



Maintaining and Troubleshooting Avaya Aura[®] Session Manager

03-603325
Release 6.1
Issue 4.2
November 2011

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.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 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 its Hardware and Software ("Product(s)"). 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://support.avaya.com>. Please note that if you acquired the Product(s) 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/](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; 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, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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://support.avaya.com/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 Toll 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://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya®, Avaya Aura®, Avaya™, and Avaya Aura™ are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Hardware Support

For full hardware support, please see *Avaya Support Notices for Hardware Documentation*, document number 03-600759 on the Avaya Support Web site, <http://support.avaya.com>.

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://support.avaya.com>.

Chapter 1: Maintenance and Troubleshooting

This guide provides information regarding 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
- 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: 6.1.0.0.600019

The list of Session Managers are displayed on the System Manager. On the System Manager Home page, under **Elements**, select **Session Manager** to view all of the administered Session Managers and their software versions.

Customer account commands

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

- SMnetSetup
- upgradeSM
- /bin/mountiso
- /opt/Avaya/bin/changeMgmtIP
- /opt/Avaya/bin/configureNMS
- /opt/Avaya/bin/initDRS
- /opt/Avaya/bin/initTM
- /opt/Avaya/bin/rebootSM
- /opt/Avaya/bin/reconfigure
- /opt/Avaya/bin/restart
- /opt/Avaya/bin/setup_snmp
- /opt/Avaya/bin/shutdownSM
- /opt/Avaya/bin/smconfig
- /opt/Avaya/bin/start
- /opt/Avaya/bin/statapp
- /opt/Avaya/bin/swversion
- /opt/Avaya/contrib/bin/traceSM

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.

Observe 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

The Secure Access Link (SAL) uses the customer's existing Internet connectivity for remote support and alarming. All communication is outbound from the customer's environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS). The SAL requires upload bandwidth (customer to Avaya/Partner) of at least 90 KB/s (720 KB/s) with latency no greater than 150 ms (round trip).

Business Partners without a SAL Concentrator must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Direct SSH access to Session Managers is available from all servers.

Configuring the laptop for direct connection to the server

About this task

You must manually configure the IP address, subnet mask, and default gateway of the laptop before you connect the laptop to the server.



Note:

The following procedure is for Microsoft Windows XP. The procedure may differ slightly for other versions of Windows.

Procedure

1. Click **Start > Control Panel**.
2. Double-click **Network Connections > Local Area Connection**.
3. In the Local Area Connection Status dialog box, click **Properties**.
4. In the **This connection uses the following items** box, click **Internet Protocol (TCP/IP)**.
5. Click **Properties**.
6. In the Internet Protocol (TCP/IP) Properties dialog box, select **Use the following IP address** on the **General** tab.



Caution:

Do not click the **Alternate Configuration** tab.

7. In the **IP address** field, type 192 . 11 . 13 . 5.
 8. In the **Subnet mask** field, type 255 . 255 . 255 . 252.
 9. In the **Default gateway** field, type 192 . 11 . 13 . 6.
 10. Click **OK**.
-

Disabling proxy servers in Microsoft Internet Explorer

About this task

To connect directly to the services port, you must disable the proxy servers in Internet Explorer.

Procedure

1. Start Internet Explorer.
2. Click **Tools > Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Clear the **Use a proxy server for your LAN** option.

**Tip:**

When you need to reenable the proxy server, select the **Use a proxy server for your LAN** option again.

6. Click **OK** to close each dialog box.
-

Disabling proxy servers in Mozilla Firefox

About this task

To connect directly to the services port, you must disable the proxy servers in Firefox.

**Note:**

This procedure is for Firefox on a Windows-based laptop. The procedure may differ slightly if your laptop is running Linux or another operating system.

Procedure

1. Start Firefox.
2. Click **Tools > Options**.
3. Select the **Advanced** option.
4. Click the **Network** tab.
5. Click **Settings**.
6. Select the **No proxy** option.

**Tip:**

When you need to reenable the proxy server, select the appropriate option again.

7. Click **OK** to close each dialog box.
-

Connecting a laptop to the server

Before you begin

- Make sure that you have an SSH application such as PuTTY installed on your laptop.
- Configure the IP settings of the laptop for direct connection to the server.
- Disable use of proxy servers.

The remote services laptop is only for SSH access to Session Manager. Web access is not supported.

Procedure

1. Connect the laptop to the services port (Eth1) with a standard or crossover Ethernet cable. See [Server Ethernet Port Labels](#) for the services port label on a particular server.
2. Start an SSH client application (i.e., PuTTY) session.
3. In the **Host Name (or IP Address)** field, enter 192.11.13.6.
The system assigned the IP address 192.11.13.6 to the services port.
4. Verify that the protocol is **SSH**.
5. Verify that the **Port** is 22
6. Click on **Open**.



Note:

The system displays the PuTTY Security Alert window the first time you connect to the server.

7. Click **Yes** to accept the server's host key and display the PuTTY window.
 8. Login using **craft** (Session Manager) or **admin** (System Platform/System Manager).
 9. When you are finished with the session, enter `exit` to close PuTTY.
-

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

Alarms are classified by their effect on system operation and identify the system component which generates the alarm.

System Manager generates alarms to notify users of system events and can be configured to forward alarms to Avaya Services. The **configureNMS.sh** script forwards SNMP traps and Session Manager Element Manager failure events to a customer Network Management System (NMS).

See *Avaya Aura™ Session Manager SNMP Agent Application Note - Release 6.0* to view the format of the traps that can be administered.

Alarm status

The status of an alarm can be:

- **Raised:** An alarm has been generated. Software recovery actions have failed to correct the problem.
- **Acknowledged:** The alarm is being investigated. This state is set manually.
- **Cleared:** The problem has been fixed and the alarm has been cleared. This state is set manually.

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 that the alarm is missing the severity but still matches one of the established alarm rules. It 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. They are not alarms but an indication that something is not quite right. These failures are not reported to a services organization. These alarms are displayed in purple.

The colors of the severities can be changed.

Forwarding alarms to Avaya Services

About this task

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

Procedure

1. On the System Manager console, under **Services**, select **Configurations > Settings > SPIRIT > DataTransport Config**
2. Enter information in the fields as described in the [DataTransportConfig field descriptions](#) on page 18.
3. Click the **Commit** button when finished.

Data Transport Config field descriptions

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

Name	Description
Connection Avaya production FQDN	Fully qualified domain name of the target enterprise for a connection (customer, Business Partner, or Avaya).
Connection Avaya production keyAlias	Alias of a key in the keyStore that is used for client authentication in HTTPS session when communicating with an upstream server. Typically is used when Avaya is the upstream server. This is an optional field.

Name	Description
Connection Avaya production platform qualifier	Logical name for the target enterprise.
Connection Avaya production primary URL	Primary URL of the platform.
Connection Avaya production useProxy	Specifies whether to use proxies for this platform (true or false)
Connection set	Set of connections used by the SAL for data transport. Each connection must have a Platform Name, Target FQDN, and Primary URL elements. Backup URL elements are optional.
Https session timeout	Specifies the maximum duration of HTTPS authentication sessions before they need to be re-negotiated.
Max message exchange size	Specifies the maximum size of the messages that the data transport may send or receive in one bundle. Avaya recommends that you do not change the default value unless there is a need.
Max queue memory	Specifies the maximum amount of memory on disk that the queue can occupy. Avaya recommends that you do not change the default value unless there is a need.
Max send transaction time	Specifies the maximum amount of time spent in a transaction when trying to send upstream. Avaya recommends that you do not change the default value unless there is a need.
Organization FQDN	A fully qualified domain name that uniquely identifies the business organization that the SAL platform resides in.
Polling interval	The time between polling for messages from each enterprise platform. Specify 0 to turn off polling.
Proxy address	The domain name or IP address of the proxy to use.
Proxy password	The password to use with the proxy.
Proxy port	The port of the proxy server.
Proxy type	The type of proxy to use (HTTP or SOCKS).

Name	Description
Proxy use authentication	Specifies whether or not to use authentication to access the proxy server (true or false).
Proxy user	The user name to use with the proxy.
Server status reset interval	The time between the server marking a URL as unreachable and attempting to connect to that URL.
Spirit platform qualifier	A logical name for the target enterprise.

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. On the System Manager console, under **Services**, select **Configurations > Settings > AlarmManagementService > Alarm Management**
2. Click the **Edit** button.
3. Enter the appropriate information in the fields as described in the [AlarmMgmt field descriptions](#) on page 20.
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.

Alarm Management field descriptions

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

Name	Description
Email from address	Email address of the alarm manager
Email hostname	Email address of the SMTP host server
Email to addresses	Address(es) where alarms are forwarded. The addresses are separated by a comma.
Email user id	Email address of the sender
Federation member platform name	A fully qualified Data Transport address to which alarms are forwarded
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, 987.65.43.21:9162]  Note: The [] must surround the destination IP address(es) and port(s).

Viewing alarms

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Alarms** in the left navigation pane.
3. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
4. Click **View**.

Result

The Alarm - View Alarm Detail page displays the alarm details.

Filtering displayed alarms

The criteria for filtering the alarms that are displayed on the alarm screen are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criterion on the selected alarms.

Procedure

1. On the System Manager console, under **Services**, select **Events**
2. On the **Alarming** page, select the alarms you want to filter.
3. Select **Filter: Enable** at the top right corner of the Alarm List table.
4. Select the filter criteria you want to apply to the selected alarms.

The **Status** and **Severity** fields have drop-down menus.

You can enter the alarm code in the Message field to find all alarms which contain a particular alarm code.

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.

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, under **Services**, click **Events**.
2. Click **Alarms** in the left navigation pane.

3. On the Alarming page, select an alarm and click **Change Status**.
You can select multiple alarms.
 4. 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 Microsoft Excel.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
 2. Click **Alarms** in the left navigation pane.
 3. On the Alarming page, perform one of the following steps:
 - To export an 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**.
 4. 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, under **Services**, click **Events**.
2. On the Alarming page, click **Advanced Search**.
3. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
The default value in the first drop-down field is **Time Stamp**.
4. Select or enter the search value in the third field.
5. If you want to add another search condition, click **+** and do the following:

- a. Select the AND or OR operator from the drop-down field.
- b. Repeat steps 3 and 4.

Click - to delete a search condition. You can delete a search condition only if you have added more than one search condition.

6. Click **Search** to find alarms for the given search conditions.

Alarming field descriptions

The Alarming home 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	Specifies the date and time when the alarm is generated.
Severity	Specifies the severity of the alarm.
Status	Specifies the current status of the alarms.
Host Name / SysName	Specifies the name of the host server that generated the alarm. In case of trap listener, this column specifies the system name.
Source IP Address	Specifies the IP address of the system that generated the alarm.
Message	A short description of the problem that generated the alarm.
M/E Ref Number / SysOID	Specifies the unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.
Identifier	Specifies the unique identifier for an alarm.
Event ID	Specifies the log event ID if the alarm is generated from logs, or the Event OID if the

Field	Description
	alarm is generated from the trap listener service.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • Acknowledged • Cleared
Auto-Refresh Mode	Changes over 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 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.
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. • 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>Criteri on</th><th>Operators</th></tr> <tr> <td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr> <tr> <td>Severit y</td><td>Equals, Not Equals</td></tr> <tr> <td>Status</td><td>Equals, Not Equals</td></tr> </table>	Criteri on	Operators	Time Stamp	=, >, <, >=, <=, >=, !=	Severit y	Equals, Not Equals	Status	Equals, Not Equals
Criteri on	Operators								
Time Stamp	=, >, <, >=, <=, >=, !=								
Severit y	Equals, Not Equals								
Status	Equals, Not Equals								

Name	Description										
	<table> <tr> <th>Criteria on</th><th>Operators</th></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.	Criteria on	Operators	Host Name	Equals, Not Equals, Starts With, Ends With, and Contains	Identifier	=, >, <, >=, <=, >=, !=	Message	Equals, Not Equals, Starts With, Ends With, and Contains	M/E Ref Number	Equals, Not Equals, Starts With, Ends With, and Contains
Criteria on	Operators										
Host Name	Equals, Not Equals, Starts With, Ends With, and Contains										
Identifier	=, >, <, >=, <=, >=, !=										
Message	Equals, Not Equals, Starts With, Ends With, and Contains										
M/E Ref Number	Equals, Not Equals, Starts With, Ends With, and Contains										

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

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.

Procedure

Refer to the corrective actions for each alarm raised as guidelines for troubleshooting the alarm.

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 197.

Chapter 5: Logging

This section describes the options for logging on the **Events > Logs** menu:

- Log Harvester
- Managing log settings
- Log Viewer

Log Viewer is only used for viewing audit logs, including Session Manager administration changes. To view Session Manager logs, either use the System Manager Log Harvester or look at the logs on the Session Manager server directly.

Log Harvester

Log Harvester supports retrieval, archival and analysis of harvested log files stored on Secure Access Link (SAL) Agent-enabled hosts or elements. SAL communicates between the Log Harvesting Agent and the Logging Service.

For harvesting log files, the user creates a Harvest Profile. The profile contains a specific type of harvest criteria. A profile needs to be created once, and can be used anytime for logs which require that particular set of harvesting requirements. Every time the saved profile is executed, a new version of the archive is created based on the selected profile criteria. The collected logs are compressed into a single archive and stored on the System Manager. Archives are rotated based on the number of files and age.

Users can specify the host machine from which logs files are to be collected and which log files to collect.

Log Harvester provides a log viewer to view and analyze log files related to the profile. The log viewer has browse and search features which help with troubleshooting and diagnosing problems.

Accessing the Log Harvester service

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

About this task

You can create a new log harvesting profile by specifying the:

- IP address of the server on which the product is running
- Product name
- Directories or log files
- Filter text if you have selected one or more directories

You can harvest log files for products running on different servers by specifying multiple search criteria.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, click **New**.
4. On the Create New Profile page, enter the appropriate information in the **Profile Name** and **Profile Description** fields.
5. Select the IP address of the server, product, and directories or files from the respective fields.
To select multiple directories or files from the respective list boxes, press the **CTRL** key and click the individual directories or files. To clear a selection, press the **CTRL** key and click the selected item.
You can use the **+** button to add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server.

6. If you have selected one or more directories, enter a text pattern as the filter criteria in the text box below the **Directories / Filter Text** list box field.
During the harvesting operation, the system harvests only those files that match the filter text.
7. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

Create New Profile field descriptions

Use this page to create a new log harvesting profile for harvesting log messages from the log files for one or more products which may reside on one or more servers.

Name	Description
Profile Name	The name of the log harvesting profile
Profile Description	A brief description of the profile. This is an optional field.
IP	The IP addresses of the servers on which products are installed
Product	The products for which you can harvest logs
Directories / Filter Text	Lists the directories that contains the log files for the selected product
Files	The log files that you can harvest for the selected product
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory /a/b/c and enter the text com in this field, the harvest operation for this profile harvests the log files present under the directory /a/b/c. The log files contain com in the file name. This field does not support wild characters.

Button	Description
+	Use this button to specify another log harvesting request for a product.
-	Deletes the log harvesting request for the product.

Button	Description
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.

Viewing details of a log harvesting profile

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvesting page, select a profile and click **View**.
The Profile Criteria View page contains the details of the selected log harvesting profile.

Filtering log harvesting profiles

Use this feature to set filter criteria to view only those log harvesting profiles that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting profiles are the filter criteria.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, click **Filter: Enable**.
You can find this button at the top right of the table containing log harvesting profiles.
4. Enter or select the filter criteria.
You can filter the log harvesting profiles by the name, description and creator of the profiles.
5. Click **Filter: Apply**.



Note:

If no records matching the filter criteria are found, the Log Harvester page displays a message that no records matching the search criteria are found.

The log harvesting profile table displays the profiles that matches the specified filter criteria.

Submitting a request for harvesting log files

About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. After the request is successfully processed, the system, on which the products are installed, returns the harvested log files that are specified in the request. When you select a profile and click the **Request** button, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, enter the relevant information in the **Archive Name** and **Archive Description** fields.
The system saves the harvested log files in the specified archive file.
5. Click **Run Profile** to send a request.
The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then the system creates a zip file containing the harvested log files and saves the file at the specified location.

Viewing details of a log harvesting request

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.
If the table does not display any request, you need to submit a new request.
5. Click **View**.

The Harvest - View Harvest detail page displays the details of the selected request.

Filtering log harvesting requests

Use this feature to set filter criteria to view only those log harvesting requests that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting requests are the filter criteria.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click **Filter: Enable**.
You can find this button at the top right of the table containing the log harvesting profiles.
5. Enter or select the filter criteria.

You can filter the log harvesting requests by the:

- Request ID of the log harvesting request. For example, to view the requests starting with Request ID 5, enter 5.
- zip file name that stores the harvested files.
- description of the log harvesting request.
- location of the archived file that stores the harvested files.
- status of the log harvesting request.
- description of the log harvesting request status.

6. Click **Filter: Apply**.



Note:

If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

Result

The table containing log harvesting requests displays only those log harvesting requests that match the specified filter criteria.

Viewing the contents of harvested log files

About this task

Use this feature to view the log messages stored in the harvested log files for a product. You can view the contents of one log file at a time.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
 2. Click **Logs > Log Harvester** in the left navigation pane.
 3. On the Log Harvester page, select a profile and click **Requests**.
 4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.
If the table does not display any request, you need to submit a new request.
 5. Click **Show Files**.
 6. On the Search Archives page, select a harvested log file.
The system displays an error message if you select the product name or the IP Address of a server on which a product is installed.
 7. Click **Search**.
-

Searching for a text in a log file

Use this feature to search for a matching text in a log file of a product.

About this task

The search is based on Lucene Search. The search results are highlighted as per the Lucene highlighter. The highlight package contains classes to provide “keyword in context” features, typically used for highlighting search terms on the results page.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.
You must select a log harvesting request for which logs are successfully harvested.

5. On the Search Archives page, in the **Enter search text** field, enter the text that you want to search for.
 6. In the Tree view, navigate to the log file by expanding the folders and select the log file.
 7. Click **Search**.
The system displays the search results in the Search Result Panel. The **Search Result Panel** field displays the line numbers as hyperlinks on which the searched text is found.
 8. Click the in the **Search Result Panel** field.
When you click the hyperlink, the system displays the page containing the highlighted searched text in the **Log Browser Panel** field.
-

Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
 2. Click **Logs > Log Harvester** in the left navigation pane.
 3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
 4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.
 5. Click **Show files**.
On the Search Archives page, navigate the folders in the archive to view the harvested log files.
-

Downloading harvested log files

About this task

Use this feature to download the harvested log files of one or more products stored in a zip file on your local server.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs > Log Harvester** in the left navigation pane.

3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.
If the table does not display any request, you need to submit a new request.
5. Click **Show Files**.
6. On the Search Archives page, select a product name, IP address of the server on which one or more products are running, or a directory.
If you select a product name, the system creates a zip file containing the harvested log files for the selected product instances running on the same server or on different servers.
If you select an IP address of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the selected server.
If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
7. Click **Download**.
The system prompts you to save the file on your local server.
8. Click **Save**.

Harvest Archives field descriptions

Use this page to create a archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip file. You can use the buttons on this page to perform the following operations:

- Run the log harvesting requests in a selected profile.
- View the details of the execution of a log harvesting request
- View the log files stored in an archived file.

Name	Description
Archive Name	The name of the archive file that you want to create for storing the harvested log files.
Archive Description	A brief description of the archive. This is an optional field.

Name	Description
Request Id	The unique identification number assigned to a log harvesting request.

Name	Description
Zip file name	The name of the zip file that contains the harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of the log harvesting request
Status	The status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager failed to harvest the log messages for the product. • PARTIAL SUCCESS: The status is PARTIAL SUCCESS if System Manager partially harvests the log messages.
Status Time Stamp	The date and time when the execution status of the log harvesting request is generated.
Status Description	A brief description of the log harvesting request status. The description provides you the information about the success or failure of the log harvesting request.
Location	The location where the harvested log messages are archived.

Button	Description
Run Profile	Runs the log harvesting requests for the selected profile.
View	Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.
Show Files	Opens the Search Archives page. You can use this page to search for a text contained in the harvested log files, download log files of one or more products running on a same or different servers, view the contents of a log file.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.

Button	Description
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles present in the system based on the filter criteria.

Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

Name	Description
Profile Name	Specifies the name of the log harvesting profile
Profile Description	A brief description of the profile
Product	Specifies the name of the product for which logs are harvested.
Hosts	Specifies the IP address of the server on which the product resides.
Files	Specifies the names of the log files for which you can harvest log messages.
Directory	Specifies the directory that contains the log files.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory /a/b/c and enter the text com in this field, the harvest operation for this profile harvests the log files present under the directory /a/b/c. The log files contain com in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and takes you back to the Harvest Profile List page.
Refresh	Refreshes the records in the table.

Search Archives field descriptions

Use this page to perform the following activities on the log files contained in an archive:

- View the contents of harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local server.

Name	Description
Enter search text	The text that you want search for in the harvested log files.
List box	Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.
Log Browser Panel	Displays the contents of the selected log files
Search Results Panel	Displays the search results. This field displays the line numbers as hyperlinks in which the searched text is found. When you click the line number, the system displays the line containing the searched text at the top in the Log Browser Panel field.

Button	Description
Previous	Displays the log file contents on the previous page. This button is available only if the contents of a log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available only if the contents of a log files span across multiple pages.
Search	Searches for the occurrences of the text specified in the Enter search text field in the selected log files.
View	Displays the contents of the selected log files in the Log Browser Panel field.
Download	Downloads the selected log files present in the archive on your local server.

Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

View Parent

Name	Description
Request ID	Specifies the unique identification number assigned to a log harvesting request.
Archive	Specifies the name of the archive file that stores the harvested log files containing the log messages.
Status	Specifies the status of log harvesting requests. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Request Description	A brief description of the log harvesting request.

Harvest View

Name	Description
Product	Specifies the unique identification number assigned to a log harvesting request.
Status	Specifies the status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Host Name	Specifies the IP Address of the server on which the product resides.
Status Description	A brief description about the execution status of the request.

Name	Description
Status Time Stamp	Specifies the date and time when the execution status of the log harvesting request is generated.

Button	Description
Done	Closes this page and takes you back to the Harvest Archives page.
Refresh	Refreshes the records in the table.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.

Log Viewer

The logging service provides an interface for viewing logs and their details generated by System Manager or other components of the system. You can:

- view the details of a log
- search for logs based on search conditions
- set filters to view logs that match the filter conditions

Log Viewer is only used for viewing audit logs including Session Manager administration changes. To view Session Manager logs, either use the System Manager Log Harvester or look at the logs on the Session Manager server directly.

Viewing log details

Procedure

1. On the System Manager console, under **Services**, click **Events**.
 2. Click **Logs > Log Viewer** in the left navigation pane.
 3. On the Logging page, select a log.
 4. Click **View**.
-

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	Provides the option to select a log.
Log ID	Specifies the unique identification number that identifies the log.
Time Stamp	Specifies the date and time of the log generation.
Host Name	Specifies the name of the system from which the log is generated.
Product Type	Specifies the 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	Specifies the 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

Name	Description
	• Notice: Normal but significant condition • Informational: Informational messages • Debug: Debug-level messages  Note: The colors of severities do not indicate logging severities.
Event ID	Specifies the 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	Specifies the process on the device that has generated the message. This is usually the process name and process ID.
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.

Button	Description
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

Name	Description
	• 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 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.

Button	Description
-	Deletes a search condition

Searching for logs

Use the advanced search function to find logs based on certain specified conditions. The system displays only those logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager console, under **Services**, click **Events**.
 2. Click **Logs > Log Viewer** in the left navigation pane.
 3. On the Logging page, click **Advanced Search**.
 4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
 5. Select or enter the search value in the third field.
 6. 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.
 7. 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.
 8. 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. To apply the filters, you need 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, under **Services**, click **Events**.
2. Click **Logs > Log Viewer** in the left navigation pane.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.

4. Enter or select the filter criteria.
5. Click **Filter: Apply**.



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.

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

Log Event Codes

The table for Event IDs, their descriptions, and troubleshooting actions are found in [Appendix A: Log and Alarm Event IDs](#), on page 197

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 SIP entity

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



Note:

Survivable Remote Session Manager (BSM) does not support CDR.

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. Note that the passwords are set up for each Session Manager which has CDR enabled in the **Elements > Session Manager > Session Manager Administration** section of System Manager . 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 209 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. On the System Manager console, under **Elements**, select **Session Manager**.
 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 **Routing > SIP Entities**
 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 57 for the command description and usage.

Avaya Aura™ Session Manager R6.0 – SNMP Agent Whitepaper - Issue 1.1 provides some details of the SNMP capabilities of the Session Manager server. It also describes the SNMP trap generation capabilities provided by the System Manager application.

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 Security Module 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::snmplnGetNexts
- SNMPv2-MIB::snmplnGetRequests
- SNMPv2-MIB::snmplnGetResponses
- SNMPv2-MIB::snmplnNoSuchNames
- SNMPv2-MIB::snmplnPkts
- SNMPv2-MIB::snmplnReadOnlys
- SNMPv2-MIB::snmplnSetRequests
- SNMPv2-MIB::snmplnTooBig
- SNMPv2-MIB::snmplnTotalReqVars
- SNMPv2-MIB::snmplnTotalSetVars
- SNMPv2-MIB::snmplnTraps
- 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::snmpOutTooBig
- 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 **avaya123**

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, the default value of **avaya123** 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: Session Manager Dashboard

The Session Manager Dashboard page displays the overall status and health summary of each administered Session Manager.

