release.
- There must be IP connectivity between the CDR adjunct and the target server at least from time to time to allow remote collection of the CDR data files.

The CDR adjunct must be compatible with Session Manager CDR formats. Contact your Avaya representative for more information.

Administering CDR on a new Session Manager instance

Procedure

1. At the bottom of the Add Session Manager screen, select the **Enable CDR** check box.
2. Enter a password that will be used by the CDR_User login.

3. Re-enter the password to confirm it.
4. Click the **Save** button.

Enabling CDR for existing Session Manager instance

Procedure

1. Select **Session Manager** on the System Manager console.
2. Select the Session Manager instance you want to administer.
3. Click the **Edit** button.
4. In the CDR section at the bottom of the screen, check the **Enable CDR** box.
5. Enter a password that will be used by the CDR_User login.
6. Re-enter the password to confirm it.
7. Click **Save**.
8. Select **Network Routing Policy** > **SIP Entities** in the left navigation pane.
9. Select the appropriate SIP Entity.
10. Click the **Edit** button.
11. Select an appropriate **Type** from the drop-down menu in the **Call Detail Recording** field.

    There are four choices (**ingress**, **egress**, **both**, **none**). The default is **egress** for SIP entities of type SIP Trunk. The default for all other types is **none**.
12. Click **Commit**.

Chapter 7: SNMP Support for Session Manager

Session Manager has a basic SNMP V1/V2c agent that provides basic SNMP discovery, inventory, and status capabilities via the MIB II and Host Resources MIBs for the server and Linux operating system. This agent:

- provides read-only access to the SNMP agent on the Session Manager server
- does not allow any SNMP Set capability to the Session Manager
- does not restrict which IP addresses are allowed to query the MIBs
- allows access control only via SNMP V1/V2c get community strings

The **setup_snmp** command sets up the basic SNMP agent on the Session Manager server. See setup_snmp on page 41 for the description and usage for the command.

Session Manager SNMP MIB

Below is a list of the SNMP MIB tables and objects that can be queried on the Session Manager server by a network management system on the same network as the Session Manager management interface. Keep in mind that the SM100 board is not included in this MIB as it is essentially a different server on the network.

- HOST-RESOURCES-MIB::hrDeviceDescr
- HOST-RESOURCES-MIB::hrDeviceErrors
- HOST-RESOURCES-MIB::hrDeviceID
- HOST-RESOURCES-MIB::hrDeviceIndex
- HOST-RESOURCES-MIB::hrDeviceStatus
- HOST-RESOURCES-MIB::hrDeviceType
- HOST-RESOURCES-MIB::hrDiskStorageAccess
- HOST-RESOURCES-MIB::hrDiskStorageCapacity
- HOST-RESOURCES-MIB::hrDiskStorageMedia
- HOST-RESOURCES-MIB::hrDiskStorageRemoveble
- HOST-RESOURCES-MIB::hrFSAccess

- HOST-RESOURCES-MIB::hrFSBootable
- HOST-RESOURCES-MIB::hrFSIndex
- HOST-RESOURCES-MIB::hrFSLastFullBackupDate
- HOST-RESOURCES-MIB::hrFSLastPartialBackupDate
- HOST-RESOURCES-MIB::hrFSMountPoint
- HOST-RESOURCES-MIB::hrFSRemoteMountPoint
- HOST-RESOURCES-MIB::hrFSStorageIndex
- HOST-RESOURCES-MIB::hrFSType
- HOST-RESOURCES-MIB::hrMemorySize
- HOST-RESOURCES-MIB::hrNetworkIfIndex
- HOST-RESOURCES-MIB::hrPartitionFSIndex
- HOST-RESOURCES-MIB::hrPartitionID
- HOST-RESOURCES-MIB::hrPartitionIndex
- HOST-RESOURCES-MIB::hrPartitionLabel
- HOST-RESOURCES-MIB::hrPartitionSize
- HOST-RESOURCES-MIB::hrProcessorFrwID
- HOST-RESOURCES-MIB::hrProcessorLoad
- HOST-RESOURCES-MIB::hrSWRunPerfCPU
- HOST-RESOURCES-MIB::hrSWRunPerfMem
- HOST-RESOURCES-MIB::hrStorageAllocationUnits
- HOST-RESOURCES-MIB::hrStorageDescr
- HOST-RESOURCES-MIB::hrStorageIndex
- HOST-RESOURCES-MIB::hrStorageSize
- HOST-RESOURCES-MIB::hrStorageType
- HOST-RESOURCES-MIB::hrStorageUsed
- HOST-RESOURCES-MIB::hrSystemDate
- HOST-RESOURCES-MIB::hrSystemInitialLoadDevice
- HOST-RESOURCES-MIB::hrSystemInitialLoadParameters
- HOST-RESOURCES-MIB::hrSystemMaxProcesses
- HOST-RESOURCES-MIB::hrSystemNumUsers
- HOST-RESOURCES-MIB::hrSystemProcesses
- HOST-RESOURCES-MIB::hrSystemUptime

- IF-MIB::ifAdminStatus
- IF-MIB::ifDescr
- IF-MIB::ifInDiscards
- IF-MIB::ifInErrors
- IF-MIB::ifInNUcastPkts
- IF-MIB::ifInOctets
- IF-MIB::ifInUcastPkts
- IF-MIB::ifInUnknownProtos
- IF-MIB::ifIndex
- IF-MIB::ifLastChange
- IF-MIB::ifMtu
- IF-MIB::ifNumber
- IF-MIB::ifOperStatus
- IF-MIB::ifOutDiscards
- IF-MIB::ifOutErrors
- IF-MIB::ifOutNUcastPkts
- IF-MIB::ifOutOctets
- IF-MIB::ifOutQLen
- IF-MIB::ifOutUcastPkts
- IF-MIB::ifPhysAddress
- IF-MIB::ifSpecific
- IF-MIB::ifSpeed
- IF-MIB::ifType
- SNMPv2-MIB::snmpEnableAuthenTraps
- SNMPv2-MIB::snmpInASNParseErrs
- SNMPv2-MIB::snmpInBadCommunityNames
- SNMPv2-MIB::snmpInBadCommunityUses
- SNMPv2-MIB::snmpInBadValues
- SNMPv2-MIB::snmpInBadVersions
- SNMPv2-MIB::snmpInGenErrs
- SNMPv2-MIB::snmpInGetNexts
- SNMPv2-MIB::snmpInGetRequests

- SNMPv2-MIB::snmpInGetResponses
- SNMPv2-MIB::snmpInNoSuchNames
- SNMPv2-MIB::snmpInPkts
- SNMPv2-MIB::snmpInReadOnlys
- SNMPv2-MIB::snmpInSetRequests
- SNMPv2-MIB::snmpInTooBigs
- SNMPv2-MIB::snmpInTotalReqVars
- SNMPv2-MIB::snmpInTotalSetVars
- SNMPv2-MIB::snmpInTraps
- SNMPv2-MIB::snmpOutBadValues
- SNMPv2-MIB::snmpOutGenErrs
- SNMPv2-MIB::snmpOutGetNexts
- SNMPv2-MIB::snmpOutGetRequests
- SNMPv2-MIB::snmpOutGetResponses
- SNMPv2-MIB::snmpOutNoSuchNames
- SNMPv2-MIB::snmpOutPkts
- SNMPv2-MIB::snmpOutSetRequests
- SNMPv2-MIB::snmpOutTooBigs
- SNMPv2-MIB::snmpOutTraps
- SNMPv2-MIB::snmpProxyDrops
- SNMPv2-MIB::snmpSilentDrops
- SNMPv2-MIB::sysContact
- SNMPv2-MIB::sysDescr
- SNMPv2-MIB::sysLocation
- SNMPv2-MIB::sysName
- SNMPv2-MIB::sysORDescr
- SNMPv2-MIB::sysORID
- SNMPv2-MIB::sysORLastChange
- SNMPv2-MIB::sysORUpTime
- SNMPv2-MIB::sysObjectID
- TCP-MIB::tcpActiveOpens
- TCP-MIB::tcpAttemptFails

- TCP-MIB::tcpCurrEstab
- TCP-MIB::tcpEstabResets
- TCP-MIB::tcpInErrs
- TCP-MIB::tcpInSegs
- TCP-MIB::tcpMaxConn
- TCP-MIB::tcpOutRsts
- TCP-MIB::tcpOutSegs
- TCP-MIB::tcpPassiveOpens
- TCP-MIB::tcpRetransSegs
- TCP-MIB::tcpRtoAlgorithm
- TCP-MIB::tcpRtoMax
- TCP-MIB::tcpRtoMin
- UDP-MIB::udpInDatagrams
- UDP-MIB::udpInErrors
- UDP-MIB::udpNoPorts
- UDP-MIB::udpOutDatagrams

setup_snmp

setup_snmp sets up a basic SNMP agent on the Session Manager server.

Syntax

```
setup_snmp  [community_string ] [-d ]
```

(no argument) **setup_snmp** with no arguments will enable SNMP and set the read-only community string to **public**

community_string **setup_snmp *community_string*** will enable SNMP and set the read-only community string to the value specified by ***community_string***

-d **setup_snmp -d** will disable SNMP

Description

The **setup_snmp** command sets up a basic SNMP agent on the Session Manager server. **setup_snmp** can be passed an optional community string and configures the V1/V2c agent with that string. If no community string is passed, a default value of **public** is used. Once the agent is configured, ANY network management system will be able to query the Session

Manager SNMP agent and view the information in certain MIB groups which are part of the standard Linux SNMP agent.

Chapter 8: Maintenance functions

Session Manager maintenance functions

The maintenance functions for Session Manager include the following:

- backing up data
- restoring backed up data
- shutting down the server
- rebooting the server

Backup and Restore

The backup and restore functions are executed on System Manager.

All of the configuration data that is needed to run the entire system, System Manager, and all of the Session Manager instances is kept centrally on the System Manager. This means one backup contains all of the data for the entire system. Individual backups of the Session Manager instances are not needed.

Backup And Restore field descriptions

Use this page to view the details of backup files.

Name	Description
File Name	Name of the backup file.
Path	Path of the backup file.
Status	Status of the backup. The values are: • SUCCESS • FAILED
Backup Time	Time of backup.

Name	Description
Backup Mode	The mode defines whether the backup is manual or automatic.
Backup Type	The type defines whether the backup is a local or remote backup.
User	The user who has performed the backup.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Schedule Backup field descriptions

Use this page to schedule a job for backup of data by specifying the date and time of running the job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In the case of a recurring job, the field also displays the time interval of recurrence. The options are: • Execute task one time only. • Task are repeated.

Name	Description
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	Closes the Schedule Backup page and takes you back to the Backup Restore page.

Creating backup of application data

Procedure

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **System Manager Data** > **Backup and Restore**.
3. Click **Backup**.
4. On the Backup page, perform one of the following steps:
   - To back up data to a local drive, do the following:
     i. Click **Local** option.
     ii. In the **File name** field, enter the name of the backup file field that you want to create.
   - To back up data to a remote location, do the following:
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Now**.

Result

If the backup is successful, the Backup and Restore page displays a message Backup created successfully!!.

Scheduling a data backup

Procedure

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **System Manager Data** > **Backup and Restore**.
3. Click **Backup**.
4. On the Backup page, perform one of the following steps:
   - To schedule a local backup, perform the following steps:
     i. Click **Local** option.
     ii. In the **File name** field, enter the name of the backup file that you want to create.
   - To schedule a remote backup, perform the following steps:
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following: Job Name, Task Time, Recurrence and Range in the respective fields.
7. Click **Commit**.

Viewing list of backup files

Procedure

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore**.

Result

The Backup and Restore page displays the list of backup files.

Restoring a backup

Procedure

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **System Manager Data** > **Backup and Restore**.
3. Click **Restore**.
4. On the Restore page, perform one of the following steps:
   - To restore data from a local backup
     i. Click **Local** option.
     ii. Enter the back up file name in the **File name** field.
   - To restore data from a remote backup
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Restore**.

Result

After the successful restore operation, the user who initiated the restore is logged out of the System Manager console.

Backup data retention

Backup data retention is controlled by a maximum number of files rather than by time. When a new backup is initiated and the maximum number of files has been reached, the oldest backup file is removed in order to make room for the new backup file.

If you choose to perform the scheduled backup on the System Manager server, you need to delete older backup files from the system since the filename is dependent upon the scheduled job.

There are two ways to remove old backup files:

- automatically by changing the **Maximum Backup Files** value
- manually by using the **`smbackup`** command.

Changing the Maximum Backup Files value

About this task

The new value for **Maximum Backup Files** will take effect when the next backup is run.

Procedure

1. Select **Settings** > **Service Profile Management** > **System Manager 5.2** > **SMGR Element Manager** on the System Manager console.
2. Click the **Edit** button at the top right of the page.
3. In the **Maximum Backup Files** field, enter the number of backup files you wish to keep.
4. Click the **Commit** button to save the change.

Using the smbackup command to remove old backup files

About this task

The value for **`–mtime`** specifies how many days to keep the files. Files older than the specified value will be removed.

Procedure

To remove backup files older than 30 days, enter `find /home/smbackup –name '*.zip' –mtime +30 –exec rm –f {} \;`

Shut down/reboot the Session Manager server

Starting with Service Pack 1, the Session Manager host server can be powered down safely and remotely if needed for hardware servicing. The shutdown/reboot feature also provides a safer last-chance restart instead of pressing the power button if the system becomes unresponsive. This feature is available for root, craft, and cust users.

If the Session Manager is shut down, on-site personnel will be required to restart the system.

There are two ways to shutdown or reboot the system:

- Using the GUI
- Using the command line interface

Note:

It is *strongly* suggested that the Session Manager be placed in the Deny New Service state, and that you wait for all active calls to end before shutting down/rebooting the server. Active calls through the affected Session Manager will drop if it remains down too long. New calls will immediately use an alternate Session Manager (if available) once the affected Session Manager is placed in the Deny New Service state.

Using the GUI to shut down or reboot the server

Procedure

1. Select **Session Manager** > **System Status** > **System State Administration** on the System Manager console.
2. Select the Session Manager which needs to be shut down or rebooted.

   Note:

   Only one Session Manager can be shutdown or rebooted at a time.
3. Change the state of the Session Manager to **Deny New Service**.
4. Wait for all active calls to end before shutting down or rebooting the server.
5. Click on the **Shutdown System** button.
6. Select **Shutdown** or **Reboot** from the drop-down menu.
7. A confirmation screen is displayed. If the Session Manager is not in the **Deny New Service** state, an additional screen with the recommended action will be displayed.

Using the CLI to shutdown or reboot the server

About this task

If you have problems accessing System Manager, use the command line interface to shutdown or reboot the specific Session Manager using the following procedure:

Procedure

1. Login to the Session Manager using the **cust** login on a laptop.
2. Enter one of the following commands:
   - **`shutdownSM`** (to shut down the server)
   - **`rebootSM`** (to reboot the server)
3. If the Session Manager has been shut down, the confirmation screen will warn that on-site personnel will be required to restart the system.

Chapter 9: Data Retention

Data Retention on Session Manager

Configuration data is kept on the system forever. However, there are other types of data that accumulate and need to be purged from time to time to avoid filling up the disk. These types of data are:

- Log Data
- Soft-deleted RTS Records
- Alarm Data
- Backup Data

Data retention rules

Log, RTS, and alarm data files are removed by data retention policies. The number of days that this data is retained is specified by a value called the **Retention Interval**. Each day, any data that is older than the specified retention interval is purged from the system.

The Data Retention web page displays the list of retention rules and allows you to edit, update, or apply a rule. An example of a retention rule is LogPurgeRule. This rule sets the value for how long logging data files are retained. Each rule is applied automatically once a day to purge old data. However, a rule can be applied immediately by selecting a rule and clicking the **Apply** button.

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	Click the option button to select a data retention rule.

Name	Description
Rule Name	Name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	The number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.
Update	Updates the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Apply	Applies the selected rule.

Changing the Retention Interval Value

About this task

The Retention Interval Value determines how long log, RTS, and alarm data files remain in the system.

Procedure

1. On the System Manager Common Console, select **Settings > Data Retention** in the left navigation pane.
2. Select the rule you want to change.
3. Click on the **Edit** button.
4. Enter the desired number of days to retain the data in the **Retention Interval** field.
5. Click the **Update** button.

Chapter 10: Session Manager Data Replication Status

The Session Manager Data Replication Status page displays the status of downward data replication from the System Manager database (master) to the Session Manager local databases (replicas). It also allows you to run audit tests and reset the modification counters.

Database changes on the master database are continuously monitored and are sent to the replicas within seconds of being committed on the master.

The Data Replication system can repair itself using automatic connection recovery and replication audits. Replication audits keep the master and the replica databases synchronized if connection problems occur, if database resource problems occur, or after a system has been down for upgrading or recovery. On replicas, the audit process is performed every 15 minutes.

Data Replication Status field descriptions

The following Data Replication statistics are displayed for each Session Manager:

Field	Description
Records Currently in Database	Total number of records in each of the databases. The number of records in each replica database should match the number in the System Manager database.
Records Pending Update	For the master database column, this means that the database modifications (insert/update/delete) have occurred on the master database, but update messages for these modifications have not yet been sent to the replica databases. For the replica databases, this means that a replica database audit has determined that these records need to be updated in this replica database, but this replica database has not yet received and processed the associated messages from the master database to perform these modifications.

Field	Description
Modifications	Total number of database modifications (insert/update/delete operations) that have occurred in the respective databases.
Modifications Resulting from Audits	For the master database column, these are the number of database modifications that were sent as update messages to any of the replica databases in response to a replica audit. For the replica databases, these are the replica database modifications that were performed as a result of a database audit. This means that the replica database determined that it was out of synchronization with the master database and requested and received update messages from the master database..
Failed Modifications (replica only)	Number of database operations that have failed to be committed (insert, update, delete operations). This could be an error or it could be because the replication messages sent from the master to a replica database were received out of order, in which case, the failure is automatically recovered..
Failed Modifications Resulting from Audit (replica only)	Number of database operations that have failed to be committed (insert, update, delete operations) only for those modifications that were executed as a result of a replica database audit
Elapsed Time Since Last Update/Audit (Days H:M:S)	On the master database, this is the elapsed time since the last time audit requests were received or responded to. On the replica databases, this is the elapsed time since the last replica database audit was performed. On the replicas, the process is performed every 15 minutes.
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	Same as above, except that an audit found a database out of sync and updates were made to the replica database.
Last JMS Message Sent (master) / Received (replica)	Time comparison of the last message sent by the master and the last message received by the replica. If the difference is a few seconds or less, the replication links are healthy. If there is a difference of more than a few seconds between any of the send times and the receive times, a connection problems is indicated.

Field	Description
Last JMS Message Received (master) / Sent (replica)	Time comparison of the last message received by the master and the last message sent by the replica. If the difference is a few seconds or less, the replication links are healthy. If there is a difference of more than a few seconds between any of the send times and the receive times, a connection problems is indicated.
JMS Connection Status	Status of the underlying message transport system used by the data replication system. An OK status means that the message transport system works as intended. Any other status implies that there could be a problem sending messages from the master to the replica and from the replica to the master.
Test String Value	Current value of the test string in the master database. For the replica columns, this is the value of the test string in the respective database and should eventually match the master database test string value..
Test String Last Update Time	Time the test string was written to the database. This is an additional confirmation of the replication test success.

Master/Replica actions

The following actions can be performed on the Session Manager Downward Data Replication Status page:

- Refresh: refreshes the display for the System Manager and the administered Session Manager instances.
- Update on Master: updates the Test String Value in the System Manager database and runs a test to verify that the test string is replicated correctly to each Session Manager database. The Test String Value and Last Update Time should match across all columns within a refresh or two.
- Reset Modification Counters (All): resets the modification counters for System Manager and all of the Session Manager instances to zero. This can be used in combination with

on-demand audits to isolate replication problems to the System Manager or a particular Session Manager.

- Start Audit/Update (Selected): starts an update of the master database or runs an audit on both the master and replica databases on selected Session Managers.

  Selecting System Manager triggers an update cycle on the master database. The System Manager looks for any modifications made to the master database and sends updates to the replica databases if necessary. This process happens automatically every few seconds, so it is typically not necessary to do this on demand.

  Selecting a Session Manager triggers a replica database audit. If the audit determines that the replica database is out of sync with the master database, it will request updates from the master database. It may take more than one audit cycle to synchronize the databases due to the amount of data to be synchronized or if there are complex relationships between the data to be synchronized.

Related topics:

Updating to Master on page 56
Resetting the Modification Counters on page 57
Running an Audit on page 57

Updating to Master

Procedure

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Enter any desired string in the **New Master Test String Value** field.

   The **New Master Test String Value** can be any string containing up to 10 alphanumeric or special characters.
3. Click the **Update on Master** button.
4. Wait a few seconds, then click the **Refresh** button.
5. Verify that the Test String Value updates on the replicas within a refresh or two, and that the timestamp updates when the test string is updated.

Resetting the Modification Counters

Procedure

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Click the **Reset Modification Counters (All)** button.

Running an Audit

Procedure

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Select the System Manager or a Session Manager instance.
3. Click the **Start Audit (Selected)** button to begin the database audit of the selected System Manager or a Session Manager instance.

Chapter 11: Security Module Status

The Security Module Status page allows you to view the status and configuration of the security module for each administered Session Manager.

The Security Module Status page also allows you to perform certain actions on the security module such as synchronize the security module or assign a certificate authority.

The **Refresh** button refreshes the display for all of the administered Session Manager instances. This page does not automatically refresh.

The **Security Module Deployment** field displays the status of the security module deployed for the Session Manager (up or down).

Security Module Status field descriptions

The following security module statistics are displayed for each Session Manager:

Field	Description
Security Module Deployment	Status of the Security Module deployed for the Session Manager (up or down).
IP Address	IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance.
Network Mask	Network Mask of the security module. This value should match the network mask administered on the Session Manager instance form.
Default Gateway	Default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.
Interface Name	The Ethernet interface used by the security module for SIP traffic. This field is display-only and is not administrable.
Name Servers	DNS servers used by the security module. This field is for informational purposes and is not administrable.

Field	Description
DNS Search	DNS search string used by the security module. This field is for informational purposes and is not administrable.
Call Control PHB	The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic as it travels from the SM100 through the IP network. The default value of 46 indicates forwarding with the highest priority.
Speed & Duplex	Allows the configuring of the security module interface speed an duplex values. The drop-down menu contains a list of the valid values.
VLAN	The VLAN ID that the security module is associated with. This field should match the VLAN ID administered on the Session Manager instance form.
QOS	802.1q priority value (Layer 2 QoS) used by the security module. This field should match the QOS priority administered on the Session Manager instance form.
Certificate Used	The identity certificate being used by the security module for establishing TLS session.
Trusted hosts (expected/actual)	The **expected** value is the number of Trusted SIP Entities configured in the Network Routing Policy which have Entity Links to the Session Manager. The **actual** value is the number of Trusted SIP Entities currently configured on the security module. If these values do not match, then the **Synchronize** action should be performed.

Security Module Status actions

The following actions can be performed on a selected Session Manager:

- **Reset** – resets the security module for the selected Session Manager. An administrator may choose to reset the security module when a connection cannot be made to the security module.

Warning:

The Session Manager cannot process calls while the security module is being reset. Refer to *Administrating Avaya Aura™ Session Manager*, 03–603324 for details on how to disable the Session Manager prior to resetting the security module.

- **Synchronize** – verifies that the administered configuration matches the actual configuration stored on the security module. This action should be performed anytime the values in the security module statistics table do not match the administered data.
- **Security Module Certificate** - Session Manager provides the capability of switching the active certificate being used by the security module to the default certificate or the unique certificate issued for that instance by the System Manager CA. Please refer to *Administrating Avaya Aura™ Session Manager*, 03–603324 for more details about this operation. Additionally, refer to **Security Design** in *Administrating Avaya Aura™ Session Manager*, 03–603324 to understand the implications of doing this operation.

Investigating Security Module Deployment “Down” status

About this task

Possible causes for the Security Module Deployment status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.
- The security module may not have received its configuration information from System Manager. See the Data Replication Status screen for the Session Manager to make sure replication is working, since that is the primary reason the SM100 would not have downloaded its configuration information properly.
- There is a problem with the security module that needs attention.

