Troubleshooting Avaya Aura® Session Manager

Release 7.0.1
Issue 2
May 2016

© 2016, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 websites 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 Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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 You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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 or an Instance of the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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 website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document contains procedures for debugging, monitoring, and troubleshooting Avaya Aura® Session Manager errors and alarms.

The primary audience for this document is support personnel who debug and troubleshoot Session Manager.

Change History

The following changes were made to this document since the last issue:

Issue	Date	Summary of changes
1.0	Aug 2015	Initial release
2.0	May 2016	Added support for the Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers.

Warranty

Avaya provides a 90-day limited warranty on Session Manager. For more information about the terms of the limited warranty, see the sales agreement or other applicable documentation.

You can view the standard warranty information about Session Manager support on the Avaya Support website at https://support.avaya.com. You can find the warranty information and license terms at the bottom of the page under:

- **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**
- **Help & Policies > Policies & Legal > License Terms**

Chapter 2: Troubleshooting fundamentals

Required equipment

For maintenance and troubleshooting activities, you need:

- A laptop
- A DVD burner
- A USB keyboard
- An SVGA monitor
- A network sniffer, such as Wireshark

Supported servers

Session Manager supports the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9

Branch Session Manager supports the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- S8300D
- S8300E

These supported servers are only for Appliance Virtualization Platform configurations.

HP and Dell will discontinue the HP DL360 G7 and Dell R610 servers in the near future. For more information, see the respective vendor websites.

Avaya no longer supports the S8510 and S8800 servers. Any S8510 or S8800 server can be migrated to a supported server using the server replacement procedure.

Supported web browsers

System Manager supports the following web browsers:

- Internet Explorer 9.x
- Internet Explorer 10.x
- Internet Explorer 11.x
- Firefox 36.0
- Firefox 37.0
- Firefox 38.0

Session Manager Dashboard

The Session Manager Dashboard page displays the overall status and health summary of each administered Session Manager instance. The Dashboard also provides the ability to:

- Change the service state of a Session Manager instance.
- Shut down the Session Manager server.
- Reboot the Session Manager server.

Note:

If the **License Mode** of Session Manager or Branch Session Manager displays **Restricted**, you cannot change the service state to **Accept New Service**. The service state cannot be changed until the cause of the license error has been corrected.

Events that cause a license error include:

- No license.
- Expired license.
- Cannot access the WebLM server.
- The number of Session Manager or Branch Session Manager instances administered exceeds the number of servers the license supports.

- The software release installed on the Session Manager or Branch Session Manager instance is not supported by the license version.

Session Manager Dashboard field descriptions

Name	Description
Session Manager	The list of administered Session Manager instances. Clicking the link displays the Session Manager Administration page.
Type	The type of Session Manager instance. The options are: • Core • BSM
Tests Pass	The current results for periodic maintenance tests. • Green indicates the tests passed. • Red indicates at least one test failed. • **Limited Connection** indicates whether Session Manager or Branch Session Manager is in the Maintenance Mode service state. Clicking the link displays the Maintenance Tests page. • **No Connection** indicates failing network connection between System Manager and Session Manager or Branch Session Manager.
Alarms	The number of active Major/Minor/Warning alarms. Clicking the link displays the Alarming page.
Security Module	The state of the Security Module. The state can be: • Up • Down • --- (unknown) Clicking the link displays the detailed summary page of the selected security module.
Service State	The current service state of Session Manager. The options are: • Accept New Service • Deny New Service • Maintenance Mode
Entity Monitoring	The monitoring status of the administered Session Manager instances. The page displays the number of down links and the number of total links. Clicking the link displays the Session Manager Entity Link Connection Status page. **Note:**

Table continues…

Name	Description
	Entity Monitoring does not apply to a Session Manager that is administered as a Branch Session Manager. The monitoring status of a Branch Session Manager is always unknown (---).
Proactive Monitoring Interval (in seconds)	The time interval of monitoring the stationary links.
Reactive Monitoring Interval (in seconds)	The time interval of monitoring the links *after* they stop working.
Number of Tries	The number of tries indicating the failed options requests before marking the link unreachable.
Active Call Count	The current number of active calls for the administered Session Manager instances.
Registrations	The current registration summary and the maximum number of registrations in the last 24 hours. Clicking the link displays the Registration Summary page.
Data Replication	The replication status for the replica node. • Green indicates synchronized. • Red indicates not synchronized. • A warning symbol indicates that the system cannot match the Session Manager management host name with the **Replica Node Host Name** on the Replication page. This error indicates a mismatch between the Session Manager configuration for the **Replica Node Host Name** and the information System Manager receives from a DNS lookup. Clicking the symbol displays the Replica Groups page.
User Data Storage Status	The status of the user data storage. • Green indicates the User Data Storage Sanity Test passed. • Red indicates the test failed. Clicking the symbol displays a detailed status report on the User Data Storage Status page. **Note:** The **User Data Storage Status** displays **– –** for: • Branch Session Manager instances. • A Session Manager instance running a release earlier than 6.3.8.
License Mode	Status of the Session Manager or Branch Session Manager license. The status can be: • **Normal:** The license is valid and no errors are detected. • **Error:** The license is not accessible or does not exist. The system displays the time remaining in the 30–day grace period.

Table continues…

Name	Description
	• **Restricted:** The 30–day grace period has expired. Session Manager or Branch Session Manager, if operational, is now in the **Deny New Service** state. Clicking the link displays the WebLM Home page.
Version	The version of the installed Session Manager software. Clicking a version string link displays the Session Manager Version Inventory page.

Button	Description
Service State > Deny New Service	Blocks incoming calls for the selected Session Manager or Branch Session Manager instances. Leave active calls connected. **Note:** In the Deny New Service mode, the system denies any new call attempts and service requests. SAL agent is restarted and monitoring is re-enabled. The Deny New Service mode can deny selected entity links during a planned WAN outage.
Service State > Accept New Service	Accepts incoming calls for the selected Session Manager instances.
Service State > Maintenance Mode	Places the selected Session Manager instances in the **Maintenance Mode** state. **Note:** In the Maintenance mode, SAL agent stops working and monitoring is disabled. Maintenance mode does not support GUI-based operations and alarms generation. Maintenance mode supports the repair or upgrade of existing Session Manager and Branch Session Manager.
Shutdown System > Shutdown	Shuts down the selected Session Manager server.
Shutdown System > Reboot	Reboots the selected Session Manager server.

Session Manager software version

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

w = Major release number

x = Minor release number

y = Feature pack number

z = Service pack number

= Build number

For example: 7.0.0.0.700019

You can view the software versions of the administered Session Manager servers on the Session Manager Dashboard.

Troubleshooting hints and recommendations

The following are hints and recommendations for troubleshooting Session Manager alarms and problems.

- Automatic alarm clearing is not available for releases earlier than Session Manager 7.0
- Currently, you can only view automatic alarm clear events on the Log Viewer page. You cannot view the automatic alarm clear events on the Alarms page.
- Become familiar with the following topics:
  - Alarming
  - Log files
  - SNMP Support for Session Manager
  - Alarm and Log Event IDs
- Become familiar with the System Manager alarming configuration of managed elements on the Services/Inventory/Manage Serviceability Agents pages:
  - **SNMPv3 User Profile:** Set user profiles for SNMPv3traps/informs.
  - **SNMP Target Profiles:** Create/modify profiles for System Manager, customer NMS, SAL gateway, test trap receivers, and so on.
  - **Serviceability Agents:** Activate the agents of managed elements, manage target profiles for each agent, assign/remove SNMPv3 profiles for sending V3 traps/informs.
- Become familiar with System Manager Alarms and Log Events displays:
  - **Services > Events > Alarms page:** Use filters to search specific information such as alarm state, host, Event ID, and NotificationOID.
  - **Services > Events > Logs > Log Viewer page:** Use filters to search specific information such as host, Severity, Product Type, and Event ID.

Remote access

Secure Access Link (SAL) uses the existing Internet connectivity of the customer for remote support and alarming. All communication from the customer environment is sent by Secure Hypertext Transfer Protocol (HTTPS).

For uploading from a customer to Avaya or an Avaya Business Partner, SAL requires a bandwidth of at least 90 Kbs with round trip latency no greater than 150 ms.

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

To access the Session Manager server, customer must establish a vSphere connection or use the services port.

Server Ethernet ports

Server	Eth0	Eth1	Eth2
HP DL360 G7	Public	Services	Out of band management
HP DL360p G8	Public	Services	Out of band management
HP DL360 G9	Public	Services	Out of band management
Dell R610	Public	Services	Out of band management
Dell R620	Public	Services	Out of band management
Dell R630	Public	Services	Out of band management

Eth0: Session Manager Management (public). Session Manager uses this port for HTTP/SIP (Security Module).

Important:

This is a change from previous releases where Session Manager used eth2 for the Security Module. While upgrading, you must switch the cable between ports.

Eth1: Session Manager services port.

Eth2: Out of band management. Session Manager uses this port for management traffic (SSH, SNMP, System Manager interface, and others.) This is a change from previous releases where Session Manager used eth0 for management traffic.

Important:

Do not mix SIP TLS traffic with the administration traffic on the Eth2 port.

Dell™ PowerEdge™ R610

The Dell™ PowerEdge™ R610 server is a replacement for the S8510 server. Unlike previous original equipment manufactured servers, this server is not re-branded as an Avaya server (S8XXX).

For information about maintaining and troubleshooting the Dell™ PowerEdge™ R610 server, see *Maintaining and Troubleshooting the Dell™ PowerEdge™ R610 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

Dell™ PowerEdge™ R620

The Dell™ PowerEdge™ R620 server is a replacement for the S8510 server. Unlike previous original equipment manufactured servers, this server is not re-branded as an Avaya server (S8XXX).

For information about maintaining and troubleshooting the Dell™ PowerEdge™ R620 server, see *Maintaining and Troubleshooting the Dell™ PowerEdge™ R620 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

Dell™ PowerEdge™ R630 Server

For information about maintaining and troubleshooting the Dell™ PowerEdge™ R630 server, see *Maintaining and Troubleshooting the Dell™ PowerEdge™ R630 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

HP ProLiant 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).

For information about maintaining and troubleshooting the HP ProLiant DL360 G7 server, see *Maintaining and Troubleshooting the HP DL360 G7 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

HP ProLiant DL360p G8 Server

The HP ProLiant DL360p G8 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).