Field	Description
Session Manager	Name of the administered Session Manager. Click on the name to go to the Session Manager Administration page.
Type	Core or BSM (Branch Session Manager)
Alarms	Raised alarm counts (Major & Critical, Minor, Warning with the format X/Y/Z). Click on the value to go to the Alarms List page.
Tests Pass	Maintenance test result. A green check mark indicates the test(s) passed, a red X indicates the test(s) failed. Click on the check mark or X to go to the Maintenance Tests page.
Security Module	Status of the Security Module of the Session Manager (UP or DOWN). Click on the status to go to the Security Module Status page.
Service State	Service state of the Session Manager.
Entity Monitoring	Number of down links and total links in the format down links/total links . Click on the value to review the down links on the Session Manager Entity Link Connection Status page.
Active Call Count	Number of calls that are active on this Session Manager.
Registrations	Current registration summary. Click on the value to go to the Registration Summary page.
Version	Current software version that is running on the Session Manager.

Session Manager Dashboard page field descriptions

The label, **As of (time)** indicates the time of the last update of information as displayed by the dashboard. The **Refresh** link in the table header refreshes the Session Manager Dashboard page with the most recent values of fields.

Button	Description
Service State > Deny New Service	Blocks incoming calls for the selected Session Manager or Session Managers but leaves active calls "up".
Service State > Accept New Service	Allows incoming calls for the selected Session Manager or Session Managers which were previously blocked using a Deny New Service request.
Shutdown System > Shutdown	Shuts down the selected Session Manager server or servers.
Shutdown System > Reboot	Reboots the selected Session Manager server or servers.

Name	Description
Session Manager	Name of administered Session Manager instance. You can click on the link to go to the Session Manager Administration page.
Type	Type of Session Manager instance. The type can be Core or Branch Session Manager.
Alarms	Count of raised alarms being demarcated on the basis of status codes as Major & Critical or Minor or Warning.
Tests Pass	The current results for periodic maintenance tests. Green means pass and red means fail.
Security Module Security Module Status	Possible states of Security Module matching existing Security Module Status page. The states are "Up", "Down", and "---" (unknown). You can click on the link to go to the detailed summary of the selected security module in the page.
Service State	The current service state of the Session Manager. The service state can be:

Name	Description
	• Accept New Service • Deny New Service You can click on the link to display the Session Manager Administration page.
Entity Monitoring	The status of monitoring the selected Session Manager entity, shown as the number of down links and number of total links. You can click on the link to display the Session Manager Entity Link Connection Status page. Entity Monitoring does not apply to a Session Manager administered as BSM, and therefore the status will always be unknown (---).
Active Call Count	The current active call counts for this session manager instance.
Registrations	The registration summary. You can click on the link to display the Registration Summary page.
Version	Version of the Session Manager software installed and has the following format: <major release number>.<minor release number>.<service pack number>.<patch number>.<build number>. Clicking on a version string displays the Session Manager Version Inventory page for that particular software version.

Chapter 9: 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	Specifies the name of the backup file.
Path	Specifies the path of the backup file.
Status	Indicates the status of the backup. The values are: • SUCCESS • FAILED
Backup Time	Specifies the 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 backing up data by specifying the date and time of running the job.

Job Details

Name	Description
Job Name	Specifies the name of the job.

Job Frequency

Name	Description
Task Time	Specifies 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 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 a data backup on a local server

Procedure

1. On the System Manager console, under **Services**, click **Backup and Restore**.
 2. On the Backup and Restore page, click **Backup**.
 3. On the Backup page, click **Local**.
 4. In the **File name** field, enter the file path and the name of the backup file that you want to create.
 5. Click **Now**.
If the backup is successful, the Backup and Restore page displays this message:
Backup created successfully!!
-

Scheduling a data backup on a local server

Procedure

1. On the System Manager console, under **Services**, click **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, Click **Local** option.
4. In the **File name** field, enter the name of the backup file that you want to create.

5. Click **Schedule**.
 6. Click **Commit**.
-

Viewing pending jobs

Procedure

1. On the System Manager console, under **Services**, click **Scheduler**.
 2. Click **Pending Jobs** in the left navigation pane.
-

Pending Jobs field descriptions

Use this page to view, edit, and delete the scheduled jobs that are pending for execution.

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. The types of job are: 1. System scheduled job: The job scheduled for the normal operation of the application. A system administrator can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job: The job that an administrator schedules for administering the application. 3. On-demand job: The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	Specifies the state of a job whether the job is active or inactive. The types of state are:

Name	Description
	• Enabled: An active job. • Disabled: An inactive job.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
View	Opens the Job Scheduling-View Job page that displays the details of the selected pending job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.
More Actions > View Log	Opens the Logging page that displays the logs for the selected pending jobs.
More Actions > Stop	Stops the selected job which is currently in running state.
More Actions > Enable	Changes the state of the selected pending job from inactive to active.
More Actions > Disable	Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.
More Actions > Schedule On Demand Job	Opens the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a pending job.
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: Apply	Filters pending jobs based on the filter criteria.

Button	Description
Select: All	Selects all the pending jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	Refreshes the pending job information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the pending jobs. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the pending jobs based on the specified search conditions and displays the search results in the Groups section.
Close	Cancels the search operation and hides the Criteria section.

Viewing list of backup files

Procedure

On the System Manager Console, click **System Manager Data > Backup and Restore**.

Result

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

Restoring a data backup from a local server

Procedure

1. On the System Manager console, under **Services**, click **Backup and Restore**.
 2. On the Backup and Restore page, click **Restore**.
 3. On the Restore page, click **Local**.
 4. In the **File name** field, type the file name that you want to restore.
 5. Click **Restore**.
 6. On the Restore Confirmation page, click **Continue**.
After the backup data is successfully restored, the system logs you out of the System Manager console.
-

Backup data retention

Backup data retention is controlled by the value of 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.

The **Maximum Backup Files** value controls the removal of old backup files.

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. On the System Manager console, under **Services**, select **Configurations > Settings > SMGR > SMGR Element Manager**
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.
-

Shut down/reboot the Session Manager server

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. On the System Manager console, under **Elements** , select **Session Manager**.
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. Click the **Service State** button.
4. Select **Deny New Service**.
5. Wait for all active calls on the Session Manager to end before shutting down or rebooting the server.

6. Click on the **Shutdown System** button.
 7. Select **Shutdown** or **Reboot** from the drop-down menu.
 8. 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 10: Data Retention

Configuration data is kept on the System Manager 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 Runtime Topology Service (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	Provides the option to select a data retention rule.
Rule Name	Specifies the name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	Specifies 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 the log, RTS, and alarm data files remain in the system.

Procedure

1. On the System Manager console, under **Services**, select **Configurations > Data Retention**
 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 11: Data Replication Service

Data Replication Service

The Data Replication Service (DRS) replicates data from the master database residing on the System Manager server to the databases on the client servers (i.e., Session Manager).

DRS supports the following two modes of replication:

- Replication in Repair mode: In repair mode, DRS replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of DRS.
- Automatic synchronization mode: After the database of the replica node is updated with the requested data, subsequent synchronizations occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after a fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.

On the DRS Replication page, you can:

- View replica nodes in a replica group.
- Replicate requested data from the System Manager master database to the database of the replica nodes if the databases are not synchronized.

Viewing replica groups

Procedure

On the System Manager console, under **Services**, click **Replication**.

Result

The system displays the Replica Groups page with the groups in a table.

Viewing replica nodes in a replica group

You can view the replica nodes in a group.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.

The Replica Nodes page displays the replica nodes for the select group.

Repairing a replica node

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of Data Replication Service.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
2. On the Replica Groups page, perform one of the following:
 - Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes**.
 - Click the name of the replica node under the **Replica Group** column.
3. On the Replica Nodes page, select a replica node and click **Repair**.

The **Synchronization Status** column displays the data replication status for the repairing replica node.

Repairing all replica nodes in a replica group

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
 2. On the Replica Groups page, select a replica group for which you want repair the replica nodes from the table displaying replica groups.
 3. Click **Repair**.
The **Synchronization Status** column displays the data replication status for the replica group.
-

Viewing replication details for a replica node

You can view the batch related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
 2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.
The Replica Nodes page displays the replica nodes for the selected replica group in a table.
 3. Select a replica node and click **View Details**.
The Data Replication page displays the replication details for the selected replica node.
-

Removing a replica node

About this task



Warning:

Removing replica nodes or groups can cause problems with systems using the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
 2. On the **Replica Groups** page, select a replica group in which you want to remove a node.
 3. Select **View Replica Nodes**.
 4. Select the **Replica Node Host Name** you want to remove.
 5. Select **Remove**.
-

Removing a replica node from queue

About this task



Warning:

Removing replica nodes or groups can cause problems with systems using the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager console, under **Services**, click **Replication**.
 2. On the **Replica Groups** page, select the replica group for which you want to remove the node from queue.
 3. Select **View Replica Nodes**.
 4. Select the **Replica Node Host Name** you want to remove.
 5. Select **Remove from Queue**.
-

Replica Groups field descriptions

You can use this page to:

- view all the replica groups in the enterprise. These replica groups are logical grouping of the replica nodes.
- replicate data requested by the replica node from the master database to the database of the replica nodes.
- view the replication status of the replica groups.

The page displays these fields when you All from the **Replica Group** field.

Name	Description
Select check box	Provides the option to select a group.
Replica Group	Specifies the name of the replica group. This is a hyperlink. When you click a group, the Replica Nodes page opens and displays the replica nodes for that group.
Synchronization Status	Specifies the replication status of the replica group. The system displays the out of sync status if any one of the group replica databases is not synchronized with the master database.

Button	Description
View Replica Nodes	Opens the Replica Nodes page. You can use this page to view replica nodes for a selected group.
Repair	Replicates data for a selected replica node that is not synchronized with the master nodes.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group which has requested data replication from the master database of System Manager.
- View the replication status of replica nodes in a group.

Name	Description
Select check box	Provides the option to select a replica node.
Replica Node Host Name	Specifies the IP address of the replica node.
Product	Specifies the name of the product running on the replica node.
Synchronization Status	Specifies the synchronization status of the replica node. The following are the status for when you click the Repair button on the page to perform a data replication for a replica node: • Ready for Repair: Indicates that database of the replica node is not synchronized with the master database. • Queued for Repair: Indicates that replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow. • Repairing: Indicates that the data replication process is in progress. The color code of the status is yellow. • Synchronized: Indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green. • Synchronization Failure: Indicates an error in data replication for the initial load. Resolving this issue requires manual intervention from the administrator.

Name	Description
	The system displays the following status during automatic replication of data from the master to the replica node: • Synchronizing: Indicates that the data replication is in progress for the replica node. The color code of the status is yellow. • Synchronized: Indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green.
Last Synchronization time	Specifies the last time when data synchronization or replication happened for the replica node.

Button	Description
View Details	Opens the Data Replication page. You can use this page to view the synchronization details for a replica node.
Repair	Replicates or synchronizes data from the master node to a selected replica node.
Remove	Removes the selected nodes from the group.
Show All Replica Groups	Takes you back to the Replica Groups page.

Data Replication field descriptions

General

Name	Description
Replica Node Group	Specifies the name of the group of the replica server.
Replica Node Host Name	Specifies the IP address of the replica server.

Name	Description
Last Synchronization Time	Specifies the last time and date when the data synchronization or replication happened for the replica node.
Synchronization Status	Specifies the synchronization status of the replica server.

Synchronization Status

Name	Description
Pending Batches	Specifies the batches for which data replication is pending.

Statistics

Name	Description
Cause of Error	A brief description of reason for failure to replicate or synchronize data.
Time of Error	Specifies the time when the error occurred.

Chapter 12: 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 and Survivable Remote 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.

Viewing Security Module status

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager**
 2. The **Session Manager Dashboard** screen displays the details and Security Module status for all administered Session Managers and Survivable Remote Session Managers (BSM).
 3. If the Security Module state of a particular Session Manager is not **Up**, see [Troubleshooting Security Module Sanity failure](#) on page 229
-

Security Module Status field descriptions

Click the **Show** or **Hide** link under **Details** column to display or hide the NIC Bonding details in the **NIC Bonding** section. The NIC bonding status column value shows the active slave interface or None in case of non-response from the security module. A warning icon in the NIC bonding column indicates the switching of slaves interfaces in the last 24 hours. An error icon indicates that there is no active interface and the NIC bonding is enabled. The **Details** column of the NIC Bonding section shows the following information:

- Slaves (eth2 and eth3) state
- Number of failures
- Time of last update on the event of switching between interfaces

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

Field	Description
Session Manager	Session Manager instance
Type	Displays the type of Session Manager instance, either Session Manager core (SM) or Survivable Remote Session Manager (BSM).
Status	Displays the status of the Security Module deployed for the Session Manager (Up or Down).
Connections	Total number of connections for the Security Module.
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.
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.
Default Gateway	Default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.
NIC Bonding	Displays whether NIC bonding is enabled or disabled.
Entity Links (expected/actual)	The expected value is the number of SIP Entities configured in the Routing Policy which have Entity Links to the Session Manager. The actual value is the number of SIP Entities currently configured on the security module. If these values do not match, the Synchronize action should be performed.

Security Module Status actions

The following actions can be performed on the Security Module Status page:

- **Refresh** – refreshes the statistics for all of the administered Session Manager instances..
- **Reset** – resets the security module for the selected Session Manager. You 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 *Administering 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.
- **Update Installed Certificates** – provides the capability of switching the active certificate being used by the security module to the default certificate. Additionally, refer to **Security Design** in *Administering Avaya Aura® Session Manager*, 03–603324 to understand the implications of doing this operation.
- **Connection Status** — allows you to view the current status of inbound and outbound links between the Session Manager security module and external hosts. It enables general-purpose monitoring and debugging activities such as:
 - identifying if Session Manager is required to be taken out of service
 - determining if links are secured or not
 - viewing link details and statistics

Investigating Security Module status

About this task

Possible causes for the Security Module 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.

Procedure

1. On the System Manager console, under **Services**, select **Replication**.
 2. The **Replica Group** associated with the Session Manager should display **Synchronized** for the **Synchronization Status**.
 3. If the **Synchronization Status** is not **Synchronized**:
 - a. Check the box in front of the affected Replica Group.
 - b. Click **View Details**.
 - c. Check the box in front of the affected Session Manager.
 - d. Click **View Details**.
 - e. Make sure the **Replica Node Host Name** is correct.
 - f. Click on **Done**.
 - g. Click on **Repair**.
 4. Click the **Refresh** button to see the latest status.
 5. If the status is **Down**, synchronize the security module to trigger an update:
 - a. Click on the button in front of the appropriate Session Manager instance in the Session Manager list.
 - b. Click the **Synchronize** button.
 - c. Click the **Refresh** button to see the latest status.
 6. If the status is still **Down**, reset the security module:
 - a. Select the appropriate Session Manager instance in the Session Manager list.
 - b. Select the **Reset** button.
-  **Warning:**
The Session Manager cannot process calls while the security module is being reset .
7. Select the **Refresh** button to see the latest status.
-

Connection Status

The Connection Status page displays the current status of inbound and outbound links between the Session Manager security module and external hosts.

This information may be used for general-purpose monitoring and debugging for:

- identifying when a Session Manager may be taken out of service
- determining if links are secured
- viewing specific connection details and statistics

The Connection Status page contains three sections:

- Summary
- Collect Filters
- Connection List

Connections Status Summary

The **Summary** section displays the total number of connections for the selected Session Manager: It displays totals for the following connection types:

- Active Connections
- Incoming
- Outgoing
- TCP
- TLS

Collect Filters

The **Collect Filters** section allows you to filter the information which is displayed in the Connection List table.

The information can be filtered by selecting one of the following in the **Type** field:

- None
- Remote FQDN
- Remote IP Address

Only one filter can be selected at a time.

Connection List

The Connection List section displays basic information for all of the active connections. You must click on the **Collect Connections** button in order to view the list.

The Connection List table displays the following information for each active connection:

- Details — Toggle button which shows/hides detailed information about the selected connection link
- Type — Link type (TH, UH, IH, User)
- Local IP — Local IP address
- Local Port — Local Security Module port
- Remote IP — Remote IP address
- Remote Port
- Remote FQDN
- Transport — Transport protocol (UDP, TCP, TLS)
- Policy — Security policy (Trusted, Default, Instance)

When you click on the **Show** button for a selected connection, the following information is displayed in a **Connection Details** box:

- Direction — Link direction (Inbound or Outbound)
- Creation time — The time when the link was created
- Last message received — The time when the last message was received on this connection
- Last message sent — The time when the last message was sent on this connection
- Messages/Bytes Received — The number of messages and bytes received
- Messages/Bytes Transmitted — The number of messages and bytes transmitted
- Message/Bytes Dropped — The number of messages and bytes dropped

For the TLS connection, the following information is also displayed:

- subject-name: The peer's name as it appears in its certificate subject-name field.
- alt-subject-name: The peer's alternative name and type as it appears in its certificate alt-subject-name field.
- CA: The certificate authority that has signed the peer's certificate.
- ciphers: The cipher-suite.

Clicking on the **Hide** button will hide the detailed information for the selected connection.

NIC bonding

NIC bonding uses multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port and to increase the redundancy for higher availability. Two NICs are bonded together to appear as if they are the same physical device, i.e., they

both have the same MAC address. NIC bonding provides backup if the primary Security Module interface fails or its port is switched off.

Before attempting NIC bonding, it is highly recommended that you verify the integrity and functionality of each NIC on its own. The cable itself or either of the ports the cable is plugged into can fail.

When NIC bonding is activated, the Security Module uses Eth2 as the primary interface and Eth3 as the secondary backup interface. A logical interface called bond0 is created to connect the two interfaces and has the IP address of the Security Module.

In order to administer NIC bonding, make sure both Eth 2 and Eth3 ports have network cables connected to the network.

Alarms are generated when one of the interfaces (Eth2/Eth3) is down. If both of the interfaces are down, an alarm is generated indicating that the bond0 interface is down.

The NIC bonding status for a Session Manager is displayed on the **Security Module Status** page.

Chapter 13: 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 checking the network connectivity to Session Manager instances and database functionality. 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 may fail if the server being tested 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. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
 2. Select **System Manager or a Session Manager to test** from the drop-down list.
 3. To run all of the tests, select **Execute All Tests**.
 4. To run only certain tests:
 - a. Select the test(s) to run from the test list.
 - b. Click on **Execute Selected Tests**.
-

Maintenance Test descriptions

Test Call Processing status

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

Test data distribution and redundancy link

This test only runs on the Session Manager. It tests if the mechanism by which Session Managers share data 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.

A test failure indicates a potential failure of link redundancy and Session Manager pass-through capabilities which could impact call processing in general and Call Admission Control.

The test is not run for a Session Manager if the current state of the Session Manager is set to **Deny New Service**.

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 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.

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.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to Avaya Technical Support.

Test Security Module Status

This test queries the basic status of the Security Module on a specified Session Manager. If the query is successful, the test passes. Otherwise, it fails.

Test Service Director Status

This test checks the status of the SIP A/S Service Director using a connection to SIP A/S. This test runs on a specified Session Manager. The test passes if the status of the service director is valid.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to Avaya Technical Support.

Test Service Host status

This test determines the running status (up/down) of a specified Session Manager. The test passes if the service host is up. The test fails if the service host has an invalid status.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to Avaya Technical Support.

Test SIP A/S Management Server Status

This test runs on a specified Session Manager. It 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, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to Avaya Technical Support.

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. Check for the following possible causes:

1. An upgrade or install is in progress.
2. The server could be down. Check the log, then check [Log Event Codes](#) on page 48 for the appropriate troubleshooting action.
3. There is a network outage. Run a ping test between the System Manager and the failing Session Manager to verify network connectivity.

Chapter 14: 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 are reduced since calls are not routed to the failed servers. The SIP Monitor continues to monitor the failed SIP entity. When the proxy replies, SIP messages are again be routed over that link.

SIP monitoring sends OPTIONS requests to SIP entities to determine whether they are up, partially up, or down. An entity is considered up if all of the addresses associated with it are up. An entity is down if all of its addresses are down. An entity is partially up if some, but not all, of its addresses are up. An address is considered down if its response to OPTIONS is:

- 408 Request Timeout
- 503 Service Unavailable (with no parenthetical text)
- 503 Service Unavailable (LSP is inactive)
- 503 Service Unavailable - System Busy
- 503 Service Unavailable (No media resources)
- 503 Service Unavailable (ESS is inactive)
- 504 Server Timeout

All other responses (including "503 Service Unavailable" with other parenthetical text, such as "503 Service Unavailable (Signaling Resources Unavailable)" results in the address to be considered up.

You can turn monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity is not 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 are monitored by that instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on are monitored.

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

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

Viewing 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 the 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, the link status is **partially down**. If all of the connections are down, the entity link status is **down**.

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager**
 2. Select **System Status > SIP Entity Monitoring**
 3. The **SIP Entity Link Monitoring Status Summary** page displays the SIP Entity Link monitoring status for all Session Manager instances.
-

SIP Entity Link Monitoring Status Summary page field descriptions

Button	Description
Entity Link Status for All Session Manager Instances: Run Monitor	Starts asynchronous demand monitor test for the selected Session Manager instances. Refresh link refreshes the status of the entity links for all administered Session Manager instances. The status displays the following details: • 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

Button	Description
	• 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: Run Monitor	Starts asynchronous demand monitor test for the selected SIP entities. 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.

Chapter 15: 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:

- SIP Tracer Configuration - defines the characteristics of messages to be traced for the capturing engine in the Security Module
- SIP 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. SIP messages that are dropped by any of the security 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 Security Module to capture packets.

SIP Tracer Configuration

The SIP Tracer Configuration page allows you to configure tracing properties for one or more Security Modules. 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 **Elements > 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 Instances:** Lists the administered Session Manager instances on which to apply the filters.

Tracer Configuration page field descriptions

Tracer Configuration

Name	Description
Tracer Enabled	SIP message tracing is enabled by default.
Trace All Messages	SIP message tracing is enabled for all SIP messages. In this case, other fields get disabled.
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.
Trace Dropped Messages	SIP message tracing is enabled to trace messages from calls dropped by the SIP firewall as well as by the SM100 proxy.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped check box is activated.
Send Trace to a Remote Server	Enables or disables SIP Tracing to an external host . This enables Session Manager to send all the (decrypted) SIP traffic out to an external host. Session Manager uses Syslog protocol for sending

Name	Description
	the SIP traffic (as used currently for SIP Tracing).
Remote Server FQDN or IP Address	FQDN or IP address of the remote syslog server.
Send Trace Method	Method used to transfer syslogs either using Stunnel (encrypted TCP) or Syslog (unsecure UDP) as mentioned below: • Syslog (unsecured UDP) — Traffic is send without being encrypted to remote server as specified in the “Remote Server FQDN or IP Address” to default syslog port. • Stunnel (encrypted TCP) — Traffic is send as encrypted (using stunnel) to remote server which is specified in the “Remote Server FQDN or IP Address” to the port specified in the input field “Stunnel Port”.
Stunnel Port	Port number that remote server’s stunnel is listening on. Stunnel provides several modes for far end certificate validation.

User Filter

Button	Description
New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
Delete	Delete a selected user filter or filters.

Name	Description
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
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

Name	Description
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Message Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.

Call Filter

Button	Description
New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.
Delete	Delete a selected call filter or filters.

Name	Description
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
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
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Call Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.

Name	Description
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 Instances

Name	Description
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.
Button	Description
Commit	Save the configuration changes.

Configuring SIP tracing

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > SIP Tracer Configuration**
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 104)
4. Set a call filter if desired ([Filtering by Call ID](#) on page 104)
5. Delete a filter if desired ([Deleting a filter](#) on page 105)
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 Security Module 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. On the System Manager console, under **Elements**, select **Session Manager > System Tools > SIP Tracer Configuration**
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 Security Module 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. On the System Manager console, under **Elements**, select **Session Manager > System Tools > SIP Tracer Configuration**
2. Scroll down to the **Call Filter** section.
3. 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 Security Module to capture packets.

7. Select the filter(s) to apply (checkbox).

Deleting a filter

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Tracer Configuration**
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

SIP 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:

Number of records retrieved versus displayed items: The Trace Viewer page displays the number of listed trace messages. Due to system performance, not all trace messages which match the filter criteria may be displayed. In this case, the value of **Number of records retrieved** in the bottom right corner of the screen 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.

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. On the System Manager Console, under **Elements**, select **Session Manager > System Tools > SIP Trace Viewer**
 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.
-

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 messages	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 active only if one or more trace records are displayed. The retrieved Trace 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.

Remote logging

Remote logging allows you to send SIP trace files to a remote server. The SIP Tracer remote logging feature supports both plain syslog (UDP) and encrypted tunnel (using stunnel). The following sections describe how to configure a Linux-based server to accept traces for these two options.