Procedure

1. Select **Session Manager > System Status > Security Module Status** on the System Manager console.
2. Use the **Refresh** button to see the latest status.
3. If the status is still **Down**, synchronize the security module to trigger an update:
   a. Select the appropriate system from the System Name list.
   b. Select the **Synchronize Security Module** button.
   c. Select the **Refresh** button to see the latest status.
4. If the Deployment status is still **Down**, reset the security module:
   a. Select the appropriate system from the System Name list

b. Select the **Security Module Reset** Button.

Warning:

The Session Manager cannot process calls while the security module is being reset . Refer to System State Administration for details on how to disable the Session Manager prior to resetting the security module.

5. Select the **Refresh** button to see the latest status.

Chapter 12: Maintenance tests

Session Manager maintenance tests

The Maintenance Tests page allows you to perform functionality tests on the System Manager server and the administered Session Manager instances. These tests include testing the functionality of data replication and network connectivity to Session Manager instances, database functionality, and the security module of each Session Manager. The tests are run periodically by the system to monitor the health of system components. The same tests can also be executed on demand.

Tests are not run for a Session Manager if its state is set to **Management Disabled**.

Tests may fail if the server is down or not responding.

Running maintenance tests

About this task

The Maintenance Tests page allows you to run maintenance tests on the System Manager or any administered Session Manager in the enterprise.

Procedure

1. Select **Session Manager** > **System Tools** > **Maintenance Tests** on the System Manager Common Console.
2. Select System Manager or a Session Manager instance to test from the drop-down list.
   a. To run all of the tests, select **Execute All Tests**
   b. To perform only selected tests, select which tests should be run from the list and select **Execute Selected Tests**.

Maintenance Test descriptions

Test network connections to each Session Manager

This test only runs on the System Manager. It tests the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. Otherwise, the test fails. The server could be down or an upgrade/install is in progress. Check the log, then check Log and Alarm Event IDs for the appropriate troubleshooting action.

Test data replication to each Session Manager local database

This test only runs on the System Manager. It tests if replication is functioning properly by sending a test string to each administered Session Manager. The test string is saved by each Session Manager within its respective database. After a short wait, each Session Manager is queried for the test string value.

If the replication succeeds, the test passes. A failure indicates a possible JMS or secure connection problem. Refer to the Data Replication Status page for more information.

A similar test can be executed on the Data Replication Status page and specifying a custom test string.

The test is not run for a Session Manager if there is a JBoss connection problem or if the current state of the Session Manager is set to **Management Disabled**.

Test Call Processing status

This is a call processing sanity test. If call processing is working properly, the test passes. If the test fails, contact Avaya Technical Support.

Test Service Host status

This test asks for a list of service hosts and determines the running (up/down) status of each. The test passes if all of the hosts are up. The test fails if one or more of the hosts has an invalid status.

If the test fails, contact Avaya Technical Support.

Test Service Director Status

This test checks the status of the SIP A/S Service Director using a connection to SIP A/S. The test passes if the status of the service director is valid. If the test fails, contact Avaya Technical Support.

Test SIP A/S Management Server Status

This test checks the status of the SIP A/S Management Server using a connection to SIP A/S. The test passes if the status of the management server is valid or a particular SIP A/S service is running.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. It checks if the Security Access Link agent is running or not on the server. If the link is up and running, the test passes. Otherwise, if the test fails, contact Avaya Technical Support.

Test management link functionality

This test checks the administrative link to a Session Manager. If this test fails, administrative changes will not take effect on Session Manager. Otherwise, the test passes.

Test Security Module Status

Queries the basic status of the SM100 Security Module. If the query is successful, the test passes. Otherwise, it fails.

Test Postgres database sanity

This test runs on either System Manager or Session Manager. System Manager tests the sanity of the master database. Session Manager tests the sanity of its local instance database. A replication test from System Manager indirectly checks the sanity of each Session Manager

replica database. The test passes if the test is successful. If the test fails, contact Avaya Technical Support.

Chapter 13: SIP Entity Monitoring

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and minimize the call setup time due to SIP link failures. The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays will be reduced since calls will not be routed to the failed servers. The SIP Monitor will continue to monitor the failed SIP entity. When the proxy replies, SIP messages will again be routed over that link.

You can turn monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity will not be monitored by any instance.

You can also turn monitoring on or off for an entire instance. If monitoring is turned off, none of the SIP entities will be monitored by that instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on will be monitored.

The SIP entity being monitored should support the SIP OPTIONS method in order to be monitored.

SIP Monitoring can only report problems if the SM100 Security Module is functional.

SIP Monitoring setup is administered through the Network Routing Policy screens on the System Manager.

SIP Entity Link Monitoring Status Summary page field descriptions

Button	Description
Entity Link Status for All Session Manager Instances: Refresh	Refreshes the status of the entity links for all administered Session Manager instances. The status displays the following details:

Button	Description
	• Name of the Session Manager instance • Entity links for the Session Manager that are totally down out of the total number of entity links for the Session Manager • Entity links for the Session Manager that are partially down • SIP entities for which monitoring has not yet started (because it is still being initialized by the Session Manager) • SIP entities that are not monitored (because they are not administered to be monitored by the Session Manager) Clicking any of the Session Managers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from a Session Manager where at least one connection is currently down. **Note:** An entity link consists of one or more physical connections between a Session Manager and a SIP entity. If all of these connections are up, then the entity link status is “up”. If one or more connections are down, but there is at least one connection up, then the entity link status is “partially down”. If all the connections are down, the entity link status is “down”.
All Monitored SIP Entities: Refresh	Clicking any of the entities in the list opens the SIP Entity, Entity Link Connection Status page that displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Accessing the SIP Monitoring Status Summary page

About this task

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager and a SIP entity.

If all of these connections are up, then the entity link status is **up**. If one or more connections are down, but there is at least one connection up, then the link status is **partially down**. If all of the connections are down, the entity link status is **down**.

Procedure

1. Select **Session Manager** > **System Status** > **SIP Entity Monitoring** on the System Manager console.
2. The **SIP Entity Link Monitoring Status Summary**screen displays the summary of SIP Entity Link monitoring status.

Chapter 14: SIP Tracing

Session Manager SIP Tracing

SIP Tracing allows tracing of SIP messages exchanged between the Session Manager server and remote SIP entities. SIP Tracing consists of two components:

- Tracer Configuration - defines the characteristics of messages to be traced for the capturing engine in the Security Module
- Trace Viewer - displays the captured SIP messages

You can use SIP message tracing to troubleshoot or monitor a selected Session Manager instance. SIP tracing logs incoming and outgoing SIP messages in the SM100 framework. SIP messages that are dropped by any of the SM100 components such as the SIP firewall are also logged by the SIP tracer.

You can trace all of the messages belonging to a user or Call ID for a call, or for a selected Session Manager instance.

Note:

It is necessary to add at least a **User Filter** or **Call Filter** when the **Max Message Count** is set in order for the SM100 to capture packets.

SIP Tracer Configuration

The SIP Tracer Configuration page allows you to configure tracing properties for each administered Session Manager. The output of the SIP Trace is viewable on the System Manager. Each time a new Tracer configuration is sent to a Session Manager, the existing Tracer configuration is overwritten.

The SIP tracing page is accessed by logging on to the System Manager console and selecting **Session Manager** > **System Tools** > **SIP Tracer Configuration**. You can filter messages by user and/or Call ID, or ignore filtering and trace all messages for a specified SIP entity.

The Tracer Configuration page contains four sections:

- **Tracer Configuration**: This section contains attributes which control the basic functionality of the SIP Message tracer. The check boxes allow you to enable or disable the attribute.
- **User Filter**: Filter messages based on the sending user, receiving user, or both.
- **Call Filter**: Filter messages based on the sending Call ID, receiving Call ID, or both.
- **Session Manager Network**: Lists the administered Session Manager instances on which to apply the filters.

Tracer Configuration page field descriptions

Name	Description
Enabled	SIP message tracing is enabled by default.
Dropped	SIP message tracing is enabled for calls dropped by the SIP firewall as well as by the ASSET proxy.
From Network to Security Module	SIP message tracing is enabled for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	SIP message tracing is enabled for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Local SIP messages originating from the Session Manager.
From Security Module to Server	Local SIP messages originating from the security module.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped checkbox is activated.

Button	Description
User Filter: New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
User Filter: Delete	Delete a selected user filter or filters.
Call Filter: New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.

Button	Description
Call Filter: Delete	Delete a selected call filter or filters.
Commit	Save the configuration changes.

Name	Description
User Filter: From	Filter SIP messages based on the user from whom the message is sent. Type the user string. For example, a rule to trace all messages from user “pqr”: to=”” from=”pqr” stop-count=50
User Filter: To	Filter SIP messages based on the user to whom the message is sent. Type the user string. For example, a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
User Filter: Source	Filter SIP messages based on the source address.
User Filter: Destination	Filter SIP messages based on the destination address.
User Filter: Max Message Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Call Filter: From	Filter SIP messages from a specific user. Call tracing identifies a call by capturing the Call ID from the first message that matches the From filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL from user “pqr”: to=”” from=”pqr” request-uri=”” stop-count=50
Call Filter: To	Filter SIP messages based on the user to whom the message is sent. Call tracing identifies a call by capturing the Call ID from the first message that matches the To filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL to user “xyz”: to=”xyz” from=”” request-uri=”” stop-count=50

Name	Description
Call Filter: Source	Filter SIP messages based on the source address.
Call Filter: Destination	Filter SIP messages based on the destination address.
Call Filter: Max Call Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Call Filter: Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.111.
Session Manager Network: Name	Select one or more configured Session Managers for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Read** button is activated. Click this button to retrieve the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page. After displaying the configuration, Session Manager closes the display so that no older configuration data is displayed.

Configuring SIP tracing

Procedure

1. Select **Session Manager** > **System Tools** > **SIP Tracer Configuration** on the System Manager console.
2. Enable/disable the configuration attributes in the **Tracer Configuration** section of the page.
3. Set a user filter if desired (Filtering by user on page 75)
4. Set a call filter if desired (Filtering by Call ID on page 75)
5. Delete a filter if desired (Deleting a filter on page 76)
6. Under the **Session Manager Network** section, select one or more of the administered Session Manager on which the filters, if any, should be used.
7. Click the **Commit** button.

If filters were selected, they will be applied to the selected Session Managers. Any previous filter configurations will be overwritten.

Note:

It is necessary to add at least a **User Filter** or **Call Filter** when the **Max Message Count** is set in order for the SM100 to capture packets.

Filtering by user

About this task

You can define up to three separate user filters. The format for a valid sender/receiver is `sip:`*`1234`*`@`*`xyz`*`.com`, where*1234* is the user and *xyz* is the domain. An empty value in the **From** and **To** fields means that every message should match.

Procedure

1. Select **Session Manager** > **System Tools** > **SIP Tracer Configuration** on the System Manager console.
2. Navigate to the **User Filter** section.
3. To create a new filter, click **New**.
4. In the **From** field, enter the user from whom the message is sent (if applicable)
5. In the **To** field, enter the user to whom the message is sent (if applicable)
6. In the **Max Message Count** field, enter the maximum number of messages that should be traced which match the filter.

   Note:

   It is necessary to add at least a **User Filter** or **Call Filter** when the **Max Message Count** is set in order for the SM100 to capture packets.
7. Select the filter(s) to apply (checkbox)

Filtering by Call ID

About this task

You can define up to three separate call filters. An example of a valid Request URI format is `.@123.456.789.123`

Procedure

1. Select **Session Manager** > **System Tools** > **SIP Tracer Configuration** on the System Manager console.
2. Navigate to the **Call Filter** section.
3. To create a new filter , click **New**.
4. In the **From** field, enter the user from whom the message is sent (if applicable)
5. In the **To** field, enter the user to whom the message is sent (if applicable)
6. In the **Max Message Count** field, enter the maximum number of messages that should be traced which match the filter.

   Note:

   It is necessary to add at least a **User Filter** or **Call Filter** when the **Max Message Count** is set in order for the SM100 to capture packets.
7. Select the filter(s) to apply (checkbox).

Deleting a filter

Procedure

1. Select **Session Manager** > **System Tools** > **Tracer Configuration** on the System Manager console.
2. Under the User Filter and/or Call Filter sections, check the box next to the filter(s) you wish to delete.
3. Click **Delete**.

SIP Trace Viewer

Trace Viewer displays SIP message trace logs based on the filters that were configured. You can view these trace logs for a range of hours or days and for selected Session Manager instances.

Note:

“Records retrieved” versus displayed items: Within the left corner of the Trace Viewer page, the number of listed trace messages is displayed. Due to system performance, not all trace messages which match the filter criteria may be displayed. In this case, the value of “Records retrieved” will be greater than the displayed Items value. It is suggested that the filter criteria

be changed to ensure that no relevant trace messages are missing within the Trace Viewer list.

Trace viewer output

The output on the Trace Viewer page displays the following information.

Name	Description
Details	Clicking on **Show** allows you to see the complete message.
Time	Time at which the trace record was written.
Tracing Entity	Name of the Session Manager which logged the trace.
From	URI from where the traced SIP message originated.
Action	The Request/Response Action of the traced SIP message (e.g., INVITE, ACK). An arrow indicates the direction of the action (e.g., --INVITE->, <-By--).
To	URI to which the traced SIP message was sent.
Protocol	Protocol which was used by the traced SIP message such as TCP, UDP, TLS.
Call ID	Call ID of the traced SIP message.

Trace viewer buttons

The **Trace Viewer** button at the bottom of the Trace Viewer page is a toggle button. When this button is in the **Show** state, the following buttons appear.

Name	Description
Dialog Filter	This button is enabled if at least one table entry is selected. Trace messages are displayed which are related to the same dialog.
Cancel	This button is enabled if a Dialog Filter is active. Selecting this button will cancel the Dialog Filter and display the original Trace Viewer page.
Hide/Show dropped message	This is a toggle button. **Hide dropped messages** will not display any dropped messages, thereby reducing the number of messages displayed. **Show dropped messages** will display all messages.
More Actions	This button is available only if Session Manager is running Service Pack 1 or greater. It is active only if one or more trace records are listed. The retrieved Trace

Name	Description
	Viewer list can be saved to a file on the client side. The **Hide/Show dropped messages** and **Dialog Filter** functions are operational for the exported file but the GUI filters and sorting operations are not.

Trace viewer file options

There are two options under the **More Actions** drop-down menu:

- **Export Trace Viewer Overview:** A tab-separated plain text file is created with all of the overview columns which appear on the Trace Viewer screen. The file can be displayed with a text editor such as Wordpad or a tabulator editor such as Excel.
- **Export Trace Viewer Details:** A plain text file is created with the details of the Trace Viewer records.

When you select one of the export options, you can:

- open the Trace Viewer list with an editor
- save the Trace Viewer list to a file
- perform the open or save function automatically for files from now on. This option appears only if you are using Mozilla Firefox as your browser. If you are using Internet Explorer, this option does not appear.

Viewing trace logs

About this task

Logs can be filtered to display only those logs within a certain time range. Due to the Trace Configuration filter options, trace records may be shown multiple times.

Procedure

1. Select **Session Manager** > **System Tools** > **SIP Trace Viewer** on the System Manager Common Console.
2. To filter trace logs for a range of hours or days, click on **Filter** and enter or select the date, time, and time zone information under the From and To areas.

   This filter criteria will cause only those logs with a time stamp between the From and To values to be displayed.

3. Select one or more Session Manager instances for which you wish to see the trace logs.
4. Click **Commit** to generate the trace output.

Chapter 15: Call Routing Test

Call Routing Test for Session Manager

The Call Routing Test provides verification of System Manager administration for routing a calling party URI to a called party URI.

Use this test to verify that you have administered the system as intended before placing it into service or to get feedback on why a certain type of call is not being routed as expected. No real SIP messages are sent during this test.

This test displays the routing decision process as it uses the SIP routing algorithms. It uses administration from the following forms:

- **Network Routing Policy** > **Adaptations**, **Dial Patterns**, **Entity Links**,**Locations**,**Routing Policies**,**SIP Domains**, **SIP Entities**, **Time Ranges**
- **Session Manager** > **Session Manager Administration**

After the test has been executed, two headings with information about the test are displayed: **Routing Decisions** and **Routing Decision Process**.

The **Routing Decisions** output contains one line per destination choice (there will be more than one line if there are alternate routing choices; the output will appear in the order that destinations are attempted). Note that each line tells you not only where the INVITE would be routed, but also what the adapted digits and domain would be.

The **Routing Decision Process** information contains details about how the Routing Decisions were made.

Call Routing Test page field descriptions

Name	Description
Calling Party URI	The SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. You can also specify a full URI such as sip: 5555555@domain.com:

Name	Description
	5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Calling Party Address	The IP address or host name from which the INVITE is received. For routing, this is the IP address of a SIP Entity. You can enter any IP address that you require, but make sure that it is recognized by Session Manager. If it is not, Session Manager considers it to have come from a non-trusted host and rejects it.
Called Party URI	The SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. You can also specify a full URI such as sip: 5555555@domain.com: 5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Session Manager Listen Port	The port on which the called Session Manager Instance receives the INVITE.
Day of Week	Day of the week. This is used for testing time of the day routing.
Time (UTC)	Time. This is used for testing time of the day based routing.
Transport Protocol	Protocol used for transportation of the call. This is used in testing the routing based on NRP entity links.
Called Session Manager Instance	The Session Manager instance that receives the INVITE sent for testing routing. This is used in testing the routing based on NRP entity links.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The Routing Decisions box displays the result of the routing test. This result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice and the lines are in the same order that the test attempted the destinations.

Button	Description
	Each line displays not only where the INVITE would be routed, but also what the adapted digits and domain would be. The Routing Decision Process box contains details about how Session Manager made the routing decisions. This gives you a tool to check your routing algorithms.

Setting up a Call Routing Test

Procedure

1. Select **Session Manager** > **System Tools** > **Call Routing Test**on the System Manager console.
2. Enter information for a SIP INVITE message for both **Calling** and **Called Party URIs**
3. Click **Execute Test**.

Call Routing Test results

The test passes if the following two conditions are met:

- **Routing Decisions** displays data similar to the following: `< sip: 12345@MyOtherCompany.com > to SIP Entity 'CalledPArtySIPentity' port 'MyPortNumber' using TCP/TLS/UDP`
- **Routing Decisions Process** displays data similar to the following:

```
NRP Sip entities: Originating SIP Entity is "SIP Entity Name"
Using digits < 12345 > and host < MyOtherCompany.com > for routing.
NRP Dial Patterns: No matches for digits < 12345 > and domain <
MyOtherCompany.com >
NRP Dial Patterns: No matches for digits < 12345 > and domain < null >
NRP Dial Patterns: No matches found for the originator's location. Trying again
using NRP Dial Patterns that specify -ALL- locations.
NRP Dial Patterns: No matches for digits < 12345 > and domain <
MyOtherCompany.com >
NRP Dial Patterns: Found a Dial Pattern match for digits < 12345 > and domain
< null >.
Ranked destination NRP Sip Entities: 'CalledPartySIPentity'
Removing disabled routes.
Ranked destination NRP Sip Entities: 'CalledPartySIPentity'
Adapting and proxying to SIP Entity 'CalledPartySIPentity'
NRP Adaptations: Doing ingress adaptation.
```

```
NRP Adaptations: Changed P-Asserted-Identity header to sip: 67890@MyCompany.com
as part of adaptation.
NRP Adaptations: Doing egress adaptation.
Routing < sip: 12345@MyCompany.com > to SIP entity 'CalledPartySIPentity'
port 'MyportNumber' using TCP/TLS/UDP.
```

Note:

Calls with multiple possible destinations will display multiple rows. Route-through scenarios will include route-through information.

Troubleshooting a Call Route Test failure

About this task

The test failed if:

- `No data to display` appears under **Routing Decisions**.
- `Unable to resolve <IP Address for Calling Party Address> to a recognized entity` appears under **Routing Decisions Process**.

These messages indicate that System Manager could not successfully route the call using the information that was entered to execute the test.

Procedure

1. Verify that all of the information was entered on the Call Route Test page according to the exact format as listed in the Call Route Test field description table
2. Retry the test.
3. If the test still fails, verify the administration associated with the Calling Party and Called Party URIs.

Chapter 16: S8510 Field replaceable hardware

This chapter describes the procedures for replacing the field replaceable hardware on the Avaya S8510 server. The field replaceable units (FRUs) are:

- S8510 server
- Hard disk drives
- SM100 Security Module card
- Memory Modules
- Power Supplies

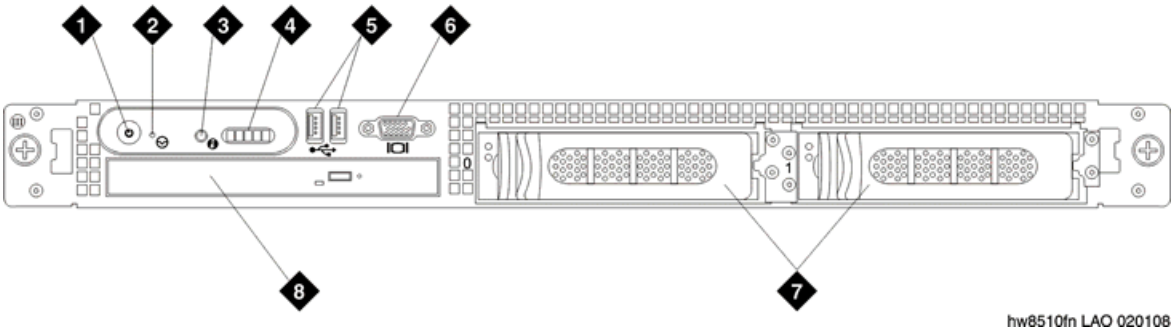
Replacing the S8510 Server

Procedure

1. On the System Manager console, select **Session Manager** > **System State Administration**
2. Click the **Shutdown System** button for the server that is to be replaced. If for some reason this does not work, the server can be hard powered down by pressing in the power button on the front panel for 5 seconds.
3. Unplug and label the existing cabling to the server for the keyboard, mouse, monitor, Ethernet port 0, SM100 Ethernet port 0, and power.
4. Remove the server from the rack. See Removing the S8510 server from the rack on page 87
5. If the new server does not already have an SM100 card installed, remove the SM100 card from the failed server and insert it into the same slot in the new server. See Replacing the SM100 Security Module on page 92
6. Install the rails on the new server. See Attaching rails to the server on page 88
7. Install the new server in the rack. See Installing the server in the rack on page 88
8. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.

9. Boot the server with the Session Manager Kickstart DVD to load the operating system.
10. Once the server ejects the DVD and reboots, insert the Session Manager software CD into the CD drive.
11. Login as sroot on the console (KVM)
12. Place a looparound network cable between the eth0 port on the Session Manager server to the port 0 on the SM100 card that is plugged into the server. This will be used to execute a sanity test of the SM100 card during the installation process.
13. Execute the following commands to mount the CD and install the Session Manager software in a factory configuration:
    a. # mount /cdrom
    b. # cd /cdrom
    c. # bash install.sh --factory
14. When the installation and looparound test complete, shut down the server with the following command: **`# shutdown –f now`**
15. After the server has shut down, re-connect the original network cables to the eth0 on the Session Manager server and to port 0 of the SM100 card.
16. Power up the Session Manager server.
17. When the server has finished booting, log into the server as root or cust.
18. Enter the command **`SMnetSetup`** to configure the server for the local network.