For information about maintaining and troubleshooting the HP ProLiant DL360p G8 server, see *Maintaining and Troubleshooting the HP ProLiant DL360p G8 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

HP ProLiant DL360 G9 Server

For information about maintaining and troubleshooting the HP ProLiant DL360 G9 server, see *Maintaining and Troubleshooting the HP ProLiant DL360 G9 server* on the Avaya Support website at http://support.avaya.com. This guide also provides a list of field replaceable units (FRUs) and component replacement procedures.

Chapter 3: Monitoring operations

Alarming

The System Manager web interface provides the following operations for alarms:

- Viewing alarms

  Note:

  Session Manager clears alarms automatically when the alarm condition has been resolved or not seen for a certain time.

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

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

Session Manager and Branch Session Manager send alarms through SNMP traps directly to the Secure Access Link (SAL) gateway. The SAL gateway then forwards the alarms to the Avaya Data Center (ADC) for processing and resolution. Session Manager can send alarms to up to ten (10) Network Management System (NMS) destinations. One of the destinations must be the SAL gateway.

The condition that one of the destinations must be the SAL gateway does not apply to Session Manager systems supported by others instead of Avaya Services.

Alarm throttling is a mechanism to reduce the frequency of alarm generation for the same events in a specified interval of time. You can configure alarm throttling and reduce the occurrence of alarm flooding events.

For information about the SNMP capabilities of the Session Manager server, see *Avaya Aura™ Session Manager R6.1 – SNMP Agent Whitepaper* on the Avaya support website.

For information regarding SNMP support, see SNMP support for Session Manager on page 74.

Alarm severities

Critical alarms indicate the system or certain components within the system are unusable. These alarms require immediate attention.

Major alarms identify failures that are causing a critical degradation of service. These alarms require immediate attention.

Minor alarms identify failures that are causing service degradation. These failures do not cause the system to be inoperable.

Warning alarms identify failures that cause no significant degradation of service. The system does not report warning alarms to a services organization.

Note:

You can change the colors of the severities.

Alarm status

The status of an alarm can be:

- Raised: An alarm has been generated. Software recovery actions cannot correct the problem.
- Acknowledged: The alarm is being investigated. This state is set manually by the customer or technician.
- Cleared: The problem has been resolved and the alarm has been cleared. This state is set by the customer or technician or by Session Manager.

Viewing alarms

Procedure

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

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

Automatic Alarm Clearing

Session Manager clears alarms automatically when possible.

Session Manager clears an alarm when:

- The alarm condition has been resolved. For example, an alarm is generated when the Security Module periodic test fails. Session Manager automatically clears the alarm when the test passes.
- The alarm condition is not seen for a certain amount of time.

Session Manager does not clear an alarm if:

- Avaya Technical Services must be involved in correcting the issue.
- The alarm is generated for log event. For example, an alarm indicating a failure event.
- Session Manager cannot determine if the alarm condition has been resolved.

When Session Manager does not automatically clear the alarm, the customer or Avaya Technical Services must manually clear the alarm.

The Alarm Event ID table in the Alarm and Log Event IDs chapter indicates how each alarm is cleared, either automatically or manually. The clear event ID column shows the event ID, if the alarm is cleared automatically.

Filtering displayed alarms

You can filter alarms displayed on the alarm screen based on certain criteria. You can use more than one filter criterion on the selected alarms.

Procedure

1. On System Manager Web Console, select **Services** > **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 that contain a particular alarm code.
5. Click **Filter: Apply**.

   Note:

   The system displays a message if no matching records are found for the specified filter criteria.

   The page displays the alarms matching the filter criteria.

Changing the alarm status

The status of an alarm can be:

- **Acknowledged**: Maintenance support must manually set the alarm to this state. Indicates the alarm is under investigation.
- **Cleared**: Maintenance support must manually set the alarm to this state. Indicates the error condition has been resolved. The auto alarm clear event might result in the Cleared status.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm and click **Change Status**.

   You can select multiple alarms.
4. Click the status that you want to apply to the selected alarms.

Exporting alarms

You can export alarms 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following actions:
   - To export an alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export the filtered alarms to a CSV file, click **More Actions** > **Export All**.

     When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
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 that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, click **Advanced Search**.
4. 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**.
5. Select or enter the search value in the third field.

6. To add another search condition, click **+** and perform the following:
   a. Select the AND or OR operator from the drop-down field.
   b. Repeat Step 4 and Step 5.

   To delete a search condition, click **-**. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

Alarming field descriptions

The Alarming home page contains two sections: upper and lower. The upper section contains 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	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name / SysName	The name of the host server that generated the alarm. In case of the trap listener service, this column displays the system name.
Source IP Address	The IP address of the system that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
M/E Ref Number / SysOID	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	The unique identifier for an alarm.
Event ID	The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	The SNMP OID of the alarm.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • **Acknowledged** • **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. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the alarms to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
More Actions > **Delete Selected**	Deletes the alarms that you select from the list.
More Actions > **Delete ALL**	Deletes all alarms that the system displays on the page.
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. 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 system displays the section 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 list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Time Stamp: Searches all 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 the alarms that match the specified severity level. • Status: Searches all the alarms that match the specified status. • Host Name: Searches all alarms that are generated from the specified host. • M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number. • Event ID: Searches all the alarms that match the specified Event ID. • Source IP address: Searches all alarms that are generated from the specified source IP address. • NotificationID: Searches all the alarms that match the specified NotificationID. • Identifier: Searches all the alarms that match the specified identifier. • Description: Searches all the alarms that match the specified description. The operators available are based on the search criterion that you select in the first drop-down field. The operators available for search criteria are as follows: • Time Stamp: =, >, <, >=, <=, >=, != • Severity: Equals, Not Equals • Status: Equals, Not Equals • Host Name: Equals, Not Equals, Starts With, Ends With, and Contains • Identifier: =, >, <, >=, <=, >=, != • Source IP address: Equals, Not Equals, Starts With, Ends With, and Contains

Name	Description
	• Event ID: Equals, Not Equals, Starts With, Ends With, and Contains • Description: Equals, Not Equals, Starts With, Ends With, and Contains • M/E Ref Number: Equals, Not Equals, Starts With, Ends With, and Contains 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.

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

Starting with 7.0 Release, the system automatically clears specific alarms. Some alarms do not have an event code that clears the event.

For more information on alarms that have associated auto clear events, see Alarm Event ID descriptions.

Use the corrective actions associated with an alarm as guidelines for troubleshooting the alarm.

Alarm event codes

For the table on alarm event codes, descriptions, and troubleshooting actions, see Alarm Event ID descriptions.

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. You can view the Session Manager logs by using the System Manager Log Harvester or by looking at the logs on the Session Manager server directly.

Viewing log details

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
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	The option to select a log.
Log ID	The unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	The name of the system from which the log is generated.
Product Type	The code that uniquely identifies the component which generated the log. For example, product, device, application, and service. An example of the log product type is GW600, which is a product type code identifier.
Severity	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.

Table continues…

Name	Description
	• **Warning**: Warning conditions. • **Notice**: Normal but significant condition. • **Informational**: Informational messages. • **Debug**: Debug-level messages. **Note:** The colors of severities do not indicate logging severities
Event ID	The unique identification number assigned to the event that generated the log.
Message	A 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	The process on the device that has generated the message, 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 the 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.
More Actions > **Export Selected**	Exports the selected logs to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the logs to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter logs based on some criteria, **Export All** exports all the filtered data.

Table continues…

Button	Description
Advanced Search	The fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	The 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 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 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 list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message. • Time Stamp: Date and time of the log generation.

Name	Description
	• 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 list 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 list. 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 list, 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 formats: • 24Hr • AM • PM

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

Searching for logs

You can specify conditions for finding logs. The system displays logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
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. 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
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**.

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

   Note:

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

Session Manager Logs

SIP Tracing and Call Processing logs

The **traceSM** command traces SIP messages of the Session Manager and displays the Session Manager routing decisions and internal call processing. The output from **traceSM** displays:

- A ladder diagram of all the SIP messages.
- A summary of each call.
- Call flow representations.

traceSM toggles between enabling and disabling the command.

When enabled, **traceSM** produces the `tracer_asset.log` file for SIP messages and the `call_proc.log` file for call processing messages. To start or stop the capture, enter `s` on the **traceSM** screen . The log files are located in the `/var/log/Avaya/trace` directory.

Warning:

Running **traceSM** can impact Session Manager server performance under call traffic.

SM100 SIP traces

The **traceSM100** command provides tracing of SIP messages directly on the SM100 process. The SIP messages captured on the SM100 display the message flow details in the network and in the SIP container. Enter `s` on the traceSM100 screen to start or stop the capture.

The log files are located in the `/var/log/Avaya/trace` directory.

Session Manager management logs

Session Manager management events are logged in the **server.log** file. The Session Manager management process uses Jboss.

The log files are located in the `/var/log/Avaya/jboss/SessionManager` directory.

DRS replication log

The **symmetric.log** file contains data replication issues between Session Manager and System Manager.

The log files are located in the `/var/log/Avaya/mgmt/drs` directory on Session Manager.

Note:

A similar log file on System Manager exists to view the System Manager perspective of replication.

The **asm.log** file located in the `/var/log/Avaya/sm/` directory contains Session Manager Call Processing logs.

PPM log

You can view the **ppm.log** file to debug issues related to configuration, including missing buttons, dial plan issues, and problems relating to adding, updating, or deleting endpoint contacts.

The log files are located in the `/var/log/Avaya/jboss/SessionManager` directory.

Enter `sm ppmlogon` to enable PPM logging.

Enter `sm ppmlogoff` to disable PPM logging.

You can view PPM logs under `/var/log/Avaya/trace/ppm.log` if it is enabled in **`TraceSM`** command

Registration and Subscriptions event log

The **operationalEvent.log** file contains REGISTER and SUBSCRIBE events for SIP endpoints.

The log files are located in the `/var/log/Avaya/sm` directory.

General System Manager log

System Manager Jboss events are logged in the **server.log** file.

The log files are located in the `/opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/log/` directory on System Manager.

NPR audit logs

The **npraudit.log** file provides an audit trail for activities on the NRP pages under **Elements** > **Routing** on the System Manager console.

The log files are located in the `/var/log/Avaya/mgmt/nrp` directory on System Manager.