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

Unsecure UDP syslog server

Requirements for UDP syslog server

System Requirements for the unsecure UDP syslog server are:

- CentOS-based Linux server
- Required RPM syslogd (syslog server)

Configuring a syslog server (unsecure UDP)

About this task

The high-level steps for configuring an unsecure UDP syslog server are:

- Configure the server firewall to accept logs on UDP port 514
- redirect the tracer messages to a specific file
- enable logging from a remote system to listen to syslog UDP port 514
- configure the Session Manager to send SIP traces to the file

The output of the **netstat** command should be similar to the following (the bold fields are the important fields to note):

```
udp 0 0.0.0.0:514 0.0.0.0:* 21907/syslogd
```

Procedure

1. Configure the firewall to accept logs on UDP port 514. If you plan to send logs from more than one Session Manager, you need to add a rule for each IP address. The following command is an example of how to configure the Linux firewall to allow remote logging from a host associated with IP address 1.2.3.4:

iptables -I INPUT 1 -s 1.2.3.4 -p udp --dport 514 -j ACCEPT

2. Redirect the tracer messages to a specific file:
 - a. Open the syslog's configuration file **/etc/syslog.config** with your favorite editor.
 - b. Add the following line to the end of the file:
local2.info -/var/log/tracer.log
 - c. Write the file and close it.
 3. Enable logging from a remote system to syslog UDP port 514:
 - a. Open the file **/etc/sysconfig/syslog** with your favorite editor.
 - b. Modify **SYSLOGD_OPTIONS** to include the **-r** flag (i.e.,
SYSLOGD_OPTIONS="-r")
 - c. Write and close the file.
 - d. Restart the syslog service by entering the command **service syslog restart**
 - e. Enter the command **netstat -unpl | grep 514** to verify that syslog can listen on UDP port 514.
 The output should be similar to the **netstat** output described above.
 4. Configure the Session Manager:
 - a. On the System Manager console, navigate to **Elements > Session Manager > System Tools > SIP Tracer Configuration**
 - b. Make sure that the **Tracer Enabled** checkbox is checked.
 - c. Specify the remote syslog server FQDN or IP Address in the **Remote Server FQDN or IP Address** field.
 - d. Select **Syslog (unsecure UDP)** from the **Send Trace Method** drop-down list.
 - e. Select one or more Session Managers in the **Session Manager Instances** table.
 - f. Click the **Commit** button. This will send the configuration to all of the selected Session Managers, and they will redirect their output to the remote syslog server.
-

Secure TCP syslog server

Requirements for Secure TCP syslog server

System Requirements for the secure TCP (stunnel) syslog server are:

- Linux CentOS-based server
- Required RPMs:
 - nc — Netcat, a simple utility for reading and writing data across network connections
 - stunnel
 - syslogd

Configuring Secure TCP syslog server

About this task

The high-level steps for configuring a Secure TCP syslog server are:

- configure the firewall to accept connections/logs on UDP port 514 and the stunnel TCP port 50614 from the Session Manager
- redirect the tracer messages to a specific file
- enable internal logging to syslog UDP port 514
- redirect the output from UDP
- create a self-signed a certificate — the stunnel server requires a certificate (X.509) in order to work. For more information, see <http://www.stunnel.org/faq/certs.html>
- create a stunnel configuration file — this file contains:
 - the port that listens for encrypted traffic
 - the port to forward the decrypted traffic
 - the certificate to send to the client on tunnel establishment
- start the stunnel server process
- start the stunnel forwarding process to forward logs to syslog UDP port 514
- configure Session Manager to send SIP traces

The output of the **netstat** command should be similar to the following (the bold fields are the important fields to note):

```
udp 0 0.0.0.0:514 0.0.0.0:* 21907/syslogd
```

Procedure

1. Configure the firewall to accept connections/logs on UDP port 514 by entering the command **iptables -I INPUT 1 -i lo -p udp --dport 514 -j ACCEPT**
2. Configure the firewall to accept connections/logs on the stunnel TCP port from the Session Manager. Assuming the syslog server can listen to stunnel port 50614 and the Session Manager has an IP address of 1.2.3.4, the following is an example of the command to configure the firewall:
iptables -I INPUT 1 -s 1.2.3.4 -p tcp --dport 50614 -j ACCEPT
3. Redirect the tracer messages to a specific file:
 - a. Open the syslog's configuration file **/etc/syslog.conf** with your favorite editor.
 - b. Add the following line to the end of the file:
local2.info -/var/log/tracer.log
 - c. Write the file and close it.
4. Enable internal logging from a remote system to syslog UDP port 514:
 - a. Open the file **/etc/sysconfig/syslog** with your favorite editor.
 - b. Modify **SYSLOGD_OPTIONS** to include the **-r** flag (i.e.,
SYSLOGD_OPTIONS="-r")
 - c. Write and close the file.
 - d. Restart the syslog service by entering the command **service syslog restart**
 - e. Enter the command **netstat -unpl | grep 514** to verify that syslog can listen on UDP port 514.
 The output should be similar to the **netstat** output described above.
5. Enter the command **mknod /dev/udp c 30 36** to redirect the UDP output to the Linux server.
6. Create a self-signed certificate if it doesn't already exist by entering the command **openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem**
7. Create the stunnel configuration file using your favorite editor:
 - a. Create the file **/etc/stunnel/stunnelSyslogServer.conf**
 - b. Enter **cert = /etc/stunnel/stunnel.pem**
 - c. Enter a blank line.
 - d. Enter **[ssyslog]**
 - e. Enter **accept = IP_ADDRESS:STUNNEL_PORT**, where **IP_ADDRESS** is the IP address of the server. It must match the value that will be entered in the **Remote Server FQDN or IP Address** field on the **Tracer Configuration**

screen, and **STUNNEL_PORT** is the port that is used to communicate with the Session Manager.



Important:

Do not omit the colon between the IP address and stunnel port (1.2.3.4:50614)

- f. Enter **connect = 127.0.0.1:50614**
 - g. Enter **verify = 1**
 - h. Write and close the file.
 8. Start the stunnel server process by entering the command **stunnel /etc/stunnel/stunnelSyslogServer.conf**
 9. Verify that the stunnel process is running by entering the command **pgrep stunnel**. The output should display the process ID number of the listening stunnel.
 10. Start the stunnel forwarding process by entering the command **nc -k -l 50614 | tr '\n' '\0' | xargs -O -L 1 echo '<151>' > /dev/upd/127.0.0.1/514**
 11. Configure the Session Manager:
 - a. On the System Manager console, navigate to **Elements > Session Manager > System Tools > SIP Tracer Configuration**
 - b. Make sure that the **Tracer Enabled** checkbox is checked.
 - c. Check the **Send Trace to a Remote Server** checkbox.
 - d. Specify the remote syslog server FQDN or IP Address in the **Remote Server FQDN or IP Address** field.
 - e. Select **Stunnel (encrypted TCP)** from the **Send Trace Method** drop-down list.
 - f. Specify the remote stunnel port on the the remote stunnel server listens on.
 - g. Select one or more Session Managers in the **Session Manager Instances** table.
 - h. Click the **Commit** button. This will send the configuration to all of the selected Session Managers, and they will redirect their output to the remote syslog server.
-

Chapter 16: 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:

- **Routing > Adaptations, Dial Patterns, Entity Links, Locations, Policies, Domains, SIP Entities, Time Ranges**
- **Elements > 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 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 entity links.  Note: These are only core Session Manager instances.

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

Button	Description
	alternate routing choice and the lines are in the same order that the test attempted the destinations. 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. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Call Routing Test**
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.

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 17: Session Manager IP address and host name changes

This section describes the procedures for changing the following:

- Session Manager server Management Network IP address (network interface between Session Manager and System Manager)
- Session Manager Security Module IP address (call processing network interface)
- Session Manager host name

These attributes can be changed after the initial installation if the server needs to be moved elsewhere on a network.

To change the IP address or host name of the System Manager, refer to *Avaya Aura® System Manager 6.1 Release Notes* on the Avaya support web site. The changes are made using the System Platform Console Domain.

Changing the Security Module IP address

About this task

You must have web login access to the System Manager that is managing the 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 that is used for SIP phone registration settings using the new Security Module 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. Change the state of the Session Manager to **Deny New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.

- b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Deny New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
4. If the server is to be relocated:
 - a. Power down the server.
 - b. Relocate the server.
 - c. Power up the server.
5. Change the Security Module address of the Session Manager:
 - a. On the System Manager console, under **Elements**, select **Routing > SIP Entities**.
 - b. Select the appropriate Session Manager and click on **Edit**.
 - c. In the **FQDN or IP Address** field, enter the new IP address for the Security Module. *This is not the management IP address.*
 - d. Click on **Commit**.
6. Update any associated Security Module information:
 - a. Under **Elements**, select **Session Manager > Session Manager Administration**
 - b. Select the appropriate Session Manager instance and click **Edit**.
 - c. Change any necessary information such as the default gateway and QoS parameters for the Security Module.
 - d. Click on **Commit**.
7. Change the provisioning for all SIP entities with links to the changed Session Manager Security Module address using the entity's administration.

For example, if a Communication Manager communicates with the Session Manager, the Communication Manager signaling groups need to be updated in order to connect to the Session Manager at its new address.
8. After all provisioning has been changed, check the status of the Security Module:
 - a. Under **Elements**, select **Session Manager > System Status > Security Module Status**.
 - b. Make sure the **Status** for the Session Manager is **Up** and the IP address is correct.
9. Test the Session Manager:

- a. Under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
 - b. Select the Session Manager instance from the drop-down list (Select Target...)
 - c. Select **Execute All Tests**.
10. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Accept New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
11. Perform a PPM reload to tell the phones where the Session Manager has moved:
 - a. Under **Elements**, select **Session Manager > System Status > Registration Summary**.
 - b. Select the appropriate Session Manager.
 - c. Click on **Reload** and select **Reload Complete** from the drop-down menu to reload the phone with all of its data in order to use the new Session Manager IP address.
 - d. Click on **Confirm**.
 - e. On the status page, verify that all SIP endpoints have registered.

Changing the Session Manager IP address or host name

About this task

You must have web login access to the System Manager that is managing the Session Manager server.

The **SMnetSetup** command takes about 15 minutes to run, depending upon the size of the database.

Procedure

1. Change the state of the Session Manager to **Deny New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.

- b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Deny New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
2. Log in to the CLI of the Session Manager using the craft or customer login.
3. Enter **./SMnetSetup**
 - a. If you are changing the IP address of the Session Manager, enter the new IP address when you are prompted for the server's IP address.
 - b. If you are changing the host name of the Session Manager, enter the new host name when you are prompted for the server's host name.
 - c. Enter additional information as needed (netmask gateway, etc.)
 - d. Enter a new customer password when prompted.
 - e. After the time has been set, enter **y** at the prompt to continue.
 - f. If the System Manager IP address has changed, enter the new IP address. Otherwise, press the Enter key.
 - g. Enter the Enrollment Password from the System Manager at the prompt.
4. Update the Session Manager information:
 - a. On the System Manager web console, under **Elements**, select **Session Manager > Session Manager Administration**
 - b. Select the appropriate Session Manager and click **Edit**.
 - c. Update the information in the **Management Access Point Host Name/IP** field.
 - d. Click **Confirm**.
5. Test the Session Manager:
 - a. Under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
 - b. Select the Session Manager instance from the drop-down list (Select Target...)
 - c. Select **Execute All Tests**.
6. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.

- c. Click on **Service State**.
 - d. Select **Accept New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
7. Update the Session Manager Element information:
- a. Under **Elements**, select **Inventory > Manage Elements**.
 - b. Check the box in front of the appropriate Session Manager and click **Edit**.
 - c. Where applicable, update the value for the **Node** in the **Application** section and the **Host** value of **Access Point**.
 - d. Click **Commit**.
8. If the Identity Certificates contain the IP address or the host name of the Session Manager, make sure the certificates are reinitialized with the new IP address and/or host name:
- a. Under **Elements**, select **Inventory > Manage Elements**
 - b. Check the box in front of the appropriate Session Manager.
 - c. Select **More Actions > Configure Identity Certificates**
 - d. Select the management certificate.
 - e. Click **Replace**.
 - f. Enter the appropriate information in the fields.
 - g. Make sure **Replace this Certificate with Internal CA Signed Certificate** is selected.
 - h. Click **Commit**.
9. If a CDR adjunct is administered, you need to change the Session Manager IP address to the new Session Manager IP address.
-

Chapter 18: Managed Bandwidth Usage

The Managed Bandwidth Usage page displays Managed Bandwidth (Call Admission Control) real-time data. Measurement of bandwidth usage helps administrators to manage networks with multimedia calls. It displays a read-only table containing one row for each administered location and provides details on actual call counts and bandwidth usage for audio and video calls respectively.

You can expand each row to display a breakdown of usage and capacity by Session Manager which can be helpful in debugging network utilization or the distribution algorithm. If no bandwidth management is administered, this table contains no data.

Viewing Managed Bandwidth Usage

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.
2. Click **System Status > Managed Bandwidth Usage**.
The Managed Bandwidth Usage screen displays system-wide bandwidth usage information for locations where usage is managed. If the Managed Bandwidth field on the location form is blank, this table has no information for that location.
3. Click **Show** under Details column to view the bandwidth usage information per Session Manager in that location. You can click **Hide** to close this table.
4. On the Managed Bandwidth Usage screen, click **Refresh** to refresh the data.

Managed Bandwidth Usage errors

The following errors may appear on the **Managed Bandwidth Usage** page. They are related to a Session Manager being unreachable from the System Manager. The diagnosis and resolution steps are similar:

- **Network fragmentation has occurred. Bandwidth limits are not being enforced.** This error indicates that communication is being disrupted among the cluster of Session Managers in the core (non-Branch).
- **Unable to access status information for xxxx — cannot connect to server, internal error.** The Session Manager is unreachable from the System Manager.

The System Manager may be able to communicate with the Session Manager, but the Session Manager itself may be isolated from the rest of the core members. During this period, total bandwidth management in the core is unable to be properly enforced.

Causes

Possible causes include:

- An upgrade is in progress among the Session Managers.
- A Session Manager is provisioned administratively but is not actively up and running.
- Misadministration could cause the Session Manager to appear to be administered, but the Session Manager is unreachable.
- There is a true network error within the core where connectivity is limited or unavailable between certain Session Managers.
- There is an error among the Session Managers that has limited their ability to maintain a full cluster of core Session Manager nodes.

Solutions

1. The condition should be transient and ultimately resolved on its own if network connections are being limited or disrupted, or if a Session Manager is being upgraded.
2. If the condition lasts for longer than 10 minutes, check the administration and verify it is correct.
3. If the condition still exists, contact an Avaya service representative to help resolve the problem.

Chapter 19: 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>

Chapter 20: 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. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 2. Select **System Manager** from the **Select Target** drop-down list.
 3. Click **Execute All Tests**.
 4. Verify all tests show Success status.
 5. On the Home page, under **Elements**, select **Session Manager > System Status > Security Module Status**.
 6. Verify that Security Module Deployment is **Up** for all Session Managers.
 7. On the Home page, under **Elements**, select **Session Manager**.
 8. Verify the installed software versions of all Session Managers are the same
 9. Verify all Session Manager servers are in the Management Enabled state.
 10. On the Home page, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
 11. Select the appropriate Session Manager instance.
 12. Select **Execute All Tests**.
 13. Verify all tests ran successfully.
 14. Check the replication status of the Session Managers:
 - a. On the Home page, under **Services**, select **Replication**
 - b. The **Synchronization Status** should be green and the status should be **Synchronized**.
 - c. If the status is not **Synchronized**, select the check box in front of **SessionManagers_6.1** and click on **View Replica Nodes** to determine which Session Manager is not synchronized with System Manager.
-

Chapter 21: Session Manager upgrades

Upgrades from a previous release of Session Manager to Release 6.1 are described in *Upgrading Avaya Aura® Session Manager*, 03-603518 on the Avaya support web site <http://www.avaya.com/support>.

Upgrade procedures for the Survivable Remote Session Manager (Branch Session Manager) are the same as for the core Session Manager when an upgrade template is not provided.

Service pack installation procedures are described in *Installing Service Packs on Avaya Aura® Session Manager*, 03-603863 on the support web site <http://www.avaya.com/support>.

The procedures for installing Session Manager and providing basic administration are described in *Installing and Configuring Avaya Aura® Session Manager*, 03-603473.

Chapter 22: S8510 and S8800 Server upgrades

This section describes the procedures for:

- adding memory to the S8510 server
- adding a disk to the S8800 server

Material list

Material Code/Part Number	Description	Supplier
A2026998	4 GB DIMM (2 X 2 GB) Replacement Memory Module kit for Dell PowerEdge 1950 Server (S8510)	Dell
700478316	146 GB SAS 2.5" 10K drive for S8800	Avaya

S8510 Memory upgrade

System Manager 1.0 customers who purchased the S8510 Server with 4 GB RAM (SAP Code 216960) can upgrade the server with additional RAM so that the S8510 Server can be used for System Manager 6.0. The minimum memory required is 8 GB; the recommended memory is 12 GB.

DIMMs sizes can be mixed, as long as they are paired (i.e., 2–2GB DIMMs).

The additional memory should be ordered from Dell. See the [Material list](#) on page 133 for the part number and other information.

Required equipment for S8510 memory modules

- Replacement or additional memory module(s)
- #2 Phillips (cross-point) screwdriver
- Electrostatic wrist ground strap and mat
- Key to front bezel

Adding S8510 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 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.*

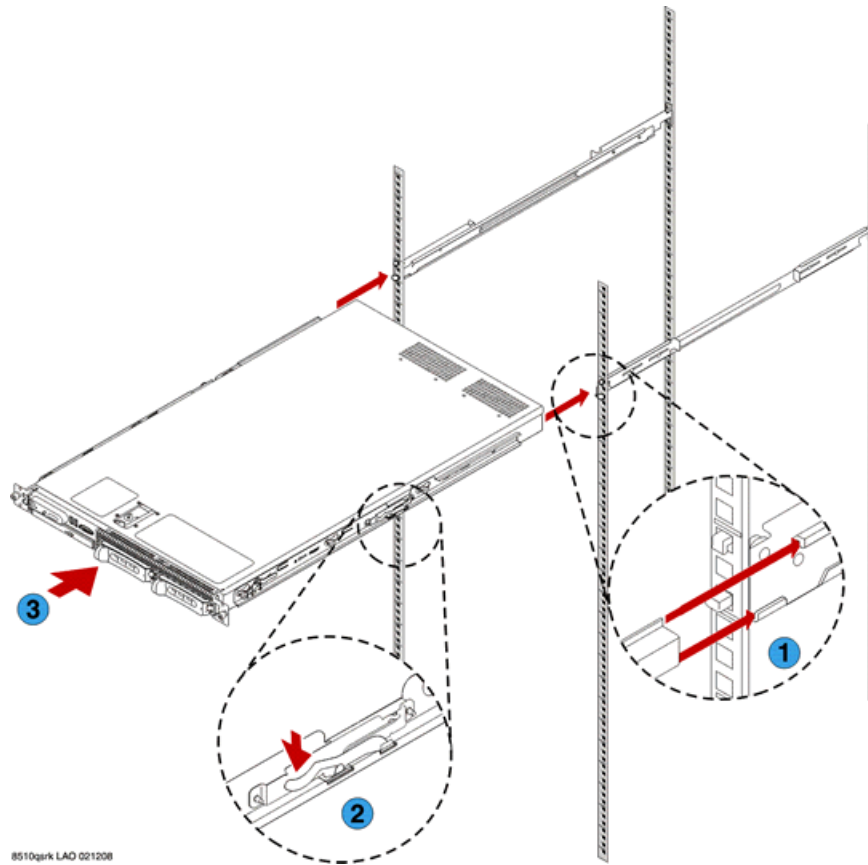
6. Loosen the captive screws on both sides of the server.
Refer to #1 in [Removing the S8510 server from the rack](#) on page 136.
7. Slide the server clear of the rails.
Refer to #2 in [Removing the S8510 server from the rack](#) on page 136.
8. Release the rail lock by pushing the lever in as you slide the server out of the rack.
Refer to #3 in [Removing the S8510 server from the rack](#) on page 136.
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 137.
10. Lift the latch up to unlock.
Refer to #2 in [Removing the cover of the S8510 Server](#) on page 137.
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 137.

12. Remove the protective cover over the memory modules.
 13. Insert the new memory modules.
 14. Replace the protective memory module cover.
 15. Ensure that any internal cables are clear of the cover before replacing it on the server.
 16. Place the cover on top of the server, aligning it with the J hooks on the sides.
 17. Slide the cover forward.
 18. Push the latch down to lock.
 19. Rotate the latch release lock clockwise to secure the cover.
 20. Install the server onto the side rails in the rack.
 21. Reconnect the Ethernet cables.
 22. Reconnect the power cords to the power supply at the back of the server.
 23. Push the server completely into the rack and secure into place with the two captive screws on both sides of the server
 24. Power up the server by pressing the power button on the front of the server.
-

Removing the S8510 server from the rack

About this task

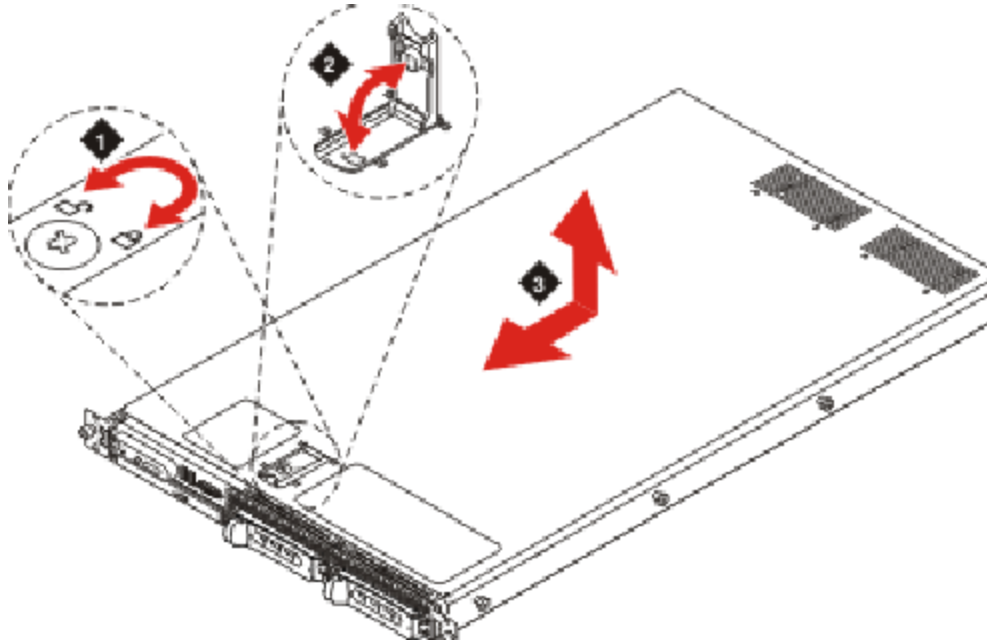


Procedure

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).

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).

S8800 Disk upgrade

An upgrade of an existing S8800 System Manager installation requires additional disk capacity. A third hard disk must be added to the S8800 server running standard RAID 1 configuration. A migration from RAID 1 to RAID 5 must be performed to extend the server's disk capacity.

S8800 servers for R6.0 are equipped with 12 GB and require no additional memory. Refer to [Material list](#) on page 133 for the hard disk part number and description.

Adding a hard disk drive to the S8800 server

About this task

The tool on the configuration CD will automatically detect the number of hard disk drives physically installed in the server. It will create a new RAID array based on the detected number of disks:

- 2 installed hard disk drives = RAID 1
- 3,4,or 5 installed hard disk drives = RAID 5

When the configuration tool has finished, one of the following 4 messages will be displayed:

- 2 Hard Drives Found, Applying Avaya RAID 1 Configuration & Settings
- 3 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
- 4 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings
- 5 Hard Drives Found, Applying Avaya RAID 5 Configuration & Settings

Procedure

1. Power down the S8800 server.
 2. Insert the new hard disk drive into Drive Bay 2 in the front of the S8800 server.
 3. Insert the configuration CD (comcode 700500063).
 4. Power up the server.
 5. Once the server has fully booted to the CD, the scripts will run automatically.
 6. Monitor the output to verify that the configuration is succeeding.
 7. Verify that the number of hard drives shown matches the number of installed hard drives.