Front view of S8510 Server

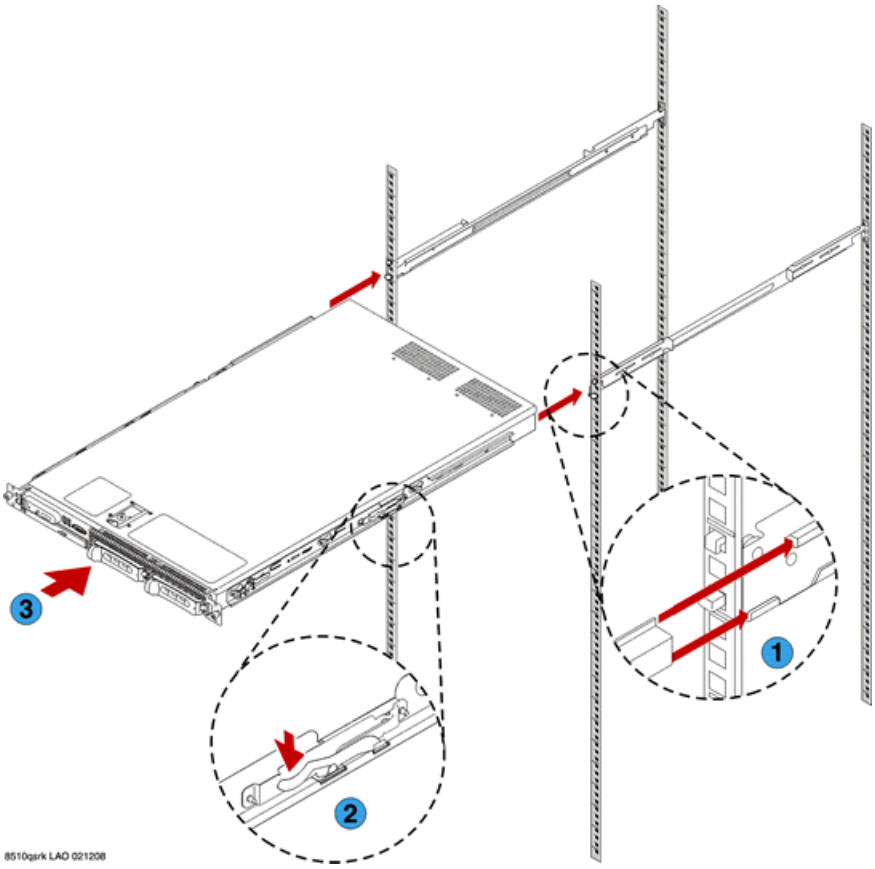


1	Power-on LED
2	NMI (Non-Maskable Interrupt) button (disabled)
3	System ID button (used to locate equipment within the rack)

4	LCD display (System ID, status information, system error messages)
5	USB ports
6	Video connector
7	Hard disk drives
8	DVD/CD drive

Removing the S8510 server from the rack

About this task

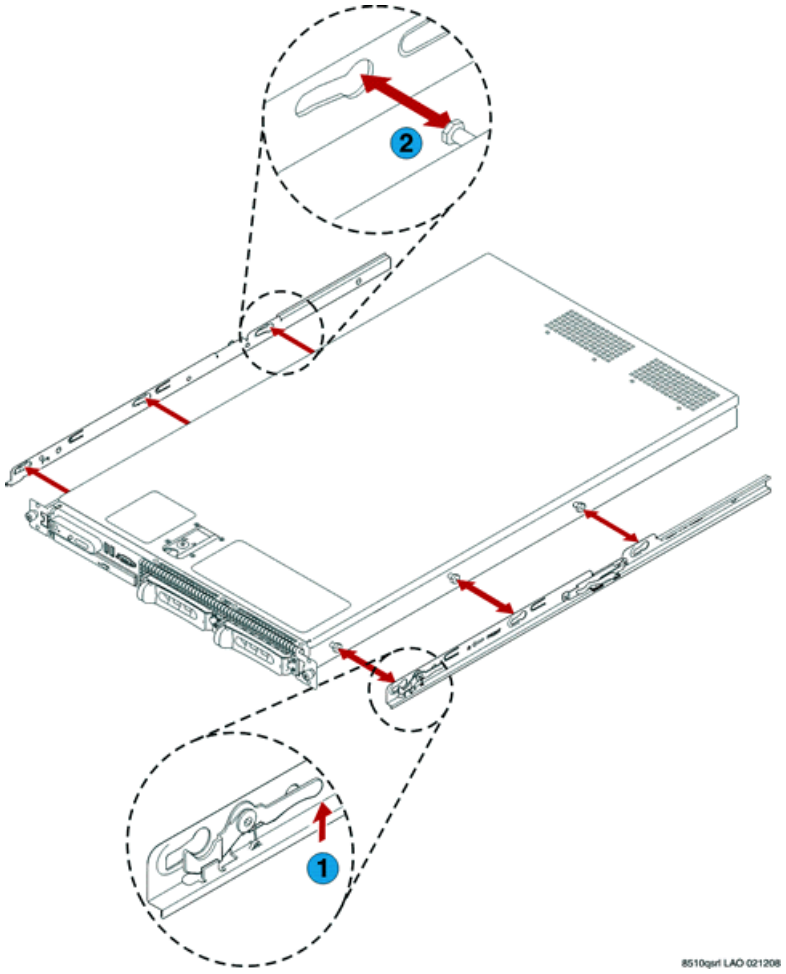


Procedure

1. Loosen the captive screws on both sides of the server (Figure 1).
2. Slide the server clear of the rails (Figure 2).
3. Release the rail lock by pushing the lever in as you slide the server out of the rack (Figure 3).

Attaching rails to the server

Procedure

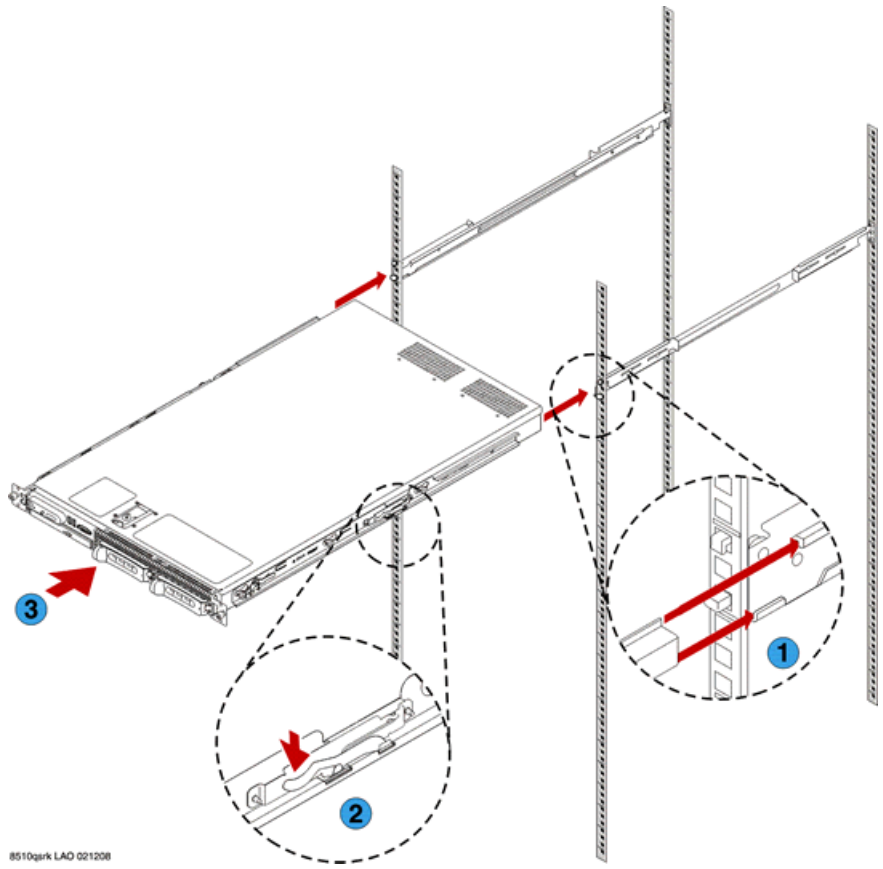


Installing the server in the rack

Before you begin

The rails must be attached to the server and the rack before installing the server in the rack. If the server is being installed in a cabinet, remove the doors, following the cabinet manufacturer's instructions.

Procedure



Next steps

If the server is being installed in a cabinet, reattach the doors, following the cabinet manufacturer's instructions.

Hard Disk Drive replacement

The Hard Disk Drive is monitored by capability built into the hard disk drive unit. Some hard disk drive problems do not occur suddenly. They are a result of a gradual degradation of components over time.

The hard drives are mirrored for speed and reliability and are hot-swappable (you do not need to power down the server to replace either drive). However, you cannot remove both drives at the same time.

Also, you should NOT remove the healthy, active hard drive. If you inadvertently remove the active hard drive, you *cannot* plug it back in. See Replacing an S8510 hard drive on page 90 for the procedures if the active hard drive has been removed.

Required equipment to replace a Hard Disk Drive

The following equipment is required to replace a Hard Disk Drive:

- S8510 replacement Hard Disk Drive
- Electrostatic wrist ground strap and mat
- Key to server keylock on front bezel

Hard Disk Drive LED status indicators

The following table describes the meaning of the LED colors and patterns for the Hard Disk Drives.

Drive status LED	Description
Off	Drive is ready for insertion or removal
Flashes green, amber, off	Drive is failing
Flashes amber four times per second	Drive has failed
Flashes green slowly	Drive is rebuilding
Steady green	Drive is online
Flashes green 3 seconds, amber 3 seconds, off 6 seconds	The rebuild aborted

Replacing an S8510 hard drive

Procedure

1. Select **Settings** > **Backup and Restore** on the System Manager console.
2. Click **Backup** to backup data from the hard disk drive.
3. Attach an antistatic wrist ground strap to your wrist.
4. Remove the front bezel and cover to access the hard drives.
5. Identify the defective hard drive by checking the status of the LEDs on the hard drives.

See Hard Disk Drive LED status indicators on page 90 for the meaning of the LED colors and patterns.

6. Remove the defective drive:
   a. Pinch together the two tabs of the drive carrier release handle.
   b. Open the carrier release handle.
   c. Wait about 10 seconds to allow the internal mechanism to stop the read/write heads so that the drive can be handled safely.
   d. Pull the hard drive out of the slot.
   e. Set the hard drive on an antistatic mat.
7. If the active hard drive was removed inadvertently, do the following:
   a. Cleanly power down the server at an appropriate time.
   b. Re-insert the active hard drive in its original slot.
   c. If the bad drive is still installed, remove the bad drive from the slot and set it aside.
   d. Power up the server with only the healthy drive present.
   e. Make sure the server comes up and is operating normally.
8. Insert the replacement hard drive in the slot and push it in until it is seated.
9. Close the hard drive carrier handle to lock the hard drive in place.
10. Replace the front bezel and cover.
11. Check the LED of the hard disk drive which was replaced.

    The LED should be flashing green slowly. It will take approximately 80 minutes for the hard disk drive to rebuild.
12. Return the defective hard drive.

SM100 Replacement on the Avaya S8510 Server

Required equipment to replace the SM100 Security Module

To replace an SM100 Security Module, you will need the following:

- Replacement SM100 card
- #2 Phillips (cross-point) screwdriver

- Electrostatic wrist ground strap and mat
- Key to front bezel

Replacing the SM100 Security Module

Procedure

1. Power down the S8510 server by pressing the power button on the front panel.
2. Wait until the server has been powered down and the power-on indicator light is off.
3. Label and disconnect the power cords from the power supplies at the back of the server.
4. Label and disconnect the LAN connection from the Ethernet port on the SM100 at the back of the server.
5. Ensure that all cables are labeled and disconnected from the server.

   Caution:

   Ensure that power is completely removed from the server. *Power cords must be detached from the power supplies.*
6. Loosen the captive screws on both sides of the server.

   Refer to #1 in Removing the S8510 server from the rack on page 87.
7. Slide the server clear of the rails.

   Refer to #2 in Removing the S8510 server from the rack on page 87
8. Release the rail lock by pushing the lever in as you slide the server out of the rack.

   Refer to #3 in Removing the S8510 server from the rack on page 87.
9. Use a #2 Phillips (cross-point) screwdriver to turn the latch release lock counter-clockwise to the unlocked position.

   Refer to #1 in Removing the cover of the S8510 Server on page 94.
10. Lift the latch up to unlock.

    Refer to #2 in Removing the cover of the S8510 Server on page 94.
11. Lift the cover back, then lift it straight up to remove. Set it aside.

    Refer to #3 in Removing the cover of the S8510 Server on page 94.
12. The SM100 security module resides in a PCI expansion card riser at the rear of the S8510 server.

    Electrostatic alert:

Take precautions against electrostatic discharge. Wear a wrist strap connected to an approved ground.

13. Lift the release latches on the PCI expansion card riser.

    Refer to #1 in Removing the SM100 card on page 95.

14. Remove the defective SM100 card by pulling it gently out of the expansion slot in the riser assembly.

    Refer to #2 in Removing the SM100 card on page 95.

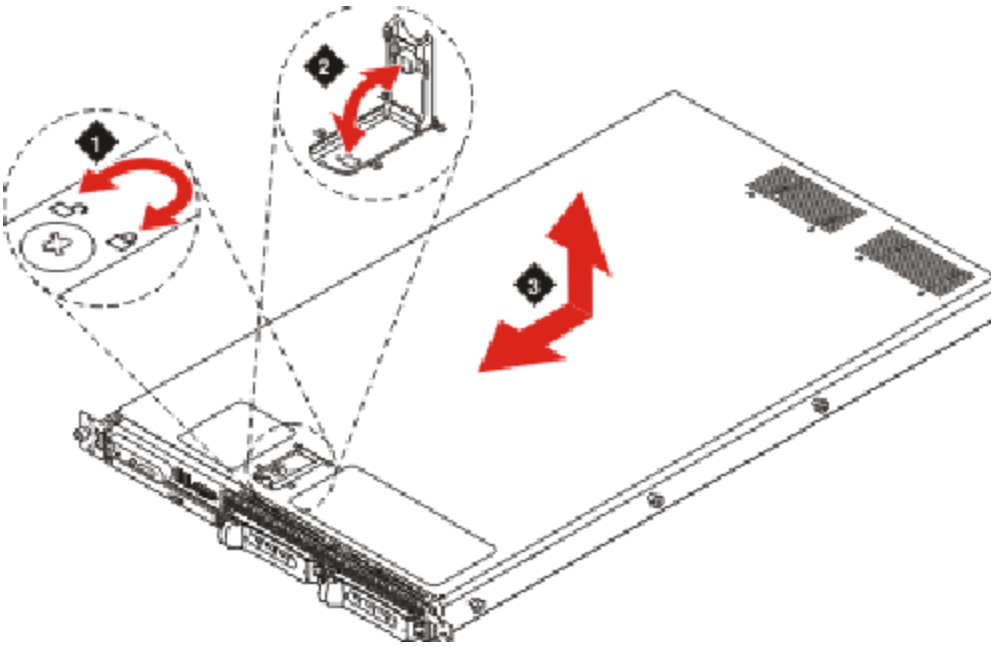
15. Carefully grasp the replacement SM100 card by the outer edges and align it with the opening on the PCI expansion slot riser assembly.
16. Insert the new SM100 card firmly into the expansion slot.

    Make sure it is completely seated.

17. Press the PCI expansion card riser release latches to secure the SM100 card and the riser assembly.
18. Ensure that any internal cables are clear of the server cover before placing the covert on the server.
19. Place the cover on top of the server, aligning it with the J hooks on the sides.
20. Slide the cover forward.
21. Push the latch down to lock.
22. Rotate the latch release lock clockwise to secure the cover.
23. Install the server onto the side rails in the rack.
24. Reconnect the Ethernet cable to the dual NIC at the back of the server.
25. Reconnect the LAN connection (if used) from the Ethernet port on the SM100 at the back of the server.
26. Reconnect the power cords to the power supply(ies) at the back of the server.
27. Push the server completely into the rack.
28. Secure the server into place with the two captive screws on both sides of the server.
29. Power up the server by pressing the power button on the front of the server.
30. Place the defective equipment in the protective packaging that accompanied the replacement part(s).
31. Return the defective equipment to Avaya using the procedures established for your region.

Removing the cover of the S8510 Server

About this task

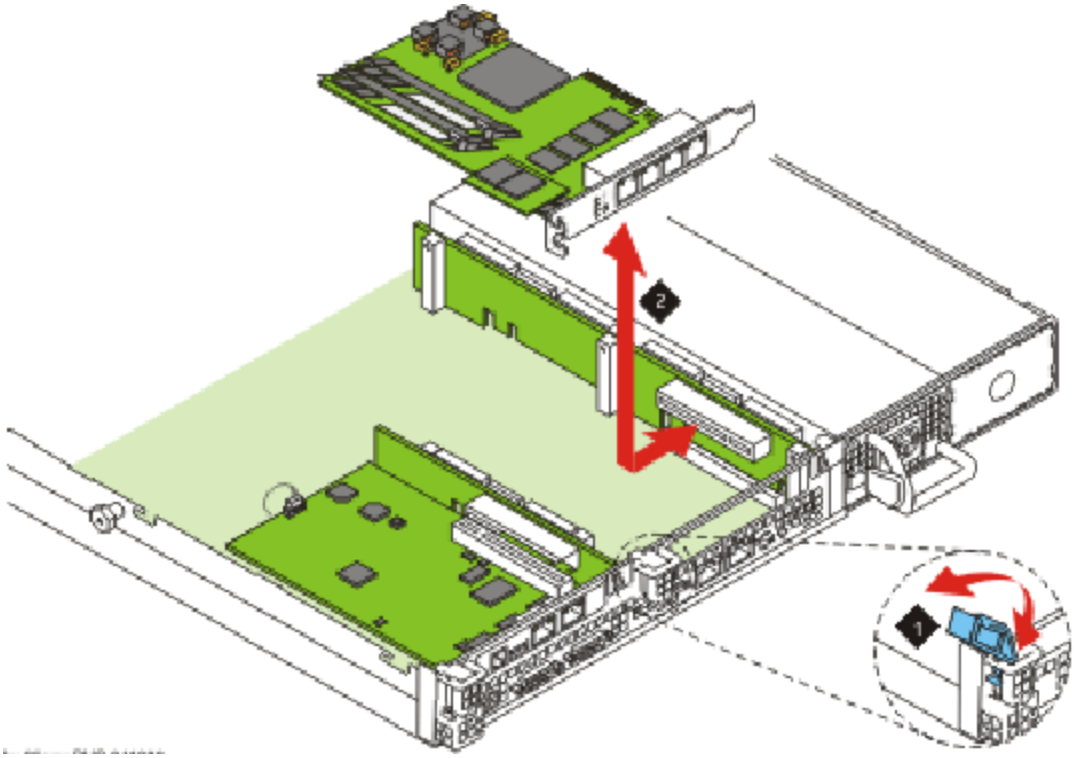


Procedure

1. Turn the latch release lock counter-clockwise to the unlock position using a Phillips screwdriver (Figure 1).
2. Lift the latch up to unlock (Figure 2).
3. Slide the cover back and lift straight up to remove (Figure 3).

Removing the SM100 card

About this task



Procedure

1. Press the release latches on the PCI expansion card riser.
2. Gently pull the SM100 card out of the expansion slot.

Memory Module replacement on the Avaya S8510 Server

Required equipment to replace memory modules

- Replacement memory module
- #2 Phillips (cross-point) screwdriver

- Electrostatic wrist ground strap and mat
- Key to front bezel

Replacing the memory modules

Procedure

1. Power down the S8510 server by pressing the power button on the front panel.
2. Wait until the server has been powered down and the power-on indicator light is off.
3. Label and disconnect the power cords from the power supplies at the back of the server.
4. Label and disconnect the LAN connection from the Ethernet port on the SM100 at the back of the server.
5. Ensure that all cables are labeled and disconnected from the server.

   Caution:

   Ensure that power is completely removed from the server. *Power cords must be detached from the power supplies.*
6. Loosen the captive screws on both sides of the server.

   Refer to #1 in Removing the S8510 server from the rack on page 87.
7. Slide the server clear of the rails.

   Refer to #2 in Removing the S8510 server from the rack on page 87.
8. Release the rail lock by pushing the lever in as you slide the server out of the rack.

   Refer to #3 in Removing the S8510 server from the rack on page 87.
9. Use a #2 Phillips (cross-point) screwdriver to turn the latch release lock counter-clockwise to the unlocked position.

   Refer to #1 in Removing the cover of the S8510 Server on page 94.
10. Lift the latch up to unlock.

    Refer to #2 in Removing the cover of the S8510 Server on page 94.
11. Slide the cover back, lift it straight up to remove, then set it aside.

    Refer to #3 in Removing the cover of the S8510 Server on page 94.
12. Remove the protective cover over the memory modules.
13. Remove the defective pair of memory modules.
14. Insert the new memory modules.
15. Replace the protective memory module cover.

16. Ensure that any internal cables are clear of the cover before replacing it on the server.
17. Place the cover on top of the server, aligning it with the J hooks on the sides.
18. Slide the cover forward.
19. Push the latch down to lock.
20. Rotate the latch release lock clockwise to secure the cover.
21. Install the server onto the side rails in the rack.
22. Reconnect the Ethernet cable to the dual NIC at the back of the server.
23. Reconnect the LAN connection (if used) from the Ethernet port on the SM100 at the back of the server.
24. Reconnect the power cords to the power supply at the back of the server.
25. Push the server completely into the rack and secure into place with the two captive screws on both sides of the server
26. Power up the server by pressing the power button on the front of the server.
27. Place the defective equipment in the protective packaging that accompanied the replacement part(s).
28. Return the defective equipment to Avaya using the procedures established for your region.

Replacing a power supply on the S8510 Server

Before you begin

Before replacing a power supply, make sure that the power cord is connected and plugged into a non-switched outlet. The problem may be the connection, not the power supply.

About this task

The power supplies are hot-swappable. You do not need to power down the server.

Procedure

1. Open the cable management arm, if present, to access the rear panel.
2. Identify the defective power supply by looking for the power supply fault indicator (middle indicator on the power supply).
3. Disconnect the power cord of the defective power supply from the power source.
4. Disconnect the power cord to the defective power supply.

5. With your thumb, press the release (orange) tab and the black handle together and pull out the power supply.

   Set it aside. To reduce the risk of personal injury from hot surfaces, allow the power supply to cool before touching it.
6. Insert the new power supply into the slot.
7. Ensure that the tab is locked into place and the power supply is securely seated in the slot.
8. Connect the power cord to the power supply.
9. Route the power cord through the cable management arm or power cord anchor, if present.
10. Close the cable management arm, if present.
11. Connect the power cord to the power source.
12. Make sure that the power supply LED is green.
13. Return the defective power supply.

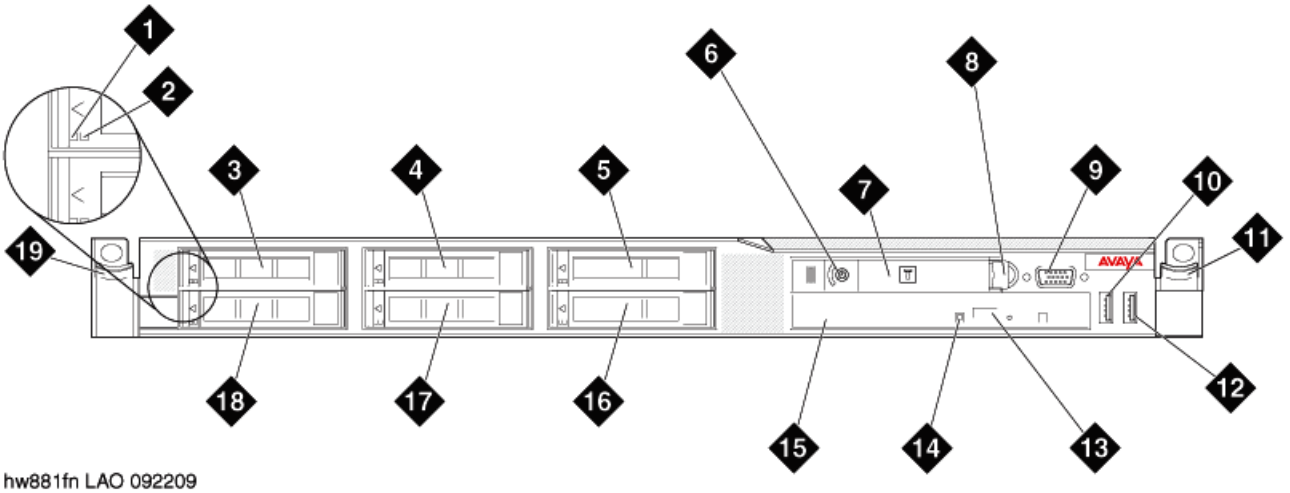
Chapter 17: S8800 Field replaceable units

S8800 Field replaceable hardware

This chapter describes the procedures for replacing the field replaceable hardware on the Avaya S8800 server. The field replaceable units (FRUs) are:

- Dual in-line Memory Modules (DIMMs)
- SM100 Security Module
- Hard Disk Drive
- Power Supply
- RAID Battery
- S8800 Server

Front of server



hw881fn LAO 092209

1	Hard disk drive activity LED (green)
2	Hard disk drive status LED (amber)

3	Drive bay 0
4	Drive bay 2
5	Drive bay 4
6	Power control button and LED
7	Operator information panel
8	Operator information panel release latch
9	Video connector
10	USB connector 1
11	Rack release latch
12	USB connector 2
13	DVD eject button
14	DVD drive activity LED
15	DVD drive
16	Drive bay 5
17	Drive bay 3
18	Drive bay 1
19	Rack release latch

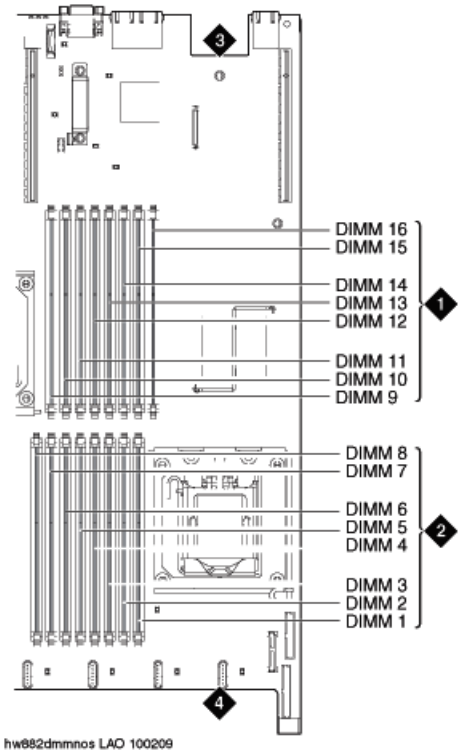
Replacing DIMMs

Sequence for populating DIMM connectors

When you install dual in-line memory modules (DIMMs), install them in the sequence shown in the following table to optimize system performance.