Alarm and events logs

The system creates different log files for several events and alarms such as:

- Servlet and Extension event log files. These events are logged in the **event.log** file in the `/var/log/Avaya/sm` directory.
- Logging and alarming process event log files. The **spirit.log** files are located in the `/opt/Avaya/SPIRIT/current/logging` directory.
- Installation or upgrade process log files. These log files are created by installation or upgrade processes and are located in the `/opt/Avaya/install_logs` directory. This install_logs directory is applicable to the System Manager.

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.

To harvest log files, you create a unique Harvest Profile that contains a specific type of harvest criteria. This profile can be used anytime for logs that require the particular set of harvesting requirements. Each time you run the saved profile, 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 System Manager. Archives are rotated based on the number of files and age.

You 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

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

Creating a new log harvesting profile

About this task

To create a new log harvesting profile, you must specify:

- The host name of the server on which the product is running
- The product name
- The directories or the log files
- The filter text if you select one or more directories

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
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 host name of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective list boxes, press `CTRL` and click the directories or files.
   - To clear a selection, press `CTRL` and click the item.
   - To add another log harvesting request for a different product or for another instance of the same product running on the same server or on a different server, click plus (**+**).
6. If you select one or more directories, in the **File Name Filter** field, enter a text pattern as the filter criteria.

   During the harvesting operation, the system harvests only those files that match the filter criteria.
7. To save the profile and the log harvesting requests in the profile, click **Save 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. The files can 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.
Host Name	The host name of the servers on which products are installed.
Product	The products for which you can harvest logs.
Directories / Filter Text	A list of 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. If you select the directory `/a/b/c` and enter `com` in this field, the harvest operation for this profile harvests the log files that are in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Specifies another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **View**.

   The Profile Criteria View page contains the details of the log harvesting profile you selected.

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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
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 **Request**, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting 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 in the specified location.

Viewing details of a log harvesting request

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click **Filter: Enable**.
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`.
   - The zip file name that stores the harvested files.
   - The description of the log harvesting request.
   - The location of the archived file that stores the harvested files.
   - The status of the log harvesting request.
   - The 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.

   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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

   The system lists the log files that are harvested.
7. Select the log file and click **View**.

   The system displays the file content in the Log Browser Panel pane.

Searching for text in a log file

Use this feature to search for matching text in the 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show Files**.
6. On the Search Archives page, in the **Enter search text** field, enter the text for which you want to search.
7. In the Tree view, navigate to the log file by expanding the folders and select the log file.
8. Click **Search**.

   The system displays the search results in the Search Result Panel. The **Search Results Panel** field displays the line numbers as hyperlinks on which the searched text is found.
9. Click the hyperlink in the **Search Results Panel** field.

   The system displays the page that contains 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 web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show files**.

   On the Search Archives page, navigate through the folders in the archive to view the harvested log files.

Downloading the harvested log files

About this task

You can download the harvested log files of one or more products that you stored in a zip file on your local server.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.
7. On the Search Archives page, select a product name, host name 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 that contains the harvested log files for the selected product instances running on the same server or on different servers.
   - If you select a host name of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the server that you selected.
   - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
8. Click **Download**.

The system prompts you to save the file on your local server.

9. Click **Save**.

Harvest Archives field descriptions

Use this page to create an archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip 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 field is optional.

Name	Description
Request Id	The unique identification number assigned to a log harvesting request.
Archive Name	The name of the archive file that you create for storing 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 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. A toggle button.
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	Displays the name of the log harvesting profile.
Profile Description	A brief description of the profile.
Product	Displays the name of the product for which logs are harvested.
Hosts	Displays the hostname of the server on which the product resides.
Files	Displays the names of the log files for which you can harvest log messages.
Directory	Displays 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 that 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 the 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 to 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	Displays the unique identification number assigned to a log harvesting request.
Archive Name	Displays the name of the archive file that stores the harvested log files containing the log messages.
Status	Displays 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.

Child Request Details

Name	Description
Product	Displays the unique identification number assigned to a log harvesting request.
Status	Displays 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	Displays the hostname of the server on which the product resides.
Status Description	A brief description about the execution status of the request.
Status Time Stamp	Displays the date and time when the system generates the status of the log harvesting request.

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

Table continues…

Button	Description
	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.

Security Module Status

The Security Module Status page displays the status and configuration of the security module for each administered Session Manager and Branch Session Manager.

Use the Security Module Status page to perform the following actions:

- **Reset :** Resets the security module for the selected Session Manager or Branch Session Manager. You can reset the security module when a connection cannot be made to the security module.

  Warning:

  Session Manager cannot process calls while the security module is resetting.

- **Synchronize:** Synchronize the administered configuration with the configuration information stored on the security module.
- **Connection Status:** Displays the current status of inbound and outbound links between the Session Manager security module and external hosts. The Connection Status page provides general-purpose monitoring and debugging activities such as:
  - identifying if Session Manager must be taken out of service.
  - determining if links are secure or not.
  - viewing link details and statistics.

Viewing the Security Module page

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 security module configuration information from System Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. If the Security Module state of Session Manager does not display as **Up**:
   a. Click on the status text of the Security Module for Session Manager to display the Security Module Status page.
   b. Verify the IP address for Session Manager is correct.
   c. Select Session Manager.
   d. Click **Synchronize**.
   e. If the status remains **Down**, click **Reset**.

   Warning:

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

Security Module Status page field descriptions

Button	Description
Reset	Resets the selected Session Manager instance.
Synchronize	Synchronizes the security module of the selected Session Manager.
Connections Status	Displays the connection status information for the selected Session Manager instance.

Name	Description
Session Manager	List of administered Session Manager instances. A warning symbol after the name indicates the Session Manager or Branch Session Manager instance is in the **Maintenance Mode** service state.
Type	Type of Session Manager instance (SM or BSM).
Status	Status of the Security Module for Session Manager (up or down).
Connections	Total number of connections for the Security Module.
IP Address	The 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 associated with the Security Module.

Table continues…

Name	Description
Default Gateway	The default Gateway used by the Security Module. This value should match the default gateway administered on the Session Manager instance form.
Entity Links (expected / actual)	The number of expected and actual Entity Links. The expected value is the number of configured SIP Entities in the Routing Policy that have Entity Links to Session Manager. The actual value is the number of Entity Links currently configured on the Security Module. These values should match. If these values do not match, there is a synchronization issue that you must investigate.
Certificate Used	Type of certificate in use.

Connection Status

Use the Connection Status page to view the current status of inbound and outbound links between the Session Manager security module and external hosts. On the Connection Status page, you can perform general-purpose monitoring and debugging activities such as:

- Identifying if Session Manager needs to be taken out of service.
- Determining if links are secured or not.
- Viewing link details and statistics.

Monitoring Connection Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. Click **System Status** > **Security Module Status**.
3. Select a system and click **Connection Status**.
4. Apply the required filters using the Connection Filter section. Select the **Non-Compliant NIST TLS Only** check box to display only the TLS connections that are not compliant with NIST standards.
5. Under Connection List, click **Apply Filter** to display the list of connection links.
6. Select a row and click **Show** to view detailed information about the selected connection.
7. Click **Return** to return to the Security Module Status page.

Connections Status field descriptions

Summary section

The Summary section displays the total number of Active Connections and the number of connections that are incoming, outgoing, TCP, and TLS.

Connection Filter section

Use the Connect Filter section to define a filter and to display the connection list based on the defined filters. A filter can be an FQDN or an IP Address and mask.

If you select **Non-compliant NIST TLS Only**, the page displays only the TLS connections having an algorithm that is not compliant with the NIST SP800-131A recommendation.

Connection List section

The Connection List table displays basic information of all the active connections. The following definitions apply to several of the fields:

- **A:** Acceptable. The algorithm and key length are safe to use. No security risk is currently known.
- **D:** Deprecated. The use of the algorithm and key length is allowed, but the user must accept some risk.
- **X:** Disallowed.
- **N:** Not approved.
- **R:** Restricted. The use of the algorithm or key length is deprecated, and there are additional restrictions required to use the algorithm or key length for applying cryptographic protection to data.
- **U:** Unknown. The system cannot determine the status.

Name	Description
Details	Show or hide the detailed information of the selected connection link.
Dir	Link direction (inbound or outbound).
Local Port	Local Security Module port.
Remote IP	Remote IP address.
Remote Port	Remote port.
Remote FQDN/IP	Remote FQDN or IP address.
Transport	Transport protocol (UDP, TCP, TLS).
Policy	Security Policy (Trusted, Default, Instance)
Cert Sign	Certificate Signature. Digital signature algorithms (for example, RSA or DSA) and the cryptographic hash function (for example, SHA) of the certificate in use by the TLS connection.
Key Exch	Key exchange algorithm (for example, RSA, DSA, Diffie-Hellman,) and key bit length (for example, 1024, 2048) to establish symmetric keys between the endpoints on the TLS connection.
Encryption	Cryptographic operation that provides confidentiality of the data being carried on the TLS connection.

Table continues…

Name	Description
MAC	Message Authentication Code algorithm (for example, SHA) that authenticates the TLS data and provides integrity and authenticity assurance on the message.

Connection Details section

The Connection Details section displays detailed information for the selected connection.

Name	Description
Direction	Link direction.
Creation time	Link creation time.
Last message received	Last message received time.
Last message sent	Last message sent time.
Messages/Bytes Received	Received message count and byte count.
Messages/Bytes Transmitted	Transmitted message count and byte count.
Messages/Bytes Dropped	Dropped message count and byte count.
Subject	The subject field identifies the entity associated with the public key stored in the subject public key field of the X.509 certificate.
Alt Subject	Alt subject is an extension to X.509 that allows various values to be associated with a security certificate.
CA	The issuer who signed the certificate.
Cipher	The negotiated TLS cipher suite. The cipher suite includes the Key Exchange, Encryption and MAC algorithms.
Public Key Algorithm	The encryption algorithm of the public key (e.g. RSA, DSA or Diffie-Hellman).
Key Size (bits)	The Public Key length.
q bits size	For DSA public keys, this represents the q parameter size.
Signature Algorithm	The identifier for the cryptographic algorithm used by the CA to sign this certificate.
MAC Algorithm	The Message Authentication Code (MAC) algorithm to verify data integrity.

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and to 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 routed over that link.

SIP monitoring sends OPTIONS requests to SIP entities to determine whether these are in up, partially up, down or deny new service state. 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 the response of address to OPTIONS is:

- 408 Request Timeout
- 500 Server Internal Error: Destination Unreachable
- 503 Service Unavailable (with no parenthetical text)
- 503 Service Unavailable (no media resources)
- 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.