Look for the first red line of text that displays one of the above 4 messages regarding the number of hard drives found.
 8. If not all of the installed hard disk drives have been detected:
 - a. Verify that the hard drives are properly installed.
 - b. Reboot the server to re-run the configuration tool.
 9. When the scripts finish running, the system will automatically eject the CD.
 10. When the CD has been ejected, remove the CD from the CD/DVD drive.
 11. Press **Enter** to reboot the server, or wait two minutes for the server to reboot automatically.
-

Chapter 23: S8510 Field replaceable hardware

This section 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
- Memory Modules
- Power Supplies

Replacing the S8510 Server

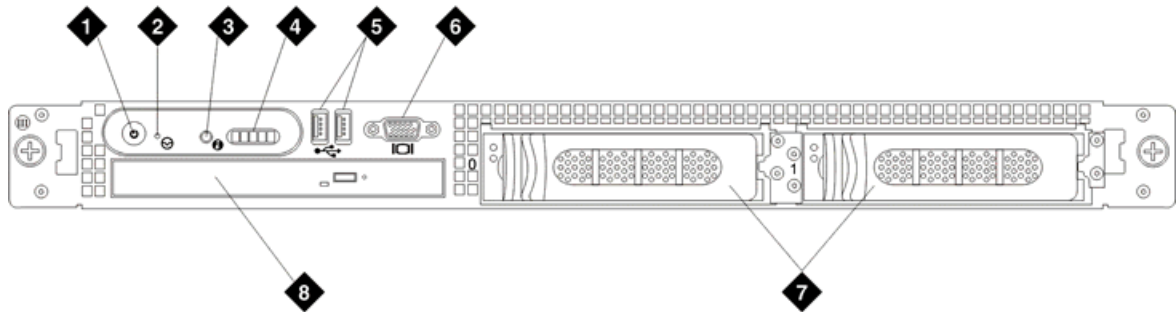
Procedure

1. Change the state of the Session Manager to **Deny New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Deny New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
2. Click on **Shutdown System**, then select **Shutdown** from the drop-down menu 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. Unplug the power cord.
4. Label and unplug the existing cables to the server for the keyboard, monitor, mouse, and Ethernet ports.
5. Remove the server from the rack. See [Removing the S8510 server from the rack](#) on page 136
6. Install the rails on the new server. See [Attaching rails to the server](#) on page 143

7. Install the new server in the rack. See [Installing the server in the rack](#) on page 143
 8. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.
 9. Install the operating system and Session Manager software:
 - a. Insert the Session Manager Kickstart DVD (OS).
 - b. Turn on the server and allow it to boot.
 - c. Wait until the server ejects the DVD and reboots.
 - d. Insert the Session Manager software CD.
 - e. Log in as sroot on the console (KVM).
 - f. Enter the following commands to mount the CD and install Session Manager software in a factory configuration:

```
# mount /cdrom
# cd /cdrom
# bash install.sh --factory
```
 - g. When the installation script has finished, enter **shutdown --f now** to shut down the server.
 - h. After the server has shut down, power it up.
 - i. When the server finished booting, log in using the root or customer login.
 - j. Enter the command **SMnetSetup** to configure the server for the local network.
 10. Reconnect the network cables to the server.
 11. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Accept New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
-

Front view of S8510 Server

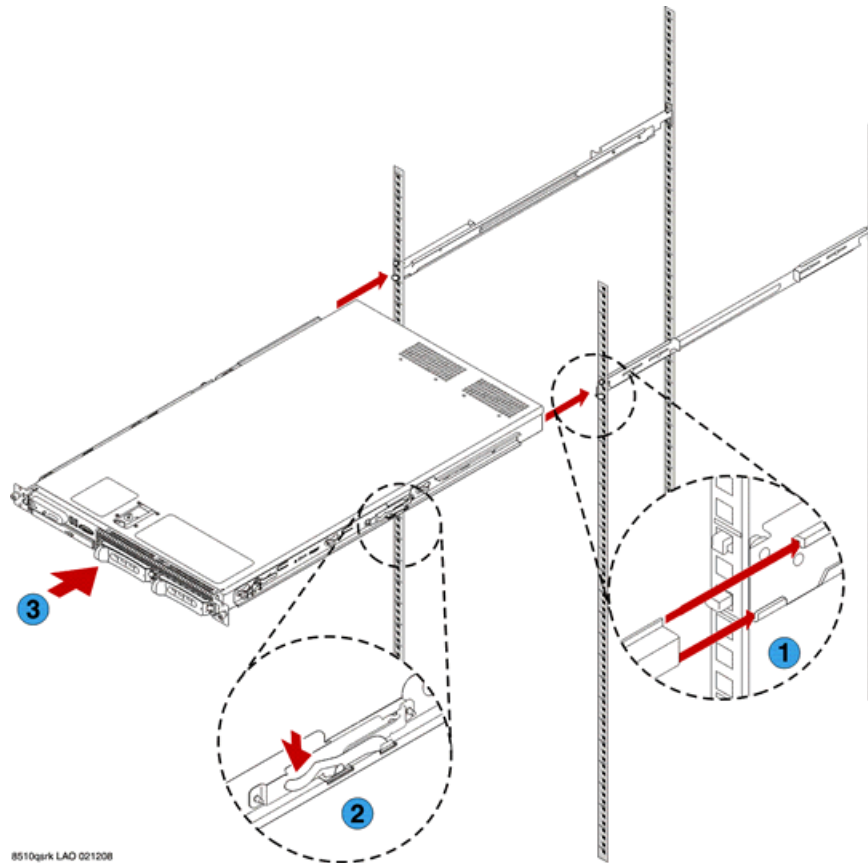


hw8510fn LAQ 020108

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

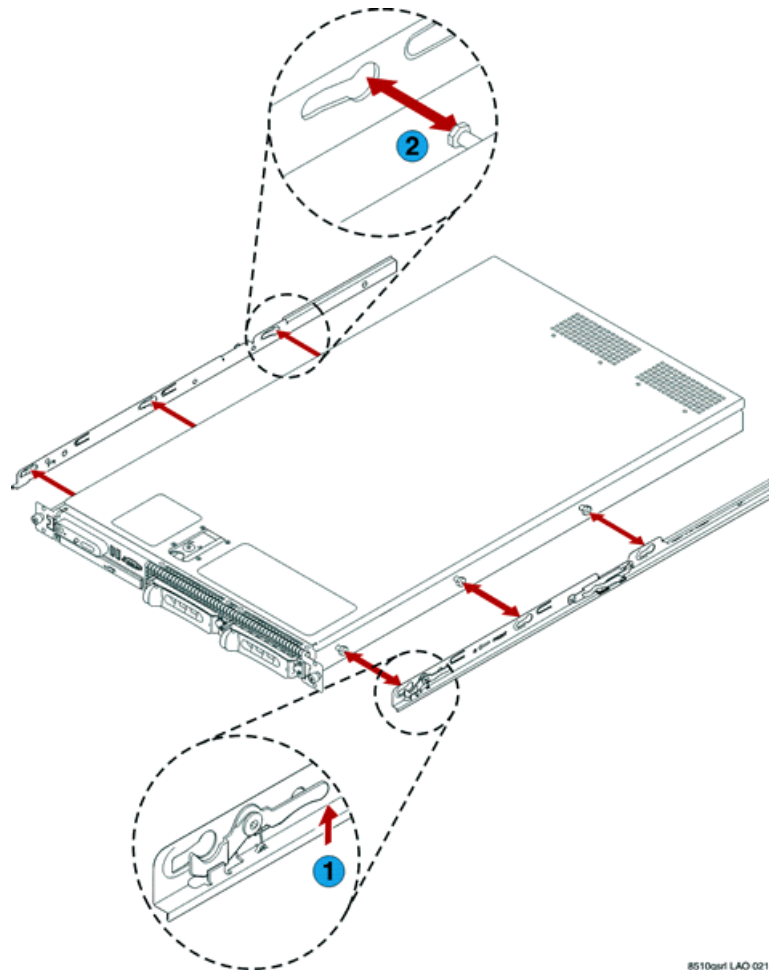


Procedure

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

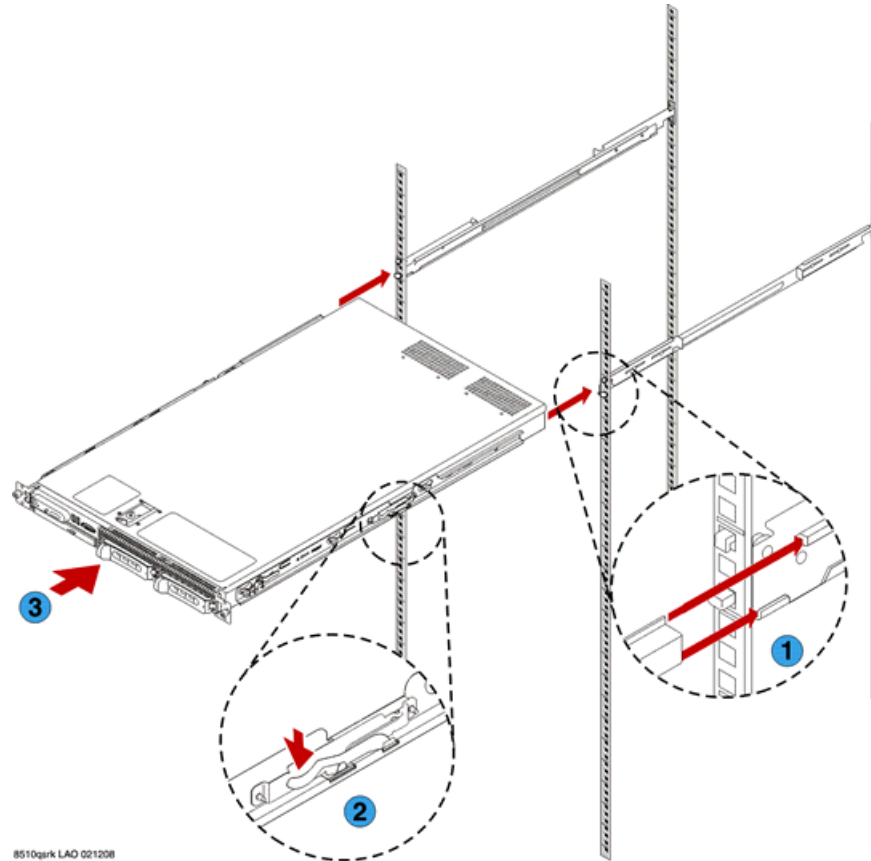


Installing the server in the rack

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 145 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. On the System Manager console, under **Services**, select **Backup and Restore**
2. Select **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 145 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 approximately 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.
-

Memory Module replacement on the Avaya S8510 Server

Required equipment for S8510 memory modules

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

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

Replacing the S8510 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(s) from the Ethernet port(s) on 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 136.
7. Slide the server clear of the rails.
Refer to #2 in [Removing the S8510 server from the rack](#) on page 136.
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 136.
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 137.
10. Lift the latch up to unlock.
Refer to #2 in [Removing the cover of the S8510 Server](#) on page 137.
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 137.
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(s) to the Ethernet port(s) on 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.
-

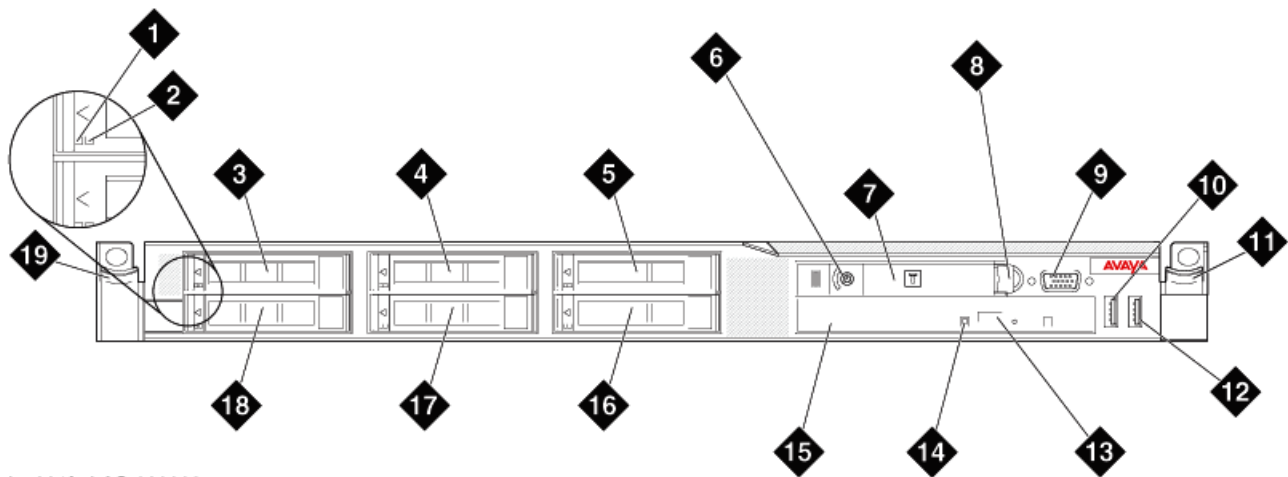
Chapter 24: S8800 Field replaceable units

S8800 Field replaceable hardware

This section 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)
- 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  Note: The operator information panel is shown in the pushed in position.
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

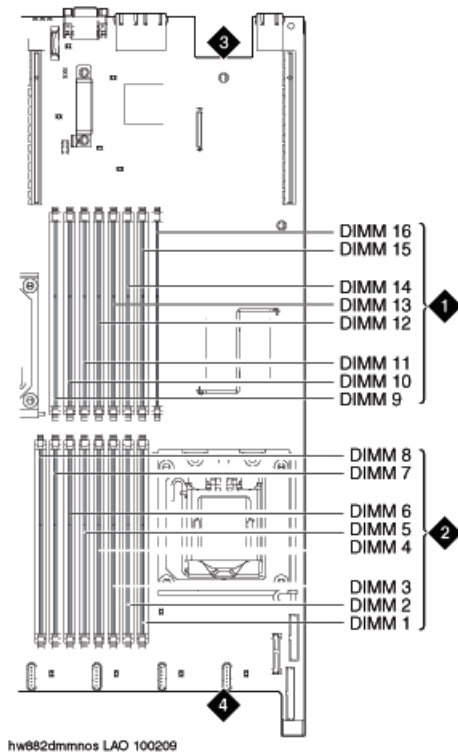
Replacing DIMMs

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 or install a memory module.



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.

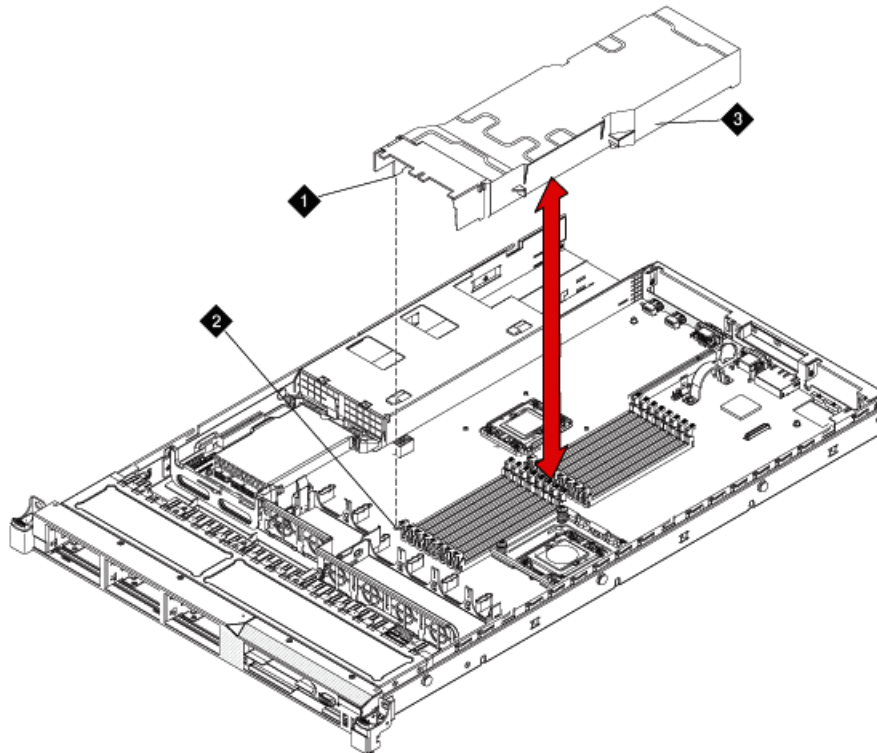


Important:

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.



hw881dmmbrfl LAQ 092209

1	Baffle pin
2	Baffle pin hole
3	DIMM air baffle

Removing a memory module

Before you begin

Remove the DIMM air baffle.

About this task

! Important:

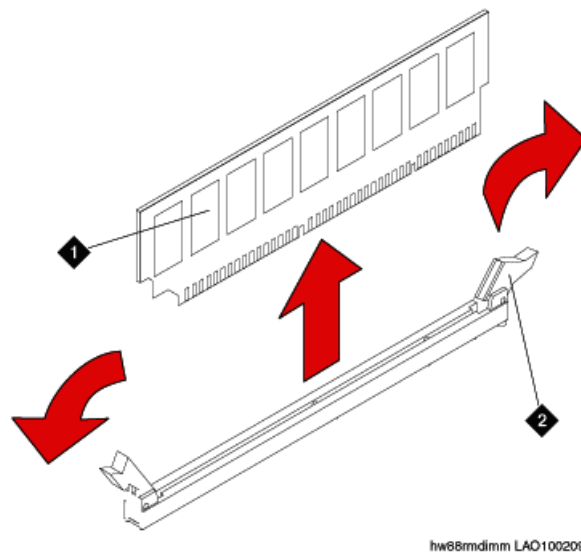
Always use an electrostatic-discharge wrist strap or other grounding system when you work inside the server. See [Protecting against ESD damage](#) on page 10 for more information.

Procedure

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

! Important:

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



1	Memory module
2	Retaining clip

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

Next steps

Install a memory module.

Installing a memory module

Before you begin

Remove the DIMM air baffle.

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.

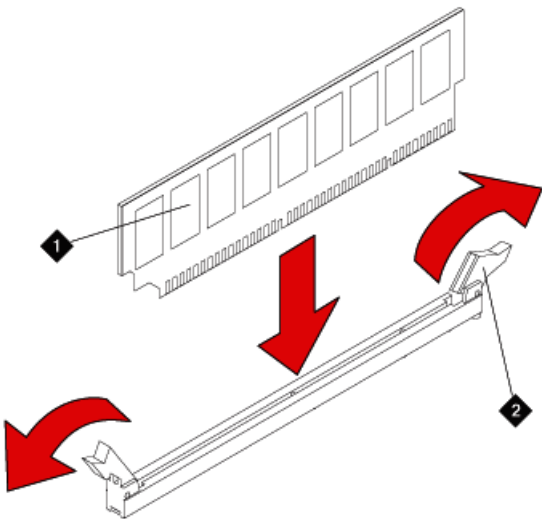
Procedure

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



Important:

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



hw88indimm LAO100209

1	Memory module
2	Retaining clip

2. Touch the static-protective package that contains the memory module to any unpainted metal surface on the server.
3. Remove the memory module from the package.

4. Turn the memory module so that the memory module keys align correctly with the connector.
5. Insert the memory module into the connector by aligning the edges of the memory module with the slots at the ends of the memory module connector.
6. Firmly press the memory module straight down into the connector by applying pressure on both ends of the memory module simultaneously.
The retaining clips snap into the locked position when the memory module is firmly seated in the connector.

 Important:

If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. Open the retaining clips, remove the memory module, and then reinsert it.

7. Replace the air baffle over the memory modules. 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 memory modules, 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 install a memory module.

 Caution:

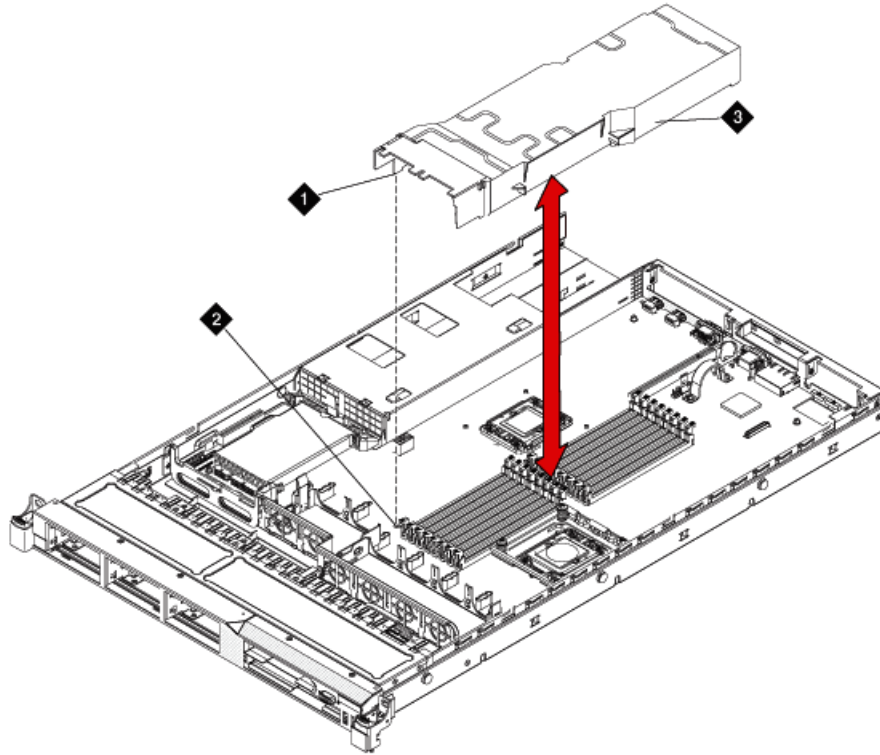
For proper cooling and airflow, replace the air baffle before you turn on the server. Operating the server with an air baffle removed might damage server components.

 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 DIMM connector on the system board. See the following figure.



hw881dmmbrfl LAO 092209

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.

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.

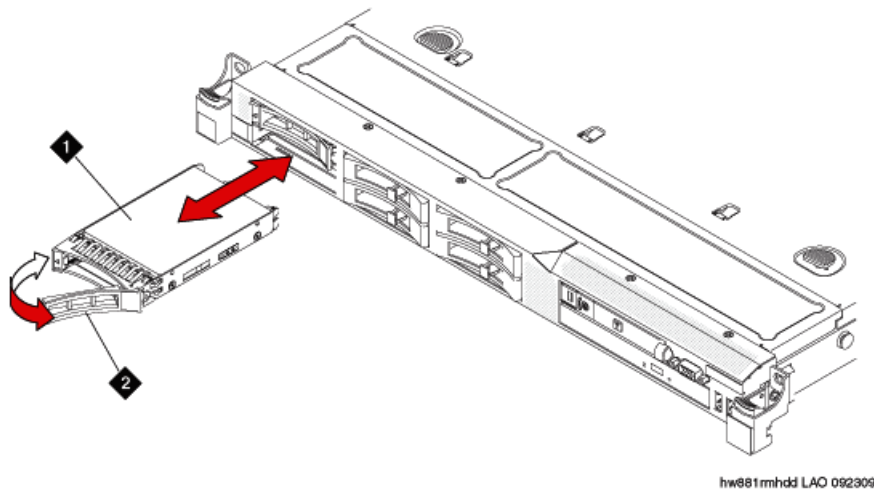


Important:

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.

Next steps

Install a hard disk drive.

Installing a hard disk drive

Before you begin

If replacing an existing hard drive, 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.

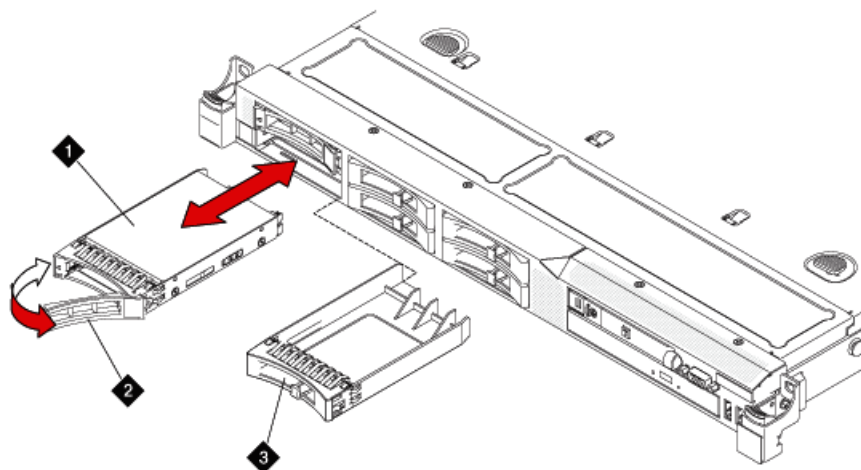


Important:

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.



hw881rnhdd LAO 092309

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.



hw88vltwm LAC100209

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:

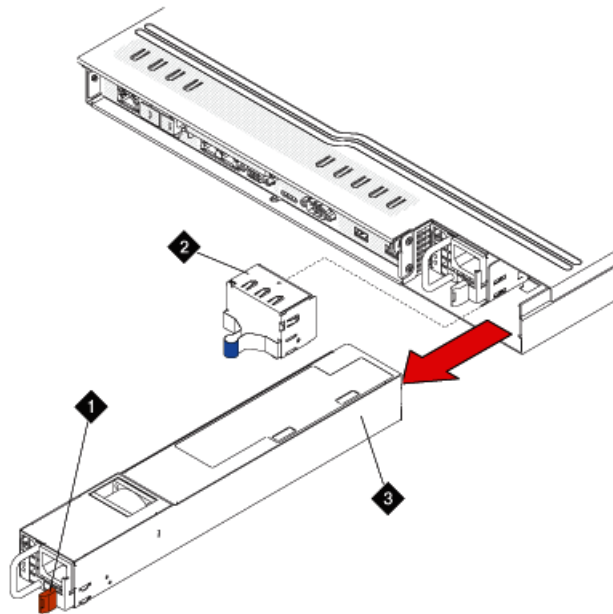
During normal operation, each power-supply bay must contain either a power supply or power-supply filler for proper cooling.

! 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.



hw881rmps LAO100209

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.

Next steps

Install a power supply.

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.



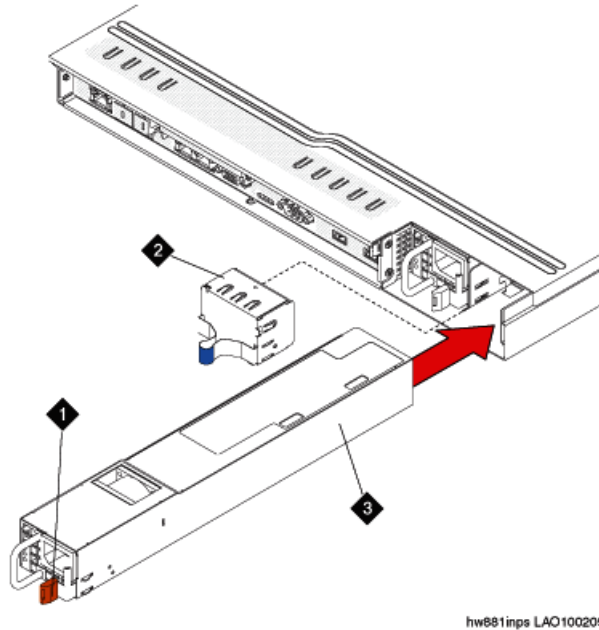
Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, replace the power supply.

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

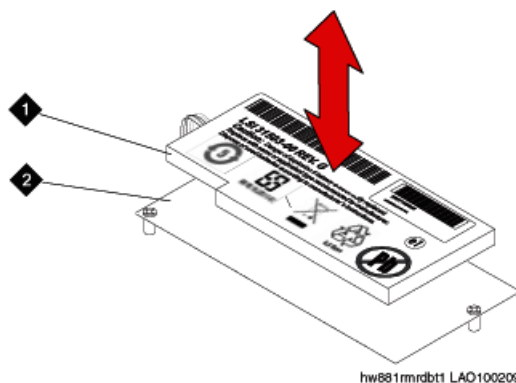


Important:

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.