Installed microprocessors	DIMM connector population sequence
Microprocessor 1	Install the DIMMs in the following sequence: 3, 6, 8, 2, 5, 7, 1, 4
Microprocessor 2	Install the DIMMs in the following sequence: 11, 14, 16, 10, 13, 15, 9, 12

The following figure shows the numbering sequence of the DIMMs.



1	DIMMs for microprocessor 2
2	DIMMs for microprocessor 1
3	Back of server
4	Front of server

Removing the DIMM air baffle

About this task

You must remove the DIMM air baffle to replace a DIMM.

Caution:

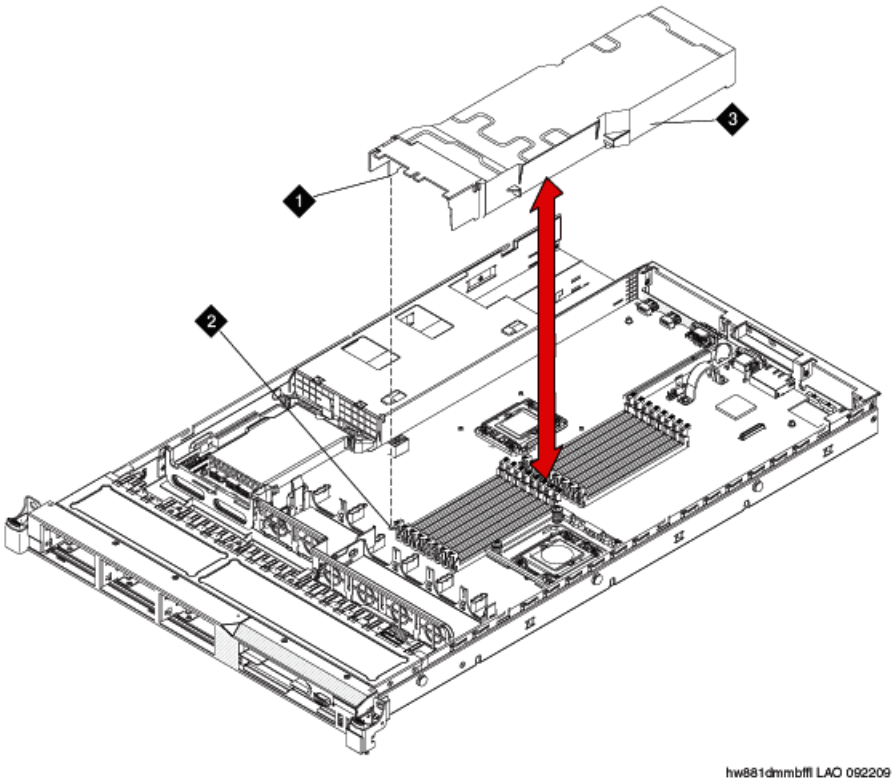
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Grasp the DIMM air baffle and lift the air baffle out of the server. Make sure that the pin comes out of the pin hole on the system board to the left of DIMM connector 8. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Removing a DIMM

About this task

Important:

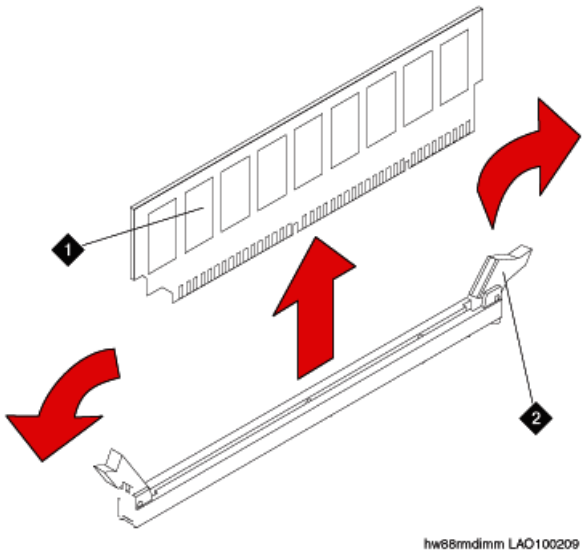
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

Carefully open the retaining clips on each end of the DIMM connector and remove the DIMM. See the following figure.

Important:

Open and close the clips gently to avoid breaking the retaining clips or damaging the DIMM connectors.



1	DIMM
2	Retaining clip

When you install or remove DIMMs, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing a DIMM

About this task

Important:

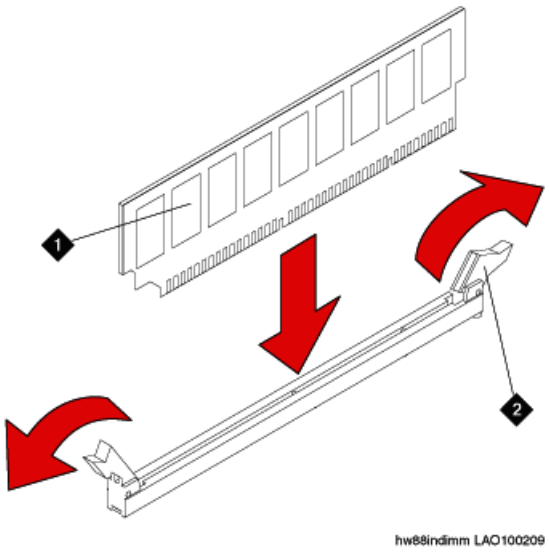
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Carefully open the retaining clips on each end of the DIMM connector. See the following figure.

   Important:

   Open and close the clips gently to avoid breaking the retaining clips or damaging the DIMM connectors.



1	DIMM
2	Retaining clip

2. Touch the static-protective package that contains the DIMM to any unpainted metal surface on the server.
3. Remove the DIMM from the package.
4. Turn the DIMM so that the DIMM keys align correctly with the connector.
5. Insert the DIMM into the connector by aligning the edges of the DIMM with the slots at the ends of the DIMM connector.

6. Firmly press the DIMM straight down into the connector by applying pressure on both ends of the DIMM simultaneously.
   The retaining clips snap into the locked position when the DIMM is firmly seated in the connector.

   Important:
   If there is a gap between the DIMM and the retaining clips, the DIMM has not been correctly inserted. Open the retaining clips, remove the DIMM, and then reinsert it.
7. Replace the air baffle over the DIMMs. Make sure all cables are out of the way.
8. Install the cover.
9. Reconnect the external cables and power cords.
10. Turn on the attached devices and the server.
    When you install or remove DIMMs, the server configuration information changes. When you restart the server, the system displays a message that indicates that the memory configuration has changed.

Installing the DIMM air baffle

About this task

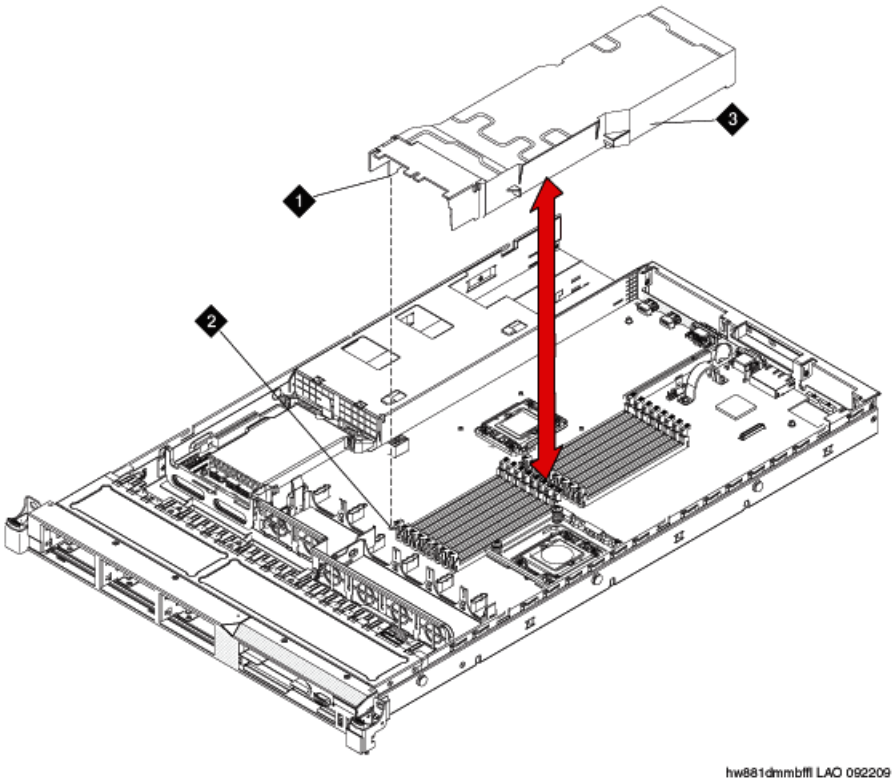
You must install the DIMM air baffle after you replace a DIMM.

Caution:
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

Important:
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Align the DIMM air baffle over the DIMMs so that the baffle pin on the left side of the air baffle aligns with the pin hole next to the DIMM connector on the system board. See the following figure.



1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

2. Lower the air baffle into place. Make sure that all cables are out of the way.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

SM100 Security Module replacement

Removing a PCI riser-card assembly

About this task

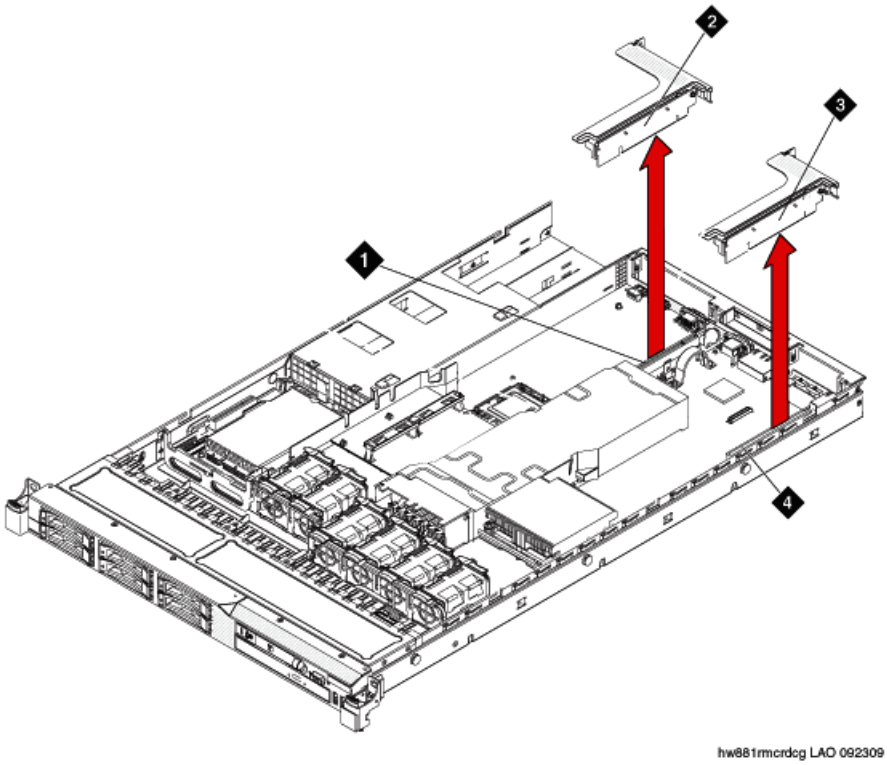
You must remove the PCI riser-card assembly to replace the PCIe card.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. If a card is installed in the PCI riser-card assembly, disconnect any cables that are connected to the card.
5. Grasp the blue tab near the rear of the PCI riser-card assembly from the rear and lift it out of the PCI riser-card slot on the system board. See the following figure.



1	PCI riser connector 2
2	PCI riser-card assembly (full-height, half-length PCIe cards)
3	PCI riser-card assembly (low profile PCIe cards)
4	PCI riser connector 1

6. Place the riser-card assembly on a flat, static-protective surface.

Next steps

Remove the PCIe card.

Removing a PCIe card

About this task

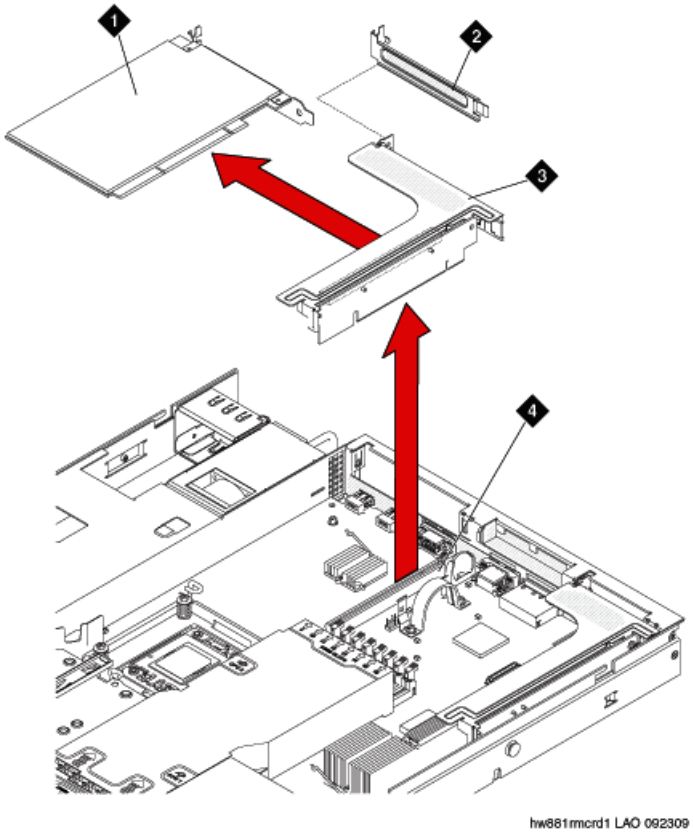
For Session Manager, the PCIe card is the SM100 Security Module.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

Carefully grasp the card by its top edge or upper corners, and pull the card from the PCI expansion slot. See the following figure.



1	PCIe card
2	Expansion slot cover
3	PCI riser-card assembly
4	PCI riser-card connector

Installing a PCIe card

About this task

For Session Manager, the PCIe card is the SM100 Security Module. It must be installed in PCI slot 2.

Caution:

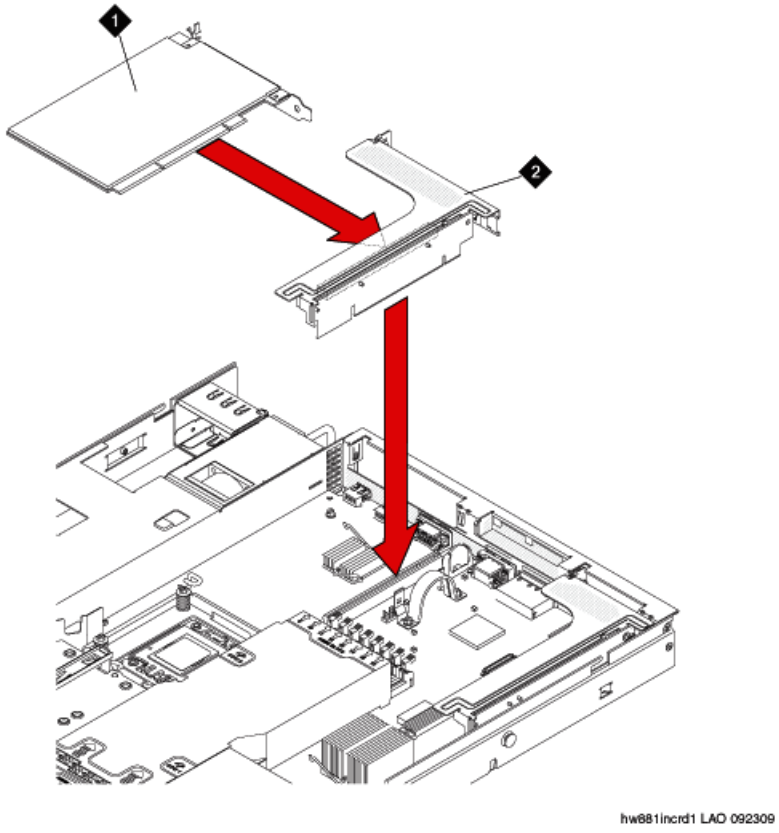
When you install a PCIe card, make sure that the card is correctly seated in the riser-card assembly and that the riser-card assembly is securely seated in the riser-card connector on the system board before you turn on the server. An incorrectly seated PCIe card might cause damage to the system board, the riser-card assembly, or the PCIe card.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Connect any required cables to the PCIe card. Follow the cabling instructions that came with the PCIe card. Route the card cables before you install the card.
2. Insert the PCIe card into the riser-card assembly, aligning the edge connector on the card with the connector on the riser-card assembly. Press the edge of the connector firmly into the riser-card assembly. Make sure that the PCIe card snaps into the riser-card assembly securely. See the following figure.



1	PCIe card
2	PCI riser-card assembly

3. Install the riser-card assembly in the server.
4. Perform any configuration tasks that are required for the PCIe card.
5. Install the cover.
6. Reconnect the external cables and power cords.
7. Turn on the attached devices and the server.

Installing a PCI riser-card assembly

Before you begin

Reinstall any PCIe cards and reconnect any internal cables that you removed.

About this task

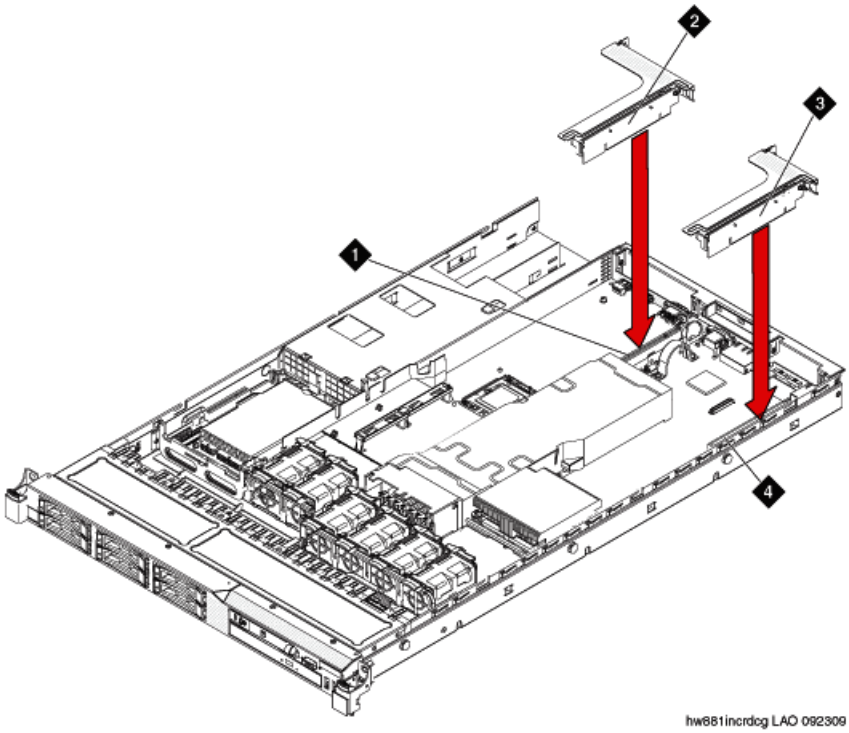
You must install the PCI riser-card assembly after you replace the PCIe card.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Align the PCI riser-card assembly with the PCI connector on the system board. See the following figure.



1	PCI riser connector 2
2	PCI riser-card assembly (full-height, half-length PCIe cards)
3	PCI riser-card assembly (low profile PCIe cards)
4	PCI riser connector 1

2. Press down on the riser-card assembly. Make sure that the assembly is fully seated in the riser-card connector on the system board.
3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Replacing a hard disk drive

Removing a hard disk drive

About this task

Important:

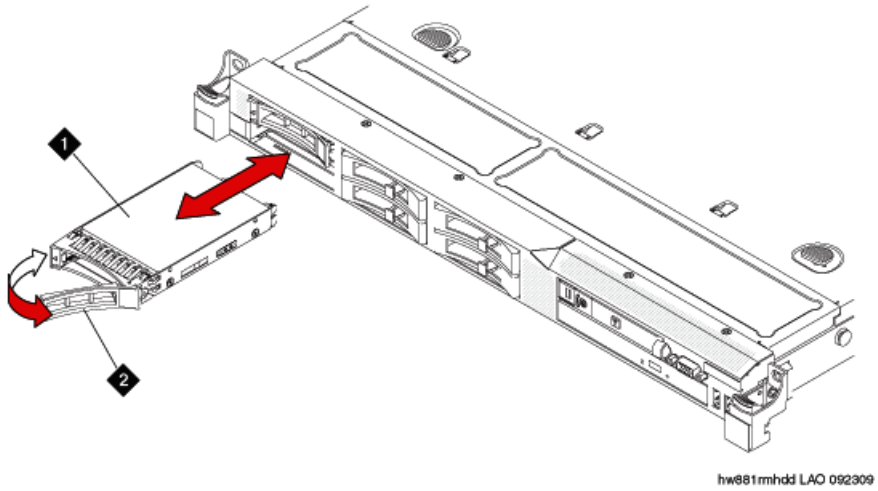
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Slide the release latch (orange) gently to the left to unlock the drive handle. See the following figure.



1	Drive tray assembly
2	Drive handle

2. Grasp the handle and slide the drive out of the drive bay approximately 25 mm (1 inch). Wait until the drive stops spinning before you remove the drive completely from the bay.

Installing a hard disk drive

Before you begin

Remove the hard drive that you want to replace.

About this task

Important:

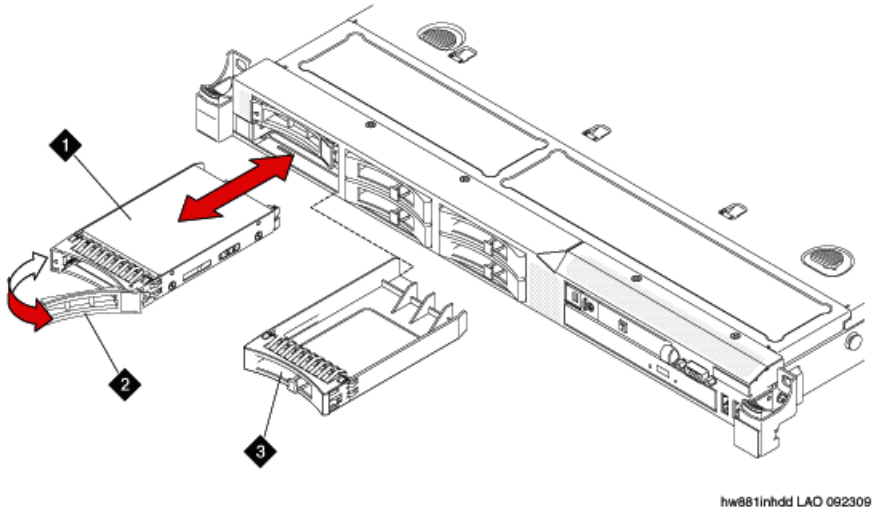
To ensure adequate system cooling, do not operate the server for more than 2 minutes without either a hard disk drive or a filler panel installed in each bay.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Touch the static-protective package that contains the drive to any unpainted metal surface on the server.
2. Remove the drive from the package and place it on a static-protective surface.
3. Make sure that the tray handle is in the open (unlocked) position.
4. Align the drive assembly with the guide rails in the bay. See the following figure.