Note:

Any 503 response is displayed as a 500 response on the SIP Monitoring GUI. SIP container converts 503 to 500 before passing the response to Session Manager.

You can turn the 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 Session Manager instance. If monitoring is turned off, none of the SIP entities are monitored by that Session Manager instance. If monitoring for the Session Manager 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 using the SIP Entity and the Session Manager Administration pages.

Related links

Viewing the SIP Monitoring Status Summary page on page 50
SIP Entity Link Monitoring Status Summary page field descriptions on page 51

Viewing the SIP Monitoring Status Summary page

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

Procedure

On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **SIP Entity Monitoring**.

Related links

Session Manager SIP Entity Monitoring on page 49

SIP Entity Link Monitoring Status Summary page field descriptions

SIP Entities Status for ALL Monitoring Session Manager Instances

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected Session Manager or Branch Session Manager instances.
Refresh	Refreshes the status of the entity links for all administered Session Manager instances.

Field	Description
Session Manager	Name of the Session Manager instance. Clicking any of Session Manager servers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from Session Manager. **Note:** An entity link consists of one or more physical connections between a Session Manager server 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**.
Type	Instances of type Session Manager and Branch Session Manager.
Monitored Entities / Down	Entity links for Session Manager that are down out of the total number of entity links for Session Manager.
Monitored Entities / Partially Up	Entity links for Session Manager that are partially up.
Monitored Entities / Up	Entity links for Session Manager that are up out of the total number of entity links for Session Manager.

Table continues…

Field	Description
Monitored Entities / Not Monitored	SIP entities that are not monitored by Session Manager.
Monitored Entities / Deny	Number of Deny New Service Entity Links.
Monitored Entities / Total	Number of total Entity Links for a SIP Entity.

All Monitored SIP Entities

Button	Description
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.

Related links

Session Manager SIP Entity Monitoring on page 49

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 the messages belonging to a user or Call ID for a call, or for a selected Session Manager instance.

Note:

You must 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 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 that control the basic functionality of the SIP Message tracer. The check boxes allow you to enable or disable the attribute.
- **User Filter**: Filters messages based on the sending user, receiving user, or both.
- **Call Filter**: Filters 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	Enable or disable SIP message tracing. The default is enabled.
Trace All Messages	Enable or disable SIP message tracing for all SIP messages.
From Network to Security Module	Enable or disable SIP message tracing for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	Enable or disable SIP message tracing for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Enable or disable tracing of local SIP messages originating from the Session Manager instance.
From Security Module to Server	Enable or disable tracing of local SIP messages originating from the security module.
Trace Dropped Messages	Enable or disable tracing of messages from calls dropped by the SIP firewall as well as the SM100 proxy.
Max Dropped Message Count	If **Trace Dropped Messages** is enabled, this field displays the value of the maximum number of traced dropped messages.
Send Trace to a Remote Server	Enable or disable SIP Tracing to an external host. When enabled, Session Manager sends all the (decrypted) SIP traffic to an external host. Session

Table continues…

Name	Description
	Manager uses the Syslog protocol for sending 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 to transfer syslogs: • Syslog (unsecured UDP) : Traffic is sent without being encrypted to a remote server as specified in the **Remote Server FQDN or IP Address** field using the default syslog port. • Stunnel (encrypted TCP) : Traffic is sent as encrypted to a remote server that is specified in the to **Remote Server FQDN or IP Address** field using the port specified in **Stunnel Port**.
Stunnel Port	Port number on which the stunnel of the remote server is listening. 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. For example, to create a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Message Count	Value for the maximum number of messages matching the filter that the Session Manager should trace. The 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, to create 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 the Session Manager should trace. The default is 25 messages.
Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.

Session Manager Instances

Name	Description
Name	Select one or more configured Session Manager instances for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Read** button is activated. You can

Name	Description
	click this button to retrieve the current Trace Configuration information for the selected Session Manager. A warning symbol indicates the Session Manager instance is in the **Maintenance Mode** service state.

Button	Description
Commit	Save the configuration changes.
Read	Retrieves the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page.

Configuring SIP tracing

Note:

You must 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.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, select **Session Manager** > **System Tools** > **SIP Tracer Configuration**.
2. Enable or disable the configuration attributes in the **Tracer Configuration** section of the page.
3. Set a user filter or call filter, or delete a filter.
4. Under the Session Manager Network section, select one or more of the administered Session Manager instances.

   Filters are applied to the selected Session Manager instances. Any previous filter configurations will be overwritten.
5. Click **Commit**.

Filtering by user

You can define up to three separate user filters.

The format for a valid sender or receiver is `sip:1234@xyz.com`, where *1234* is the user and *xyz* is the domain.

An empty field matches all messages.

This example is for From/To field.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Tools** > **SIP Tracer Configuration**.

2. In the User Filter section, click **New**.
3. In the **From** field, enter the user from whom the message is sent, if applicable.
4. In the **To** field, enter the user to whom the message is sent, if applicable.
5. In the **Source** field, enter the source expression for the filter, if applicable.
6. In the **Destination** field, enter the destination expression for the filter, if applicable.
7. In the **Max Message Count** field, enter the maximum number of messages that should be traced that match the filter.

   Note:

   You must 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.
8. Select the appropriate filters to be applied.

Filtering by Call ID

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 home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Tools** > **SIP Tracer Configuration**.
2. In the Call Filter section, click **New**.
3. In the **From** field, enter the user from whom the message is sent, if applicable.
4. In the **To** field, enter the user to whom the message is sent, if applicable.
5. In the **Source** field, enter the source expression for the filter, if applicable.
6. In the **Destination** field, enter the destination expression for the filter, if applicable.
7. In the **Max Message Count** field, enter the maximum number of messages that should be traced which match the filter.

   Note:

   You must 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.
8. In the **Request URI** field, enter the Request-URI expression for the filter, if applicable.
9. Select the filters to apply to the trace.

Deleting a filter

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Tools** > **SIP Tracer Configuration**.

2. In the User Filter and/or Call Filter sections, select the filter you wish to delete. You can select more than one filter.
3. Click **Delete**.

SIP Trace Viewer

SIP Trace Viewer displays SIP message trace logs based on configured filters. 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 that 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. To ensure that no relevant trace messages are missing within the Trace Viewer list, change the filter criteria.

Viewing trace logs

You can set filters to display only those logs within a certain time range. Due to the filter options, trace records may be shown multiple times.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Tools** > **SIP Trace Viewer**.
2. To filter trace logs for a range of hours or days, click **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	Details about the trace. Clicking **Show** displays the complete message.
Time	The time when the trace record was written.
Tracing Entity	Name of the Session Manager instance that logged the trace.
From	URI from where the traced SIP message originated.

Table continues…

Name	Description
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 that 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 that appear on the Trace Viewer screen. The file can be displayed with a text editor such as Wordpad or a spreadsheet application 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

You can send SIP trace files to a remote server using remote logging. 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 instance is required for shell access.

Requirements for UDP syslog server

System Requirements for the unsecure UDP syslog server are:

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

Configuring an unsecure UDP syslog server

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. For example, **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 following. The bold fields are the important fields to note: **udp** 0 **0.0.0.0:514 0.0.0.0:*** 21907/**syslogd**

4. Configure the Session Manager:
    a. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Tools** > **SIP Tracer Configuration**.
    b. Verify the **Tracer Enabled** checkbox is selected.
    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 menu.
    e. Select one or more Session Manager instances in the **Session Manager Instances** table.
    f. Click **Commit** to cause all of the selected Session Manager instances to redirect the output to the remote 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
    - sysklogd

Configuring Secure TCP syslog server

For more information about creating a self-signed certificate for the stunnel server, see http://www.stunnel.org/faq/certs.html.

Procedure

1. Configure the firewall to accept connections/logs on UDP port 514. Enter 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.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.
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. For example, **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 following. The bold fields are the important fields to note: **udp** 0 **0.0.0.0:514 0.0.0.0:*** 21907/**syslogd**

5. Enter the command **`mknod /dev/udp c 30 36`** to redirect the UDP output to the Linux server.
6. If a self-signed certificate does not exist, create the certificate with the command **`openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem`**
7. Using your favorite editor, create the stunnel configuration file **/etc/stunnel/stunnelSyslogServer.conf**
8. Open the stunnel configuration file and do the following:
   a. Enter the line **cert = /etc/stunnel/stunnel.pem**
   b. Enter a blank line.
   c. Enter the line **[ssyslog]**
   d. Enter the line **accept = IP_ADDRESS:STUNNEL_PORT**, where **IP_ADDRESS** is the IP address of the server. The IP address must match the value that you will enter in the **Remote Server FQDN or IP Address** field on the **Tracer Configuration** screen. **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. For example, 1.2.3.4:50614

   e. Enter **connect = 127.0.0.1:50614**
   f. Enter **verify = 1**
   g. Write and close the file.
9. Start the stunnel server process by entering the command **`stunnel /etc/stunnel/stunnelSyslogServer.conf`**
10. 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.
11. Start the stunnel forwarding process by entering the command **`nc -k -l 50614 | tr '\n' '\0' | xargs -0 -L 1 echo '<151>' > /dev/upd/127.0.0.1/514`**

12. Configure the Session Manager:
    a. On the home page of the System Manager web console, under **Elements**, click **Session Manager** > **System Tools** > **SIP Tracer Configuration**.
    b. Verify the **Tracer Enabled** check box is selected.
    c. Select the **Send Trace to a Remote Server** check box.
    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 menu.
    f. Specify the remote stunnel port on which the remote stunnel server listens.
    g. Select one or more Session Manager instances in the **Session Manager Instances** table.
    h. Click **Commit** to cause all of the selected Session Manager instances to redirect the output to the remote syslog server.

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.

Viewing Managed Bandwidth Usage

The Managed Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed.

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **Managed Bandwidth Usage**.
2. Click **Show** under the **Details** column to view the bandwidth usage information the Session Manager in that location.
3. Click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

The Manage Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed. If no bandwidth management is implemented, this table has no information.