Next steps

Install a new RAID battery.

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.

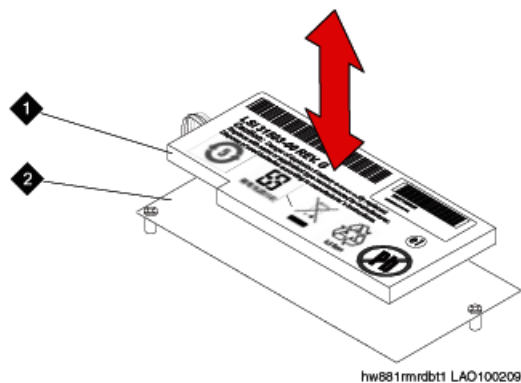
The RAID configuration data is preserved when you replace the battery.

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. Change the state of the Session Manager to **Deny New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Deny New Service** from the drop-down menu.

- e. On the **Confirmation** page, click on **Confirm**.
2. Click on **Shutdown System**, then select **Shutdown** from the drop-down menu 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. Label all power cords and external cables.
4. Disconnect all power cords and external cables.
5. Remove the server from the rack. See [Removing the server from the rack](#) on page 169.
6. Remove the reusable components from the failed server. See [Reuse of hardware components in replacement servers](#) on page 167.
7. Install the reusable components into the new server. See [Reuse of hardware components in replacement servers](#) on page 167.
8. Install the new server in the rack. See [Installing the server in the rack](#) on page 169.
9. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.
10. Install the operating system and Session Manager software:
 - a. Insert the Session Manager Kickstart DVD (OS).
 - b. Turn on the server and allow it to boot.
 - c. Wait until the server ejects the DVD and reboots.
 - d. Insert the Session Manager software CD.
 - e. Log in as sroot on the console (KVM).
 - f. Enter the following commands to mount the CD and install Session Manager software in a factory configuration:

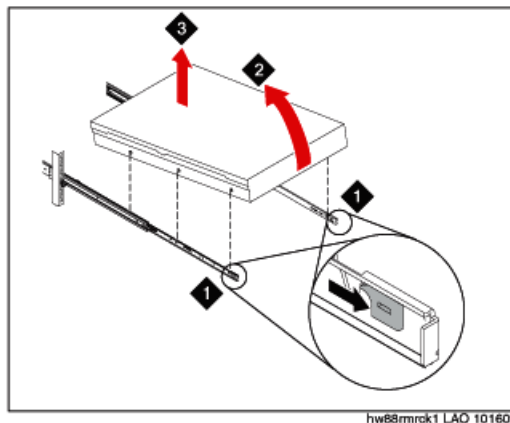
```
# mount /cdrom
# cd /cdrom
# bash install.sh --factory
```
 - g. When the installation script has finished, enter **shutdown --f now** to shut down the server.
 - h. After the server has shut down, power it up.
 - i. When the server finished booting, log in using the root or customer login.
 - j. Enter the command **SMnetSetup** to configure the server for the local network.
11. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.

- b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
- c. Click on **Service State**.
- d. Select **Accept New Service** from the drop-down menu.
- e. On the **Confirmation** page, click on **Confirm**.

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.

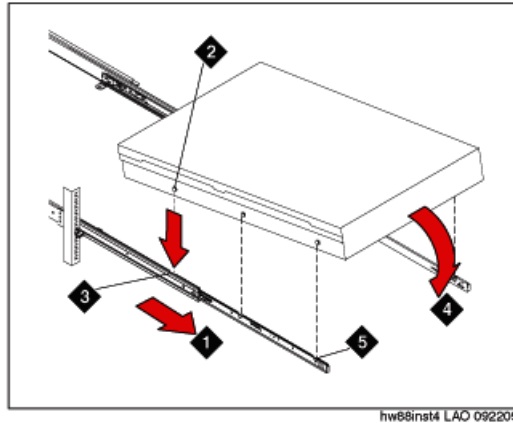


4. Lift up the front of the server (2). See the preceding figure.
5. Pull the server out of the rack (3). See the preceding figure.

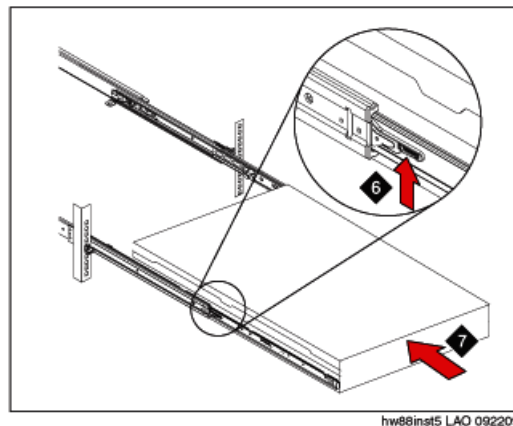
Installing the server in the rack

Procedure

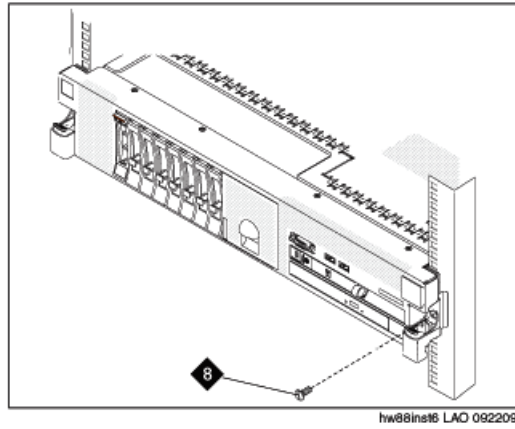
1. Pull the slide rails forward (1) until they click, two times, into place. See the following figure.



2. Carefully lift the server and tilt it into position over the slide rails so that the rear rail 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 rail heads slip into the two rear slots.
4. Slowly lower the front of the server (4) until the other rail 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 rail 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.



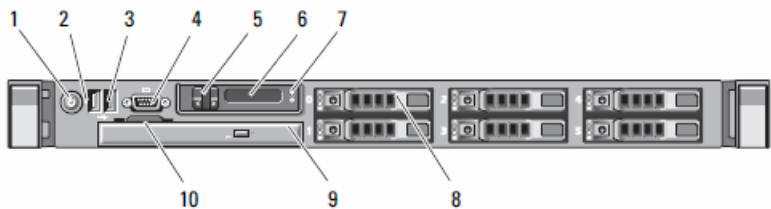
Chapter 25: Dell R610 Server

The Dell™ PowerEdge™ R610 server is a replacement for the S8800 server. Unlike previous original equipment manufactured servers, this server is not re-branded as an Avaya server (S8XXX).

The following table contains a list of the field replaceable units (FRUs) for the Dell R610 server, whether the component is internal or external, and a link to the procedures for replacing the component.

Component	Type	Link to replacement procedure
Hard Disk Drive	External	Replacing external components on page 177
Power Supply	External	Replacing external components on page 177
Server		Replacing the Dell R610 Server on page 178
Dual port NIC	Internal	Replacing internal components on page 182
DVD-RW Drive	Internal	Replacing internal components on page 182
Fan	Internal	Replacing internal components on page 182
2 GB or 4GB Memory DIMM	Internal	Replacing internal components on page 182
RAID Battery	Internal	Replacing internal components on page 182

Front of server

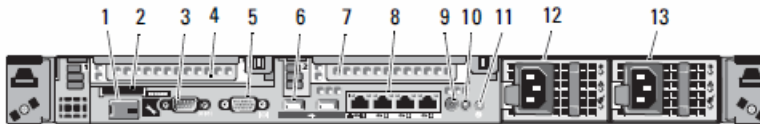


*** Note:**
Servers ship with 2–4 hard disk drives, depending upon product requirements.

Reference	Description
1	Power-on indicator, power button
2	NMI button
3	USB connectors (2)

Reference	Description
4	Video connector
5	LCD menu buttons
6	LCD panel
7	System identification button
8	Hard drives (maximum 4)
9	DVD-RW
10	System identification panel

Back of server



Reference	Description
1	iDRAC6 Enterprise port (optional)
2	VFlash media slot (optional)
3	Serial connector
4	PCIe slot 1  Note: Servers might ship with a PCI card installed, depending upon product requirements.
5	Video connector
6	USB connectors (2)
7	PCIe slot 2  Note: Servers might ship with a PCI card installed, depending upon product requirements.
8	Ethernet connectors (4)
9	System status indicator connector
10	System status indicator

Reference	Description
11	System identification button
12	Power supply 1 (PS1)
13	Power supply 2 (PS2)

Downloading Dell documentation

Use this procedure to find and download the Dell™ PowerEdge™ R610 documentation from Dell.

Procedure

1. Open a browser and go to <http://www.support.dell.com/>.
 2. On the Welcome to Dell Support page click on the Start Here button in the Support for Enterprise IT section.
 3. On the Welcome to Enterprise IT Support click on Select a product in the Product Support section.
 4. On the next page click on Select Model in the Choose a Model section.
 5. On the Select Product by Model page, click on Servers, Storage, Networking.
 6. On the Select Product by Model > Server, Storage, Networking page use the scroll bar in the Select Your Product Line column and click on PowerEdge Server.
 7. On the Select Product by Model > Server, Storage, Networking > PowerEdge Server page, use the scroll bar in the Select Your Product Model column and click on R610.
 8. On the Select Product by Model > Server, Storage, Networking > PowerEdge Server > R610 page, click on the Confirm button in the Confirm your selection section.
 9. On the Product Support for PowerEdge R610 page click on Manuals and Documentation.
 10. On the Dell™ PowerEdge™ R610 System page, click the Download link that corresponds to the document that you want to download.
 11. Download the documents in the *Dell R610 document set > Documents to download* section below.
-

Dell R610 documentation set

Refer to the documents listed below for Dell R610 server installation information and procedures.



Note:

Download the documents listed in the *Documents to download* section below. Printed copies of the documents listed in the *Documents included in the shipping container* section below ship with the server.

Documents to download

Abbreviation	Title	Part number
CMAI	Cable Management Arm Installation	0F880KA00
GS	Getting Started With Your System	R465D
HOM	Hardware Owner's Manual	No number
RI-SR	Rack Installation (Sliding Rails)	0J171KA00



Note:

If you want to locate and download an individual document:

- Go to <http://www.dell.com/>.
- Type R610 plus the keywords of the document title in the Search field in the upper-right corner and press Enter.

Examples:

- Type R610 Technical Guidebook to search for the *Technical Guidebook* document.
- Type R610 Getting Started to search for the *Getting Started with your System* document.

Documents included in the shipping container

Abbreviation	Title	Part number
PS	Product Safety, EMC & Environmental Datasheet	No number
TG	Technical Guidebook	No number

Replacing external components

Use the checklist below to replace any of the following external server components:

Part number	Description	Hot-swappable?
700501316	R610 SRVR 146GB 10K SAS 2.5" HDD	Y
700501317	R610 SRVR 146GB 15K SAS 2.5" HDD	Y
700501315	R610 SRVR 300GB 10K SAS 2.5" HDD	Y
700501421	R610 SRVR 600GB 10K SAS 2.5" HDD	Y
700501183	R610 SRVR AC PWR SUP 502W ES	Y, if redundant
700501311	R610 SRVR AC PWR SUP 717W	Y, if redundant



Note:

Hard disk drives and redundant power supplies are hot-swappable; you do not have to power down the server. Replacing a power supply usually does not require removing the server from the rack unless cables or other obstructions prevent removing and replacing the power supply.

No.	Task	Reference	Avaya recommendation	✓
1	Power down server (if necessary)		Determine whether the replaceable component is hot-swappable.	
2	Slide the server out of the rack (if necessary)	RI-SR CMAI: <i>Moving the CMA Away from the CMA Tray</i>	Ensure that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
3	Replace the component:			
	• R610 SRVR 146GB 10K SAS 2.5" HDD • R610 SRVR 146GB 15K SAS 2.5" HDD • R610 SRVR 300GB 10K SAS 2.5" HDD • R610 SRVR 600GB 10K SAS 2.5" HDD	HOM: <i>Hard drives</i>		

No.	Task	Reference	Avaya recommendation	✓
	• R610 SRVR AC PWR SUP 502W ES • R610 SRVR AC PWR SUP 717W	HOM: <i>Power supplies</i>	Ensure that the replacement power supply matches the specifications of the defective power supply.	
4	Slide the server into the rack (if necessary)	RI-SR	Ensure that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
5	Connect the power cable(s) to the power supply (if necessary)	GS: <i>Connecting the Power Cables</i> GS: <i>Securing the Power Cord</i>		
6	Power up the server (if necessary)	GS: <i>Turning on the System</i>		

Replacing the Dell R610 Server

Procedure

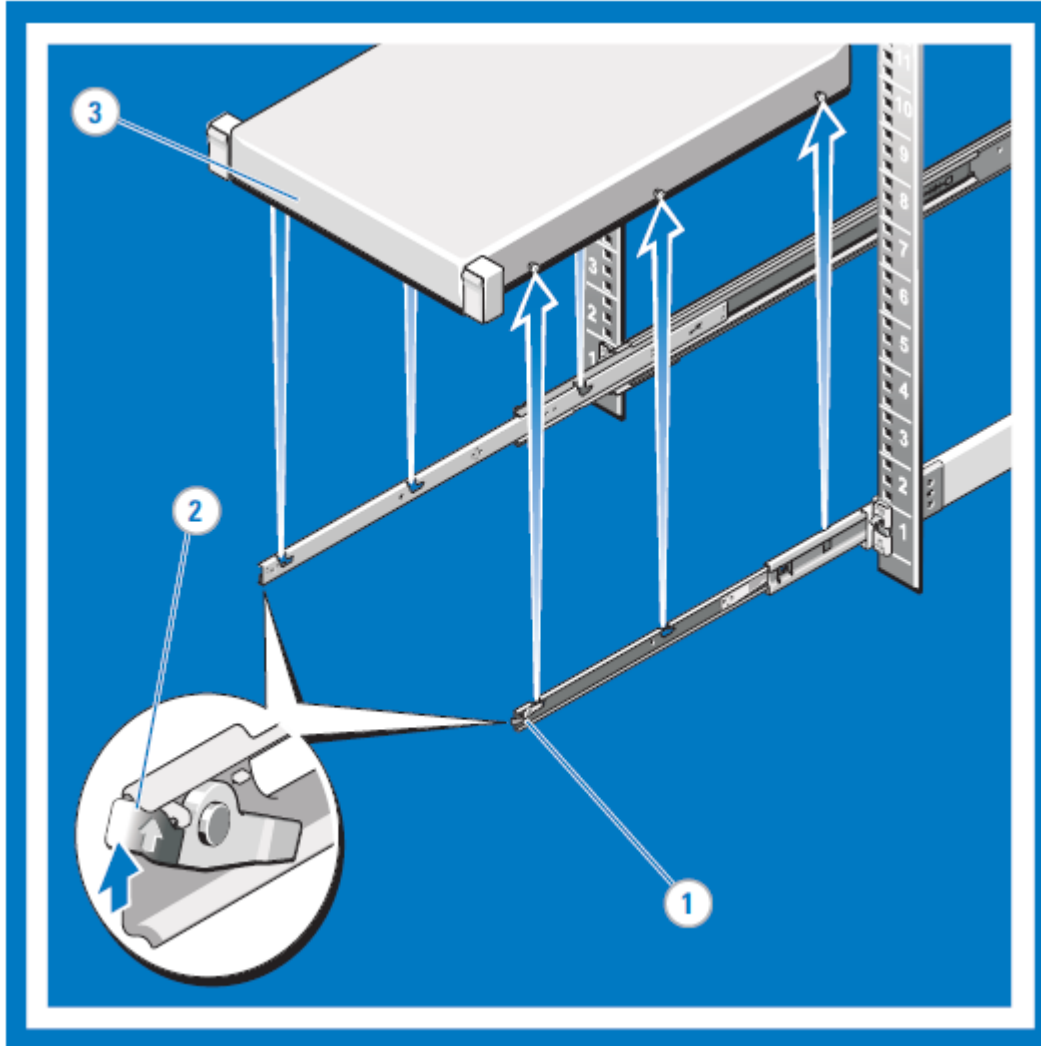
- Change the state of the Session Manager to **Deny New Service**:
 - On the System Manager console, under **Elements**, select **Session Manager**.
 - On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - Click on **Service State**.
 - Select **Deny New Service** from the drop-down menu.
 - On the **Confirmation** page, click on **Confirm**.
- Click on **Shutdown System**, then select **Shutdown** from the drop-down menu 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.
- Unplug the power cord.
- Label and unplug the existing cables to the server for the keyboard, monitor, mouse, and Ethernet ports.
- Remove the server from the rack. See [Removing the Dell R610 server from the rack](#) on page 180

6. Install the new server. See [Installing the Dell R610 server in the rack](#) on page 181
 7. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.
 8. Install the operating system and Session Manager software:
 - a. Insert the Session Manager Kickstart DVD (OS).
 - b. Turn on the server and allow it to boot.
 - c. Wait until the server ejects the DVD and reboots.
 - d. Insert the Session Manager software CD.
 - e. Log in as sroot on the console (KVM).
 - f. Enter the following commands to mount the CD and install Session Manager software in a factory configuration:

```
# mount /cdrom
# cd /cdrom
# bash install.sh --factory
```
 - g. When the installation script has finished, enter **shutdown --f now** to shut down the server.
 - h. After the server has shut down, power it up.
 - i. When the server finished booting, log in using the root or customer login.
 - j. Enter the command **SMnetSetup** to configure the server for the local network.
 9. Reconnect the network cables to the server.
 10. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Accept New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
-

Removing the Dell R610 server from the rack

About this task

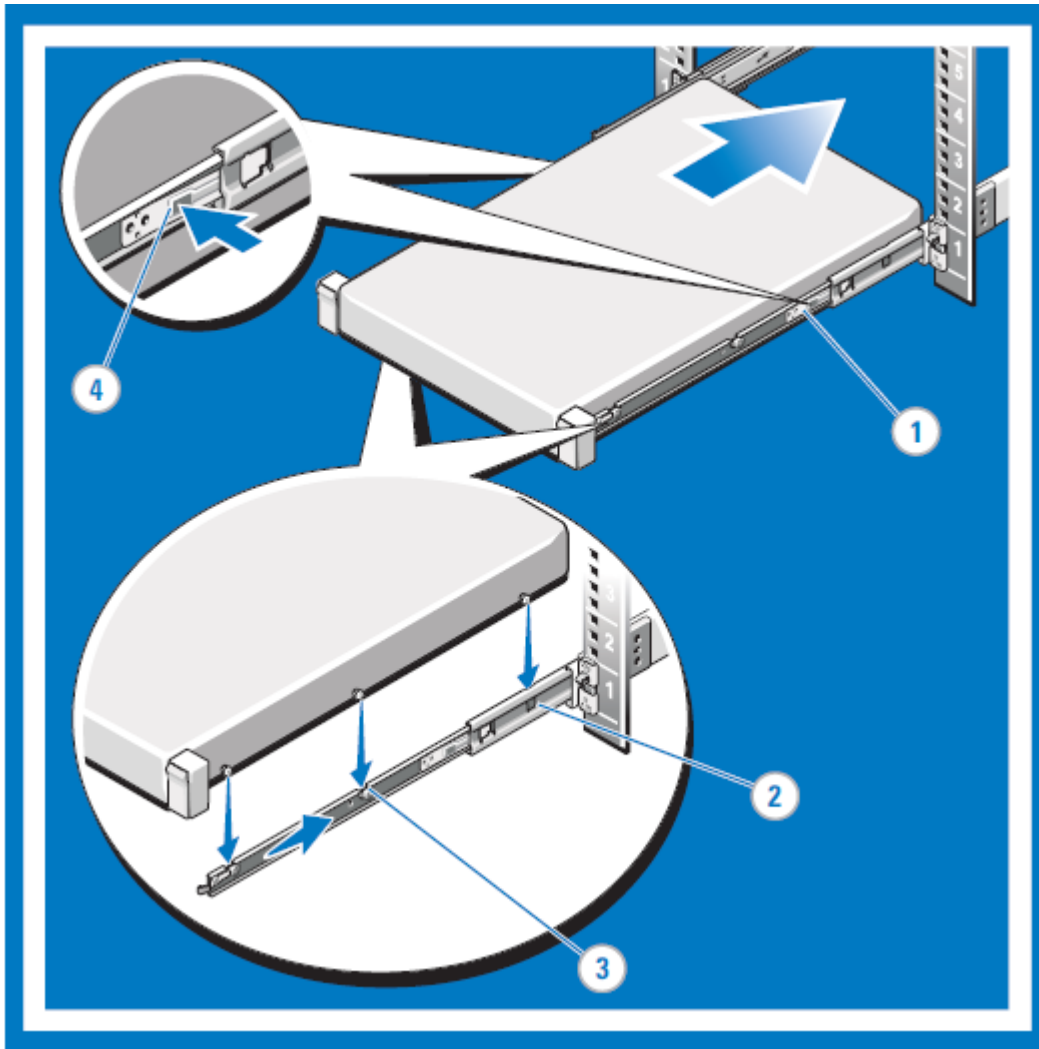


Procedure

1. Locate the lock levers on the front ends of both inner rails (Figure 1).
2. Pull up on each lever into the release position to unlock (Figure 2).
3. Grasp the sides of the server firmly and pull forward and up to unseat the server from the J-slots.
4. Lift the server up and away from the rack and place on a level surface (Figure 3).

Installing the Dell R610 server in the rack

About this task



Procedure

1. Pull the inner slide rails out of the rack until they lock into place (Figure 1).
2. Lower the server's back shoulder screws into the back J-slots on the slide assemblies (Figure 2).
3. Lower the server until all shoulder screws engage in the J-slots (Figure 3).

4. Push the server inward until the front release latch clicks into place.
5. Press the slide-release lock buttons on both rails and slide the server into the rack (Figure 4).

Replacing internal components

Use the checklist below to replace any of these internal server components:

Part number	Description
700501323	R610 SRVR DUAL PORT 1GB NIC
700501422	R610 SRVR DVD-RW DRIVE W/ BRKT
700501423	R610 SRVR FAN FRU
700501320	R610 SRVR 2GB MEMORY DIMM
700501320	R610 SRVR 4GB MEMORY DIMM
700501325	R610 SRVR RAID BATTERY



Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by installation and/or servicing technicians.

No.	Task	Reference	Avaya recommendation	✓
1	Have the proper tools	HOM: <i>Recommended Tools</i>		
2	Observe safety warnings	HOM: <i>Safety First—For You and Your System</i>		
3	Power down server			
4	Slide the server out of the rack	RI-SR		
5	Remove the cover	HOM: <i>Opening and Closing the System</i>	 Electrostatic alert: Ensure that you are properly grounded before handling internal components.	

No.	Task	Reference	Avaya recommendation	✓
6	Replace the component:			
	• R610 SRVR DUAL PORT 1GB NIC	HOM: <i>Expansion Cards</i>	Mark any external cables connected to the NIC and reconnect to the same ports after the NIC is replaced.	
	• R610 SRVR DVD-RW DRIVE W/ BRKT	HOM: <i>Optical Drive</i>	In the <i>Removing an Optical Drive</i> section perform steps 2–5 only. In the <i>Installing an Optical Drive</i> section perform steps 2–6, 8, and 10 only.	
	• R610 SRVR FAN FRU	HOM: <i>Cooling Fans</i>	 Caution: Do not attempt to hot-swap a fan.	
	• R610 SRVR 2GB MEMORY DIMM • R610 SRVR 4GB MEMORY DIMM	HOM: <i>System Memory</i>	Consult server cover label for memory placement. Consult application/solution documentation for specific procedures.	
	• R610 SRVR RAID BATTERY	HOM: <i>RAID Battery</i>	Remove the battery from the cable. Do not replace the battery cable unless it is defective.  Note: Monitor, keyboard, and mouse might be necessary for server reboot.	
7	Replace the cover	HOM: <i>Opening and Closing the System</i>		
8	Slide the server into the rack	RI-SR	Ensure that the Cable Management Arm (if present)	

No.	Task	Reference	Avaya recommendation	✓
			moves freely out of the way of rear panel components.	
9	Connect and secure the power cords	GS: <i>Connecting the Power Cables</i> GS: <i>Securing the Power Cord</i>		
10	Power up the server	GS: <i>Turning on the System</i>		

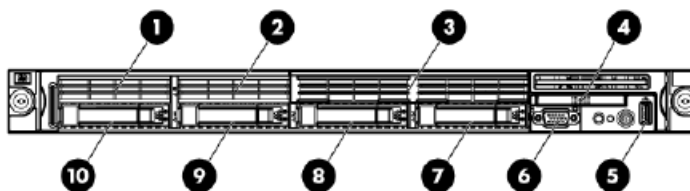
Chapter 26: HP DL360 G7 Server

The HP Proliant DL360 G7 server is a replacement for the S8800 server. Unlike previous original equipment manufactured servers, this server is not re-branded as an Avaya server (S8XXX).

The following table contains a list of the field replaceable units (FRUs) for the HP DL360 G7 server, whether the component is internal or external, and a link to the procedures for replacing the component.