1	Drive-tray assembly
2	Drive handle
3	Filler panel

5. Gently push the drive assembly into the bay until the drive stops.

6. Push the tray handle to the closed (locked) position.
7. If the drive was hot-swapped, check the hard disk drive status LED to verify that the hard disk drive is operating correctly.

   After you replace a failed hard disk drive, the green activity LED flashes as the disk is accessed. When the new drive starts to rebuild, the amber LED flashes slowly, and the green activity LED remains lit during the rebuild process. The rebuild process takes approximately 30 minutes. If the amber LED remains lit, the drive is faulty and must be replaced.

Replacing a power supply

Removing a power supply

About this task

Caution:

To remove all electrical current from the server, ensure that all power cords are disconnected from the power source. The power control button on the server does not turn off the electrical current supplied to the server. The server also might have more than one power cord.

Caution:

Never remove the cover on a power supply or any part that has the following label attached:



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, replace the power supply.

Important:

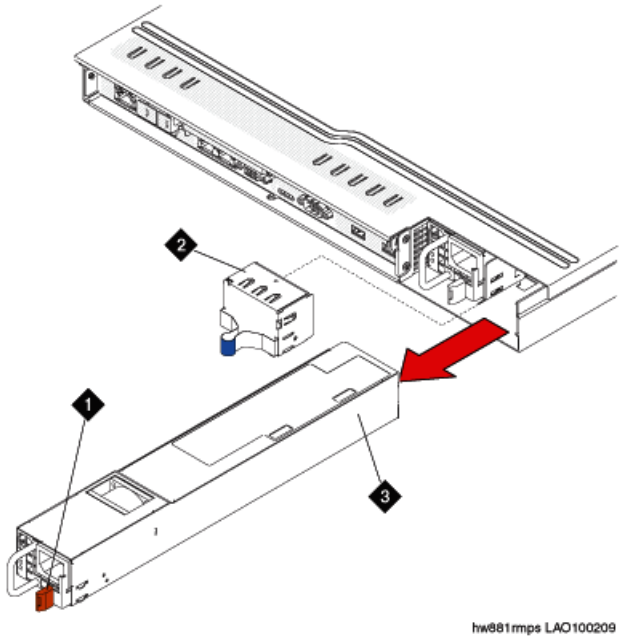
During normal operation, each power-supply bay must contain either a power supply or power-supply filler for proper cooling.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. If the server has only one power supply, turn off the server and peripheral devices and disconnect all power cords. If the server has two power supplies, you can replace one power supply while the server is running.
2. If the server is in a rack, at the back of the server, pull back the cable management arm to gain access to the rear of the server and the power supply.
3. Press and hold the orange release tab to the left. See the following figure.



1	Power supply release tab
2	Power supply filler
3	Power supply

4. Pull the power supply part of the way out of the bay, then release the latch and support the power supply as you pull it the rest of the way out of the bay.

Installing a power supply

About this task

Caution:

To remove all electrical current from the server, ensure that all power cords are disconnected from the power source. The power control button on the server does not turn off the electrical current supplied to the server. The server also might have more than one power cord.

Caution:

Never remove the cover on a power supply or any part that has the following label attached:



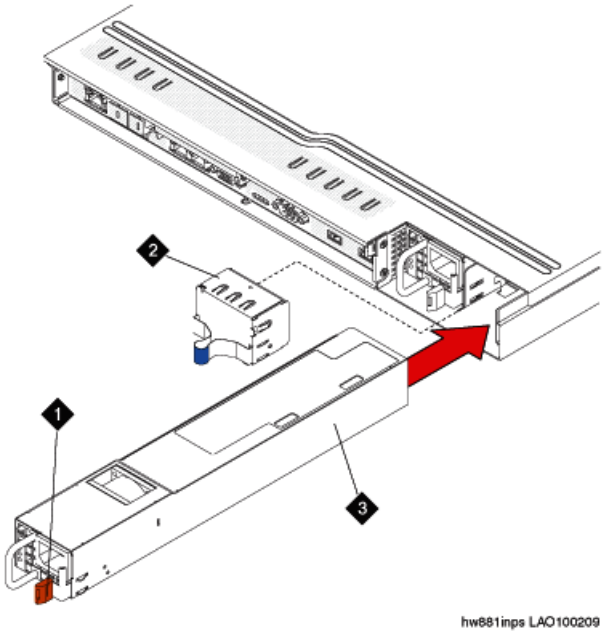
Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, replace the power supply.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Touch the static-protective package that contains the power supply to any unpainted metal surface on the server.
2. Remove the power supply from the package and place it on a static-protective surface.
3. If you are installing a power supply into an empty bay, remove the power-supply filler panel from the power-supply bay.
4. Grasp the handle on the back of the power supply and slide the power supply into the power-supply bay until it clicks. Make sure that the power supply connects firmly into the power-supply connector. See the following figure.



1	Power supply release tab
2	Power supply filler
3	Power supply

5. Route the power cord through the handle so that it does not accidentally become unplugged.
6. Connect the power cord for the new power supply to the power-cord connector on the power supply.
7. Connect the other end of the power cord to a properly grounded electrical outlet.
8. Make sure that both the AC LED and the DC LED on the power supply are lit.

   Both LEDs are lit when the power supply is operating correctly.

Replacing the RAID battery

Removing the RAID battery

Before you begin

The RAID battery is located on top of the RAID controller card.

The RAID configuration data is preserved when you replace the battery.

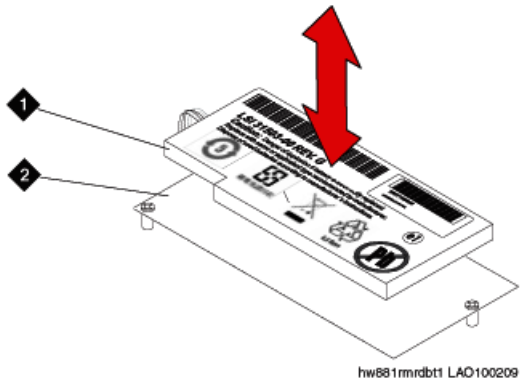
About this task

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Remove the cover.
4. Disconnect the cable from the connector on the battery. Leave the other end of the cable connected to the battery carrier.
5. Squeeze the clip on the side of the battery to remove the battery from the battery carrier. See the following figure.



1	Battery
2	Battery carrier

6. Put the old battery aside.

Related topics:

Removing the server cover

Installing the RAID battery

Before you begin

Remove the existing RAID battery.

About this task

The RAID battery is located on top of the RAID controller card.

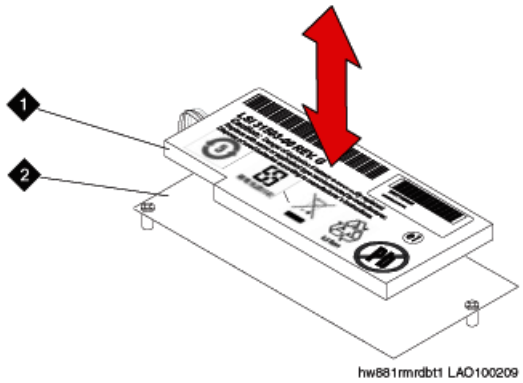
The RAID configuration data is preserved when you replace the battery.

Important:

Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

Procedure

1. Connect the battery cable to the connector on the battery.
2. Press the new battery onto the battery carrier until the clip on the side of the battery snaps into place. See the following figure.



1	Battery
2	Battery carrier

3. Install the cover.
4. Reconnect the external cables and power cords.
5. Turn on the attached devices and the server.

Related topics:

Installing the server cover

S8800 Server replacement

Reuse of hardware components in replacement servers

When you replace the Avaya S8800 Server, you must reuse the following components:

- DIMMs if more than two (4 GB capacity)
- Redundant power supply if used
- Any PCIe cards
- Hard disk drives if more than two.

You must remove these components from the defective server and install them in the replacement server.

Required equipment and tools

- Replacement Avaya S8800 Server
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor
- Electrostatic wrist ground strap and mat

Replacing the S8800 Server

Procedure

1. On the System Manager console, select **Session Manager** > **System State Administration**
2. Select the **Shutdown System** button for the server that is to be replaced. If for some reason this does not work, power down the server by pressing in the power button on the front panel for 5 seconds.
3. Disconnect all power cords and external cables.

   Important:

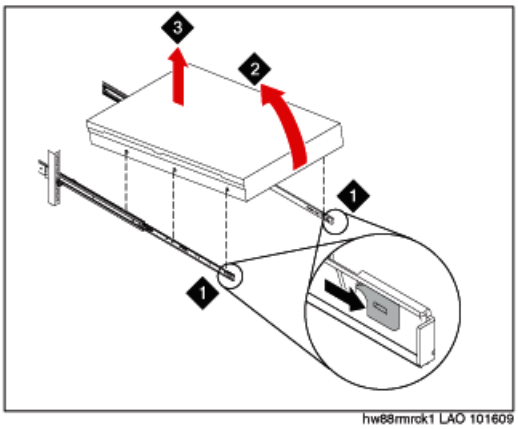
   Label the cables for reconnection.

4. Remove the server from the rack. See
5. Remove the reusable components from the failed server. See Reuse of hardware components in replacement servers on page 121
6. Install the reusable components into the new server. See Reuse of hardware components in replacement servers on page 121
7. Install the new server in the rack. See Installing the server in the rack on page 123
8. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.
9. Insert the Session Manager Kickstart DVD.
10. Turn on the server and allow it to boot.
11. When the server ejects the DVD and reboots, insert the Session Manager software CD into the CD drive.
12. Login as sroot on the console (KVM)
13. Place a looparound network cable between the eth0 port on the Session Manager server to the port 0 on the SM100 card that is plugged into the server. This will be used to execute a sanity test of the SM100 card during the installation process.
14. Execute the following commands to mount the CD and install the Session Manager software in a factory configuration:
    a. # mount /cdrom
    b. # cd /cdrom
    c. bash install.sh --factory
15. When the installation and looparound test complete, shut down the server with the following command: **`# shutdown –f now`**
16. Re-connect the original network cables to the eth0 on the Session Manager server and to port 0 of the SM100 card.
17. Power up the Session Manager server.
18. When the server finishes booting, log into the server as root.
19. Enter the command **`SMnetSetup`** to configure the server for the local network.

Removing the server from the rack

Procedure

1. Turn off the server and all attached devices.
2. Label and disconnect all power cords and external cables.
3. Push the locking levers (1) forward. See the following figure.

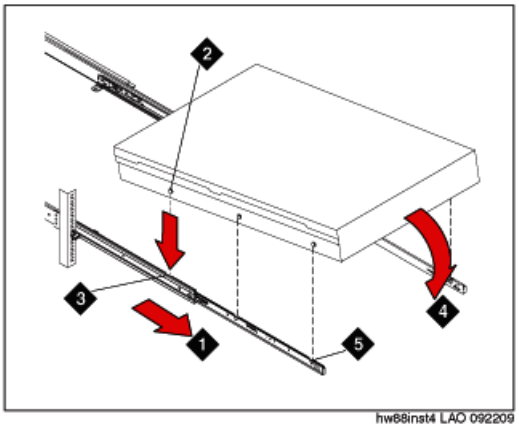


4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

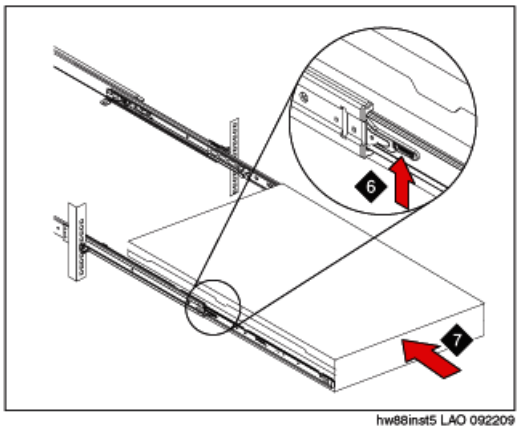
Installing the server in the rack

Procedure

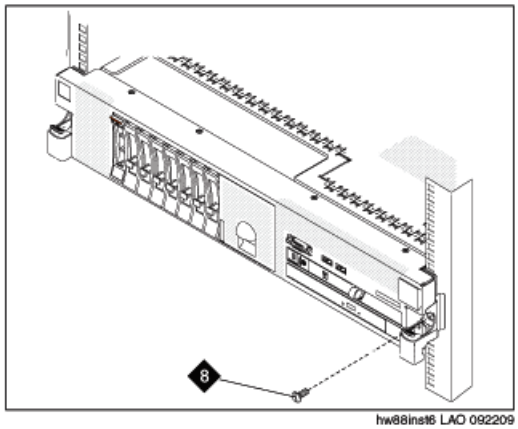
1. Pull the slide rails forward (1) until they click, two times, into place. See the following figure.



2. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads (2) on the server line up with the rear slots (3) on the slide rails. See the preceding figure.
3. Slide the server down until the rear nail heads slip into the two rear slots.
4. Slowly lower the front of the server (4) until the other nail heads slip into the other slots on the slide rails. See the preceding figure.
5. Make sure that the front latch (5) slides over the nail heads. See the preceding figure.
6. Lift the locking levers (6) on the slide rails. See the following figure.



7. Push the server (7) all the way into the rack until it clicks into place. See the preceding figure.
8. Insert the optional M6 screws (8) in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See the following figure.


8
hw88inst6 LAO 092209

Chapter 18: IP address, server name, and FQDN changes

The following sections describe the procedures for:

- changing the SM100 IP address or name on a Session Manager instance
- updating the IP/FQDN of the System Manager virtual appliance present on the System Platform for System Manager Release 5.2 and the associated Session Manager instance(s)

These attributes can be changed after the initial installation.

Changing the SM100 IP address or server name

About this task

The person performing the IP address or server name change must have access to the System Manager that is managing the affected Session Manager server.

Procedure

1. Make the appropriate changes to the DHCP server if needed.
2. Make the appropriate changes to the 96xxsettings.txt file on the network file server used for SIP phone registration settings, using the new SM100 address.

   Note:

   The 96xxsettings.txt parameter ENABLE_PPM_SOURCED_SIPPROXYSRVR should be set to 0 to prevent the phone from retaining the previous address downloaded from the Session Manager.
3. Log in to System Manager and navigate to **Session Manager** > **System Status** > **Registration Summary**
4. Select the appropriate Session Manager.
5. Click on **Reboot** to notify all SIP AST phones to reboot, thereby picking up the new SM100 address.
6. Verify all phones have unregistered before continuing. If a device does not unregister:
   a. Make note of each device that does not unregister
   b. Manually reset the device

7. On the System Manager, navigate to **Session Manager** > **System Status** > **System State Administration**
8. Select the appropriate Session Manager.
9. Click on the **Service State** button.
10. Select **Deny New Service**.
11. Confirm this selection.
12. Wait for the active call count for Session Manager to be acceptably low (ideally, zero).
13. For all other SIP entities with links to the changed Session Manager SM-100 address, change the provisioning of these links using the entity's administration.

    For example, if an Avaya Communication Manager communicates with Session Manager, its signaling groups will need to be updated to connect to Session Manager at its new address.
14. If the address change requires physically moving the SM100 network cable, relocate the cable at this time. If the server is to be relocated:
    a. Power down the server
    b. Relocate the server
    c. Power up the server
15. Log in to Session Manager and navigate to **Network Routing Policy** > **SIP Entities**
16. Change the associated Fully Qualified Domain Name or IP address for the SM100 to the new address.
17. Submit the change.
18. Navigate to **Session Manager** > **Session Manager Administration**
19. Select the appropriate Session Manager instance.
20. Click the **Edit** button.
21. Change any necessary information such as the default gateway and QoS parameters for the SM100.
22. Submit the change.
23. Once all provisioning has been changed, navigate to **Session Manager** > **System Status** > **Security Module Status** on the System Manager console.
24. Make sure the SM100 is functioning and is now using the new address.
25. Navigate to **Session Manager** > **System Tools** > **Maintenance Tests** on the System Management console.
26. Select the Session Manager instance from the pull-down list.
27. Click **Execute All Tests**.

28. On System Manager, select **Session Manager** > **System Status** > **System State Administration**
29. Select **Accept New Service** for the Session Manager.
30. Navigate to **Session Manager** > **System Status** > **Registration Summary** on the System Management console.
31. Verify all SIP endpoints have registered.

Changing the System Manager IP and FQDN

Before you begin

Updates which were made to the profiles after the original System Manager installation must be noted. The IP/FQDN change procedure restores the default profiles. The profiles need to be re-entered once the System Manager IP/FQDN procedure has completed.

The person performing the System Manager IP address change must have access to the craft login on each Session Manager and the root login on System Manager.

About this task

The backup and log directory is created under the $AVAYA_LOG directory.

A unique directory whose name begins with **IPChangedFilesBackup**_ is created under the $AVAYA_LOG directory every time the script is run.

If the services do not stop after the stipulated wait time, the services are killed. As a result, errors could be reported on the console. Those errors can be ignored.

Procedure

1. Log onto the System Manager as **root**
2. If changes were made to the profiles after the original System Manager installation:
   a. Navigate to **Settings** > **Service Profile Management**
   b. Note the updates made to the service profiles.
3. Enter **cd $MGMT_HOME/utils/ipfqdnchange**
4. Enter **ls**
5. Verify that the file **Ip-fqdn-r5.2.sh** is listed. If the file does not exist:
   a. Copy the **Ip-fqdn-r5.2.sh** file from the Avaya support web site to the System Manager virtual machine. The script may be copied to any directory.
   b. Go to the directory where the file was copied (i.e., if the file was copied to /tmp, enter the command **cd /tmp**)

c. Enter **dos2unix lp-fqdn-r5.2.sh**

6. Enter **chmod +x lp-fqdn-r5.2.sh**
7. Run the script. Enter **sh lp-fqdn-r5.2.sh**
   a. Seelp-fqdn-r5.2.sh on page 131 for usage and description information.
   b. If there are errors, check **Return Values** under lp-fqdn-r5.2.sh on page 131 for a list of errors which can be ignored.
   c. The script updates one particular DNS entry in resolve.conf. If there are other DNS entries in resolve.conf which need to be updated, those updates need to be done manually.
8. Run the same command on the console of the System Manager virtual machine:
   a. Log on to the dom-0 of the System Platform.
   b. Login to the System Manager virtual machine by entering the command **xm console <name>**
   c. Enter the same command for **sh lp-fqdn-r5.2.sh** that you entered previously.
9. Once the script has completed, you should see the message **Backup of modified files, old logs, and Db change logs can be found at <location-of-logs>.**
10. Go to the directory where the logs are located as specified in the message. Enter **cd <location-of-logs>**
11. Verify that the script executed successfully in the log. If the log reports a failure:
    a. Restart JBOSS
    b. Enter **cd $MGMT_HOME/trs:**
    c. Enter **./trust_initializer_install.sh -RMIPORT 1399 -HTTPSPORT 443 -TMCONFIGLOC $JBOSS_HOME/server/avmgmt/conf/tm/**
12. If there were updates to the profiles which were noted in the first step:
    a. Navigate to **Settings** > **Service Profile Management**
    b. Update the service profiles with the changes which were noted.
13. If the IP address of the System Manager was changed, update the Session Manager instance(s):
    a. For each Session Manager instance, log into the Session Manager server.
    b. Enter **changeIP <new IP address of System Manager>**
14. If the FQDN of System Manager was changed, update the SAL Agent on the Session Manager instance(s) with the following:

Note:
$SPIRIT_HOME = /opt/Avaya/SPIRIT/<version #>

a. Update the following values in **$SPIRIT_HOME/config/agent/SPIRITAagent_1_0_DataTransportConfig_orig.xml**

   Connection.AvayaBase.PlatformQualifier

   Connection.AvayaBase.URL.0

b. Update the following values in **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_SpiritComponentConfig_orig.xml**

   Address.AgentHeartbeat

   Address.Inventory

   Address.ConfirmConfiguration

   Address.SNMP

   Address.ProcessLog

c. Update the following value in **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml**

   SPIRIT.LoggingServiceURL

d. Restart the SAL Agent.

15. Verify management connectivity using the Test String mechanism on the **Data Replication Status** page.

    See Updating to Master on page 56.

16. Make sure that replication to Session Manager is functioning correctly.

    If the status displays a connection error, reinitialize Trust Management.

Ip-fqdn-r5.2.sh

The **Ip-fqdn-r5.2.sh** command updates the IP or FQDN or both on a System Manager virtual machine.

Syntax

```
Ip-fqdn-r5.2.sh [ -OLDIP x.w.y.z -NEWIP  w.x.y.z ] [ -OLDFQDN a.platform.company.com
-NEWFQDN b.platform.company.com] [ -INSTALLPATH  path ] [ -ENCRYPTKEY  key ] [ -
DBPASSWORD  password ] [ -GATEWAY w.x.y.z ] [ -NETMASK  255.255.255.0 ] [ -OLDDNS
w.x.y.z -NEWDNS w.x.y.z ]
```

OLDIP w.x.y.z
NEWIP w.x.y.z

Original IP address and new IP address. Both of these options are required for changing the IP address of the System Manager.

OLDFQDN a.platform.company.com

Original FQDN and new FQDN. Both of these options are required for changing the FQDN of the System Manager.

NEWFQDN b.plaform..company.com	
INSTALLPATH	This is an optional field. The default value is **/opt/Avaya**
ENCRYPTKEY key	A default value is used if this argument is not specified. Use the default value if this option was not used during the original installation. Otherwise, set *key* to the value which was used during the installation.
DPBASSWORD password	A default value is used if this argument is not specified. Use the default value if this option was not used during the original installation. Otherwise, set *password* to the value which was used during the instllation.
GATEWAY w.x.y.z	This is an optional field. This option is used if the gateway configuration on the System Manager virtual machine is being updated.
NETMASK 255.255.255.0	This is an optional field. This option is used if the netmask on the System Manager virtual machine is being updated.
OLDDNS w.x.y.z **NEWDNS w.x.y.z**	Original DNS and new DNS. Both of these options are required for changing the DNS configuration on the System Manager virtual machine.

Return values

During the script execution, you may see the following errors. These errors can be ignored:

- log4j: WARN no such property [conversionPattern] in com.avaya.common.logging.client.CommonLoggingLayout
- cp: cannot stat 'Binary': No such file or directory
- sed: can't ready Binary: No such file or directory

When the script completes, the following message is displayed: **Backup of modified files, old logs, and Db change logs can be found at <location-of-logs>** where **>location-of-logs>** is the directory displayed in the message.

Description

The **`Ip-fdqn-r5.2.sh`** script is located under **$MGMT_HOME/utils/ipfqdnchange** which is available as part of the System Manager 5.2 release. It performs the following steps:

- Stops JBoss, SAL agent, and postgres services
- Changes the network information of the System Manager server
- Makes IP and FQDN changes in the required files and databases
- Starts JBoss, SAL agent, and postgres services
- Uninstalls the Service Profile Management profiles
- Reinstalls the Service Profile Management profiles with the new IP/FQDN changes

Example

```
sh Ip-fqdn-r5.2.sh –OLDIP 146.147.w.x –NEWIP 148.147.y.z –OLDFQDN
a.platform.company.com –NEWFQDN b.platform.company.com –INSTALLPATH
/opt/Avaya –ENCRYPTKEY avaya –DBPASSWORD asd123 –GATEWAY 148.147.xxx.y
–NETMASK 255.255.255.0 –OLDDNS 148.147.xxx.z –NEWDNS 148.147.yyy.b
```

Considerations

The script must be run by the **root** login.