Field	Description
Details	Displays the breakdown of usage among the administered instances Session Manager in the enterprise. You can click the **Show** or **Hide** arrow on any row under **Details** to display or hide the detailed usage for that location.
Location	Displays the locations that are administered in the Routing Policy.
Audio Call Count	The total number of audio calls of Session Manager in a given location.
Audio BW Used	The bandwidth used for audio calls of Session Manager in a given location.
Multimedia Call Count	The total number of multimedia calls of Session Manager instances in a given location.
Multimedia BW Used	The bandwidth used for multimedia calls of Session Manager instances in a given location.
Multimedia BW Allow	Administered value, if any, of multimedia Bandwidth allowed for a given location.
Multimedia BW %Used	The bandwidth used for multimedia calls into or out of a given location divided by the value in the **Multimedia BW Allow** column.
Total BW Used	The total audio and multimedia bandwidth into or out of a given location
Total BW Allow	Administered value, if any, of the total bandwidth for a given location.
Total BW %Used	The audio and multimedia bandwidth for calls into or out of a given location divided by the value in the **Total BW Allow** column.

Field	Description
Session Manager	Name of the Session Manager instance. A warning symbol indicates the Session Manager instance is in the **Maintenance Mode** service state.
Audio Call Count	Number of audio calls terminated by the selected Session Manager for the given location.

Table continues…

Field	Description
Audio BW Used	Sum of bandwidth used by audio calls terminated by the selected Session Manager for the given location.
Multimedia Call Count	Number of multimedia calls terminated by the selected Session Manager for the given location.
Multimedia BW Used	The bandwidth used by multimedia calls terminated by the selected Session Manager for the given location.

Managed Bandwidth Usage errors

The following errors may appear on the **Managed Bandwidth Usage** page. They are related to a Session Manager instance being unreachable from 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 instance is unreachable from System Manager.
- **Data displayed may be inaccurate due to connection problems to one or more Session Managers.** If one of the Session Managers is not accessible by System Manager, the values may not be accurate.

System Manager may be able to communicate with the Session Manager instance, but the Session Manager instance 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.
- 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 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.

Data Retention

The following types of data accumulate and you need to delete regularly to avoid filling up the disk.

- Log Data
- Alarm Data
- Backup Data

Data retention rules

Log and alarm data 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 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	The option to select a data retention rule.
Rule Name	The name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	The number of days the data is retained.

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

Changing the Retention Interval Value

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

Procedure

1. On the home pages of the System Manager Web Console, under **Services**, click **Configurations** > **Data Retention**.
2. Select the rule you want to change.
3. Click **Edit**.
4. Enter the number of days to retain the data in the **Retention Interval** field.
5. Click **Update**.

User Data Storage and Data Center management

Use the User Data Storage status screen to manage, monitor, backup, and restore User Data Storage on Session Manager instances.

User Data Storage only stores the call logs of a user.

Note:

The User Data Storage backup is *not* related in any way to the System Manager backup.

Related links

Viewing User Data Storage Status on page 67

Viewing User Data Storage Status

Note:

The system displays `No status details while in Maintenance Mode` for those instances that are in the **Maintenance Mode** service state.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Select the Session Manager instance for which you want the system to display the data.

Related links

User Data Storage and Data Center management on page 67

Chapter 4: Troubleshooting features

Session Manager maintenance tests

Use the Maintenance Tests page to perform tests on System Manager server and the administered Session Manager instances. The tests verify functionality such as network connectivity, data replication, and database operation.

The system runs the tests periodically in the background to monitor the status of system components. You can also run the tests on demand.

Note:

Tests can fail if the server under test is out of service or is not responding.

Maintenance Tests page field descriptions

Name	Description
Select System Manager or Session Manager to test:	Select System Manager or a Session Manager from the drop-down menu on which to perform the maintenance tests.

Button	Description
Execute Selected Tests	Run the selected maintenance tests on System Manager or the selected Session Manager.
Execute All Tests	Run all the maintenance tests on System Manager or the selected Session Manager.

Name	Description
Test Description	Description of the test.
Test Result	The outcome of executing the test (pass or fail).
Test Result Time Stamp	The last time the test was run.

Note:

The system loads Maintenance test data asynchronously in the background. The system displays the message **Loading..** when data is loading in the background. The system displays the message **Loading Complete** when data loading finishes. If the wait time exceeds a certain

limit, the system displays the message **Loading failure. Please try again.** and requests the user to try again later.

Running maintenance tests

Run the maintenance tests on System Manager or any administered Session Manager or Branch Session Manager.

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager**, a Session Manager instance, or a Branch Session Manager instance from the drop-down menu.
3. Do one of the following:
   - To run all the tests, select **Execute All Tests**.
   - To run only certain tests, select the tests you want to run and click **Execute Selected Tests**.
4. Verify the tests pass.

Maintenance Test descriptions

Test Call Processing status

This test checks the call processing functionality for a particular Session Manager instance. If call processing is working correctly, the test passes. If the test fails, contact Avaya Technical Support.

Test data distribution and redundancy link

This test only runs on Session Manager. This test verifies the Session Manager data share mechanism is functioning properly by sending a test string to each configured Session Manager. Each Session Manager saves the test string Session Manager within its respective database. After a short wait, the system queries each Session Manager for the test string value.

The test passes if each Session Manager returns the correct value.

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

Test host name resolution of each Session Manager

This test only runs on System Manager. The test verifies that the DNS server can resolve the host name of each configured Session Manager.

If the DNS server can resolve the host name for each Session Manager, the test passes. Otherwise, the test fails. Check for the following possible causes:

- The Session Manager host name is incorrect on the DNS server.
- The Session Manager host name is missing on the DNS server.

Test management link functionality

This test checks the administrative link to the Session Manager. If the test fails, administrative changes cannot take effect on Session Manager.

Test Postgres database sanity

This test runs on either System Manager or a Session Manager.

System Manager tests the functionality of the master database.

The Session Manager tests the functionality of the 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. The test checks if the Security Access Link agent is running on the server. If the link is up and running, the test passes.

If the test fails, see the troubleshooting procedure for this test in *Troubleshooting Avaya Aura® Session Manager*.

Test Security Module Status

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

Test network connections to each Session Manager

The Network Connections test runs only on System Manager. This test verifies the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. If connectivity is down, the test fails. The following are possible causes of test failure:

1. An upgrade or install is in progress.
2. The server might be out of service. Check the log for an event code. If an event code exists, check the Log Event Codes in *Troubleshooting Avaya Aura® Session Manager* for the appropriate troubleshooting action.
3. The network might be out of service. Run a ping test between System Manager and the failing Session Manager to verify network connectivity.

Test User Data Storage sanity

Note:

This test is not available for:

- Branch Session Manager instances
- Session Manager instances that are running a release earlier than 6.3.8.

This test checks the status of the **Cassandra** application and the connectivity to the **Cassandra** database. The test passes if the application and the connectivity are operating correctly. The test fails otherwise.

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**
- **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**

After the test has finished, two headings 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	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:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Calling Party Address	IP address or host name from which the INVITE is received.
Called Party URI	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	Port on which the called Session Manager instance receives the INVITE.
Day of Week	Day of the week. Call times can influence routing policies.
Time (UTC)	Time. Call times can influence routing policies.
Transport Protocol	The transport protocol used by the calling party, which may impact routing options. This field is used for testing the routing based on entity links.
Called Session Manager Instance	The Session Manager instance that receives the initial INVITE from the calling party. **Note:** These are only core Session Manager instances. A Session Manager name in light gray text indicates the Session Manager instance is in the **Maintenance Mode** service state. You cannot run the Call Routing Test on Session Manager instances that are in **Maintenance Mode**.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The **Routing Decisions** field displays the result of the routing test. The result displays one line per destination choice. For a destination that has

Button	Description
	alternate routing choices available, the result displays one line per alternate routing choice, and the lines are displayed in the same order that the test attempted to test 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** field contains information about how the Session Manager made the routing decisions. This tool allows you to test your routing administration.

Setting up a Call Routing Test

Procedure

1. On System Manager Web Console, select **Elements** > **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 Call Route Test failure

About this task

Test failures can be due to the following reasons:

1. Failure to connect to a Session Manager to administer the test. System displays the following message:

   ```
   The following errors have occurred: Failed to retrieve output from
   <Session Manager Name> — cannot connect to server.
   ```

   This error means that the Session Manager could not be accessed from System Manager. Check the Session Manager server and the administration details.

2. Failure to route the test INVITE.

   Verify the administration associated with the Calling Party and Called Party URIs.

SNMP support for Session Manager

This section describes the procedures to create SNMP User and Target profiles and how to attach the profiles to Serviceability Agents.

The Session Manager SNMP master agent is installed as part of a factory installation. This agent provides basic IP discovery, inventory, and status capabilities through the MIB II and Host Resources MIBs for the server and Linux operating system. You configure the Session Manager agent using System Manager to assign an SNMP V3 user. The agent:

- Provides read-only access to the SNMP agent on the Session Manager server.
- Does not provide any SNMP Set capability to the Session Manager.
- Does not restrict the IP addresses to query the MIBs.
- Provides access control only using SNMP V3.

The System Manager server also provides a basic SNMP V3 agent.

For more information on fault management using SNMP, see *Avaya Aura® System Manager Fault Management and monitoring using SNMP* on the Avaya support web site.

Serviceability Agents

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMP and SNMP V3 traps/informs to the configured NMS destinations. Two of the mandatory destinations are System Manager and the SAL Gateway.

Using the Serviceability Agent user interface on System Manager, you can:

- Remotely manage and configure SNMP V3 users.
- Remotely manage and configure SNMP trap destinations.
- Create, edit, view, and delete user and target profiles, and attach or detach the profiles from agents.

The **Manage Serviceability Agents** interface has the following pages:

- **SNMPv3 User Profiles:** Create, view, edit, and delete SNMP V3 user accounts. The system uses these accounts for SNMP V3 traps/informs and for SNMP V3 queries of the SNMP master agent.
- **SNMP Target Profiles:** Create, view, edit, and delete SNMP trap/inform destinations for System Manager, SAL Gateway, and customer NMS. The profile setup interface supports both SNMP V2 and SNMP V3 with either a trap or inform type for notifications.
- **Notification Filter Profile:** Create, view, edit, and delete alarm notification profiles, and attach the profiles to serviceability agents.
- **Serviceability Agents:** Activate Serviceability agents. Send SNMP V3 user profiles and SNMP target profiles to the selected Serviceability Agents. The System Manager host name is automatically included in the list of agents.

Configuring the Session Manager Serviceability Agent

Configure the Session Manager serviceability agent to send alarm traps.