Component	Type	Link to replacement procedure
Hard Disk Drive	External	Replacing external components on page 188
Power Supply	External	Replacing external components on page 188
AC Power Supply	External	Replacing external components on page 188
DC Power Supply	External	Replacing external components on page 188
Server		Replacing the HP DL360 G7 Server on page 190
Dual port NIC	Internal	Replacing internal components on page 192
DVD-RW Drive	Internal	Replacing internal components on page 192
Fan	Internal	Replacing internal components on page 192
2 GB or 4 GB Memory DIMM	Internal	Replacing internal components on page 192
RAID Battery	Internal	Replacing internal components on page 192

Front of server

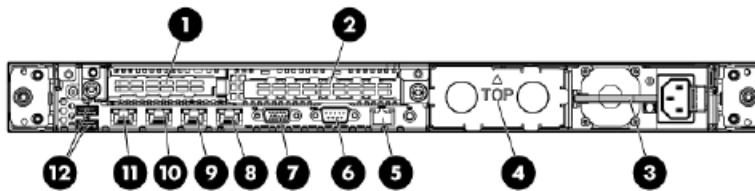


*** Note:**

Servers ship with 2–4 hard disk drives, depending upon product requirements.

No.	Description
1	Not present
2	Not present
3	DVD-RW
4	HP Systems Insight Display
5	Front USB connector
6	Video connector
7	Hard drive bay 4
8	Hard drive bay 3
9	Hard drive bay 2
10	Hard drive bay 1

Back of server



Reference	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1)  Note: Servers might ship with a PCI card installed, depending upon product requirements.
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1), 75W +EXT 75W*  Note: Servers might ship with a PCI card installed, depending upon product requirements.
3	Power supply bay 1 (populated)
4	Power supply bay 2
5	iLO 3 connector

Reference	Description
6	Serial connector
7	Video connector
8	NIC 4 connector
9	NIC 3 connector
10	NIC 2 connector
11	NIC 1 connector
12	USB connectors (2)

*This expansion slot provides 75 W of power to an adapter, with an additional 75 W of power supplied by external power.

Downloading HP documentation

Use this procedure to find and download the HP ProLiant DL360 G7 documentation from HP.

Procedure

1. Open a browser and go to <http://www.hp.com/>.
2. Click on Support and Drivers.
3. Select See support and troubleshooting information in the Step 1 area.
4. In the Step 2 area of the page type ProLiant DL360 in the For product field.
5. Select HP ProLiant DL360 G7 Server series from the list of search results.
6. Select Manuals (guides, supplements, addendums, etc.).
7. Download the document(s) listed in the *HP DL360 G7 document set > Documents to download* section below.

HP DL360 document set

Refer to the documents listed below for HP DL360 server information and procedures.

**Note:**

Download the documents listed in the *Documents to download* section below. Printed copies of the documents listed in the *Documents included in the shipping container* section below ship with the server.

Documents to download

Abbreviation	Title	Part number
SI	Important Safety Information for Server Storage, Power, Networking, and Rack Products	No number
MSG	HP ProLiant DL360 G7 Server Maintenance and Service Guide	608339-003
TS	HP ProLiant Servers Troubleshooting Guide	375445-009
UG	HP ProLiant DL360 G7 Server User Guide	608341-003

**Note:**

If you want to locate an individual document:

- Go to <http://www.hp.com/>.
- Type DL360 G7 plus the keywords of the document title in the Search field in the upper-right corner and press Enter.

Examples:

- Type DL360 User Guide to search for the *HP ProLiant DL360 G7 Server User Guide* document.
- Type DL360 Maintenance Service to search for the *HP ProLiant DL360 G7 Server Maintenance and Service Guide* document.

Documents included in the shipping container

Abbreviation	Title	Part number
1URH	1U Rack Hardware Installation Instructions	365 494-004
PCS	Power Cord Strain Relief Kit	407 454-021

Replacing external components

Use the checklist below to replace any of the following external server components:

Part number	Description	Hot-swappable?
700501426	DL360G7 SRVR 146GB 10K SAS 2.5" HDD drive	Y
700501249	DL360G7 SRVR 146GB 15K SAS 2.5" HDD	Y
700501314	DL360G7 SRVR 300GB 10K SAS 2.5" HDD	Y
700501182	DL360G7 SRVR PWR SUP 460W HE	Y, if redundant
700501312	DL360G7 SRVR AC PWR SUP 750W	Y, if redundant
700501313	DL360G7 SRVR DC PWR SUP 1200W	Y, if redundant

**Note:**

Hard disk drives and redundant power supplies are hot-swappable; you do not have to power down the server. Replacing a power supply usually does not require removing the server from the rack unless cables or other obstructions prevent removing and replacing the power supply.

No.	Task	Reference	Avaya recommendation	✓
1	Power down server (if necessary)	MSG: <i>Power down the server</i>	Determine whether the replaceable component is hot-swappable.	
2	Slide the server out of the rack (if necessary)	MSG: <i>Extend the server from the rack</i> MSG: <i>Remove the server from the rack</i>	Check that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
3	Replace the component:			
	• DL360G7 SRVR 146GB 10K SAS 2.5" HDD • DL360G7 SRVR 146GB 15K SAS 2.5" HDD • DL360G7 SRVR 300GB 10K SAS 2.5" HDD	MSG: Removal and replacement procedures > <i>SAS and SATA hard drive</i> MSG: Removal and replacement procedures > <i>Hard drive blank</i>		

No.	Task	Reference	Avaya recommendation	✓
	• DL360G7 SRVR PWR SUP 460W HE • DL360G7 SRVR AC PWR SUP 750W • DL360G7 SRVR DC PWR SUP 1200W	MSG: Removal and replacement procedures > <i>Hotplug power supply</i> MSG: Removal and replacement procedures > <i>Power supply blank</i>	Ensure that the replacement power supply matches the specifications of the defective power supply.	
4	Slide the server into the rack (if necessary)	UG: <i>Installing the server into the rack</i>	Check that the Cable Management Arm (if present) moves freely out of the way of rear panel components.	
5	Connect the power cable(s) to the power supply (if necessary)	UG: <i>Powering up and configuring the server</i>		
6	Power up the server (if necessary)	UG: <i>Power up the server</i>		

Replacing the HP DL360 G7 Server

Procedure

1. Change the state of the Session Manager to **Deny New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Deny New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
2. Click on **Shutdown System**, then select **Shutdown** from the drop-down menu 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. Unplug the power cord.

4. Label and unplug the existing cables to the server for the keyboard, monitor, mouse, and Ethernet ports.
 5. Remove the server from the rack. See the installation instructions that shipped with the original server.
 6. Install the new server in the rack. See the installation instructions that shipped with the original server.
 7. Reconnect the keyboard, monitor, mouse, and power cables. Do not connect the network cables at this time.
 8. Install the operating system and Session Manager software:
 - a. Insert the Session Manager Kickstart DVD (OS).
 - b. Turn on the server and allow it to boot.
 - c. Wait until the server ejects the DVD and reboots.
 - d. Insert the Session Manager software CD.
 - e. Log in as `sroot` on the console (KVM).
 - f. Enter the following commands to mount the CD and install Session Manager software in a factory configuration:

```
# mount /cdrom
# cd /cdrom
# bash install.sh --factory
```
 - g. When the installation script has finished, enter **shutdown --f now** to shut down the server.
 - h. After the server has shut down, power it up.
 - i. When the server finished booting, log in using the root or customer login.
 - j. Enter the command **SMnetSetup** to configure the server for the local network.
 9. Reconnect the network cables to the server.
 10. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager by checking the box in front of the Session Manager name in the table.
 - c. Click on **Service State**.
 - d. Select **Accept New Service** from the drop-down menu.
 - e. On the **Confirmation** page, click on **Confirm**.
-

Replacing internal components

Use the checklist below to replace any of these internal server components:

Part number	Description
700501424	DL360G7 DVD-RW DRIVE W/ BRKT
700501322	DL360G7 SRVR DUAL PORT 1GB NIC
700501425	DL360G7 SRVR FAN FRU
700501318	DL360G7 SRVR 2GB MEMORY DIMM
700501319	DL360G7 SRVR 4GB MEMORY DIMM
700501324	DL360G7 SRVR 650 MAH RAID BATTERY



Note:

Although not used frequently, Avaya customers are required to have a monitor, keyboard, and mouse available for use by installation and/or servicing technicians.

No.	Task	Reference	Avaya recommendation	✓
1	Have the proper tools	MSG: <i>Required tools</i>		
2	Observe safety warnings	TG: <i>Important safety information</i> MSG: <i>Safety considerations</i>		
3	Power down the server	MSG: Removal and replacement procedures > <i>Power down the server</i>		
4	Slide the server out of the rack	MSG: Removal and replacement procedures > <i>Extend the server from the rack</i> MSG: Removal and replacement procedures > <i>Remove the server from the rack</i>		
5	Remove the cover	MSG: Removal and replacement procedures > <i>Access panel</i>	 Electrostatic alert: Ensure that you are properly grounded	

No.	Task	Reference	Avaya recommendation	✓
			before handling internal components.	
6	Replace the component:			
	• DL360G7 DVD-RW DRIVE W/ BRKT	MSG: Removal and replacement procedures: • <i>DVD tray</i> • <i>DVD-ROM or DVD-RW drive</i>	Omit Steps 4 and 5 from both procedures. You do not need to remove the air baffle or the BBWC battery pack.	
	• DL360G7 SRVR DUAL PORT 1GB NIC	MSG: Removal and replacement procedures: • <i>PCI riser board assembly</i> • <i>Expansion boards</i> • <i>PCIe riser board</i>	Mark any cables connected to the NIC and reconnect to the same ports after the NIC is replaced. The NIC requires a half-HT faceplate. You might need to remove the full faceplate and replace it with the half faceplate, which requires a crosshatch (Phillips) screwdriver.  Note: If adding a NICs: populate PCI Slot 1 first, followed by Slot 2.	
	• DL360G7 SRVR FAN FRU	MSG: Removal and replacement procedures > <i>Fan module</i>	Refer to the Systems Insight Display LEDs to identify the defective fan.	
	• DL360G7 SRVR 2GB MEMORY DIMM • DL360G7 SRVR 4GB MEMORY DIMM	MSG: Removal and replacement procedures > <i>DIMMs</i>	Refer to the Systems Insight Display LEDs to identify the defective DIMM.  Caution: When removing the air baffle, ensure that the RAID battery does not fall out of its compartment in the baffle.	

No.	Task	Reference	Avaya recommendation	✓
			 Caution: Refer to the information on the top of the air baffle and inside cover for correct DIMM placement.	
	DL360G7 SRVR 650 MAH RAID BATTERY	MSG: Removal and replacement procedures > <i>BBWC battery pack or FBWC capacitor pack</i>	 Caution: Consult the internal label with directions for removing the air baffle. Be careful that the RAID battery does not fall out of its compartment in the baffle. To remove the cable from the battery, gently rock the connector back and forth and free of the alignment slots.  Caution: When replacing the air baffle and facing the front of the server, insert the left side into the alignment slots, then gently flex the baffle so that the right side slides into its alignment slot easily. DO NOT attempt to force or pound the baffle into place.  Caution: DO NOT pinch the battery cable when replacing the air baffle.	
7	Replace the cover	MSG: Removal and replacement procedures > <i>Access panel</i>		
8	Slide the server into the rack	RI-SR	Check that the Cable Management Arm (if present) moves freely	

No.	Task	Reference	Avaya recommendation	✓
			out of the way of rear panel components.	
9	Connect and secure the power cords	GS: <i>Connecting the Power Cables</i> GS: <i>Securing the Power Cord</i>		
10	Power up the server	GS: <i>Turning on the System</i>		

Appendix A: Alarm and Log Event IDs

Alarm Event ID descriptions

The following table contains a list of alarm event IDs, the severity of the alarm, and either a description of the message or a link to the description of the alarm and how to troubleshoot the problem.

The event ID is found in the message of the alarm.

Alarm Event ID Table		
Event ID	Alarm Severity	Alarm Description
OP_AASL10900	Minor	Certificate load failure Certificate Status on page 210
OP_ANFW11001	Warning	Network firewall stopped on page 222
OP_APLM10300	Minor	Failure pinholing Network Firewall Network Firewall Pinholing on page 222
OP_APLM10302	Minor	Failure configuring network parameters Network Configuration on page 221
OP_APLM10304	Minor	Ethernet interface is down Network Configuration on page 221
OP_AWTC10405	Warning	Identity certificate is about to expire Certificate Expiration on page 210
OP_AWTC10406	Minor	Identity certificate expired Certificate Expiration on page 210
OP_CCAC54000	Warning	Call Admission Control Call Denial on page 207
OP_CCAC54001	Warning	Call Admission Control Call Denial on page 207
OP_CCAC54003	Warning	Bandwidth threshold exceeded. Exceeding Location Bandwidth on page 215
OP_CDAO50001	Minor	The database connection is down. Database Connection on page 211
OP_CDAO50002	Minor	Database query failure (SQL Exception). Database Query on page 214

Alarm Event ID Table		
Event ID	Alarm Severity	Alarm Description
OP_CDAO50003	Minor	The database is corrupted. Database Corrupted on page 212
OP_CDAO50004	Warning	The database connection is down. Database Connection on page 211
OP_CDAO50006	Minor	Database Corrupted on page 212
OP_CDAO50009	Minor	A file I/O error occurred trying to write the local DNS server configuration or zone files. Zone File I/O on page 241
OP_CDAO50011	Major	The Session Manager Instance cannot be resolved. Session Manager Instance Resolution on page 230
OP_CDAO50012	Minor	Multiple Session Manager IP addresses map to the local Session Manager Instance. Session Manager Instance Resolution on page 230
OP_CDAO50013	Minor	DNS resolved to multiple IP addresses. Security Module Multiple DNS Resolutions on page 228
OP_CDAO50014	Warning	A file I/O error occurred trying to write the local DNS server configuration or zone files. Zone File I/O on page 241
OP_CDAO50020	Minor	CDR Not Operational on page 209
OP_CDAO50022	Warning	The direct link for Session Manager to Route Through is missing. Route Through on page 224
OP_CDAO50024	Warning	BSM Entity links not administered on page 205
OP_CDAO50026	Minor	BSM avaya-lsp entry missing in /etc/hosts. BSM missing avaya-lsp entry on page 206
OP_CMN55001	Warning	SIP Monitor Alarm on page 235
OP_CMN55002	Warning	SIP Monitor Alarm on page 235
OP_CSRE52003	Minor	Extension Module Deployment on page 216
OP_CURE56001	Warning	Registration authorization failure on page 224
OP_CURE56004	Warning	Registration interval too short on page 224
OP_CURE56006	Warning	URE route to application local port not found on page 238
OP_CURE56008	Warning	URE route to application entity link not found on page 238
OP_CURE56010	Warning	Registration service unavailable on page 225

Alarm Event ID Table		
Event ID	Alarm Severity	Alarm Description
OP_CURE56012	Warning	URE failure removing registrations on page 237
OP_CURE56014	Warning	URE failure querying for registrations on page 238
OP_CURE56016	Warning	URE failure matching registrations on page 237
OP_CURE56018	Warning	Subscription authorization failure on page 236
OP_CURE56021	Warning	URE failure storing registration on page 237
OP_CURE56023	Warning	URE application unreachable on page 236
OP_CURE56027	Minor	User failed over, manual fallback mode on page 239
OP_CURE56029	Minor	User failed over to Branch Survivability Server on page 240
OP_MAMA20100	Minor	Security Module Management Agent unable to connect to SIP A/S Management Server on page 227
OP_MAMA20102	Minor	Security Module Management Agent unable to configure Security Module on page 226
OP_MMTC20011	Minor	The Postgres database is inaccessible. Postgres database sanity check failed on page 222
OP_MMTC20013	Minor	SIP A/S Service Host(s) sanity check failed on page 232. Call processing is down.
OP_MMTC20015	Minor	SIP A/S Service Director sanity check failed on page 233. Call processing is down.
OP_MMTC20017	Minor	SIP A/S administration is unavailable. SIP A/S Management Server sanity check failed on page 231
OP_MMTC20019	Minor	Alarms are not being processed. SAL Agent sanity check failed on page 225
OP_MMTC20025	Minor	Security Module Sanity Failure on page 229
OP_MMTC20029	Minor	Call Processing SAR is not deployed on page 207
OP_MMTC20031	Minor	Data Distribution/Redundancy is down on page 213
OP_MMTC20033	Minor	Management Instance check failed on page 219
OP_MMTC20043	Minor	Management BSM instance check failed on page 217
OP_MMTC20045	Minor	Host name resolution failed on page 216
OP_MWD20202	Minor	Service <name of service> has totally failed on page 230
OP_PCFF40000	Critical	Missing file on page 220

Log Event ID descriptions

The following table contains an alphabetical list of log event IDs and a description of what caused the event. These events do not generate an alarm. Log events are not forwarded by the Session Manager or Survivable Remote Session Manager and cannot be viewed with the log viewer. Use the System Manager Log Harvester or search for the log on the Session Manager.

Audit log events (AU_MSEM203XX) may be viewed the log viewer for tracking administration changes.

The log severities are:

- EMERGENCY — system is unusable
- ALERT — immediate action is required
- CRITICAL — critical condition
- ERROR — error condition
- WARNING — warning condition
- NOTIFICATION — normal but significant condition
- INFORMATIONAL — informational message only

Log Event ID Table		
Event ID	Severity	Log Message
AU_MSEM20304	INFO	Database UPDATE on page 215
AU_MSEM20306	INFO	Database INSERT on page 214
AU_MSEM20308	INFO	Database DELETE on page 214
AU_MSEM20310	INFO	Request was made that affects a Session Manager. Action on Session Manager on page 205
AU_MSEM20312	INFO	Request was made that affects the System Manager. Action on System Manager on page 205
OP_AASL10901	INFO	Certificate load successful Certificate Status on page 210
OP_AASL10903	INFO	Connection Limit exceeded Connection limit exceeded on page 211
OP_AFWL15001	INFO	SIP Firewall: new configuration imposed SIP Firewall Configuration on page 235
OP_AFWL15002	INFO	Busyout mode is ON OFF Camp-on busyout mode on page 208
OP_AFWL16001	INFO	SIP firewall deep inspection disabled or no active rules

Log Event ID Table		
Event ID	Severity	Log Message
		SIP Firewall Configuration on page 235
OP_AFWL16002	ALERT	SIP firewall deep inspection configuration update failed, retaining existing configuration SIP Firewall Configuration on page 235
OP_AFWL16003	ALERT	SIP firewall configuration failed schema validation, retaining existing configuration SIP Firewall Configuration on page 235
OP_AFWL16501	ALERT	SIP Firewall Actions on page 234
OP_AFWL16502	INFO	SIP Firewall Actions on page 234
OP_AFWL16503	INFO	SIPFW block flow action summary log SIP FW Block flow action summary log on page 235
OP_AFWL17501	INFO	SIP firewall blacklist disabled or no active rules SIP Firewall Configuration on page 235
OP_AFWL17502	INFO	SIP firewall whitelist disabled or no active rules SIP Firewall Configuration on page 235
OP_AFWL17503	ALERT	SIP firewall blacklist configuration update failed, retaining existing configuration SIP Firewall Configuration on page 235
OP_AFWL17504	ALERT	SIP firewall whitelist configuration update failed, retaining existing configuration SIP Firewall Configuration on page 235
OP_ANFW11000	INFO	Network firewall started
OP_APLM10301	INFO	Success pinholing Network Firewall Network Firewall Pinholing on page 222
OP_APLM10303	INFO	Success configuring network parameters Network Configuration on page 221
OP_APLM10305	INFO	Ethernet interface is up Network Configuration on page 221
OP_AWTC10406	ALERT	Identify certificate expired Certificate Expiration on page 210
OP_CDAO50005	INFO	The database connection has been restored. Administration updates should be taking effect now. Database Connection on page 211
OP_CDAO50007	INFO	There was corrupt data in the database, but it has been corrected. Database Corrupted on page 212
OP_CDAO50008	INFO	There was an SQL query error, but it has been corrected. Database Query on page 214

Log Event ID Table		
Event ID	Severity	Log Message
OP_CDAO50010	INFO	There was a file I/O error, but it has been corrected. Zone File I/O on page 241
OP_CDAO50016	INFO	The Session Manager Instance resolution issue has been corrected. Session Manager Instance Resolution on page 230
OP_CDAO50017	INFO	DNS no longer resolves to multiple IP addresses for the Security Module. Security Module Multiple DNS Resolutions on page 228
OP_CDAO50019	INFO	Bandwidth threshold no longer exceeded for the <location name> location. Exceeding Location Bandwidth on page 215
OP_CDAO50021	INFO	The Call detail Recording (CDR) system is now operational. Call accounting is resumed. CDR Not Operational on page 209
OP_CDAO50023	INFO	The missing Entity Link for Session Manager to Route-Through has been inserted. Route Through on page 224
OP_CM0N55000	INFO	SIP monitoring state for entity has changed. SIP Monitor Alarm on page 235
OP_CSRE52000	INFO	The extension module now working properly and is deployed.
OP_CSRE52001	INFO	Call Admission Control did not deny an emergency call even though bandwidth would have been exceeded.
OP_CSRE53000	INFO	Call Admission Control denied a call on the Routing phase.
OP_CURE56000	INFO	Registration Authorizations no longer failing for user.
OP_CURE56003	INFO	Registration Expiration Interval no longer failing for user.
OP_CURE56004	INFO	Registration Expiration Interval Too Short for user.
OP_CURE56006	INFO	URE Proxy: Local Port Not Found for Application {Application name}, {phase} Phase, for user {user} at domain {domain}.
OP_CURE56007	INFO	URE Proxy: Entity Link No Longer Alarming for Application, user, domain.
OP_CURE56008	INFO	URE Proxy: Entity Link Not Found for Application for user at domain.

Log Event ID Table		
Event ID	Severity	Log Message
OP_CURE56009	INFO	Registration Service no longer failing for user, domain.
OP_CURE56010	INFO	Registration Service Failure, user , domain.
OP_CURE56011	INFO	Registrar no longer failing removing registrations for user, domain.
OP_CURE56012	INFO	Failure Removing Registrations for user, domain.
OP_CURE56013	INFO	Registrar no longer failing query for registrations, user, domain.
OP_CURE56014	INFO	Failure Querying for Registrations, user, domain.
OP_CURE56015	INFO	Registrar no longer failing matching registration for user, domain.
OP_CURE56016	INFO	Failure Matching Registration for user, domain.
OP_CURE56017	INFO	Subscription Authorizations no longer failing for user , domain.
OP_CURE56018	INFO	Subscription Authorizations failing for user, domain.
OP_CURE56020	INFO	No longer failing storing subscription, user, domain.
OP_CURE56021	INFO	Failure Storing Subscription, user, domain.
OP_CURE56022	INFO	Application {Application handle} at SIP Entity {Application's SIP Entity name} is no longer unreachable.
OP_CURE56023	INFO	Application {Application handle}} at SIP Entity {Application's SIP Entity name} is Unreachable.
OP_CURE56024	INFO	Receiving Subscription Notification errors for user {user}, domain {domain}, {date}.
OP_CURE56025	INFO	Call denied because route back route header was changed to {Route header URI}
OP_CURE56026	INFO	Emergency call with contact URI, originating location, to destination SIP entity.
OP_CURE57000	INFO	Unregistering the user removed through administration.
OP_CURE57001	INFO	User has registered.
OP_CURE57002	INFO	User has unregistered.
OP_CURE57003	INFO	User registration has expired.

Log Event ID Table		
Event ID	Severity	Log Message
OP_CURE57004	INFO	Unregistering user due to duplicate user registration. Only one active user is allowed with the current forking policy.
OP_CURE57005	INFO	User @ domain, event package subscription has expired.
OP_CURE57006	INFO	User, domain failed authentication.
OP_MAMA20101	INFO	Security Module Management Agent connected to SIP A/S Management Server
OP_MAMA20103	INFO	Security Module Management Agent is able to configure the Security Module.
OP_MMTC20012	INFO	Postgres database sanity check passed
OP_MMTC20014	INFO	SIP A/S Service Host(s) sanity check passed
OP_MMTC20016	INFO	SIP A/S Service Director sanity check passed.
OP_MMTC20018	INFO	SIP A/S Management Server sanity check passed
OP_MMTC20020	INFO	SAL-Agent sanity check passed
OP_MMTC20026	INFO	Security Module sanity check passed
OP_MMTC20030	INFO	Call Processing SAR is deployed successfully
OP_MMTC20032	INFO	Data Distribution/Redundancy is up.
OP_MMTC20034	INFO	Management Instance check passed
OP_MMTC20036	INFO	Forcing Garbage Collection of SM Management JBoss Server due to High Memory Usage of {0}
OP_MMTC20038	INFO	Restarting SM Management JBoss Server due to High Memory Usage of {0}
OP_MMTC20040	INFO	Restarting SM Management JBoss Server due to High CPU Average Utilization of {0}%
OP_MMTC20042	INFO	Restarting SM Management JBoss Server due to Thread Deadlock Condition
OP_MMTC20044	INFO	Management BSM Instance check passed
OP_MWD20200	INFO	Service <service name> has started.
OP_PCFF40001	INFO	Found [FnuFile LabelFile SmsConfigFile ButtonRangesFile]

Action on Session Manager

This event indicates that an administrator has initiated an administrative request from the System manager web console using a Session Manager Element Manager web page that affects a Session Manager or Survivable Remote Session Manager (Branch Session Manager). For example, an administrator may have put a Session Manager into the **Deny New Service** state using the **Session Manager Administration** web page in order to busyout this Session Manager.

The log messages for this event have the following format:

- LoginID:<Name of user logged into the System Manager web console>
- ClientHost :<IP address of the web user's computer>
- Action on Session Manager: <name of Session Manager or Branch Session Manager>
- Description: <description of the requested action>

An example of the log message is: LoginID: admin ClientHost: 123.4.56.789 Action on Session Manager:MySessionManager.dr.avaya.com Description: Initiated Deny New Service

Action on System Manager

This event indicates that an administrator has initiated an administrative request from the System manager web console using a Session Manager Element Manager web page that affects the System Manager server itself.