Chapter 19: Testing the System/Session Manager installation

About this task

The following steps should be done in order to verify the successful installation and configuration of System Manager and Session Manager. These steps verify that the software is installed and configured properly, and that the servers and applications are communicating.

Procedure

1. Select **Session Manager** > **System Tools** > **Maintenance Tests** on the System Manager console.
2. Select the System Manager server in the drop-down list.
3. Click **Execute All Tests**.
4. Verify all tests show Success status.
5. If the data replication test fails, refer to the Data Replication Status page to identify which Session Manager is having replication problems.
6. Select **Session Manager** > **System Status** > **Security Module Status** on the System Manager console.
7. Verify that Security Module Deployment is **Up** for all Session Managers.
8. Select **Session Manager** > **System Status** > **System State Administration**.
9. Verify the installed software versions of all Session Managers are the same
10. Verify all Session Manager servers are in the Management Enabled state.
11. Select **Session Manager** > **System Tools** > **Maintenance Tests**.
12. For each Session Manager instance:
    a. Select **Execute All Tests**.
    b. Verify all tests ran successfully.

Result

.

Chapter 20: Session Manager Upgrades

The upgrade procedures for Service Packs are described in *Installing Service Packs on Avaya Aura™ Session Manager*, 03–142740 on the support web site http://www.avaya.com/support.

Upgrades to new releases of Session Manager are described in *Upgrading Avaya Aura™ Session Manager*, 03–603518.

Chapter 21: Postgres database recovery

Postgres database corruption

After a power failure or database crash, the Postgres database may become corrupted and the Postgres server may not restart.

The recovery action is to clear the Write-Ahead Log (WAL) and optionally reset other control information using the **pg_resetxlog** command. Write-Ahead Logging is a standard method for ensuring data integrity. Changes to data files are written only after those changes have been copied to permanent storage. In the event of a crash, any changes that have not been applied to the data files can be recovered from the log records.

pg_resetxlog command

pg_resetxlog resets the write-ahead log and other control information of a PostgreSQL database cluster.

Syntax

```
pg_resetxlog [-n] [-f] datadir
```

-f Force **pg_resetxlog** to proceed anyway if it complains that it cannot determine valid data for **pg_control**

-n Print the values reconstructed from **pg_control** and exit.

datadir Data directory (required)

Description

pg_resetxlog resets the write-ahead log and other control information stored in the **pg_control** file. It should be used only as a last resort when the server will not start due to database corruption.

pg_resetxlog can only be run by the user who installed the server because it requires read/write access to the data directory. For safety reasons, you must specify the data directory on the command line.

Note:

pg_resetxlog has more options which can be used at an advanced level. For more information regarding **pg_resetxlog** see http://www.postgresql.org/docs/8.2/static/app-pgresetxlog.html

The -f option forces **pg_resetxlog** to proceed anyway if it complains that it cannot determine valid data for **pg_control**.

The -n option prints the values reconstructed from **pg_control** and exits without modifying any values. This option is mainly used for debugging, but may be useful as a sanity check before allowing **pg_resetxlog** to proceed for real.

Troubleshooting Postgres database problems

About this task

If the Postgres database is able to start up without any errors and the database is consistent, there is no need to execute the **pg_resetxlog** command.

Procedure

1. Log in as root.
2. Enter the command `service postgresql start` to restart the PostgreSQL service.
3. If there are errors or the database is inconsistent:
   a. Create an archival backup of the postgresql database directories with the command `tar czvf /var/avaya/backup/pgsqlbackup.tgz /var/lib/pgsql/data`
   b. Log in as Postgres superuser with the command `su - postgres`
   c. Enter `pg_resetxlog /var/lib/pgsql/data`.
      The message “Transaction log reset” should be displayed.
   d. Enter `exit`.
   e. Enter `service postgresql start`.
      The message “Starting postgresql server:” should be displayed, followed by “[OK]” when the server has restarted.
   f. After running the above commands, check for inconsistencies.
4. Log off as root.
5. If the above steps do not fix the problem, contact Avaya Technical Support.

Troubleshooting pg_resetxlog

pg_resetxlog won't start

The **pg_resetxlog** command will not run if the server is running or if it finds a server lock file in the data directory. If the server crashed, a lock file may have been left behind.

Proposed solution

Procedure

1. Log in as root.
2. Enter **service postgresql status** to make certain there is no server process still alive.
3. If the status is `running`:
   a. Enter `service postgresql stop`
   b. Enter service postgresql status until the status is `stopped`.
4. Remove the lock file in the data directory to allow **pg_resetxlog** to run by entering the following commands:
   a. `rm -f /var/lib/pgsql/data/postmaster.pid`
   b. `su - postgres`
   c. `pg_resetxlog /var/lib/pgsql/data`
      The message "Transaction log reset" should be displayed.
   d. Enter `exit`.
5. Enter `service postgresql start`
   The message "Starting postgresql server:" should be displayed, followed by "[OK]" when the server has restarted.
6. Log off as root.

pg_resetxlog cannot determine valid data

If **pg_resetxlog** complains that it cannot determine valid data for **pg_control**, you can force it to proceed anyway using the -f option. Plausible values will be substituted for the

missing data, but manual assistance may be needed for the next OID, next transaction ID and epoch, next multitransaction ID and offset, WAL starting address, and database locale fields using the specific options.

If you are not able to determine the correct values for all of these fields, -f can still be used, but the recovered database may still be corrupted.

References

For more information regarding data integrity on Postgres, see http://www.postgresql.org/docs/8.1/static/wal.html#WAL_RELIABILITY

For more information regarding **pg_resetxlog** see http://www.postgresql.org/docs/8.2/static/app-pgresetxlog.html

Appendix A: Log and Alarm Event IDs

Event ID format

Event IDs use the format <*SP*><*X*[*YYY*][*#####*]>. Some examples of Event IDs are:

OP_APRX10011

AU_MEMG20100

SP is the Standardized Prefix, and can be one of the following:

Prefix	Description
AU_	audit trail
OP_	operational, including error and performance
SE_	security records
TR_	trace and debug

X is a single capital letter which indicates a major Session Manager functional category:

G	General
A	ASSET (SM100)
M	Management
C	Call Processing
P	Personal Profile Manager

YYY are three capital letters which indicate a sub-category, if needed. Some examples are:

AAPX	SM100 ASSET Proxy
AFWL	SM100 ASSET Firewall
AHWM	SM100 ASSET Test
CMON	CP SIP Monitor
CSRE	CP SRE
MSEM	Management Session Manager Element Manager

MAMA	Management SM100 Management Agent

are 5 digits for event IDs within an area. Each area has a unique number range, such as:

SM100	10000-19999
PPM	40000–49999
Call Processing	50000-59999

Log Event and Alarm Event ID descriptions

The following table contains an alphabetical list of log and alarm event IDs, the level/severity of the log or alarm event, and either a description of the log event message or a link to the description of the alarm event and how to troubleshoot the alarm.

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
AU_MSEM20304	INFO No alarm	LoginID (Login name) ClientHost (IP address) Action: Database UPDATE on table (name) with key (name) and properties (list)
AU_MSEM20306	INFO No alarm	LoginID: (Login name) ClientHost: (IP address) Action: Database INSERT on table (name) with key (name) and properties (list)
AU_MSEM20308	INFO No alarm	LoginID: (Login name) ClientHost: (IP address) Action: Database DELETE on table (name) with key (name) and properties (list)
AU_MSEM20310	INFO No alarm	LoginID (Login name) ClientHost (IP address) Action on Session Manager (Session Manager name) Description (action description)
AU_MSEM20312	INFO No alarm	LoginID: (Login name) ClientHost: (IP address) Action on System Manager: (action description)
OP_AAPX10800	INFO No alarm	Connection established to SD or IH, IP=#ip address port=#port transport =(TCP|TLS|UDP) Connection Status on page 156
OP_AAPX10801	INFO No alarm	Connection broken to SD or IH, IP=#ip address port=#port transport =(TCP|TLS|UDP) Connection Status on page 156
OP_AAPX10802	INFO No alarm	Connection broken to TH, IP=#ip address port=#port transport =(TCP|TLS|UDP)

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
		Connection Status on page 156
OP_AASL10900	ERROR Minor	Certificate load failure certificate type=(Identity|CA) Certificate Status on page 157
OP_AASL10901	INFO No alarm	Certificate load success certificate type=(Identity|CA) Certificate Status on page 157
OP_ACLB10002	INFO No alarm	Board cold boot Board Running Status on page 153
OP_ACLB10003	INFO No alarm	Board restart Board Running Status on page 153
OP_ACLB10004	INFO No alarm	Board stop Board Running Status on page 153
OP_AFWL15001	INFO No alarm	SIP Firewall new configuration imposed SIP Firewall Configuration on page 157
OP_AFWL15002	INFO No alarm	Busyout mode is ON | OFF SIP Firewall Configuration on page 157
OP_AFWL16001	INFO No alarm	SIP firewall deep inspection disabled or no active rules SIP Firewall Configuration on page 157
OP_AFWL16002	ALERT	SIP firewall deep inspection configuration update failed (rule #, <rule name string>), retaining existing configuration SIP Firewall Configuration on page 157
OP_AFWL16003	ALERT	SIP firewall configuration failed schema validation SIP Firewall Configuration on page 157
OP_AFWL16501	ALERT	SIP firewall action <ALERT|PERMIT|DROP|RATE-LIMIT|RATE-BLOCK> message (length:#) - matched rule: <rulename>, [optional message,] <TCP|TLS|UDP>, remote <addr:port#>, local <addr:port#> SIP Firewall Actions on page 158
OP_AFWL16502	INFO No alarm	SIP firewall action <ALERT|PERMIT|DROP|RATE-LIMIT|RATE-BLOCK> message (length:#) - matched rule: <rulename>, [optional message,] <TCP|TLS|UDP>, remote <addr:port#>, local <addr:port#> SIP Firewall Actions on page 158
OP_AFWL17501	INFO No alarm	SIP firewall blacklist disabled or no active rules SIP Firewall Configuration on page 157
OP_AFWL17502	INFO No alarm	SIP firewall whitelist disabled or no active rules SIP Firewall Configuration on page 157

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_AFWL17503	ALERT	SIP firewall blacklist configuration update failed (network rule # | content rule #), retaining existing configuration SIP Firewall Configuration on page 157
OP_AFWL17504	ALERT	SIP firewall whitelist configuration update failed (network rule # | content rule #), retaining existing configuration SIP Firewall Configuration on page 157
OP_AHWM10100	ALERT	Board overheating event (yellow zone) Board Temperature Alarms on page 153
OP_AHWM10101	CRITICAL Major	Board overheating event (red zone) Board Temperature Alarms on page 153
OP_AHWM10102	INFO No alarm	Temperature normal Board Temperature Alarms on page 153
OP_AHWM10103	INFO No alarm	90 percent of total memory was consumed Board Memory on page 154
OP_ANFW11000	INFO No alarm	Network firewall started
OP_ANFW11001	WARN Warning	Network firewall stopped
OP_APLM10300	ERROR Minor	Failure pinholing Network Firewall, interface=(intf|all) port=#port transport=(TCP|TLS|UDP) Network Firewall Pinholing on page 154
OP_APLM10301	INFO No alarm	Success pinholing Network Firewall, interface=(intf|all) port=#port transport=(TCP|TLS|UDP Network Firewall Pinholing on page 154
OP_APLM10302	ERROR Minor	Failure configuring network parameters Network Configuration on page 155
OP_APLM10303	INFO No alarm	Success configuring network parameters Network Configuration on page 155
OP_APLM10304	ERROR Minor	Eth(0) interface is down Network Configuration on page 155
OP_APLM10305	INFO No alarm	Eth(0) interface is up Network Configuration on page 155
OP_ASMT10700	INFO No alarm	Start sip trace SIP Tracing on page 156
OP_ASMT10701	INFO No alarm	Stop sip trace SIP Tracing on page 156

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_AWTC10400	ERROR Minor	Application <name> restart failure Application Failure on page 155
OP_AWTC10405	WARNING	Identity certificate is about to expire Certificate Expiration on page 156
OP_AWTC10406	ALERT	Identify certificate expired Certificate Expiration on page 156
OP_CDAO50001	ERROR Minor	The database connection is down. Administration updates will not function during this outage. Database Connection on page 159
OP_CDAO50002	ERROR Minor	Administration relating to the <admin> screen(s) may have caused a database query failure (SQL Exception). The failing object was the <object>. Database Query on page 160
OP_CDAO50003	ERROR Minor	Administration relating to the <admin> screen(s) may have caused the database to become corrupt. The failing object was the <object> Database Corrupted on page 160
OP_CDAO50004	WARN Warning	The database connection is currently down. Trying again <warning count> more times before alarming an error. Database Connection on page 159
OP_CDAO50005	INFO No alarm	The database connection has been restored. Administration updates should be taking effect now. Database Connection on page 159
OP_CDAO50006	INFO No alarm	There is corrupt data in the database relating to the <admin> screen(s), for the <class> class. Database Connection on page 159
OP_CDAO50007	INFO No alarm	There was corrupt data in the database for relating to the <admin> screen(s), but it has been corrected in the <class> class. Database Corrupted on page 160
OP_CDAO50008	INFO No alarm	There was an SQL query error relating to the <GUI> screen(s) for the <class> class, but it has been corrected. Database Query on page 160
OP_CDAO50009	ERROR Minor	A file I/O error for <file> occurred trying to write the local DNS server configuration or zone files. Zone File I/O on page 161
OP_CDAO50010	INFO No alarm	There was a file I/O error for <file>, but it has been corrected.

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
		Zone File I/O on page 161
OP_CDAO50011	ERROR Minor	The Session Manager Instance cannot be resolved. Double check the administration on the <admin> screen(s). Session Manager Instance Resolution on page 162
OP_CDAO50012	ERROR Minor	Multiple Session Manager IP addresses map to the local Session Manager Instance. Double check administration screen(s) <admin>, or real DNS such as /etc/hosts. For now, choosing entity <sip entity name>. Session Manager Instance Resolution on page 162
OP_CDAO50013	ERROR Minor	DNS resolved to multiple IP addresses for SM100; choosing address <ip address>. SM100 Multiple DNS Resolutions on page 162
OP_CDAO50014	WARN Warning	A file I/O error for <file> occurred trying to write the local DNS server configuration or zone files. Attempting <warning count> more times to correct. Check the file permissions, directory existence, disk space, etc. Zone File I/O on page 161
OP_CDAO50016	INFO No alarm	The Session Manager Instance resolution issue has been corrected. Session Manager Instance Resolution on page 162
OP_CDAO50017	INFO No alarm	DNS no longer resolves to multiple IP addresses for the SM100. SM100 Multiple DNS Resolutions on page 162
OP_CDAO50018	WARN Warning	Bandwidth threshold exceeded for the <location name> location. Used/allowed bandwidth: <used>/<allowed> Exceeding Location Bandwidth on page 163
OP_CDAO50019	INFO No alarm	Bandwidth threshold no longer exceeded for the <location name> location. Exceeding Location Bandwidth on page 163
OP_CDAO50020	ERROR Minor	There is a problem with the Call Detail Recording (CDR) system. Call accounting is not operational. CDR Not Operational on page 164
OP_CDAO50021	INFO No alarm	The Call detail Recording (CDR) system is now operational. Call accounting is resumed. CDR Not Operational on page 164
OP_CDAO50022	WARN Warning	The direct link for Session Manager to Route-Through using the Entity Link to <session manager name> on port <port number> using <port number> is missing.

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
		Double check the administration on <admin> screen(s) to correct. Route Through on page 164
OP_CDAO50023	INFO No alarm	The missing Entity Link for Session Manager to Route-Through to <session manager name> has been inserted. Route Through on page 164
OP_CMON55000	INFO No alarm	SIP monitoring state for entity < entity name> is no longer <entity state>. SIP Monitor Alarm on page 165
OP_CMON55001	WARN Warning	SIP monitoring state for entity < entity name> is <entity state>. SIP Monitor Alarm on page 165
OP_CMON55002	WARN Warning	SIP monitoring state for entity <entity name> is <entity state>. SIP Monitor Alarm on page 165
OP_CSRE52000	INFO No alarm	<extension module> extension module now working properly and is deployed.
OP_CSRE52001	INFO No alarm	Call Admission Control did not deny an emergency call even though bandwidth would have been exceeded for location {location}.
OP_CSRE52003	ERROR Minor	Attempted DNS resolution while extension module was not deployed. The DNS Extension Module is missing or is corrupted. Any non-provisioned, DNS Fully Qualified Domain Names (FQDN) will not be resolved. Contact Avaya Technical support.
OP_CSRE53000	INFO No alarm	Call Admission Control denied a call on the {Routing phase (originating or terminating)}, location {location}, (id = {location id (database id)})
OP_CURE56000	INFO Warning	Registration Authorizations no longer failing for user {user}, domain {domain}, {date}.
OP_CURE56001	INFO Warning	Registration Authorizations failing for user {user}, domain {domain}, {date}.
OP_CURE56003	INFO Warning	Registration Expiration Interval no longer failing for user {user}, domain {domain}, {date}
OP_CURE56004	INFO Warning	Registration Expiration Interval Too Short for user {user}, domain {domain}, {date}

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_CURE56006	INFO Warning	URE Proxy: Local Port Not Found for Application {Application name}, {phase} Phase, for user {user} at domain {domain}.
OP_CURE56007	INFO Minor	URE Proxy: Entity Link No Longer Alarming for Application {Application name}, user {user handle}, domain {domain}
OP_CURE56008	INFO Minor	URE Proxy: Entity Link Not Found for Application {Application name}, {phase} Phase, for user {user handle} at domain {domain}. {
OP_CURE56009	INFO Warning	Registration Service no longer failing for user {user}, domain {domain}, {date}.
OP_CURE56010	INFO Warning	Registration Service Failure, user {user}, domain {domain}, {date}.
OP_CURE56011	INFO Warning	Registrar no longer failing removing registrations for user {user}, domain {domain}, {date}.
OP_CURE56012	INFO Warning	Failure Removing Registrations for user {user}, domain {domain}, {date}.
OP_CURE56013	INFO Warning	Registrar no longer failing query for registrations, user {user}, domain {domain}, {date}.
OP_CURE56014	INFO Warning	Failure Querying for Registrations, user {user}, domain {domain}, {date}.
OP_CURE56015	INFO Warning	Registrar no longer failing matching registration for user {user}, domain {domain}, {date}.
OP_CURE56016	INFO Warning	Failure Matching Registration for user {user}, domain {domain}, {date}.
OP_CURE56017	INFO Warning	Subscription Authorizations no longer failing for user {user}, domain {domain}, {date}.
OP_CURE56018	INFO Warning	Subscription Authorizations failing for user user {user}, domain {domain}, {date}.
OP_CURE56020	INFO Warning	No longer failing storing subscription, user {user}, domain {domain}, {date}.
OP_CURE56021	INFO Warning	Failure Storing Subscription, user {user}, domain {domain}, {date}.
OP_CURE56022	INFO Warning	Application {Application handle} at SIP Entity {Application's SIP Entity name} is no longer unreachable.

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_CURE56023	INFO Minor	Application {Application handle}} at SIP Entity {Application's SIP Entity name} is Unreachable.
OP_CURE56024	INFO Warning	Receiving Subscription Notification errors for user {user}, domain {domain}, {date}.
OP_CURE56025	INFO Warning	Call denied because route back route header was changed to {Route header URI}
OP_CURE56026	INFO Warning	Emergency call with contact URI {Contact URI}, originating location {Originating location name}, to destination SIP entity {SIP Entity name}
OP_CURE57000	INFO No alarm	Unregistering the user {User URI} removed through administration.
OP_CURE57001	INFO No alarm	User {User URI} has registered.
OP_CURE57002	INFO No alarm	User {User URI} has unregistered.
OP_CURE57003	INFO No alarm	User {User URI} registration has expired.
OP_CURE57004	INFO No alarm	Unregistering user {User URI} due to duplicate user registration. Only one active user is allowed with the current forking policy.
OP_CURE57005	INFO No alarm	User {user} @ {domain}, event package {event package (dialog, message-summary, etc)}, subscription has expired.
OP_CURE57006	INFO No alarm	User {User URI}, domain {domain} failed authentication.
OP_MAMA20100	ERROR Minor	Security Module Management Agent is unable to connect to SIP A/S Management Server
OP_MAMA20101	INFO No alarm	Security Module Management Agent connected to SIP A/S Management Server
OP_MAMA20102	ERROR Minor	Security Module Management Agent is not able to configure SM100
OP_MAMA20103	INFO No alarm	Security Module Management Agent is able to configure SM100.
OP_MMTC20011	ERROR Minor	Postgres database sanity check failed; the database is unaccessible
OP_MMTC20012	INFO No alarm	Postgres database sanity check passed

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_MMTC20013	ERROR Minor	Service Host sanity check failed; call processing is down
OP_MMTC20014	INFO No alarm	Service Host(s) sanity check passed
OP_MMTC20015	ERROR Minor	Session Manager sanity check failed; call processing is down.
OP_MMTC20016	INFO No alarm	Session Manager sanity check passed.
OP_MMTC20017	ERROR Minor	Management Server sanity check failed; SIP A/S admin is unavailable
OP_MMTC20018	INFO No alarm	Management Server sanity check passed
OP_MMTC20019	ERROR Minor	SAL-Agent sanity check failed; alarms are not being processed
OP_MMTC20020	INFO No alarm	SAL-Agent sanity check passed
OP_MMTC20021	ERROR Minor	Management jboss sanity check failed; services are unavailable
OP_MMTC20022	INFO No alarm	Management jboss sanity check passed
OP_MMTC20023	ERROR Minor	System Replication sanity check failed
OP_MMTC20024	INFO No alarm	System Replication sanity check passed
OP_MMTC20025	ERROR Minor	SM100 sanity check failed; call processing is down
OP_MMTC20026	INFO No alarm	SM100 sanity check passed
OP_MMTC20027	ERROR Minor	System Manager Replication test failed
OP_MMTC20028	INFO No alarm	System Manager Replication test passed
OP_MMTC20029	ERROR Minor	Call Processing SAR is not deployed
OP_MMTC20030	INFO No alarm	Call Processing SAR is deployed successfully

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_MMTC20031	ERROR Minor	Data Distribution/Redundancy is down.
OP_MMTC20032	INFO No alarm	Data Distribution/Redundancy is up.
OP_MWD20200	INFO No alarm	Service <service name> has started.
OP_MWD20201	ERROR Minor	Service <service name> has died.
OP_MWD20202	ERROR Minor	Service <service name> failing to start after several attempts
OP_PCFF40000	FATAL Critical	Could not find [FnuFile | LabelFile | SmsConfigFile | ButtonRangesFile] {actualfilename} log an alarm Missing file on page 166
OP_PCFF40001	INFO No alarm	Found [FnuFile | LabelFile | SmsConfigFile | ButtonRangesFile]

Board Running Status

These events are normal and report the last known running state of the SM100 card. When the SM100 successfully boots, is restarted, or has been stopped, the associated log message is sent to System Manager. These events are informational.

Board Temperature Alarms

These alarms will continue to be sent until the temperature of the SM100 returns to normal, at which time a `temperature normal` log message will be sent to indicate the problem has been resolved. When this occurs, the alarm status can be changed to `Cleared`.

A yellow zone warning alarm indicates the SM100 card has reached a temperature above its expected normal operating range.

A red zone warning alarm indicates the temperature has reached a critical level such that the SM100 might be damaged.

Troubleshooting yellow and red zone alarms

Procedure

1. Verify there are no blockages of the air inlets to the Session Manager hardware.
2. Verify the external climate-control systems are functioning properly.
3. If the problem persists, contact Avaya Technical Support for repair or replacement.

   The cooling fans have failed or the SM100 card is failing.

Board Memory

Under normal situations, the SM100 is capable of running with installed memory. However, memory leakage may cause unnecessary consumption of memory. If this occurs, a log message is sent to the System Manager.

Avaya Technical Support should be contacted if the problem persists.

Network Firewall Pinholing

By default, the SM100 network firewall restricts access to all but those interfaces and ports defined in the *Avaya Aura™ Session Manager: Port Matrix* documentation (available by logging into the support website and using the InSite Knowledge Management Database at http://support.avaya.com).

However, the pinhole mechanism permits applications to make on-demand requests to open (close) temporary “pinholes” through the network firewall. The result of these requests is logged to System Manager. Information contained in the message identifies the network interface (specific interface or all interfaces), the port that is being opened, and the transport protocol to which the port is associated.