#	Action	Link/Notes	✔
1	View and note the System Manager TrapListener settings.	Viewing the SMGR TrapListener settings on page 88.	
2	Create an SNMP V3 user profile using the same settings as the System Manager TrapListener settings.	Creating an SNMPv3 user profile on page 79.	
3	Create an SNMP user profile and assign the System Manager user profile.	Creating an SNMP target profile on page 82. Use the following values: • **Port** 10162 • **Domain Type** UDP	

Table continues…

#	Action	Link/Notes	✔
		• **Protocol** V3	
4	Verify the Session Manager serviceability agent can register with System Manager.	Verifying the Session Manager serviceability agent registration on page 76.	
5	Assign the System Manager target profile.	Managing target profiles for the selected serviceability agents on page 77.	
6	Attach the user profile to the Session Manager serviceability agent.	Managing SNMPv3 user profiles for the selected serviceability agents on page 76.	
7	Verify the Session Manager serviceability agent can forward alarms to the System Manager.	Generating test alarms on page 77.	

Verifying the Session Manager serviceability agent registration

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Verify the Session Manager **Hostname** and **IP address** appear in the Agents List.
3. Verify the status of the Session Manager serviceability agent is **active**.
4. If the status of the Session Manager serviceability agent is not **active**, select the serviceability agent and click **Activate**.

Activating a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents that you must activate.
4. Click **Activate**.

   The system activates the SNMPv3 functionality in the remote serviceability agent that you selected. If the system does not activate the SNMPv3 functionality, refresh the Web page and repeat Step 3 and Step 4.

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select an active agent that you must manage.

4. Click **Manage Profiles**.
5. Click the **SNMPv3 User Profile** tab.
6. In the **Assignable Profiles** section, select the user profiles that you want to assign.
7. Click **Assign**.

   To remove user profiles, in the **Removable Profiles** section, select the user profiles and click **Remove**.
8. To assign the user profiles to the selected agent, click **Commit**.

   Note:

   You can also select more than one serviceability agents and assign the same user profiles to all agents.

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In Agent List, select the active agents that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMP Target Profiles** tab.
6. Select the target profiles you must assign from the Assignable Profiles section.
7. Click **Assign**.

   You can unassign or remove target profiles from the Removable Profiles section by clicking **Remove**.
8. Click **Commit** to assign the profiles to the selected agent.

   Note:

   You can also select more than one serviceability agents and assign the same target profiles to all the agents.

Generating the test alarm from the web console

About this task

You can generate test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents for which you want to generate alarms.

4. Click **Generate Test Alarm**.

   The system generates the alarm.

5. To view the alarm, click **Events** > **Alarms**.

   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.

Repairing serviceability agents

About this task

If the alarming functionality of an element fails, you can repair the serviceability agent. The repair process triggers the SNMP configuration.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more active agents that you want to repair.
4. Click **Repair Serviceability Agent**.

   The system starts the SNMP configuration of the serviceability agent. At the subsequent heartbeat of the agent, the system notifies System Manager about the start of the SNMP configuration. Therefore, wait for about 15 minutes, the heartbeat interval, to test alarms from the element.

   When System Manager receives the subsequent heartbeat, the system reactivates the agent. The system also assigns the target profiles and user profiles to the agent and the alarming functionality starts working.

5. **(Optional)** To make the changes immediately, log in to the server on which the serviceability agent runs and type `restart sal-agent`.

   You can perform this step if you do not want to wait for the next heartbeat of the agent.

Serviceability Agents list

Name	Description
Hostname	The host name of the server on which the serviceability agent runs.
IP Address	The IP address of the server on which the serviceability agent runs.
System Name	The system name of the server on which the serviceability agent runs.
System OID	The system OID of the server on which the serviceability agent runs.

Table continues…

Name	Description
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **New**.
4. On the New User Profile page, complete the User Details section.
5. Click **Commit**.

Editing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile you want to edit from the profile list.
4. Click **Edit**.
5. Edit the required fields in the Edit User Profile page.

   Note:

   You cannot edit an SNMPv3 user profile that is assigned to the serviceability agent of an element or that is attached to a target profile.

6. Click **Commit**.

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click the user profile you want to view from the profile list.
4. Click **View**.

   You can view the details, except the password, of the SNMPv3 user profile in the View User Profile page.

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile or profiles you want to delete from the profile list.
4. Click **Delete**.
5. On the User Profile Delete Confirmation page, click **Delete**.

Note:

You cannot delete a user profile that is attached to an element or a target profile.

Filtering SNMPv3 user profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the User Profile List.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

SNMPv3 user profiles field descriptions

Name	Description
User Name	The SNMPv3 user name. **Note:** The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be blank.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5 • SHA The default is MD5.
Authentication Password	The password used to authenticate the user.

Table continues…

Name	Description
	Note: The password can contain any printable and non-whitespace characters. The password must be at least 8 characters in length and can contain up to 255 characters. The password cannot be an empty string.
Confirm Authentication Password	The authentication password that you re-enter for confirmation.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • DES: Use DES encryption for SNMP-based communication. • AES: Use AES encryption for SNMP-based communication. • None The default value is AES.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Privileges	The privileges that determines the operations that you can perform on MIBs. • Read/Write: Use to perform GET and SET operations. • Read: Use to perform only GET operation. • None The default is None.

Button	Description
Commit	Use to create a new SNMPv3 user profile. Saves the changes after an edit operation.
Back	Cancels the action and takes you to the previous page.
Delete	Use to delete the user profiles you select.
Edit	Use to edit the user profile you select.

Managing SNMP target profiles

Creating an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. On the SNMP Target Profiles page, click **New**.
4. On the New Target Profiles page, complete the Target Details section.
5. **(Optional)** Click the **Attach/Detach User Profile** tab to attach a user profile.

   Perform the step only if you select the SNMPv3 protocol.
6. Click **Commit**.

Editing an SNMP target profile

About this task

Note:

Modify the target profiles that point to System Manager to reflect the changed IP address in the event of an IP address change on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. In the Target Profile list, click the profile that you must edit.
4. Click **Edit**.
5. On the Edit Target Profiles page, modify the required fields.

   Note:

   You cannot edit a target profile that is assigned to the serviceability agent of an element. You must unassign the target profile before you edit the profile.
6. Click **Commit**.

Viewing an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile you must view.
4. Click **View**.

The system displays the details of the target profile in the View Target Details page.

Deleting an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile or profiles you want to delete.
4. Click **Delete**.
5. On the Delete Confirmation page, click **Delete**.

Note:

You cannot delete a target profile that is attached to an element or an agent.

Filtering target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the Target Profile List.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

SNMP Target profile list

Name	Description
Name	The name of the SNMP target profile. This name should be a unique value.
Domain Type	The type of transport for the flow of messages. The default value is UDP.
IP Address	The IP address of the SNMP target profile.
Port	The port of the SNMP target profile.
SNMP Version	The version of the SNMP protocol.

Button	Description
New	To go to the New Target Details page where you can add a new SNMP target profile.
View	To go to the View Target Details page where you can view an existing SNMP target profile.

Table continues…

Button	Description
Edit	To go to the Edit Target Details page where you can edit an existing SNMP target profile.
Delete	To delete the existing SNMP target profiles that you select.
Filter: Enable	To filter the SNMP target profiles list by one or multiple criteria.

SNMP target profiles field descriptions

Name	Description
Name	The name of the SNMP target profile.
Description	The description of the SNMP target profile.
IP Address	The IP address of the target.
Port	The port number of the target.
Domain Type	The type of the message flow. The default is UDP.
Notification Type	The type of notification. The options are: • Trap • Inform
Protocol	The type of the SNMP protocol.

Button	Description
Commit	Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page.
Back	Cancels your action and takes you to the previous page.

Notification Filter Profile

System Manager supports alarm filtering capability. You can select a product that System Manager supports and send filtered alarms only to specific targets.

When you send notifications to System Manager, a SAL Gateway, or a Network Management System (NMS), you can exclude or include notifications from certain elements. Using the Notification Filter Profile pages, you can:

- create filter profiles and assign the profiles to the target and serviceability agent pair.
- remove the filter profiles from the target and serviceability agent pair.
- select alarms that you want to receive from a product on an NMS.

An NMS can be a System Manager or a third-party system.

For a product, you can define the filter criteria to receive or block notifications on the target serviceability agent from specific Object Identifiers (OID)s.

Creating a Notification Filter Profile

Create a Notification Filter Profile to include or exclude alarms from the notification IDs that you select.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Click **New**.
3. Click the Filter Profile Details tab and enter the required information.
4. Select one of the following:
   - Select **Include** to include the notification OIDs.
   - Select **Exclude** to exclude the notification OIDs.
5. Click the Attach/Detach Notification Oids tab and do one of the following:
   - In the **Notification Subtree** field, enter a value that ends with dot star (.*) and click **Add**. For example: 6889.2.35.*
   - a. Open the Select Notifications section.
     b. In the **Products** field, select a product from the drop-down menu.
     c. In the **NotificationOID** list, select one or more notification IDs.
6. Click **Commit**.

Viewing a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Select a filter profile.
3. Click **View**.

Editing a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Select a filter profile.
3. Click **Edit**.
4. Change the information as needed.
5. Click **Commit**.

Deleting a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Select the filter profile or profiles you wish to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Assigning a Notification Filter Profile to a serviceability agent

You can assign only one filter profile to the target agent for a serviceability agent. For example, for a Session Manager serviceability agent, if the target is System Manager, you can add only one filter profile to the System Manager target for the same Session Manager system.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the serviceability agent server from the **Serviceability Agents** list.
3. Click **Manage Profiles**.
4. Click the SNMP Target Profiles tab.
5. Select System Manager or the third-party NMS target agent, and click **Assign**.
6. To assign the filter profile from the serviceability agent:
   a. In the Removable Profiles section, select the target.
   b. After the **Assign/Remove Filter Profile** link becomes active, click the link.
   c. In the Profile List section, click the plus sign (+).

      The system displays the filter profile that you selected in the Assigned Filter Profiles section.
7. Click **Commit**.

Unassigning a Notification Filter Profile from a serviceability agent

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the serviceability agent server from the **Serviceability Agents** list.
3. Click **Manage Profiles**.
4. Click the SNMP Target Profiles tab.
5. In the Removable Profiles section, select the target.
6. After the **Assign/Remove Filter Profile** link becomes active, click the link.

7. In the Profile List section, click the minus sign (-).

   The system displays the filter profile in the Profile List section.

8. Click **Commit** to disassociate the filter profile from the serviceability agent.

Filter Profiles field descriptions

Name	Description
Name	The name of the notification filter profile.
Description	A description of the notification profile.