The log messages for this event have the following format:

- LoginID:<Name of user logged into the System Manager web console>
- ClientHost :<IP address of the web user's computer>
- Action on System Manager Description:<description of the requested action>

BSM Entity links not administered

This event indicates that the mandatory entity links from the Survivable Remote Session Manager (BSM) have not been administered. When the BSM initializes, it uses these entity links to set up the connections between the BSM and LSP. Failure to find those links will raise this warning.

During BSM initialization, links between the BSM instance and the core Communication Manager being subtended by the branch could not be found. The most likely cause is that the entity links have not been administered through the System Manager. The BSM was probably

installed before the links were administered on the System Manager and will therefore resolve after administration is completed.

There should be one or two links administered depending on the Communication Manager configuration in the core. The links should use the same ports administered between the core Communication Manager and the primary (core) Session Manager. It may also indicate that one or more branch users have a Communication Manager application to a Communication Manager that the branch does not subtend.

Troubleshooting unadministered BSM entity links

Procedure

1. Add the correct entity link or entity links between the BSM instance and the core Communication Manager to which it subtends.
The ports and transports used should mirror those used on the entity links between the core Communication Manager and the primary Session Manager.
 2. If the above step does not clear the warning, verify that all users on the branch use a Communication Manager application mapping to the subtended Communication Manager.
 3. If this does not resolve the problem, contact Avaya Technical Support.
-

BSM missing avaya-lsp entry

About this task

This event indicates the avaya - lsp entry was not found in the /etc/hosts file on the survivable remote Session Manager server (BSM).

This entry is added during the template installation. It informs the BSM of the LSP IP address. If this entry is not in the /etc/hosts file, the BSM cannot connect to the LSP, resulting in severely limited service in survivability mode.

Procedure

1. Log in to the System Platform Web Console.
 2. Select **Server Management > Network Configuration**
 3. Review the administration information and correct values, if needed.
 4. Log out of the System Platform Web Console.
-

Call Admission Control Call Denial

This event is related to the Call Admission Control functionality for Session Manager.

When there are multiple call failures due to lack of bandwidth for a call on a particular location, the alarm will trip. The alarm will continue periodically checking the system for the number of calls denied through a particular location within the last interval (defaulted to one hour). When there have not been any calls denied for the location within the last interval (hour), the alarm will clear.

This 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. However, traffic exceeds actual network capacity.

Troubleshooting CAC Call Denial

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.
-

Call Processing SAR is not deployed

The periodic maintenance sanity check has detected the Session Manager Call Processing SAR is not deployed on the SIP A/S Service Host. This SAR provides the Session Manager SIP call processing and is an essential component.

Troubleshooting Call Processing SAR is not deployed

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 2. Select the affected Session Manager from the **Select Target** list.
 3. Select the following tests:
 - **Test Call Processing status**
 - **Test Service Host status**
 4. Click **Execute Selected Tests**
 5. If both of the tests pass, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 6. If one or both of the tests fail, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 7. Enter **statapp** to verify the status of **sipas-SH**.
 8. If the status of **sipas-SH** is **Down**, enter **restart sipas-SH** and wait for the SIP A/S server host to restart.
 9. If the status of **sipas-SH** is **Partially Up**, wait for the status to change to completely **Up**.
 10. Enter **statapp** to verify the status of **sipas-SH**.
 11. Re-run the **Test Call Processing status** test and the **Test Service Host Status** test.
 12. If the problem persists, a re-install of Session Manager may be required.
-

Camp-on busyout mode

This log event indicates that the Camp-on Busyout mode has changed from ON to OFF or vice versa.

When this mode is turned on:

- new calls or registration attempts are rejected
- active calls are not affected

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 database process may not be running.
- The CDR Extension Module is unable to process CDR call events or it may not be running.
- The connection to the CDR database has been lost or it is experiencing timeouts between queries.
- The user name and/or password that the system uses does not match the user name and/or password in the CDR database.
- The CDR database may not be running on the Service Director or is on a different IP address than expected.

Troubleshooting CDR Not Operational Alarms

Procedure

1. Ensure the CDR database process is running on the Service Director.
 2. Ensure that the CDR Extension module is deployed and running.
 3. Ensure no errors or exceptions are logged by the CDR Extension module.
 4. Ensure there is an actual connection to the CDR database. Also check that this connection is stable and not experiencing outages.
 5. Make sure the CDR database user name and passwords match the default values provided by the system.
 6. Ensure that the CDR database is running on the Service Director.
 7. Ensure that the Service Director IP address is configured properly for the running Instance.
 8. If the problem persists, contact Avaya Technical Support.
-

Certificate Expiration

The Security Module requires a certificate for securing SIP connections. If this certificate has expired, the Security Module 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 Security Module 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.

Certificate Status

The Security Module 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 210 in this document.
 4. See Trust Management in *Administering Avaya Aura® Session Manager*, 03-603324 .
-

Connection limit exceeded

The Security Module limits the number of concurrent connections for a single remote IP.

When this limit is exceeded, the following information is displayed:

- value of the limit
- the remote IP violating the limit
- the transport layer used

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 database may not be running.
- The connection to the database has been lost or is experiencing timeouts between queries.
- The user name or password that the system uses may not match the user name or password in the database.
- The database process may not be running on the Service Director or is on a different IP address than expected.

Troubleshooting Database Connection Alarms

Procedure

1. Ensure the database process is running on the Session Manager. Log into the Session Manager system and execute one or all of the following commands:
 - a. Enter **ps —ef | grep postgres**
There should be two process entries. One of the entries should be similar to **/usr/java/jdk1.6.0_11/bin/java -server -XX:NewSize=32m...**
 - b. Enter **statapp —s postgres —db**
The output should be similar to **postgres—db 18/ 18 UP**
 - c. As root, enter **service postgresql status**

The output should be similar to **postmaster (pid 32617 32570 32569 32568) is running...**

- d. If none of the above conditions are true, enter `start -s postgres-db`. This command requires the root login.
 2. Ensure there is an actual connection to the database. Also check that this connection is stable and not experiencing outages. Ensure the Service Director 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 Service Director.
 - b. If there is no answer, the system is either in an unresponsive state or is currently off or in the middle of a reboot.
 3. Ensure Service Director IP address or DNS name is configured properly for the running Instance.
 - a. As root, edit the Service Host's file **/opt/Avaya/SIPAS/current/ServiceHost0/var/server.config**
 - b. Verify that the XML entry for **UscINSLBHostName** matches the proper IP address of the Service Director. If it doesn't match, the value that was entered during installation for this field was entered incorrectly.
 - c. To recover from this event, reinstall the Session Manager on this machine and enter the correct IP address or DNS name.
 4. If the problem continues after performing the above steps, contact Avaya Technical Support.
-

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.

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.

Data Distribution/Redundancy is down

The Session Manager data distribution and redundancy system has failed a periodic maintenance status check. This service is required for SIP call processing to distribute provisioned and status data.

Troubleshooting data distribution/redundancy down alarm

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 2. Select the affected Session Manager from the **Select Target** list.
 3. Select the **Test data distribution and redundancy link** test.
 4. Click **Execute Selected Tests**
 5. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 6. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 7. Run **statapp** to verify the status of the **sipas-SH** and **sm-mgmt** processes.
 8. If the status of **sipas-SH** is **Down**, run **restart sipas-SH** and wait for the SIP A/S Service Host to restart.
 9. If the status of **sipas-SH** is **Partially Up**, wait for the status to change to completely **Up**.
 10. Run **statapp** and verify that the status of **sipas-SH** is **Up**.
 11. Re-run the **Test data distribution and redundancy link** test.
 12. If the test fails, run **restart sm-mgmt** and wait for the Management Jboss service to restart.
 13. If the problem persists, reboot the Session Manager using the **Session Manager > Dashboard** page.
 14. If the reboot does not solve the problem, re-install the affected Session Manager.
-

Database DELETE

This event indicates that an administrator has deleted an existing record in the System Manager database. For example, an administrator may have deleted a Session Manager instance using the **Session Manager Administration** web page.

The log messages for this event have the following format:

- LoginID:<Name of user logged into the System Manager web console>
- ClientHost :<IP address of the web user's computer>
- Action: Database DELETE from table <database table name> with key <database record primary key value>

An example of the DELETE log message is: LoginID: admin ClientHost: 123.4.56.789
Action: Database DELETE from table asminstance with key 1

Database INSERT

This event indicates that an administrator has added a new record into the System Manager database. For example, an administrator may have added a new Session Manager instance using the **Session Manager Administration** web page.

The log messages for this event have the following format:

- LoginID:<Name of user logged into the System Manager web console>
- ClientHost :<IP address of the web user's computer>
- Action: Database INSERT into table <database table name> with key <database record primary key value> and properties: <database table column name>:<column value>, ...

An example of the INSERT log message is: LoginID: admin ClientHost: 123.4.56.789
Action: Database INSERT into table asminstance with key 1 and properties:
assetDNSIPAddress:<NULL>, assetDNSSearch:<NULL>, assetDefaultGateway:
255.255.255.0, assetIPAddress:<NULL>, assetInterfaceName:<NULL>,
assetNetMask:255.255.255.0...

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.

Call Avaya Technical Support to check the database versions and 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 UPDATE

This event indicates that an administrator has updated an existing record in the System Manager database. For example, an administrator might have edited a Session Manager instance using the **Session Manager Administration** web page.

The log messages for this event have the following format:

- LoginID:<Name of user logged into the System Manager web console>
- ClientHost :<IP address of the web user's computer>
- Action: Database UPDATE into table <database table name> with key <database record primary key value> and properties: <database table column name>:[<previous value>]=><new value>, ...

An example of the UPDATE log message is: LoginID: admin ClientHost: 123.4.56.789 Action: Database UPDATE into table asminstance with key 1 and properties: description: [<NULL>]=>This is my sm

Exceeding Location Bandwidth

This event is related to the Call Admission Control functionality for Session Manager.

The used bandwidth for a specific Location has consistently exceeded a predefined high threshold (currently, 85% of the bandwidth capacity). It is not uncommon to see the same alarm coming from other Session Managers in the core around the same time.

When the bandwidth is at 100% capacity for a particular Location, new calls are not allowed on 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. However, 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.
-

Extension Module Deployment

The DNS Extension Module is missing or is corrupted.

The Extension Module described in the alarm log was not properly deployed. Currently, the only supported module that can produce this error is the DNS Extension Module. During this outage, any non-provisioned, DNS Fully Qualified Domain Names (FQDN) will not be resolved.

There is no corrective action. Call Avaya Technical Support.

Host name resolution failed

The on-demand or periodic maintenance test run on the System Manager has detected connection problems with resolving the host name of Session Managers (SM) or Branch Session Managers (BSM).

Troubleshooting Host name resolution failed

Procedure

1. If the DNS server is administered on System Manager, make sure it is reachable from System Manager.
 2. Make sure the Session Manager and/or survivable remote Session Manager (BSM) host name is administered properly on the DNS server(s).
 3. If the DNS server is not administered, make sure the host name-to-IP address map of the Session Manager and/or survivable remote Session Manager (BSM) is in the **/etc/hosts** file on System Manager. If it is not:
 - a. Log in to the System Platform Web Console.
 - b. Select **Server Management > Network Configuration**
 - c. Make sure the administration is correct. If not, enter the correct information.
 - d. Log out of the System Platform Web Console.
-

Management BSM instance check failed

The periodic maintenance test which runs on the System Manager has detected connection problems with the listed Branch Session Managers (BSM).

Troubleshooting Management BSM instance check failure

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > Dashboard**
2. Check the latest status for each administered Branch Session Manager.
3. Note the Branch Session Managers which are currently failing tests, if any. The failing tests may indicate connectivity problems from the System Manager.
4. For each failing Branch Session Manager:
 - a. Under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - b. Select the Branch Session Manager from the **Select Target** list.

- c. Run the associated demand Maintenance Tests to verify the current connection status to the administered Branch Session Manager.
 5. If the demand tests pass for all previously failing Branch Session Managers, clear this alarm. The problem no longer exists, and nothing further needs to be done.
 6. Resolve all network problems including possible incorrect DNS and network firewall settings.
 7. If a network problem is resolved:
 - a. Verify the status on the Dashboard.
 - b. Run the demand Maintenance Tests on the previously failing Branch Session Managers.
 8. If the tests fail, bring up the web console for the System Platform hosting the Branch Session Manager.
 9. Select **Virtual Machine Management > Manage**
 10. Check the **Application State** for the Branch Session Manager.
 11. If the application state is **Running**, the Branch Session Manager is running normally.
 12. If the application state is **Starting**, the Branch Session Manager is starting up. Wait for the application state to change to **Running**.
 13. If the application state is **Stopped**, the Branch Session Manager is inactive.
 14. If the application state is **Unknown**, installation has just completed and progress information has not been received. Wait for the application state to change.
 15. If the application state is **Partially**, not all of the services are up and running. Wait for the application state to change.
 16. If the application state is **Error**:
 - a. Select the link under the **Version** column to see a log of what happened during the Branch Session Manager startup.
 - b. Log on to the Branch Session Manager.
 - c. Check for trouble deploying with SFS.
 - d. Check for trust management initialization failures and resolve, if any.
 - e. Check for DRS replication initialization failures and resolve, if any.
 17. Re-run the demand Maintenance Tests for the failing Branch Session Manager.
 18. If the tests are still failing, run **initTM** on the Branch Session Manager to clear possible trust relationship problems.
 19. Re-run the demand Maintenance Tests.
-

Management Instance check failed

The periodic maintenance test which runs on the System Manager has detected connection problems with the listed Session Managers.

Troubleshooting Management instance check failure

About this task

If multiple Session Managers are failing the ping tests, a network problem may be the cause of the alarms.

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > Dashboard**
2. Check the latest status for each administered core Session Manager.
3. Note which Session Managers are currently failing tests, if any. The failing tests may indicate connectivity problems from the System Manager.
4. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
5. Select **System Manager** from the **Select Target** list.
6. Select the **Test network connections to each Session Manager** test.
7. Click **Execute Selected Tests**
8. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
9. If the tests fails, do the following for *each* of the failing administered core Session Managers:
 - a. Run a ping test for the failing Session Manager using either **ping <IP address of the Session Manager >** or **ping <hostname of the Session Manager>** from the System Manager shell.
 - b. If the ping test fails:
 - i. Establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 - ii. Enter **statapp** to verify the status of **sm-mgmt**.
 - iii. If the status of **sm-mgmt** is **Down**, enter **restart sm-mgmt** and wait for the Management JBoss server to restart.

- iv. If the status of **sm-mgmt** is **Partially Up**, wait for the status to change to completely **Up**.
 - v. Enter **statapp** to verify that the status of **sm-mgmt** is **Up**.
 - vi. Re-run the **Test network connections to each Session Manager** test.
 - vii. If the test fails, enter **initTM** on the Session Manager to clear possible trust relationship problems.
 - viii. Re-run the **Test network connections to each Session Manager** test.
 - ix. Note if the test passes or fails for this Session Manager.
 10. If multiple Session Managers are failing the ping test:
 - a. Resolve all network problems including possible incorrect DNS and network firewall settings.
 - b. If a network problem is resolved, verify the latest status on the Session Manager Dashboard.
 - c. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - d. Select **System Manager** from the **Select Target** list.
 - e. Select the **Test network connections to each Session Manager** test.
 - f. Click **Execute Selected Tests**.
 11. If the problem persists and no known network problems exist, reboot the Session Manager. This may required physical access to the server if you are unable to reboot using the **Session Manager > Dashboard** page or cannot establish an ssh connection.
-

Missing file

One of the following files is missing:

- FnuFile
- LabelFile
- SmsConfigFile
- ButtonRangesFile

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

Clearing a missing file alarm

Procedure

1. Use a copy of the backup file:
 - a. Copy a saved backup of the missing file to the proper directory.
 - b. Restart sm-mgmt.
 2. If a backup file of the missing file does not exist, reinstall the server.
-

Network Configuration

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

When the Security Module is stopped or restarted, you will see the Security Module interface (Eth2) change state between up and down, unless NIC bonding is being used as noted below. During normal operation, the interface should be up only. Failure to properly configure the Security Module network may be the result of incorrect settings.

The primary Security Module interface is Eth2. When NIC bonding is activated:

- the Security Module will use Eth3 as its secondary interface
- a logical interface called **bond0** will be defined

When NIC bonding is not activated, the following alarms/log events are displayed:

- OP_APLM10304 eth2 Interface is down
- OP_APLM10305 eth2 Interface is up

When first activating NIC bonding, the following four alarms/logs are shown:

- OP_APLM10304 bond0 Interface is down
- OP_APLM10304 eth3 Interface is down
- OP_APLM10305 eth2 Interface is up
- OP_APLM10305 bond0 Interface is up

When NIC bonding is active, alarms/logs will indicate the status changes of each interface. For example, when the primary interface goes down and the secondary takes over, the following alarm/log sequence appears:

- OP_APLM10304 eth2 Interface is down
- OP_APLM10305 eth3 Interface is up
- OP_APLM10305 bond0 Interface is up

Network Firewall Pinholing

By default, the Security Module 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 firewall stopped

Network firewall cannot be stopped using the GUI.

This alarm indicates that someone has manually turned off Network Firewall.

Postgres database sanity check failed

The periodic maintenance sanity check of the Postgres database has failed and possibly Postgres service is not running.

This failure requires actions on both Session Manager and System Manager. System Manager requires root privileges.

Troubleshooting Postgres database sanity check failed

Procedure

1. For Session Manager:
 - a. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - b. Select the affected Session Manager from the **Select Target** list.
 - c. Select the **Test Postgres database sanity** test.
 - d. Click **Execute Selected Tests**
 - e. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 - f. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 - g. Run **statapp** to verify the status of **postgres-db**.
 - h. If the status of **postgres-db** is **Down**, run **restart postgres-db** and wait for the Postgres service to restart.
 - i. If the status of **postgres-db** is **Partially Up**, wait for the status to change to completely **Up**.
 - j. Run **statapp** to verify the status of **postgres-db**.
 - k. Re-run the **Test Postgres database sanity** test.
 - l. If the test still fails, reboot the Session Manager server using the reboot option on the **Session Manager > Dashboard** page.
2. For System Manager: (requires root privilege)
 - a. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - b. Select System Manager from the **Select Target** list.
 - c. Select the **Test Postgres database sanity** test.
 - d. Click **Execute Selected Tests**
 - e. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 - f. Run **service postgresql status** to verify if the Postgres service is running.
 - g. If the Postgres service is up, nothing further needs to be done.
 - h. If the service is down, run **service postgresql restart** to start service.
 - i. Wait for the Postgres service to restart.

- j. Run **service postgresql status** to verify that the Postgres service is running.
 - k. If the Postgres service is still down, check the available disk space under the /var partition.
 - l. If there is enough disk space, reboot the server.
 - m. If there are still problems, contact Avaya Technical Support.
-

Registration authorization failure

This event is related to the Registrar functionality for the URE. This event indicates that a user has attempted to register with Session Manager and failed to provide valid authorization credentials. A warning is logged after five registration attempts fail in one minute. The event is cleared automatically if no more registration authorization failures occur.

The credentials provided at login by the endpoint are invalid or incorrect.

Ensure the credentials used for endpoint registration are correct.

Registration interval too short

The expiration interval provided at login by the endpoint is of insufficient length.

This event is related to the Registrar functionality for the URE. It indicates that a user has attempted to register with Session Manager and failed to provide a valid registration expiration time interval. A warning is logged after three registration attempts fail in one minute. .

To fix this problem, ensure the expiration interval used for endpoint registration is greater than 300 seconds (5 minutes). The event is cleared automatically if no more registration failures occur.

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.

To fix this problem, add the correct Entity Link between the two Session Managers. The alarm message should identify which Session Managers experienced the “Can't Route Through” problem

Registration service unavailable

This event is related to the endpoint processing function in the URE. . This event means that the system experienced a problem or failure while processing a SIP domain resolution for an endpoint. A warning event is logged after four failures occur within five minutes. The event is automatically cleared when such events stop.

This event can occur if the Data Manager component experiences a failure for one or more users. The failure could be due to an internal corruption or an error condition.

If the problem persists or reoccurs, call Avaya Technical Support.

SAL Agent sanity check failed

The periodic maintenance sanity check of the SAL Agent has failed and possibly Session Manager alarming service is not running.

The troubleshooting actions are performed on both Session Manager and System Manager. Root privilege is required only for the System Manager corrective action.

Troubleshooting SAL Agent sanity check failure

Procedure

1. For Session Manager:
 - a. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - b. Select the affected Session Manager from the **Select Target** list.
 - c. Select the **Test sanity of Secure Access Link (SAL) agent** test.
 - d. Click **Execute Selected Tests**
 - e. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 - f. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 - g. Run **statapp** to verify the status of **sal-agent**.

- h. If the status of **sal-agent** is **Down**, run **restart sal-agent** and wait for the sal-agent service to restart.
 - i. If the status of **sal-agent** is **Partially Up**, wait for the status to change to completely **Up**.
 - j. Run **statapp** to verify the status of **sal-agent**.
 - k. Re-run the **Test sanity of Secure Access Link (SAL) agent** test.
 - l. If the test still fails, reboot the Session Manager server using the reboot option on the **Session Manager > Dashboard** page.
2. For System Manager: (requires root privilege)
- a. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 - b. Select System Manager from the **Select Target** list.
 - c. Select the **Test sanity of Secure Access Link (SAL) agent** test.
 - d. Click **Execute Selected Tests**
 - e. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 - f. Run **service spiritAgent status** to verify if the SAL agent service is running.
 - g. If the Postgres service is up, nothing further needs to be done.
 - h. If the service is down, run **service spiritAgent restart** to restart service.
 - i. Wait for the SAL Agent service to restart.
 - j. Run **service spiritAgent status** to verify that the SAL agent service is running.
 - k. Re-run the **Test sanity of Secure Access Link (SAL) agent** test.
 - l. If the test still fails, contact Avaya support services.
-

Security Module Management Agent unable to configure Security Module

The management configuration of the Security Module is failing. Without the configuration, the Security Module will not setup the network configuration for accepting SIP connections.

Troubleshooting unable to configure Security Module

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
2. Run the maintenance test **Test Security Module Status** for the failing Session Manager to verify the sanity of the Security Module.
3. Under **Elements**, select **Session Manager > System Status > Security Module Status**
4. If the test passes and the **Status** for the Session Manager is **Up**, clear the alarm. The problem no longer exists.
5. If the test fails or if the **Status** is **Down**
 - a. Select the appropriate Session Manager 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.

- c. Use the **Refresh** button to display the current status.
 - d. Re-run the **Test Security Module Status** maintenance test in step 2 for this Session Manager.
-

Security Module Management Agent unable to connect to SIP A/S Management Server

This important connection is down and is blocking retrieval of information for setup of the Security Module

Troubleshooting unable to connect to SIP A/S Management Server

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 2. Run the maintenance test **Test SIP A/S Management Server Status** for the failing Session Manager.
 3. If the test passes and the Security Module status displays **Up** for this Session Manager, change the alarm status to **clear**. The problem no longer exists.
 4. If the test fails:
 - a. Establish an ssh connection to the Session Manager.
 - b. Log in with either the craft login (Avaya) or the established customer login.
 - c. Run the **statapp** command to verify the status of **sipas-MS**.
 - d. If the status displays **Down**, run **restart sipas-MS**.
 - e. If the status displays **Partially up**, wait for the status to change to completely up.
 - f. Wait for the SIP A/S Management Server to restart.
 - g. Verify application status using the **statapp** command.
 - h. Re-run the **Test SIP A/S Management Server Status** maintenance test for this Session Manager.
-

Security Module Multiple DNS Resolutions

The DNS name resolves to more than one IP address.

The Security Module 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, whether it is correct or not. This means the system may work just fine, however it is highly dangerous in terms of having a reliable system.

Troubleshooting Security Module Multiple DNS Resolution Alarms

Procedure

1. Check the IP address in the Session Manager's Security Module administration and make sure it is correct.
 2. Check what the name resolves to by entering one of the following commands:
 - a. Enter host *someDNSname* where *someDNSname* is the server name.
 - b. Use some other equivalent DNS reverse look-up tool such as dig
 3. Check /etc/hosts to ensure that the name resolves to the proper single IP address.

The file should have entries in the form of <IP Address> <FQDN> <domain>
 4. Fix real DNS to resolve to one IP address.
-

Security Module Sanity Failure

The Security Module failed a sanity check.

Troubleshooting Security Module Sanity failure

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Status > Security Module Status**
2. Select **Refresh** to display the current status.
3. The **Status** for the indicated Session Manager should be **Up**.
4. If the status is **Down**, reset the security module:
 - a. Select the appropriate system from the System Name list.
 - b. Select **Security Module Reset**



Warning:

The Session Manager cannot process calls while the security module is being reset.

5. Select **Refresh** to display the current status.
-

Service <name of service> has totally failed

The Session Manager watchdog service is unable to start the service specified in the alarm message.

Troubleshooting Session Manager service failure

Procedure

1. Make sure the Session Manager is properly configured for the failing service.
2. Run **statapp** to see which services are running. Not all monitored services are displayed with this command.
3. Run **/sbin/service <failing-service-name> status** to see if the service is running. This command requires root privilege.
4. If the service is not running, reboot the Session Manager server using the **Session Manager > Dashboard** web page.



Warning:

Rebooting the Session Manager server will affect calls.

5. If the problem persists, contact Avaya Technical Support.
-

Session Manager Instance Resolution

This event occurs when the administration for the Session Manager instance does not match the IP address of the configured Service Director. During this failure, the Service Host(s) will not service any calls.

Possible causes are:

- The web interface's Session Manager Administration configuration has an IP address that does not match the Service Director's IP Address in the Management Access Point field.
- The IP address of the Security Module was entered in place of the Service Director's IP address.
- The DNS name resolves to multiple IP addresses or no IP addresses.