Failure of an application to open a pinhole indicates an internal Session Manager problem. Avaya Technical Support should be contacted if the problem persists.

Network Configuration

The SM100 network parameters are configured during the installation and administration of Session Manager. Both successful and unsuccessful configurations are reported. If the SM100 network cannot be configured, an alarm is sent to System Manager.

When the SM100 is stopped or restarted, you will see the SM100 public interface (Eth0) change state between up and down. During normal operation, the interface should be up only.

Failure to properly configure the SM100 network may be the result of incorrect settings.

Troubleshooting Network Configuration alarms

Procedure

1. Check the configuration.
2. Reset the SM100.
3. If this does not resolve the problem, there may be an internal Session Manager problem.

   Contact Avaya Technical Support.

Application Failure

If an SM100 application fails to start or restart, this may indicate a problem with SM100 resources (i.e. memory), a configuration issue, or a problem with the application itself. The name of the application which fails to start is shown in the log message.

Troubleshooting Application Failure Alarms

Procedure

1. Review the log to determine if any other problems might be affecting the application’s ability to load (e.g., 90% memory consumed).
2. If there are no other problems, there may be an internal software problem.

   Contact Avaya Technical Support.

Certificate Expiration

The SM100 requires a certificate for securing SIP connections. If this certificate has expired, the SM100 will not be able to establish any new SIP TLS connects, and security will be compromised. In many cases, TCP and UDP are not options, so it is imperative that certificate lifetime be monitored.

When the SM100 certificate is approaching its expiration, a warning message is periodically logged starting 30 days before expiration. If the certificate has expired, a daily alarm is sent to System Manager.

Troubleshooting Certificate Expiration Alarms

Procedure

Refer to *Administering Avaya Aura™ Session Manager*, 03–603324 for instructions for getting a new certificate.

SIP Tracing messages

Session Manager provides a tool for tracing SIP messages (see Session Manager SIP Tracing on page 71). When tracing is started or stopped, a log message is sent to System Manager. These messages are informational and no action is required. SIP tracing may impact SM100 performance in some cases and normally should be turned off.

Connection Status

The state changes of Session Manager connections are logged to System Manager. The specific hosts reported are:

- Trusted SIP Entities (also referred to as Trusted Hosts)
- Service Director (SD)
- Service Hosts (SH, also called Instance Hosts, IH).

Trusted SIP Entity examples are Communication Manager and CLAN.

SD and SH are components of the Session Manager SIP Server. Information contained in these log messages includes host IP address, port, and the transport protocol associated with

the port. This information can be used to diagnose network wiring or network configuration problems (host interface, protocol, address/mask assignment, etc.)

Troubleshooting Connection Status Alarms

Procedure

1. Check if certificate maintenance is required.
2. Make sure the Credential name in the Network Routing Protocol is configured correctly.

Certificate Status

The SM100 identity certificate and CA (trusted) certificate must be present for SIP TLS. If one of these certificates cannot be loaded (i.e., the certificate is invalid, expired, revoked), an alarm is sent to System Manager.

Troubleshooting Certificate Status Alarms

Procedure

1. Make sure that valid identity certificates are installed on the system.
2. Make sure that valid CA certificates are installed on the system.
3. See Certificate Expiration on page 156 in this document.
4. See Trust Management in *Administering Avaya Aura™ Session Manager*, 03-603324 .

SIP Firewall Configuration

Changes to the SM100 SIP firewall configuration are always reported to System Manager. Most of the messages are informational (configuration successful, ruleslist/blacklist/whitelist disabled). However, configuration failures are serious and cause alarms. When alarms are generated, information about the failure is provided: effected list, list rule number, and some rule details.

Configuration failure is not an expected occurrence.

Troubleshooting SIP Firewall Configuration Alarms

Procedure

1. Refer to the SIP Firewall Configuration section of *Administering Avaya Aura™ Session Manager* , 03-603324 to ensure that the rule is correctly configured.
2. If the problem persists, report the problem to Avaya Technical Support.

SIP Firewall Actions

If administration has configured SIP firewall rules with logs or alarms, all received SIP messages matching that rule will cause System Manger to be notified. These log/alarm messages are rate-limited to prevent Denial of Service attacks on the logging/alarming systems.

Information contained in the log or alarm message includes the action taken on the SIP message, the matched rule name, an administration-customized message, the transport protocol over which the message was received, originating host address/port, and destination host address/port. These logging details can be used to further analyze and mitigate threats to the system.

Troubleshooting SIP Firewall Actions Alarms

About this task

Complete the following steps if too many “matched-rule” log/alarm messages are received.

Procedure

1. Review the log/alarm messages.
2. Consider additional changes to the SIP Firewall configuration to reduce messages.

   Refer to the SIP Firewall Configuration section of *Administering Avaya Aura™ Session Manager*, 03-603324.

Database Connection

This alarm is related to the database which contains the administered data for routing, users, etc. The connection to the database is either timing out or has been lost. During this outage, any new administration will not be recognized by the running system.

Possible causes include:

- The connection to the database has been lost or is experiencing timeouts between queries.
- The database may not be running on the Session Manager or is on a different IP address than expected.
- The database process may not be running.

Troubleshooting Database Connection Alarms

Procedure

1. Ensure there is an actual connection to the database.
2. Make sure this connection is stable and not experiencing outages.
3. Ensure the Session Manager is reachable by pinging it from another machine that should be able to reach it:
   a. Enter `ping` *`w.x.y.z`* where *w.x.y.z* is the IP address of the Session Manager.
   b. If there is no answer, the system is either in an unresponsive state, is currently off, or is in the middle of a reboot.
4. Make sure the Session Manager IP address or DNS name is configured properly for the running Instance.

   This requires root access.
5. Check if the database process is running on the Session Manager.

   This action requires root access.
6. Make sure the database user name and passwords match the default values provided by the system.
7. If none of the above steps solve the problem, contact Avaya Technical Support.

Database Query

This event occurs when a database query cannot complete or experiences a failure. This would likely only be seen after an upgrade which would indicate that the upgrade had problems. As a result, the Session Manager will likely not behave correctly or at all.

This event can occur if the database schemas do not match, indicating that variable types are different, fields are non-existent, etc. For example, an Integer type column becomes a Boolean type.

Troubleshooting Database Query Alarms

Procedure

Call Avaya Technical Support to check the database versions and to ensure they are correct and compatible.

In particular, the table schemaversion in the System Manager and Session Manager databases should have appropriate and matching version entries in the major, minor, revision, and schemaname columns.

Database Corrupted

Corrupted or bad data has been copied into the database. Components of Session Manager which depend on this data will likely not be operating properly.

This event may be caused by administration which contained bad data that was not properly checked for errors. This event can also occur if someone writes directly into the database. An example would be if someone enters a digit pattern “5555” but sets the minimum and maximum limits to 3. They should both be at least 4.

Troubleshooting Database Corrupted Alarms

Procedure

1. Check any recent administration relating to the alarm's suggested configuration pages.
2. If nothing appears out of the ordinary, contact Avaya Technical Support.

Zone File I/O

Zone files are written to the local file system to reflect the host name resolution data administered on the Local Host Name Resolution page. The SM100 uses this data when performing DNS resolution.

A Zone File I/O alarm indicates that an error occurred while trying to access the file system to read or write data for zone files. Causes may include:

- No space on the disk
- Missing files
- Permission errors
- Other errors which cause a read or write to the zone files to fail.

Troubleshooting Zone File I/O Alarms

Procedure

1. Ensure there is enough space on the disk:
   a. Execute **`df`** and make sure that the Use% value is not greater than 95%.
   b. If the Use% value is greater than 95%, remove any unnecessary large files and old log files on the system.
2. Check if the file `/etc/named.nre.zones` exists and has read permissions for all users plus write permissions only for the owner, root (-rw-r--r--).

   If the file does not exist or the permissions are incorrect, contact Avaya Technical Support.
3. If the above steps do not solve the problem, contact Avaya Technical Support.

Session Manager Instance Resolution

This event occurs when the IP address of the configured Session Manager does not match the administration of any Session Manager instance. During this failure, the Session Manager will not service any calls.

Possible causes are:

- No Session Manager that is administered in System Manager has a Management Access Point Host Name/IP address that matches the Session Manager instance's IP address. This could be an administration error, possibly due to entering the IP address of the SM100 by mistake.
- A DNS name is resolving to multiple IP addresses or to no IP address.

Troubleshooting Session Manager Resolution Alarms

Procedure

1. Check the IP address in the Session Manager Administration's Management Access Point Host Name/IP field and make sure it is correct.
2. If the Management Access Point Host Name/IP is a DNS name, check to what it resolves using the command `host` *`someDNSname`* where*someDNSname* is the server name.
3. Check `/etc/hosts` on the Session Manager to ensure that the name resolves to one IP address.

   The file should have entries in the form of `<IP Address> <FQDN> <domain>` .Change the DNS to resolve to exactly one IP address if necessary.

SM100 Multiple DNS Resolutions

The SM100 is provisioned as a DNS name in the Session Manager, but the name resolves to more than one IP address. The default behavior is to use the first IP address to which the DNS name maps. This may cause unintended results. The system may appear to operate normally, but behavior may be very unreliable.

Troubleshooting SM100 Multiple DNS Resolution Alarms

Procedure

1. Check the IP address in the Session Manager's SM100 administration and make sure it is correct.
2. Check what the name resolves to using the command `host` *`someDNSname`* where *someDNSname* is the server name.
3. Check `/etc/hosts` to ensure that the name, if it appears here, resolves to one IP address.

   The file should have entries in the form of `<IP Address> <FQDN> <domain>`

Exceeding Location Bandwidth

This event is related to the Call Admission Control functionality for the SIP Routing Element (SRE), a component of Session Manager. This event usually means the used bandwidth for a specific Location has consistently exceeded a pre-defined high threshold (currently, 90% of the bandwidth capacity), or no more usable bandwidth is available for calls using that specific Location (bandwidth is at 100% capacity).

When the bandwidth is at 100% capacity for a particular Location, new calls are not allowed to or from that Location and will be denied.

This event may be caused by one of the following:

- There is more simultaneous call traffic than anticipated at a specific Location.
- The provisioned bandwidth for a specific Location is insufficient for the actual carried traffic.
- The provisioned bandwidth for a specific Location is correctly set according to LAN characteristics, but traffic exceeds actual network capacity.

Troubleshooting Exceeding Location Bandwidth Alarms

Procedure

1. Ensure the traffic is consistent with the bandwidth capacity.
2. Consider rerouting part of the traffic through a different, under-utilized Location.

3. Increase bandwidth provisioning if allowed by the network.
4. Consider splitting the Location into two or more different Locations and route traffic accordingly.

CDR Not Operational

This event is related to the Call Detail Recording (CDR) functionality for the SIP Routing Element (SRE), a component of Session Manager. This event means that call accounting is not available for calls to or from certain SIP entities for which CDR is enabled. During this outage, some or all calls will not be recorded in CDR.

Possible causes include:

- The CDR Extension Module is unable to process CDR call events
- The CDR Extension Module may not be running.

Troubleshooting CDR Not Operational Alarms

Procedure

If the problem persists, contact Avaya Technical Support.

Route Through

This event indicates that Route Through is being attempted on calls, but it cannot route through to another Session Manager Instance. Calls may be denied as a result of not being able to Route Through. This may or may not be a real problem, depending on the customer's desired configuration.

The most likely cause is that the Entity Link between the Session Managers is missing on the NRP Entity Link page. The alarm message should identify which Session Managers experienced the “Can't Route Through” problem

Troubleshooting Route Through Alarms

Procedure

Add the correct Entity Link between the two Session Managers on the NRP Entity Link page.

SIP Monitor Alarm

SIP Monitoring has detected that the alarmed SIP entity is not successfully responding to SIP OPTIONS requests. A SIP entity may be reachable via several addresses, depending on Local Host Name Resolution administration and DNS address resolution. If the state of the entity is “down”, none of the entity’s addresses will respond to OPTIONS requests successfully. If the state of the entity is “partially up”, at least one of the entity’s addresses is responding successfully and at least one is not responding successfully.

The SIP Monitoring Status page on the System Manager will provide more detail, including the status of the entity’s various addresses and the response codes returned by the various addresses. The response codes are the standard SIP responses according to RFC 3261, section 21.

This event may be caused by the OPTIONS request not reaching the alarmed SIP entity because of problems with the network, or the alarmed SP entity may not be responding to the OPTIONS request.

Troubleshooting SIP Monitoring Alarms

Procedure

1. Check the SIP Monitoring Status page for more details.
2. Verify network connectivity exists between the Session Manager and the alarmed SIP entity using the **`ping`** command.
3. Using the SIP Tracer tool or a network protocol analyzer such as Wireshark, verify that an OPTIONS request is sent from the Session Manager to the alarmed entity, and that the entity responds successfully (typically with a “200 OK” response).

SM100 Sanity Failure

The SM100 failed a sanity check.

Troubleshooting SM100 Sanity Failure Alarms

Procedure

1. Select **Security Module Status** on the System Manager console.
2. Use the **Refresh** button to display the current status.
3. The **Security Module Deployment** status should be **Up**.
4. If the Deployment status is still **Down**, reset the security module:
   a. Select the appropriate system from the System Name list.
   b. Select the **Security Module Reset** button.

   Warning:
   The Session Manager cannot process calls while the security module is being reset. In a multiple Session Manager installation, refer to System State Administration for details on how to disable the Session Manager prior to resetting the security module.
5. Use the **Refresh** button to display the current status.

Missing file

One of the following files is missing:

- FnuFile
- LabelFile
- SmsConfigFile
- ButtonRangesFile

The name of the missing file will appear in the message.

To clear this alarm:

1. Copy a saved backup of the missing file to the proper directory, then restart **sm-mgmt**
2. If the above step does not fix the problem, reinstall the server.

Appendix B: S8510 Server alarms

S8510 Server hardware and environment events

The following table contains a list of the S8510 server hardware and environment monitoring alarms. All of the failure events are major alarms. The table contains information regarding the Event ID, the severity of the event, and a link to the description and recovery action(s).

The alarm message for hard disk drives contains the disk number of the failing or failed drive. An example of an alarm message for Event ID 2048 would be:

```
Storage Service EventID: 2048 Device failed: Physical disk 0:0:1 Controller
0, Connector 0
```

Also, the LED display on the Avaya S8510 server indicates which disk failed or is failing.

Event ID	Severity	Description/Action
1354	Error	Power supply detected a failure on page 170
2048	Failure	Device failed on page 171
2056	Failure	Virtual disk failed on page 171
2057	Warning	Virtual disk degraded on page 171
2076	Failure	Virtual disk check consistency failed on page 172
2080	Failure	Physical disk initialize failed on page 172
2083	Failure	Physical disk rebuild failed on page 173
2102	Failure	Temperature exceeded maximum threshold on page 173
2103	Failure	Temperature dropped below minimum threshold on page 174
2107	Failure	SMART configuration change on page 174
2163	Failure	Rebuild completed with errors on page 175
2169	Failure	Controller battery needs to be replaced on page 176
2268	Failure	Storage Management has lost communication on page 176
2270	Failure	Physical disk Clear operation failed on page 176

Event ID	Severity	Description/Action
2272	Failure	Uncorrectable media error detected on page 177
2273	Failure	Physical disk puncture on page 177
2282	Failure	Hot spare SMART polling failed on page 178
2289	Failure	Multi-bit ECC error on page 178
2299	Failure	Bad physical connection on page 179
2307	Failure	Bad block table is full on page 179
2320	Failure	Single-bit ECC error
2321	Failure	Single-bit ECC error, no further alerts on page 180
2340	Failure	BGI completed with uncorrectable errors on page 180
2347	Failure	Rebuild failed on source physical disk on page 181
2348	Failure	Rebuild failed on target physical disk on page 181
2349	Failure	Bad disk block could not be reassigned on page 182
2350	Failure	Unrecoverable disk media error during rebuild on page 182

Power supply detected a failure

A power supply has been disconnected or has failed. The following information is displayed:

- Sensor location (location in chassis)
- Chassis location: (name of chassis)
- Previous state was: (state)
- Power Supply type: (type of power supply)
- <Additional power supply status info)
- Configuration error type: (if in configuration error state, the type of configuration error)

Troubleshooting a power supply failure

Procedure

1. Check if the power supply has been disconnected.
2. If the power supply is connected, it has failed.

Replace the power supply.

Device failed

A storage component such as a physical disk has failed.

Troubleshooting a device failure

Procedure

1. Replace the failed component.
2. Perform a rescan after replacing a disk.

Virtual disk failed

One or more physical disks included in the virtual disk have failed.

Troubleshooting a virtual disk failure

Procedure

1. Replace the failed disk(s).
2. Create a new virtual disk and restore from a backup.

Virtual disk degraded

There are two possible causes:

- A physical disk in the disk group has been remove
- A physical disk included in a redundant virtual disk has failed

Troubleshooting a virtual disk degradation

Procedure

1. If a physical disk was removed from the disk group:
   a. Replace the disk or restore the original disk.
   b. Perform a rescan after replacing the disk.
2. If a physical disk included in a redundant virtual disk has failed:
   a. Configure a hot spare for the virtual disk if one is not already configured.
   b. Rebuild the virtual disk.

   When using an Expandable RAID Controller (PERC) PERC 3/SC, 3/DCL, 3/DC, 3/QC, 4/SC, 4DC, 4eDC, 4/Di, CERC ATA100/4ch, PERC5/E, PERC5/i or a Serial Attache SCSI (SAS) 5/iR controller, rebuild the virtual disk by first configuring a hot spare for the disk, then initiating a write operation to the disk. The write operation will initiate a rebuild of the disk.

Virtual disk check consistency failed

A physical disk in the virtual disk failed or there is an error in the parity information.

Troubleshooting a virtual disk consistency failure

Procedure

1. Replace the failed physical disk.
2. Rebuild the physical disk.
3. When the rebuild is finished, restart the check consistency operation.

Physical disk initialize failed

The physical disk has failed or is corrupt.

Troubleshooting a physical disk initialization failure

Procedure

1. Replace the failed or corrupt disk.
2. Restart the initialization.

Physical disk rebuild failed

A physical disk in the virtual disk has failed or is corrupt, or a user may have cancelled the rebuild.

Resolving a physical disk rebuild failure

Procedure

1. Replace the failed or corrupt disk.
2. Rebuild the virtual disk.

Temperature exceeded maximum threshold

The temperature has exceeded the maximum failure threshold. The physical disk enclosure is too hot. There are several possible causes: a fan may have failed, the thermostat may be set too high, or the room temperature may be too hot.

Troubleshooting a temperature above maximum threshold alarm

About this task

Check for the following factors which may cause overheating.

Procedure

1. Verify the fan is working.
2. Check the thermostat settings.
3. Check if the enclosure is near a heat source.
4. Make sure the enclosure has enough ventilation.
5. Make sure the room is not too hot.
6. See the physical disk enclosure documentation for more diagnostic information.

Temperature dropped below minimum threshold

The temperature has dropped below the minimum failure threshold. The physical disk enclosure is too cool

Troubleshooting a temperature below minimum threshold alarm

Procedure

1. Check if the thermostat setting is too low.
2. Check if the room temperature is too cool.

SMART configuration change

A disk has received a SMART alert (predictive failure) after a configuration change. The disk is likely to fail in the near future.

Troubleshooting a SMART configuration change alarm

Procedure

1. If the physical disk is a member of a non-redundant virtual disk, back up the data before replacing the disk.
2. Replace the disk that has received the SMART alert.

Rebuild completed with errors

In some situations, a rebuild may complete successfully while also reporting errors. This may occur when a portion of the disk containing redundant (parity) information is damaged.

Restoring data from a rebuild which completed with errors

About this task

The rebuild process can restore data from the healthy portions of the disk but not from the damaged portion. If the backup on the virtual disk is successful, the user data on the virtual disk has not been damaged.

If the backup encounters errors, the user data has been damaged and cannot be recovered from the virtual disk. In this case, the only possibility for recovery is to restore from a previous backup of the virtual disk.

Procedure

1. Backup the degraded virtual disk.
   a. If the backup is successful, continue with Step 2.
   b. If the backup encounters errors, restore from a previous backup of the virtual disk.
2. Perform a consistency check on the virtual disk that you have backed up.
3. Restore the virtual disk onto the healthy array disks.

Controller battery needs to be replaced

The controller battery cannot recharge. The battery may be old or the charger may not be working.

Replacing the battery pack

Procedure

Replace the battery pack.

Storage Management has lost communication

%1 Storage Management has lost communication with the controller. The controller driver or firmware may be experiencing a problem. The %1 in the message is a substitution variable which displays text and varies depending on the situation.

Restoring communication with Storage Management

Procedure

1. Reboot the system.
2. If the problem is not resolved, contact Avaya Technical Support.

Physical disk Clear operation failed

A Clear task was being performed on a physical disk but the task did not complete successfully. The controller may have lost communication with the disk, the disk may have been removed, or the cables may be loose or defective.

Troubleshooting a disk Clear failure

Procedure

1. Verify that the disk is present and not in a failed state.
2. Make sure the cables are attached securely
3. Restart the Clear task.

Uncorrectable media error detected

The Patrol Read task has encountered an error that cannot be corrected. There may be a bad disk block that cannot be remapped.

Troubleshooting an uncorrectable media error

Procedure

1. Backup the data.
2. If you are able to back up the data successfully:
   a. Fully initialize the disk
   b. Restore from backup.

Physical disk puncture

A block on the physical disk has been punctured by the controller.

The controller encountered an unrecoverable medium error when attempting to read a block on the physical disk and marked that block as invalid. If the controller encountered an unrecoverable medium error on a source physical disk during a rebuild or reconfigure operation, it will also puncture the corresponding block on the target physical disk. The invalid block will be cleared on a write operation.

Resolving a physical disk puncture problem

Procedure

Backup the data.

Hot spare SMART polling faile

The controller firmware attempted a SMART polling on the hot spare but was unable to complete it. The controller has lost communication with the hot spare.

Restoring communication with hot spare

Procedure

1. Check the health of the disk assigned as a hot spare.
2. If the disk assigned as a hot spare is not in a healthy state:
   a. Replace the unhealthy disk.
   b. Reassign the hot spare.
3. Make sure the cables are securely attached.

Multi-bit ECC error

An error involving multiple bits has been encountered during a read or write operation, indicating data loss.

Resolving a Multi-bit ECC error

Procedure

1. See the hardware documentation for information on replacing the dual in-line memory module (DIMM).

The DIMM is a part of the controller battery pack.

2. Replace the DIMM.
3. You may need to restore data from backup.

Bad physical connection

The message `Bad PHY %1` indicates there is a problem with a physical connection or PHY. The %1 is a text string which varies depending on the situation.

Restoring a bad physical connection

Procedure

Contact Avaya Technical Support.

Bad block table is full

The bad block table is used for remapping bad disk blocks. When the table is full, bad disk blocks can no longer be remapped, disk errors can no longer be corrected, and data loss occurs. The %1 in the message indicates which block is bad - `Unable to log block %1`.

Resolving a bad block table error

Procedure

1. Replace the disk which is generating this alert.
2. If necessary, restore your data from backup.

Single-bit ECC error

The DIMM is malfunctioning. Data loss or data corruption may be imminent.

Resolving a single-bit ECC error

Procedure

1. See your hardware documentation for information on replacing the DIMM.
   The DIMM is a part of the controller battery pack.
2. Replace the DIMM immediately to avoid data or loss data corruption.

Single-bit ECC error, no further alerts

The DIMM is malfunctioning. Data loss or data corruption is imminent. No further alerts will be generated.

Resolving a single-bit ECC error

Procedure

1. See your hardware documentation for information on replacing the DIMM.
   The DIMM is a part of the controller battery pack.
2. Replace the DIMM immediately to avoid data or loss data corruption.

BGI completed with uncorrectable errors

The BGI task encountered errors that cannot be corrected. The virtual disk contains physical disks that have unusable disk space or disk errors that cannot be corrected.

Troubleshooting BGI uncorrectable errors

Procedure

1. Review other alert messages to identify the physical disk that has errors.
2. Replace the physical disk that contains the disk errors.
3. If the virtual disk is redundant, you can replace the physical disk and continue using the virtual disk.
4. If the virtual disk is non-redundant, recreate the virtual disk after replacing the physical disk.
5. Run Check Consistency to check the data after replacing the disk.