Button	Description
New	Displays the New Filter Profile page where you can create a notification filter profile.
View	Displays the View Filter Profile page where you can view a notification filter profile.
Edit	Displays the Edit Filter Profile page where you can view a notification filter profile.
Delete	Marks the notification filter profile that you select. You must confirm for the system to delete the profile.

Create, View, Edit, or Delete Filter Profiles field descriptions

Filter Profile Details

Name	Description
Name	The name of the notification filter profile.
Description	A description of the notification filter profile.
Specify Include/Exclude criteria	An option to include or exclude the notification OIDs. • **Include** • **Exclude** The default is **Include**.

Attach/Detach Notification Oids Specify Notification Subtrees

Name	Description
Notification Subtree	The notification subtree that you want to add to the subtree list. The value you enter must end with dot followed by asterisk (.*), for example, 6889.4.*. Otherwise the system does not add notification subtree to the list.
Add	Adds the notification subtree to the list.

Specify Notifications

Name	Description
Product	The product for which you want to filter the notifications while sending notifications to System Manager, SAL Gateway or other NMS systems.

Button	Description
Commit	Saves the changes made to the page and returns to the Filter Profile page.
Back	Discards the changes and returns to the Filter Profile page.

System Manager TrapListener service

The TrapListener service receives traps and informs from different applications and displays the traps and alarms on the System Manager alarming page.

The TrapListener receives SNMP V2 and SNMP V3 traps and informs the applications that are defined in the common alarm definition file. The TrapListener also processes the Common Alarm Definition file for applications, where all the trap definitions are present.

You configure the TrapListener service using the Service Profile Management pages on System Manager.

Configuring the TrapListener service

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. Click **TrapListener**.
4. On the View Profile: TrapListener Service page, click **Edit**.
5. Edit the required fields in the Edit Profile: TrapListener Service page.
6. Click **Commit**.

Viewing the System Manager TrapListener Service settings

Procedure

1. On the home page of the System Manager web console, under **Services**, click **Configurations** > **Settings** > **SMGR**.
2. Click **TrapListener**.
3. Click **Done** when you are finished viewing the settings.

TrapListener service field descriptions

Name	Description
Authentication Password	The password used to authenticate the user. The default is avaya123.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The options are: • md5 • SHA The default is md5.
Community	The community for TrapListener.
Privacy Password	The password that you use to encrypt the SNMP data. The default is avaya123.
Privacy Protocol	The encryption policy for an SNMP V3 user. The options are: • **DES**: Use the DES encryption for the SNMP-based communication. • **AES**: Use the AES encryption for the SNMP-based communication. The default is AES.
TrapListener Port	The port on which TrapListener listens. The default is 10162. The field is read-only.
V3 UserName	The SNMP V3 user name. The default is initial. Although you can change the SNMP V3 user name, use the default value.

Note:

The system configures the **Privacy Password**, **Authentication Password**, **Users**, and **Community** fields with default values. You must change the values immediately after you deploy System Manager.

Button	Description
Commit	Saves the changes you have made in the **TrapListener Configuration Parameters** section.
Cancel	Cancels the edit and returns to the previous page.

Session Manager SNMP MIB

This section lists 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. The Security Module is not included in this MIB. The Security Module is a different network interface and does not support SNMP queries.

- HOST-RESOURCES-MIB::hrDeviceDescr
- HOST-RESOURCES-MIB::hrDeviceErrors
- HOST-RESOURCES-MIB::hrDeviceID
- HOST-RESOURCES-MIB::hrDeviceIndex
- HOST-RESOURCES-MIB::hrDeviceStatus
- HOST-RESOURCES-MIB::hrDeviceType
- HOST-RESOURCES-MIB::hrDiskStorageAccess
- HOST-RESOURCES-MIB::hrDiskStorageCapacity
- HOST-RESOURCES-MIB::hrDiskStorageMedia
- HOST-RESOURCES-MIB::hrDiskStorageRemoveble
- HOST-RESOURCES-MIB::hrFSAccess
- HOST-RESOURCES-MIB::hrFSBootable
- HOST-RESOURCES-MIB::hrFSIndex
- HOST-RESOURCES-MIB::hrFSLastFullBackupDate
- HOST-RESOURCES-MIB::hrFSLastPartialBackupDate
- HOST-RESOURCES-MIB::hrFSMountPoint
- HOST-RESOURCES-MIB::hrFSRemoteMountPoint
- HOST-RESOURCES-MIB::hrFSStorageIndex
- HOST-RESOURCES-MIB::hrFSType
- HOST-RESOURCES-MIB::hrMemorySize
- HOST-RESOURCES-MIB::hrNetworkIfIndex
- HOST-RESOURCES-MIB::hrPartitionFSIndex
- HOST-RESOURCES-MIB::hrPartitionID
- HOST-RESOURCES-MIB::hrPartitionIndex
- HOST-RESOURCES-MIB::hrPartitionLabel
- HOST-RESOURCES-MIB::hrPartitionSize
- HOST-RESOURCES-MIB::hrProcessorFrwID
- HOST-RESOURCES-MIB::hrProcessorLoad
- HOST-RESOURCES-MIB::hrSWRunPerfCPU
- HOST-RESOURCES-MIB::hrSWRunPerfMem
- HOST-RESOURCES-MIB::hrStorageAllocationUnits

- HOST-RESOURCES-MIB::hrStorageDescr
- HOST-RESOURCES-MIB::hrStorageIndex
- HOST-RESOURCES-MIB::hrStorageSize
- HOST-RESOURCES-MIB::hrStorageType
- HOST-RESOURCES-MIB::hrStorageUsed
- HOST-RESOURCES-MIB::hrSystemDate
- HOST-RESOURCES-MIB::hrSystemInitialLoadDevice
- HOST-RESOURCES-MIB::hrSystemInitialLoadParameters
- HOST-RESOURCES-MIB::hrSystemMaxProcesses
- HOST-RESOURCES-MIB::hrSystemNumUsers
- HOST-RESOURCES-MIB::hrSystemProcesses
- HOST-RESOURCES-MIB::hrSystemUptime
- IF-MIB::ifAdminStatus
- IF-MIB::ifDescr
- IF-MIB::ifInDiscards
- IF-MIB::ifInErrors
- IF-MIB::ifInNUcastPkts
- IF-MIB::ifInOctets
- IF-MIB::ifInUcastPkts
- IF-MIB::ifInUnknownProtos
- IF-MIB::ifIndex
- IF-MIB::ifLastChange
- IF-MIB::ifMtu
- IF-MIB::ifNumber
- IF-MIB::ifOperStatus
- IF-MIB::ifOutDiscards
- IF-MIB::ifOutErrors
- IF-MIB::ifOutNUcastPkts
- IF-MIB::ifOutOctets
- IF-MIB::ifOutQLen
- IF-MIB::ifOutUcastPkts
- IF-MIB::ifPhysAddress
- IF-MIB::ifSpecific

- IF-MIB::ifSpeed
- IF-MIB::ifType
- SNMPv2-MIB::snmpEnableAuthenTraps
- SNMPv2-MIB::snmpInASNParseErrs
- SNMPv2-MIB::snmpInBadCommunityNames
- SNMPv2-MIB::snmpInBadCommunityUses
- SNMPv2-MIB::snmpInBadValues
- SNMPv2-MIB::snmpInBadVersions
- SNMPv2-MIB::snmpInGenErrs
- SNMPv2-MIB::snmpInGetNexts
- SNMPv2-MIB::snmpInGetRequests
- SNMPv2-MIB::snmpInGetResponses
- SNMPv2-MIB::snmpInNoSuchNames
- SNMPv2-MIB::snmpInPkts
- SNMPv2-MIB::snmpInReadOnlys
- SNMPv2-MIB::snmpInSetRequests
- SNMPv2-MIB::snmpInTooBigs
- SNMPv2-MIB::snmpInTotalReqVars
- SNMPv2-MIB::snmpInTotalSetVars
- SNMPv2-MIB::snmpInTraps
- SNMPv2-MIB::snmpOutBadValues
- SNMPv2-MIB::snmpOutGenErrs
- SNMPv2-MIB::snmpOutGetNexts
- SNMPv2-MIB::snmpOutGetRequests
- SNMPv2-MIB::snmpOutGetResponses
- SNMPv2-MIB::snmpOutNoSuchNames
- SNMPv2-MIB::snmpOutPkts
- SNMPv2-MIB::snmpOutSetRequests
- SNMPv2-MIB::snmpOutTooBigs
- SNMPv2-MIB::snmpOutTraps
- SNMPv2-MIB::snmpProxyDrops
- SNMPv2-MIB::snmpSilentDrops
- SNMPv2-MIB::sysContact

- SNMPv2-MIB::sysDescr
- SNMPv2-MIB::sysLocation
- SNMPv2-MIB::sysName
- SNMPv2-MIB::sysORDescr
- SNMPv2-MIB::sysORID
- SNMPv2-MIB::sysORLastChange
- SNMPv2-MIB::sysORUpTime
- SNMPv2-MIB::sysObjectID
- TCP-MIB::tcpActiveOpens
- TCP-MIB::tcpAttemptFails
- TCP-MIB::tcpCurrEstab
- TCP-MIB::tcpEstabResets
- TCP-MIB::tcpInErrs
- TCP-MIB::tcpInSegs
- TCP-MIB::tcpMaxConn
- TCP-MIB::tcpOutRsts
- TCP-MIB::tcpOutSegs
- TCP-MIB::tcpPassiveOpens
- TCP-MIB::tcpRetransSegs
- TCP-MIB::tcpRtoAlgorithm
- TCP-MIB::tcpRtoMax
- TCP-MIB::tcpRtoMin
- UDP-MIB::udpInDatagrams
- UDP-MIB::udpInErrors
- UDP-MIB::udpNoPorts
- UDP-MIB::udpOutDatagrams

Shut down or 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, onsite personnel must restart the system.

You can shut down or reboot the system in two ways:

- Using the System Manager console
- Using the command line interface of the Session Manager

Note:

Place Session Manager in the Deny New Service state and wait for all active calls to end before shutting down or rebooting the server. Active calls through the affected Session Manager will drop if the Session Manager remains inoperational for a long time. 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 System Manager to shut down or reboot the server

Procedure

1. On System Manager Web Console, select **Elements** > **Session Manager**.
2. Select the Session Manager server that you want to shut down or reboot.