Troubleshooting Session Manager Resolution Alarms

Procedure

1. Check the IP address in the Session Manager Administration's Management Access Point Host Name/IP field:
 - a. Enter **/sbin/ifconfig**
 - b. The IP address should match the Session Manager's eth0 IP address.
 2. If the Management Access Point Host Name/IP is a DNS name, check what it resolves to using one of the following commands:
 - a. Enter **host *someDNSname*** where *someDNSname* is the server name.
 - b. Use some other DNS reverse lookup tool such as **dig**.
 3. Check the **/etc/hosts** file on the Session Manager to ensure that the name resolves to the proper, single IP address. The file should have entries in the form of **<IP Address> <FQDN> <hostname>**.
 4. If the information in the **/etc/hosts** file is incorrect or missing:
 - a. Log in to the System Platform Web Console.
 - b. Select **Server Management > Network Configuration**
 - c. Verify the administration information or correct as needed.
 - d. Log out of the System Platform Web Console.
-

SIP A/S Management Server sanity check failed

The SIP A/S Management Server has failed a periodic maintenance sanity check. This service is required for administration, configuration, and status queries of SIP A/S including console from System Manager.

Troubleshooting SIP A/S Management Server sanity check failure

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
 2. Select the affected Session Manager from the **Select Target** list.
 3. Select the **Test SIP A/S Management Server status** test.
 4. Click **Execute Selected Tests**
 5. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 6. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 7. Run **statapp** to verify the status of **sipas-MS**.
 8. If the status of **sipas-MS** is **Down**, run **restart sipas-MS** and wait for the SIP A/S service to restart.
 9. If the status of **sipas-MS** is **Partially Up**, wait for the status to change to completely **Up**.
 10. Run **statapp** to verify the status of **sipas-MS**.
 11. Re-run the **Test SIP A/S Management Server status** test.
-

SIP A/S Service Host(s) sanity check failed

The SIP A/S Service Host has failed a periodic maintenance sanity check. This service is required for SIP call processing.

Troubleshooting SIP A/S Service Host sanity check failed

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
2. Select the affected Session Manager from the **Select Target** list.
3. Select the **Test Service Host Status** test.

4. Click **Execute Selected Tests**
 5. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
 6. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
 7. Run **statapp** to verify the status of **sipas-SH**.
 8. If the status of **sipas-SH** is **Down**, run **restart sipas-SH** and wait for the SIP A/S service to restart.
 9. If the status of **sipas-SH** is **Partially Up**, wait for the status to change to completely **Up**.
 10. Run **statapp** to verify the status of **sipas-SH**.
 11. Re-run the **Test Service Host Status** test.
-

SIP A/S Service Director sanity check failed

The SIP A/S Service Director has failed a periodic maintenance sanity check. This service is required for SIP call processing.

Troubleshooting SIP A/S Service Director sanity check failed

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**
2. Select the affected Session Manager from the **Select Target** list.
3. Select the **Test Service Director Status** test.
4. Click **Execute Selected Tests**
5. If the test passes, clear the alarm. The problem no longer exists, and nothing further needs to be done.
6. If the test fails, establish an ssh connection to the Session Manager using either the craft login (Avaya) or an established customer login.
7. Run **statapp** to verify the status of **sipas-SD**.
8. If the status of **sipas-SD** is **Down**, run **restart sipas-SD** and wait for the SIP A/S service to restart.

9. If the status of **sipas-SD** is **Partially Up**, wait for the status to change to completely **Up**.
 10. Run **statapp** to verify the status of **sipas-SD**.
 11. Re-run the **Test Service Director Status** test.
-

SIP Firewall Actions

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

The log or alarm message includes the following information:

- 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
- destination host address/port

For rules with track operation, the concrete track value is displayed. 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.

SIP Firewall Configuration

Changes to the Security Module 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 **Configuring SIP Firewall** section of *Administering Avaya Aura® Session Manager* at <http://support.avaya.com/css/P8/documents/100068081> to ensure that the rule is correctly configured.
 2. If the problem persists, report the problem to Avaya Technical Support.
-

SIP FW Block flow action summary log

Whenever the SIPFW is stopping a block attack (for example, when an attack is detected to be stopped or goes below the predefined threshold), a summary log is generated. This log contains information on the packet dropped during the blocking period.

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).
-

Subscription authorization failure

This event is related to the Eventing Handler functionality of the URE. This alarm means that a user has attempted to subscribe with Session Manager and failed to provide a valid authorization credentials. A warning is logged after five subscription attempts fail in one minute.

The credentials provided at subscription are invalid.

Ensure the credentials used for endpoint subscription are correct.

URE application unreachable

This event is related to the URE routing functionality. This event means that routing to an application failed because the application is down or unreachable. A warning is logged after five such routing attempts fail in one minute.

Possible causes:

- The application is down or the application is experiencing problems and it is rejecting requests.
- Network connectivity to the application is temporarily experiencing problems.

Troubleshooting URE application unreachable

Procedure

1. Ensure connectivity to the application.
 2. Ensure the application is up and able to accept requests.
-

URE failure matching registrations

This event is related to the Registrar functionality for the URE. This event means that the Registrar's Data Manager component is experiencing problems while matching data for registered contacts. A warning event is logged after three such failures occur in one minute. The event is automatically cleared when such events stop.

This event can occur if the Data Manager component experiences a failure for one or more users. The failure could be due to an internal corruption or error condition.

If the problem persists or reoccurs, call Avaya Technical Support.

URE failure removing registrations

This event is related to the endpoint processing function in the URE. This event means that a user has logged off with Session Manager or a registration expired and the Registrar's Data Manager component is experiencing problems while removing the user's registration data. A warning event is logged after three such failures occur in one minute. The event is automatically cleared when such events stop.

This event can occur if the Data Manager component experiences a failure for one or more users. The failure could be due to an internal corruption or error condition.

If the problem persists or reoccurs, call Avaya Technical Support.

URE failure storing registration

This event is related to the Eventing Handler functionality for the URE. This event means that the Handler is experiencing problems while storing subscription data. A warning event is logged after three such failures occur in one minute. The event is automatically cleared when such events stop.

This event can occur if the Data Manager component experiences a failure for one or more users. The failure could be due to an internal corruption or error condition.

If the problem persists or reoccurs, call Avaya Technical Support.

URE failure querying for registrations

This event is related to the Registrar functionality for the URE. This event means that the Registrar's Data Manager component is experiencing problems while querying for a registered user. A warning event is logged after three such failures occur in one minute. The event is automatically cleared when such events stop.

This event can occur if the Data Manager component experiences a failure for one or more users. The failure could be due to an internal corruption or error condition.

If the problem persists or reoccurs, call Avaya Technical Support.

URE route to application entity link not found

This event is related to the Proxy functionality for the URE relative to Application sequencing and routing. This alarm means that routing to an application failed because the SIP Entity Link to the application could not be found. An alarm is logged as soon as the failure occurs. After the alarm is raised, the condition is monitored every hour thereafter. The alarm is cleared when the failure condition is corrected.

The SIP Entity Link to the Application does not exist. Ensure the SIP Entity Link to the Application is provisioned.

URE route to application local port not found

This event is related to the Proxy functionality for the URE relative to application sequencing and routing. This alarm means that routing to an application failed because the local port could not be found. An alarm is logged as soon as the failure occurs. After the alarm is raised, the condition is monitored every hour thereafter. The alarm is cleared when the failure condition is corrected.

The port provisioning on the SIP Entity Link to the application is incorrect .

Ensure the port provisioning on the SIP Entity Link to the application is correct.

User failed over, manual failback mode

This event occurs when one or more users fail over to their non-primary, redundant Session Manager and the Global failback policy is set to **manual**.

Manual failback policy means that without manual intervention, the failed over user(s) will stay on this non-primary Session Manager forever. This does not necessarily mean that there is a loss in service, but rather a notification of a potential problem.

The primary Session Manager is defined on the User's administration page under the **Communication Profile** and **Session Manager Profile** section, and is indicated as the first drop-down menu for Primary Session Manager.

Possible causes for this event are:

- The primary Session Manager is not running.
- The user has lost connectivity to its primary Session Manager. This could be due to network issues or something else.
- The primary Session Manager is currently in the **Deny New Service** state.
- The primary Session Manager is currently overloaded.
- The primary Session Manager is in an error state which is preventing the user from receiving service from it.

Troubleshooting User failed over, manual failback mode

Procedure

1. Make sure the Session Manager is up and running.
2. Verify the Session Manager is in the **Accept New Service** state.
3. Check the **SIP Entity Monitoring** page to see if there are any network connectivity problems to the primary Session Manager.
4. Using the **User Registration** page:
 - a. Find the affected users.
 - b. Select the affected users.
 - c. Click the **Failback** button.
5. Change the Global Failback Policy on the **Session Manager Administration** screen from **Manual** to **Auto**.
6. If none of these steps work, contact your Avaya support representative.

User failed over to Branch Survivability Server

This event occurs when one or more users fail over to their branch survivability server due to a loss of connectivity to their core Session Managers. Users active on the Survivable Remote Session Manager (BSM) will not receive the full service of the core. The only sequenced application available in survivability mode is the Communication Manager application for the Communication Manager subtended by the branch. Calls placed from a branch SIP user to a user outside the branch must be dialed using the user's public number. Calls placed to a branch SIP user from outside the branch must be placed by dialing the public number.

Possible causes are:

- connectivity loss between the branch and core.
- partial network outages to the core.
- the core Session Managers are overloaded.
- the core Session Managers are in the **Deny New Service** state.
- the core Session Managers are in an error state which is preventing consistent survivability state service.

Troubleshooting User failed over to Branch Survivability Server

Procedure

1. Make sure the core Session Manager(s) is up and running.
2. Restore network connectivity between the branch and core.
3. Verify the Session Manager(s) is (are) in the **Accept New Service** state.
4. Check the **SIP Entity Monitoring** page to see if there are any network connectivity problems to the primary and secondary Session Managers.
5. Once the core Session Managers are available to the users to provide service, initiate a failback to move the users active on Session Manager from the Branch Session Manager to the Primary Session Manager. The failback of the users is based on the failback policy of the LSP in the branch. When the LSP fails back, the users will follow. Refer to Communication Manager documentation on ways to administer failback and activate failback on a system.
6. If none of these steps work, contact your Avaya support representative.

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 Security Module 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. Possible causes include:

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

Troubleshooting Zone File I/O Alarms

About this task

To troubleshoot the error, you must be logged on as **root**

Procedure

1. Verify the master directory exists:
 - a. Enter **ls -ltr /var/named/ | grep master**
 - b. If the directory does not exist, enter **mkdir /var/named/master**
2. Check the **/var/named/master** directory for problems (missing, permission errors):
 - a. Enter **ls -ltr /var/named/ | grep master**
The output should be similar to **drwxr-x--x 2 root root 4096 Apr 16 11:52 master**
 - b. If the permissions are not **drwxr-x--x**, enter **chmod 751 /var/named/master**
 - c. If the file ownership is not **root**, enter **chown root /var/named/master**
 - d. If the group is not **root**, enter **chgrp root /var/named/master**
3. Ensure there is enough space on the disk:
 - a. Enter **df**
 - b. If the **Use%** value is greater than 95%, remove any unnecessary large and old log files on the system.
The first place to check would be the log files under **/var/log/Avaya/sml/ServiceHost** and ensure their size is not too large (100's of MB).

4. Ensure the file **/etc/named.nre.zones** exists:
 - a. Enter **ls -l /etc/named.nre.zones**
The output should be similar to **-rw-r--r-- 1 root root 219 Apr 16 11:52 /etc/named.nre.zones**
 - b. If the file does not exist, create it with the command **> /etc/named.nre.zones**
 - c. If the permissions are not **-rw-r--r--**, enter **chmod 644 /etc/named.nre.zones**
 - d. If the file ownership is not **root**, enter **chown root /etc/named.nre.zones**
 - e. If the group is not **root**, enter **chgrp root /etc/named.nre.zones**
 5. If the above steps do not solve the problem, contact Avaya Technical Support.
-

Appendix B: S8510 Server alarms

S8510 Server hardware and environment alarm 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

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

Event ID	Severity	Description/Action
1354	Major	Instrumentation Service EventID: 1354 Power supply detected a failure Power supply detected a failure on page 245
2048	Major	Storage Service EventID: 2048 Device failed Device failed on page 245
2056	Major	Storage Service EventID: 2056 Virtual disk failed Virtual disk failed on page 246
2057	Major	Storage Service EventID: 2057 Virtual disk degraded Virtual disk degraded on page 246
2076	Major	Storage Service EventID: 2076 Virtual disk check consistency failed Virtual disk check consistency failed on page 246
2080	Major	Storage Service EventID: 2080 Array disk initialize failed Physical disk initialize failed on page 247
2083	Major	Storage Service EventID: 2083 Array disk rebuild failed Physical disk rebuild failed on page 247
2102	Major	Service EventID: 2102 Temperature exceeded the maximum failure threshold Temperature exceeded maximum threshold on page 247
2103	Major	Service EventID: 2103 Temperature dropped below the minimum failure threshold

Event ID	Severity	Description/Action
		Temperature dropped below minimum threshold on page 248
2107	Major	Service EventID: 2107 Smart configuration change SMART configuration change on page 248
2163	Major	Service EventID: 2163 Rebuild completed with errors Rebuild completed with errors on page 248
2169	Major	Storage Service EventID 2169: The controller battery needs to be replaced Controller battery needs to be replaced on page 249
2268	Major	Service EventID: 2268 Storage Management has lost communication Storage Management has lost communication on page 249
2270	Major	Service EventID: 2270 Clear operation failed Physical disk Clear operation failed on page 249
2272	Major	Service EventID: 2272 Uncorrectable media error detected Uncorrectable media error detected on page 250
2273	Major	Service EventID: 2273 Physical disk puncture Physical disk puncture on page 250
2282	Major	Service EventID: 2283 Hot spare SMART polling failed Hot spare SMART polling failed on page 250
2289	Major	Service EventID: 2289 Multi-bit ECC error Multi-bit ECC error on page 251
2299	Major	Service EventID: 2299 Bad physical connection Bad physical connection on page 251
2307	Major	Service EventID: 2307 Bad block table is full Bad block table is full on page 252
2320	Major	Service EventID: 2320 Single-bit ECC error Single-bit ECC error
2321	Major	Service EventID: 2321 Single-bit ECC error, no further alerts Single-bit ECC error, no further alerts on page 252
2340	Major	Service EventID: BGI completed with uncorrectable errors BGI completed with uncorrectable errors on page 253
2347	Major	Service EventID: 2347 Rebuild failed on source physical disk Rebuild failed on source physical disk on page 253
2348	Major	Service EventID: 2348 Rebuild failed on target physical disk Rebuild failed on target physical disk on page 254
2349	Major	Service EventID: 2349 Bad disk block could not be reassigned Bad disk block could not be reassigned on page 254

Event ID	Severity	Description/Action
2350	Major	Service EventID: 2350 Unrecoverable disk media error during rebuild Unrecoverable disk media error during rebuild on page 254

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.

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.

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 removed.
- 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.

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.

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.

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.

Check for the following factors which may cause overheating:

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.

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.

1. If the physical disk is a member of a non-redundant virtual disk, back up the data on the disk that received the SMART alert.
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.

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.

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.

The only action that can be taken is to backup the data.

Hot spare SMART polling failed

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.

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.

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.

Replace the disk. There is no other corrective action for this error.

Unrecoverable disk media error during rebuild

The rebuild encountered an unrecoverable disk media error.

Replace the disk. There is no other corrective action for this error.

Appendix C: S8800 Alarm Messages

The following table contains alarm messages for the S8800 server.

Severity	Description
Major	Temperature sensor Ambient Temp Upper Critical going high (Reading 45 > Threshold 41 degrees C)
Major	Voltage sensor Planar 3.3V Upper Critical going high (Reading 3.59 > Threshold 3.56 Volts)
Major	Voltage sensor Planar 3.3V Lower Critical going low (Reading 3.01 < Threshold 3.04 Volts)
Major	Voltage sensor Planar 5V Upper Critical going high (Reading 5.63 > Threshold 5.58 Volts)
Major	Voltage sensor Planar 5V Lower Critical going low (Reading 4.43 < Threshold 4.47 Volts)
Major	Voltage sensor Planar 12V Upper Critical going high (Reading 13.55 > Threshold 13.45 Volts)
Major	Voltage sensor Planar 12V Lower Critical going low (Reading 10.58 < Threshold 10.69 Volts)
Major	Voltage sensor Planar VBAT Lower Critical going low (Reading 2.07 < Threshold 2.10 Volts)
Major	Fan sensor Fan 1A Tach Lower Critical going low (Reading 424 < Threshold 530 RPM)
Major	Power Supply sensor Power Supply 1 - Failure detected Asserted
Major	Power Supply sensor Power Supply 2 - Failure detected Asserted
Major	Power Supply sensor Power Supply 1 - Power Supply AC lost Asserted
Major	Power Supply sensor Power Supply 2 - Power Supply AC lost Asserted
Major	Power Supply sensor Power Unit - Redundancy Lost
Major	Drive Slot sensor Drive 0 - Drive Present Asserted
Major	Drive Slot sensor Drive 1 - Drive Present Asserted
Major	Drive Slot sensor Drive 0 - Drive Fault Asserted
Major	Drive Slot sensor Drive 1 - Drive Fault Asserted
Major	Drive Slot sensor Drive 0 - Predictive Failure Asserted
Major	Drive Slot sensor Drive 1 - Predictive Failure Asserted

S8800 Alarm Messages

Major	Drive Slot sensor Drive 0 - In Critical Array Asserted
Major	Drive Slot sensor Drive 1 - In Critical Array Asserted
Major	Drive Slot sensor Drive 0 - In Failed Array Asserted
Major	Drive Slot sensor Drive 1 - In Failed Array Asserted
Major	Drive Slot sensor Drive 0 - Rebuild Aborted Asserted
Major	Drive Slot sensor Drive 1 - Rebuild Aborted Asserted

Appendix D: S8800 Server 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.

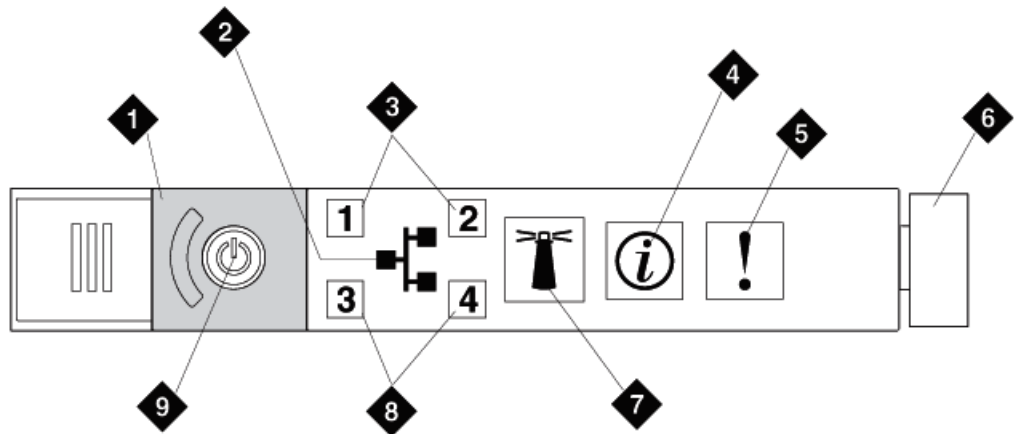
Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped, which means that you can remove or install the component while the server is running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing 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 258
- [Accessing the light path diagnostics panel](#) on page 260
- [System board LEDs](#) on page 270

Operator information panel

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



hw88opinfpnl LAO 092209

1	Power control button cover
---	----------------------------

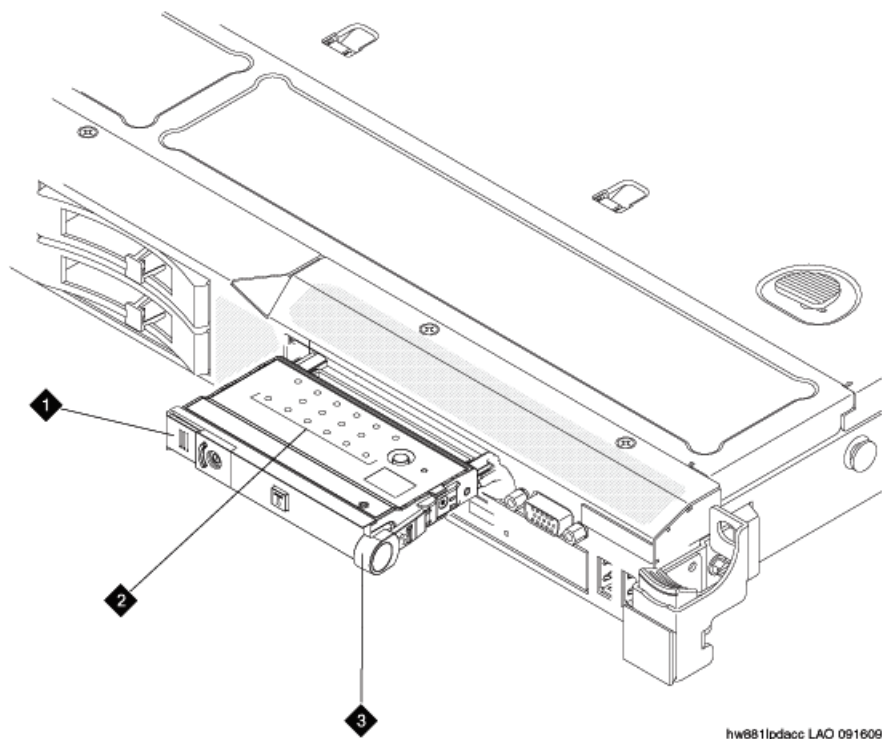
2	Ethernet icon LED
3	Ethernet activity LEDs These LEDs indicate that the server is transmitting or receiving signals on the Ethernet port that corresponds to the lit LED.
4	Information LED This LED indicates that a noncritical event has occurred. An LED on the light path diagnostics panel is also lit 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:

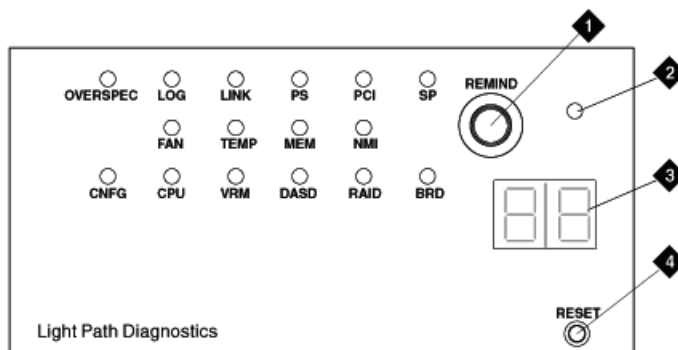
When you slide the light path diagnostics panel out of the server to check the LEDs, do not run the server continuously with light path diagnostics panel outside

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 261

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 161

[Installing a power supply](#) on page 163

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 161

[Installing a power supply](#) on page 163

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](#)

[Installing a PCIe card](#)

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 152

[Removing a memory module](#) on page 154

[Installing a memory module](#) on page 156

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 152

[Removing a memory module](#) on page 154

[Installing a memory module](#) on page 156

[System board LEDs](#) on page 270

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 152

[Removing a memory module](#) on page 154

[Installing a memory module](#) on page 156

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 reseal 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 159

[Installing a hard disk drive](#) on page 160

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.

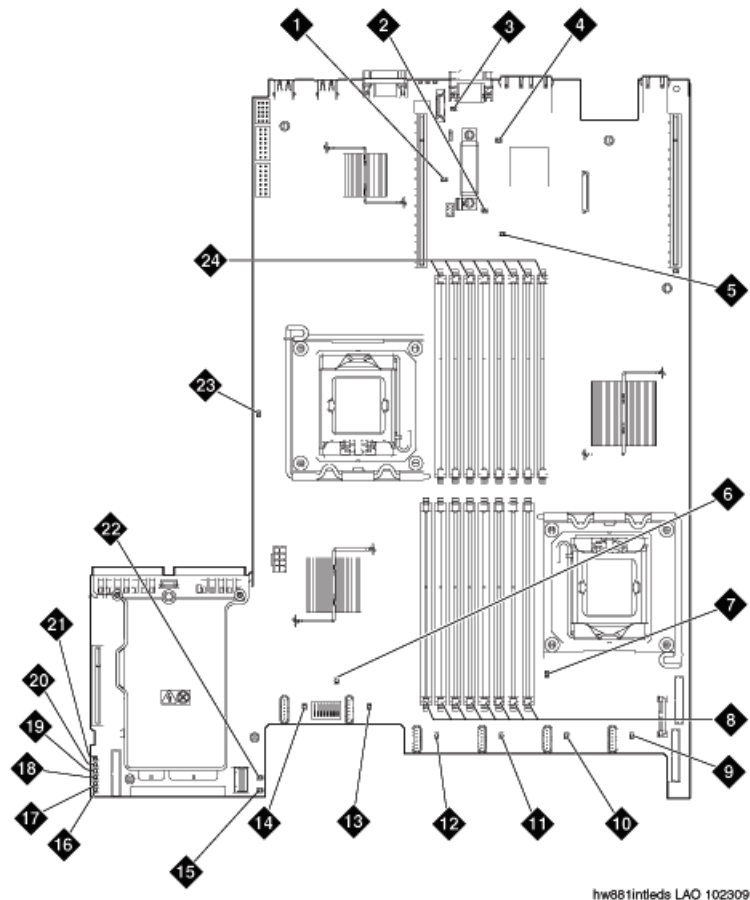
Troubleshooting steps

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.



hw681intleds LAO 102309

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