Rebuild failed on source physical disk

The rebuild failed due to errors on the source physical disk. You are attempting to rebuild data on a disk that is defective.

Resolving a source rebuild failure

Procedure

1. Replace the source disk.
2. Restore from backup.

Rebuild failed on target physical disk

The rebuild failed due to errors on the target physical disk. You are attempting to rebuild data on a disk that is defective.

Resolving a target rebuild failure

Procedure

1. Replace the target disk.
2. If a rebuild does not automatically start after replacing the disk, initiate the rebuild task.
3. If the rebuild still does not start, assign the new disk as a hot spare to initiate the rebuild.

Bad disk block could not be reassigned

A bad disk block could not be reassigned during a write operation.

A write operation could not complete because the disk contains bad disk blocks which could not be reassigned. Data loss may have occurred and data redundancy may also be lost.

Resolving a bad disk block reassignment

Procedure

Replace the disk.

Unrecoverable disk media error during rebuild

The rebuild encountered an unrecoverable disk media error.

Resolving an unrecoverable rebuild disk media error

Procedure

Replace the disk.

Appendix C: S8800 Alarm Messages

Some hardware or environment alarms can be tested by simply pulling the power supply AC cord or the power supply itself, pulling the hard disk, and for the ambitious, removing the server cover and pulling a fan. for other alarms, the **`ipmitool`** command is more practical. Examples of using **`ipmitool`** are:

- ipmitool event “Drive 0 Status” “Predictice Failure” asserted
- ipmitool event “Ambient Temp” “ucr” asserted
- ipmitool event “Planar 5V” “ucr” asserted

The following table contains alarm messages for the S8800 server.

Source	Message	Event Type	Alarm Level
ipmievd	Temperature sensor Ambient Temp Upper Critical going high (Reading 45 > Threshold 41 degrees C)	Alarm	Major
ipmievd	Temperature sensor Ambient Temp Upper Critical going low (Reading 40 < Threshold 41 degrees C)	Clear	
ipmievd	Voltage sensor Planar 3.3V Upper Critical going high (Reading 3.59 > Threshold 3.56 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 3.3V Upper Critical going low (Reading 3.54 < Threshold 3.56 Volts)	Clear	
ipmievd	Voltage sensor Planar 3.3V Lower Critical going low (Reading 3.01 < Threshold 3.04 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 3.3V Lower Critical going high (Reading 3.07 > Threshold 3.04 Volts)	Clear	
ipmievd	Voltage sensor Planar 5V Upper Critical going high (Reading 5.63 > Threshold 5.58 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 5V Upper Critical going low (Reading 5.54 < Threshold 5.58 Volts)	Clear	
ipmievd	Voltage sensor Planar 5V Lower Critical going low (Reading 4.43 < Threshold 4.47 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 5V Lower Critical going high (Reading 4.52 > Threshold 4.47 Volts)	Clear	
ipmievd	Voltage sensor Planar 12V Upper Critical going high (Reading 13.55 > Threshold 13.45 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 12V Upper Critical going low (Reading 13.34 < Threshold 13.45 Volts)	Clear	

ipmievd	Voltage sensor Planar 12V Lower Critical going low (Reading 10.58 < Threshold 10.69 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar 12V Lower Critical going high (Reading 10.80 > Threshold 10.69 Volts)	Clear	
ipmievd	Voltage sensor Planar VBAT Lower Critical going low (Reading 2.07 < Threshold 2.10 Volts)	Alarm	Major
ipmievd	Voltage sensor Planar VBAT Lower Critical going high (Reading 2.12 > Threshold 2.10 Volts)	Clear	
ipmievd	Fan sensor Fan 1A Tach Lower Critical going low (Reading 424 < Threshold 530 RPM)	Alarm	Major
ipmievd	Fan sensor Fan 1A Tach Lower Critical going high (Reading 636 > Threshold 530 RPM)	Clear	
ipmievd	Power Supply sensor PS 1 Status - Failure detected Asserted	Alarm	Major
ipmievd	Power Supply sensor PS 1 Status - Failure detected Deasserted	Clear	
ipmievd	Power Supply sensor PS 2 Status - Failure detected Asserted	Alarm	Major
ipmievd	Power Supply sensor PS 2 Status - Failure detected Deasserted	Clear	
ipmievd	Power Supply sensor PS 1 Status - Power Supply AC lost Asserted	Alarm	Major
ipmievd	Power Supply sensor PS 1 Status - Power Supply AC lost Deasserted	Clear	
ipmievd	Power Supply sensor PS 2 Status - Power Supply AC lost Asserted	Alarm	Major
ipmievd	Power Supply sensor PS 2 Status - Power Supply AC lost Deasserted	Clear	
ipmievd	Power Supply sensor Power Unit - Redundancy Lost	Alarm	Major
ipmievd	Power Supply sensor Power Unit - Fully Redundant	Clear	
ipmievd	Drive Slot sensor Drive 0 Status - Drive Present Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 0 Status - Drive Present Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 1 Status - Drive Present Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - Drive Present Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 0 Status - Drive Fault Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - Drive Fault Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 0 Status - Predictive Failure Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 0 Status - Predictive Failure Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 1 Status - Predictive Failure Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - Predictive Failure Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 0 Status - In Critical Array Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 0 Status - In Critical Array Deasserted	Clear	

ipmievd	Drive Slot sensor Drive 1 Status - In Critical Array Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - In Critical Array Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 0 Status - In Failed Array Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 0 Status - In Failed Array Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 1 Status - In Failed Array Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - In Failed Array Deasserted	Clear	
ipmievd	Drive Slot sensor Drive 0 Status - Rebuild Aborted Asserted	Alarm	Major
ipmievd	Drive Slot sensor Drive 1 Status - Rebuild Aborted Asserted	Alarm	Major

Appendix D: Light path diagnostics

About light path diagnostics

Light path diagnostics is a system of LEDs on various external and internal components of the server. When an error occurs, LEDs are lit throughout the server. By viewing the LEDs in a particular order, you can often identify the source of the error.

When LEDs are lit to indicate an error, they remain lit when the server is turned off, provided that the server is still connected to power and the power supply is operating correctly.

Using light path diagnostics to identify system errors

About this task

If an error occurs, view the light path diagnostics LEDs in the following order:

Procedure

1. Look at the operator information panel on the front of the server. Check if the information LED or system error LED is lit
2. View the light path diagnostics panel. Lit LEDs on this panel indicate the type of error that has occurred.

   Important:

   The checkpoint code display does not provide error codes or suggest components to be replaced. The checkpoint code is an internal code used for IBM development only and is subject to change over time. Ignore this code unless you have a specific request from Avaya to note it .
3. Remove the server cover while the server is connected to power and look inside the server for lit LEDs.

   Important:

   Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See Protecting against ESD damage on page 10 for more information.

   Certain components inside the server have LEDs that are lit to indicate the location of a problem. For some components, such as dual inline memory modules (DIMMs)

and fans, these LEDs can help you identify the problem. For other components, these LEDs are not useful.

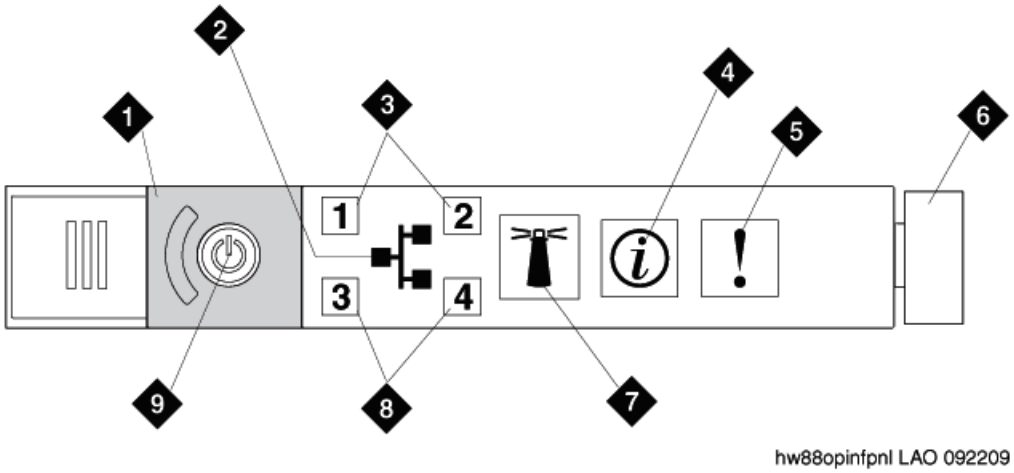
Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped, which means that you can remove or install the component while the server is running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.

Related topics:

Removing the server cover
Operator information panel on page 188
Accessing the light path diagnostics panel on page 189
System board LEDs on page 200

Operator information panel

The operator information panel is located on the front of the server.



1	Power control button cover
2	Ethernet icon LED
3	Ethernet activity LEDs These LEDs indicate that the server is transmitting or receiving signals on the Ethernet port that corresponds to the lit LED.
4	Information LED

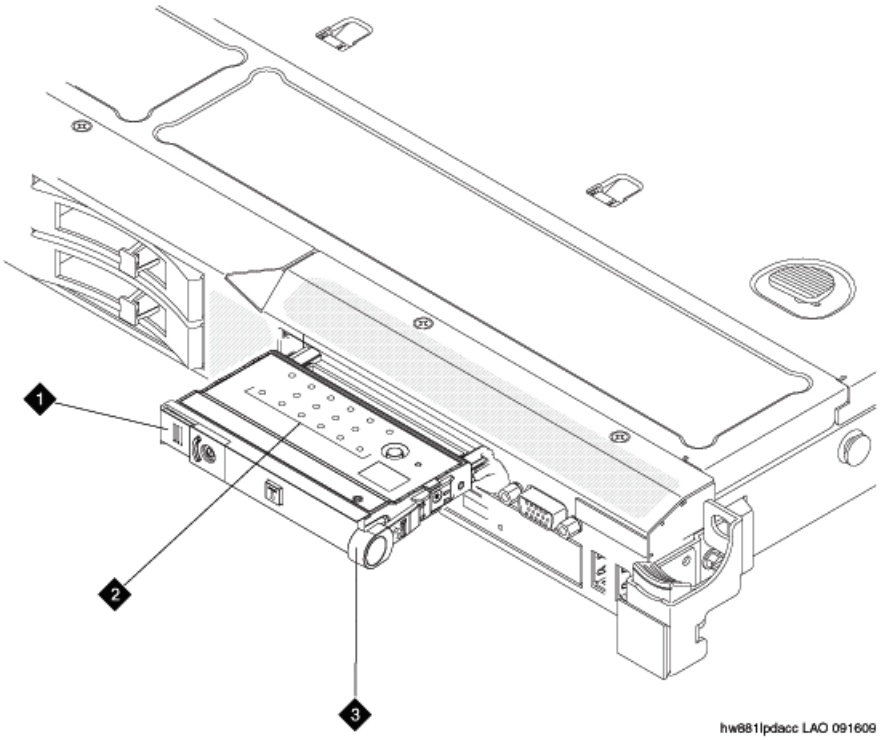
	This LED indicates that a noncritical event has occurred. An LED on the light path diagnostics panel is also lit to help isolate the error.
5	System error LED This LED indicates that a system error has occurred. An LED on the light path diagnostics panel is also lit to help isolate the error.
6	Release latch Slide this latch to the left to access the light path diagnostics panel, which is behind the operator information panel.
7	Locator button and LED Use this LED to visually locate the server among other servers. It is also used as the physical presence for Trusted Platform Module (TPM). Press this button to turn on or turn off this LED locally. You can use IBM Systems Director to light this LED remotely. A system locator LED on the back of the server is also lit when this LED is lit.
8	Ethernet activity LEDs These LEDs indicate that the server is transmitting or receiving signals on the Ethernet port that corresponds to the lit LED.
9	Power control button and power-on LED Press this button to turn on and turn off the server. The states of the power-on LED are: • Off: AC power is not present, or the power supply or the LED itself has failed. • Flashing rapidly (4 times per second): the server is turned off and is not ready to be turned on. The power-control button is disabled. Approximately 3 minutes after the server is connected to AC power, the power-control button becomes active. • Flashing slowly (once per second): the server is turned off and is ready to be turned on. You can press the power-control button to turn on the server. • Lit: The server is turned on. **Note:** If this LED is off, it does not mean that there is no electrical power in the server. The LED might be burned out. To remove all electrical power from the server, you must disconnect the power cord from the electrical outlet.

Accessing the light path diagnostics panel

The light path diagnostics panel is on the top of the operator information panel.

Procedure

1. Slide the blue release button on the operator information panel to the left. Pull forward on the unit until the hinge of the operator panel is free of the server chassis.
2. Pull down on the unit, so that you can view the light path diagnostics panel information.



1	Operator information panel
2	Light path diagnostics LEDs
3	Release latch

3. Note any LEDs that are lit, and then reinstall the light path diagnostics panel in the server.

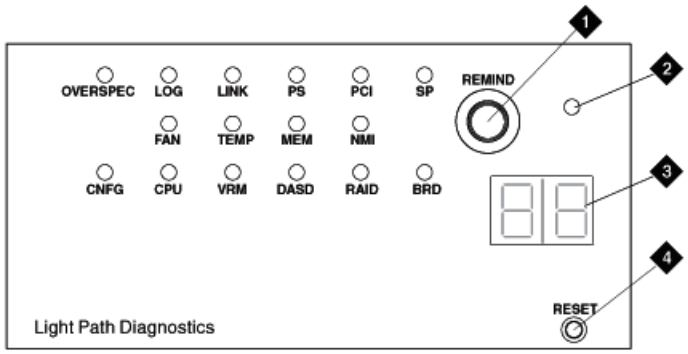
Important:

When you slide the light path diagnostics panel out of the server to check the LEDs, do not run the server continuously with light path diagnostics panel outside of the server. The panel should be outside of the server for only a short time. The light path diagnostics panel must remain in the server when the server is running to ensure proper cooling.

Related topics:

Light path diagnostics panel on page 191

Light path diagnostics panel



hw88lpdpnl LAO 092309

1	Remind button This button places the system-error LED on the front panel into Remind mode. In Remind mode, the system-error LED flashes once every 2 seconds until the problem is corrected, the server is restarted, or a new problem occurs. By placing the system-error LED indicator in Remind mode, you acknowledge that you are aware of the last failure but will not take immediate action to correct the problem. The remind function is controlled by the Integrated Management Module (IMM).
2	NMI button Pressing this button forces a nonmaskable interrupt to the microprocessor. You might have to use a pen or the end of a straightened paper clip to press the button. Use this button only when directed by your service provider.
3	Checkpoint code display The checkpoint code is an internal code used for IBM development only and is subject to change over time. The checkpoint code does not provide error codes or suggest components to be replaced. Ignore this code unless you have a specific request from Avaya to note it .
4	Reset button Pressing this button resets the server and runs the power-on self-test (POST). You might have to use a pen or the end of a straightened paper clip to press the button. The Reset button is in the lower-right corner of the light path diagnostics panel.

Troubleshooting light path diagnostic LEDs

OVERSPEC LED is lit

The OVERSPEC LED on the light path diagnostics panel is lit when the power supplies are using more power than their maximum rating.

Troubleshooting steps

Procedure

1. Check the power-supply LEDs for an error indication (AC LED and DC LED are not both lit, or the information LED is lit). Replace a failed power supply.
2. Replace the server.

Related topics:

Power supply LEDs

Removing a power supply on page 115

Installing a power supply on page 117

LOG LED is lit

The LOG LED on the light path diagnostics panel is lit when an error occurs.

Troubleshooting steps

Procedure

1. If any replaceable components need to be replaced, replace them.
2. If a faulty component is not replaceable, replace the server.

LINK LED is lit

The LINK LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

PS LED is lit

The PS LED on the light path diagnostics panel is lit when power supply 1 or power supply 2 fails.

Troubleshooting steps

Procedure

1. Check the power supply LEDs for an error indication (AC LED and DC LED are not both lit).
2. Make sure that the power supplies are seated correctly.
3. Remove one of the power supplies to isolate the failed power supply.
4. Replace the failed power supply.

Related topics:

Power supply LEDs

Removing a power supply on page 115

Installing a power supply on page 117

PCI LED is lit

The PCI LED on the light path diagnostics panel is lit when an error occurs on a PCI bus or on the system board. An additional LED is lit next to a failing PCI slot.

Troubleshooting steps

Procedure

1. Check the LEDs on the PCI slots to identify the component that caused the error.
2. If you have a monitor, check the system error log for information about the error.
3. If you cannot isolate the failing PCIe card by using the LEDs and the information in the system error log, remove one card at a time from the failing PCI bus. Restart the server after each card is removed.
4. Reseat the failing PCIe card.
5. Replace the server.

Related topics:

Removing a PCIe card on page 108
Installing a PCIe card on page 110

SP LED is lit

The SP LED on the light path diagnostics panel is lit when an error occurs on the service processor.

Troubleshooting steps

Procedure

1. Remove power from the server; then, reconnect the server to power and restart the server.
2. Report this error to your service provider for possible server replacement.

FAN LED is lit

The FAN LED on the light path diagnostics panel is lit when a fan fails, is operating too slowly, or has been removed. The TEMP LED might also be lit.

Troubleshooting steps

Procedure

1. Reseat the failing fan, which is indicated by a lit LED near the fan connector on the system board.
2. Replace the server.

TEMP LED is lit

The TEMP LED on the light path diagnostics panel is lit when the system temperature exceeds a threshold level. A failing fan can cause the TEMP LED to be lit.

Troubleshooting steps

Procedure

1. Make sure that the room temperature is not too high.
2. Make sure that the air vents are not blocked.
3. Determine whether a fan has failed. If it has, replace the server.

MEM LED is lit

The MEM LED on the light path diagnostics panel is lit when a memory configuration is invalid or a memory error occurs (both the MEM LED and CNFG LED might be lit).

Troubleshooting steps when both MEM LED and CNFG LED are lit

Procedure

1. Make sure that the DIMM configuration is supported.
2. Replace the DIMMs with a supported configuration.

Related topics:

Sequence for populating DIMM connectors on page 100
Removing a DIMM on page 103
Installing a DIMM on page 104

Troubleshooting steps when only MEM LED is lit

- If the server did not boot and a failing DIMM LED is lit:
  a. If you have a monitor, check for a PFA log event in the system event log .
  b. Reseat the DIMM.
  c. If the problem still exists, move the DIMM to a different slot.
  d. Look at the DIMM LEDs on the system board:
     - If the DIMM LED that corresponds to the new DIMM socket is lit, replace the DIMM.
     - If the DIMM LED that corresponds to the original DIMM socket is lit, replace server.
- If the server booted, the failing DIMM is disabled, and the DIMM LED is lit:
  a. If the LEDs are lit by two DIMMs and you have a monitor, check the system event log for a PFA event for one of the DIMMs, and then replace that DIMM. Otherwise, replace both DIMMs
  b. If the LED is lit by only one DIMM, replace that DIMM.

Related topics:

Sequence for populating DIMM connectors on page 100
Removing a DIMM on page 103
Installing a DIMM on page 104
System board LEDs on page 200

NMI LED is lit

The NMI LED on the light path diagnostics panel is lit when a nonmaskable interrupt occurs, or the NMI button is pressed.

Troubleshooting steps

Procedure

1. If you have a monitor, check the system event log for information about the error.
2. Shut down server and remove the power cord.
3. Check that all plug-in cards and devices are firmly installed.
4. Turn on the server.
5. If the server does not boot, replace server.

CNFG LED is lit

The CNFG LED on the light path diagnostics panel is lit when a hardware configuration error occurs. This LED is used with the MEM and CPU LEDs.

Troubleshooting steps

Procedure

1. Check that the memory modules are installed in the correct sequence.
2. Check that the memory modules are properly seated.
3. Replace the server.

Related topics:

Sequence for populating DIMM connectors on page 100
Removing a DIMM on page 103
Installing a DIMM on page 104

CPU LED is lit

When only the CPU LED is lit, a microprocessor has failed.

When the CPU and CNFG LEDs are lit, an invalid microprocessor configuration has occurred.

Troubleshooting steps

Procedure

1. Determine whether the CNFG LED is also lit.
   - If the CNFG LED is not lit, a microprocessor has failed.
   - If the CNFG LED is lit, then an invalid microprocessor configuration has occurred.
2. Replace the server if the microprocessor has failed.
3. Make sure that the microprocessors are compatible with each other if the microprocessor configuration is invalid.

   The microprocessors must match in speed and cache size. To compare the microprocessor information, run the Setup utility and select **System Information** > **System Summary** > **Processor Details**.

VRM LED is lit

The VRM LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

DASD LED is lit

The DASD LED on the light path diagnostics panel is lit when a hard disk drive fails or is missing.

Troubleshooting steps

Procedure

1. Check the LEDs on the hard disk drives for the drive with a lit status LED and reseat the hard disk drive.
2. If the error remains, replace the hard disk drive and then restart the server.

Related topics:

Hard disk drive LEDs

Removing a hard disk drive on page 113

Installing a hard disk drive on page 114

RAID LED is lit

The RAID LED on the light path diagnostics panel is not used.

Troubleshooting steps

Procedure

Ignore unless directed otherwise by Avaya.

BRD LED is lit

The BRD LED on the light path diagnostics panel is lit when an error occurs on the system board.

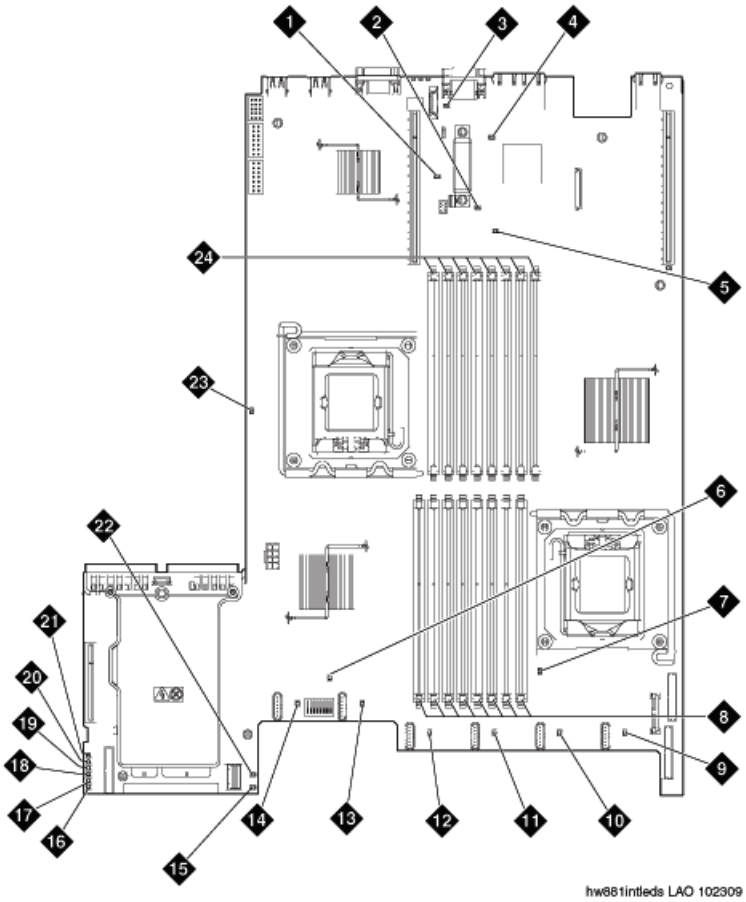
Troubleshooting steps

Procedure

Replace the server.

System board LEDs

The following figure shows the LEDs on the system board. A lit LED on or beside a component identifies the component as causing an error.



1	Slot 2 missing PCI riser card LED
2	Enclosure manager heartbeat LED
3	Battery LED
4	IMM heartbeat LED
5	Slot 1 missing PCI riser card LED
6	System error LED
7	Microprocessor 1 error LED
8	DIMM 1 through 8 error LEDs

9	Fan 1 error LED
10	Fan 2 error LED
11	Fan 3 error LED
12	Fan 4 error LED
13	Fan 5 error LED
14	Fan 6 error LED
15	240 VA error LED
16	Power channel A error LED
17	Power channel B error LED
18	Power channel C error LED
19	Power channel D error LED
20	Power channel E error LED
21	AUX power channel error LED
22	RAID riser-card LED
23	Microprocessor 2 error LED
24	DIMM 9 through 16 error LEDs