   Note:

   You can shut down or reboot only one Session Manager at a time.
3. Click **Service State**.
4. Select **Deny New Service**.
5. Wait for all active calls on Session Manager to end before shutting down or rebooting the server.
6. Click **Shutdown System**.
7. Select **Shutdown** or **Reboot** from the drop-down menu.

   The system displays a confirmation screen. If Session Manager is not in the **Deny New Service** state, the system displays an additional screen with the recommended action.

Using the CLI to shut down or reboot the server

If you experience problems accessing System Manager, use the CLI to shut down or reboot that particular Session Manager using the following procedure:

Procedure

1. Log in to the Session Manager using the customer login.
2. Enter one of the following commands:
   - **`shutdownSM`** (to shut down the server)

- **rebootSM** (to reboot the server)

3. If Session Manager is shut down, the confirmation screen warns that onsite personnel must restart the system.

Chapter 5: Resolving common problems

Testing the System Manager and Session Manager installation

This procedure verifies:

- System Manager and Session Manager are installed and configured properly.
- The servers and applications are communicating.

Procedure

1. On the System Manager Web Console home page, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
2. Select **System Manager** from the **Select Target** drop-down menu.
3. Click **Execute All Tests**.
4. Verify all tests display **Success**.
5. On the System Manager Web Console home page, under **Elements**, select **Session Manager** > **System Status** > **Security Module Status**.
6. Verify the status is **Up** for the deployed Session Manager.
7. Verify the IP address is correct.
8. If the status is **Down**, reset the security module:
   a. Select the appropriate Session Manager from the table.
   b. Click **Reset**.

   Warning:

   The Session Manager cannot process calls while the security module is being restarted.
9. On the System Manager Web Console home page, under **Elements**, select **Session Manager**.
10. On the **Session Manager Dashboard** page, verify the installed software versions of all Session Managers are the same.
11. On the System Manager Web Console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.

12. Select the appropriate Session Manager instance from the drop-down menu.
13. Click **Execute All Tests**.
14. Verify all tests ran successfully.
15. Check the replication status of the Session Managers:
    a. On the System Manager Web Console, under **Services**, click **Replication**.

       The **Synchronization Status** should be green and the status should be **Synchronized**.

    b. If the status is not **Synchronized**, select the check box next to **SessionManagers** (type Replica Node) and click **View Replica Nodes** to determine which Session Manager is not synchronized with System Manager.
16. Verify there are no active alarms for the Session Manager. On the System Manager Web Console home page, under **Services**, click **Events** > **Alarms**.
17. If the System Manager and customer NMS are configured to forward alarms, generate a test alarm to verify forwarding of alarms. See Generating a test alarm on page 97.
18. For Geographic Redundant systems:
    a. On the System Manager Web Console home page, under **Services**, select **Inventory** > **Managed Elements**.
    b. Verify the managed elements in the **Managed by** column display the correct value of the managing System Manager.

Generating a test alarm

Generate a test alarm to the targets assigned to the serviceability agent. These targets can include:

- A SAL Gateway

  The alarm is forwarded to ADC
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

Procedure

1. If using the Session Manager CLI:
   a. Login to the Session Manager server.
   b. Run the Session Manager CLI command **generateTestAlarmSM.sh**.

      In Session Manager 7.0, you can run **generateTestAlarmSM.sh** to automatically clear the test alarm.

2. If using the **Generate Test Alarm** button on the **Serviceability Agents** screen:
   a. On the System Manager web console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
   b. Select a hostname from the list, and click **Generate Test Alarm**.
3. To verify that the System Manager received the test alarm message, do one of the following:
   a. On the System Manager web console, in **Services**, click **Events** > **Alarms**.
   b. Check that the system displays the message **Test alarm for testing only, no recovery action necessary** in the **Description** column.
4. If the serviceability agent is configured with other targets, verify that the other targets also received the test alarm and also verify the clearing of the alarm.

Note:

The test alarms are not generated when Session Manager is in Maintenance Mode.

Data Replication Service

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

DRS supports the following modes of replication:

- Replication in Repair mode: DRS replicates the requested data from the master database to the database of the replica node. Repair is only necessary if an installation of DRS fails.
- 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.

DRS sends the data in batches from the master database to the replica node. DRS creates replication batches when 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 web console, click **Services** > **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 web console, click **Services** > **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 web console, click **Services** > **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.

Related links

Replica Nodes field descriptions on page 102

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 web console, click **Services** > **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 web console, click **Services** > **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 that use 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 web console, click **Services** > **Replication**.
2. On the **Replica Groups** page, select the 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 that use 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 web console, click **Services** > **Replication**.
2. On the **Replica Groups** page, select the replica group 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**.

Troubleshooting Replica Nodes

About this task

Perform the following troubleshooting steps if the replica group state is not **Synchronized**, **Queued for Repair**, or **Repairing**, or if the replica group is stuck in the **Starting** state.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, select **Replication**.
2. Select the appropriate **Replica Group** for the Session Manager server.
3. Click **View Replica Nodes**.
4. Verify that the Enrollment password has not expired.
5. Enter **`initTM`**. The command should complete within 5 minutes. If it does not complete within that time, continue with the next step.
6. Verify that the system date and time on the Session Manager server is in sync with the system date and time on the System Manager virtual machine. Trust certificate initialization can fail if the clocks differ by more than a few seconds.
7. Enter **`SMnetSetup`**.
    a. Verify that all information is correct.
    b. Verify the Enrollment password is correct on the System Manager Security screen.
    c. Re-enter the Enrollment password.

8. On System Manager, verify the Session Manager is now synchronized.

Replica Groups field descriptions

The replica groups are logical groupings of the replica nodes. You can use the replica groups field descriptions page to:

- View all the replica groups in the enterprise.
- View the replication status of the replica groups.

The page displays the following fields when you select `All` from the **Replica Group** field.

Name	Description
Select check box	An option to select a replica group.
Replica Group	The name of the replica group. Each replica group in the list is a hyperlink. When you click a group, the system displays the replica nodes for that group on the Replica Nodes page.
Synchronization Status	For each replica group, displays the combined synchronization status of all replica nodes under the group
Group Description	A brief description of the replica group.

Button	Description
View Replica Nodes	Displays the Replica Nodes page. Use this page to view replica nodes for a group that you select.
Repair	Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.
Filter: Enable	Displays fields under **Replica Group** and **Synchronization Status** columns where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters replica nodes based on the filter criteria.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group when you request data replication from the master database of System Manager.
- View the replication status of the replica nodes in a group.

Name	Description
Select check box	Provides the option to select a replica node.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Product	Displays the name of the product.
Synchronization Status	Displays the synchronization status of the replica node. When you install a node, the node goes from a **Ready for Repair** state to the **Queued for Repair** to **Repairing**, and finally to the **Synchronized** state. During this phase, the replica node receives a full-sync, wherein configured data is replicated to the replica node. Once the replica node is prepared with a full-sync, thereafter the node receives the subsequent changes in the form of regular-sync. A replica node can be in any one of the following states during the lifecycle: • **Ready for Repair**. The database of the replica node is not synchronized with the master database. • **Queued for Repair**. The replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow. • **Repairing**. The data replication process is in progress. The color code of the status is yellow. • **Synchronized**. The system has successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. **Note:** If you encounter the following, contact the administrator who can manually intervene to resolve the problem: • `Not Reachable`. System Manager is unable to connect to the replica node. This indicates that the replica node is switched off for maintenance, a network connectivity failure, or any other issue that affects general

Table continues…

Name	Description
	connectivity between System Manager and the replica node. • `Synchronization Failure`. Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure. During the automatic replication of data from the master to the replica node, the system displays the following status: • **Synchronizing**. The data replication is in progress for the replica node. The color code of the status is yellow. • **Synchronized**. The system successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. • **Pending Audit**. The replica node is marked for audit. In this state, DRS dishonors any request from the node until audit is successfully conducted for the node. On completion of audit activity, the node displays any of the other states as applicable. The color code of the status is yellow.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
GR Enabled	Displays whether the replica node is GR-enabled or not.
Last Replication Request Time	Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later.

Button	Description
View Details	Opens the Data Replication page. Use this page to view the synchronization details for a replica node.
Repair	Replicates or resynchronizes data from the master node to a selected replica node.
Remove	Removes the nodes you select from the replica group.
Remove From Queue	Removes the replica node you select from the queue.
Show All Replica Groups	Takes you back to the Replica Groups page.

Replication Node Details field descriptions

You can use this page to view the following details:

- The batch-related information such as total number of batches received, processed, and skipped for a replica node.
- The last time when the replication server performed the synchronization or replication.
- Synchronization or replication error details.

General

Name	Description
Replica Node Group	Displays the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Last Down Time	Displays the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.
Last Repair Start Time	Displays the last time and date when a full-sync was started for the node.
Last Repair End Time	Displays the last time and date when a full-sync was completed for the node.
Last Pull Time	Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later.
Build Version	Displays the version of the element configuration.
GR Enabled	Displays whether the replica node is GR-enabled or not.

Synchronization Statistics

Name	Description
Pending Batches	Lists the batches that are yet to be replicated to the replica node. During the data replication process, System Manager records the changes for a particular replica

Table continues…

Name	Description
	node in the form of events. When a replica node requests System Manager for change events, the change events are made into batches. These batches are then replicated to the replica node.
Pending Unbatched Events	Lists the change events that are yet to be formed into batches. The recorded change events are formed into batches and only a predefined number of batches are replicated to a replica node in a request. The remaining events wait for the subsequent request from the replica and are called unbatched events pending batching and subsequent replication.
Synchronization Status	Displays the synchronization status of the replica node. For details, see Replica Nodes field descriptions.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
Last Batch Acknowledged	Displays the last batch that an element acknowledged as successfully processed on the element side. During an audit, Data Replication Service (DRS) compares the last successfully committed batch on the node with the data in the last batch acknowledged batch. If the node has a more recent batch, then DRS schedules a full-sync for the node.
Marked For Audit	Marks all replica nodes that are GR-enabled for audit: The status can be: • : Indicates that the node is marked for audit. • : Indicates that the node is not marked for audit. When the node is marked for audit, the replica status changes to **Pending Audit**, and the color changes to yellow. • When you activate the secondary System Manager or when you enable GR after the primary System Manager restores • When the primary System Manager restores and you choose the database of the primary System Manager

Table continues…

Name	Description
	• When the primary System Manager restores and you choose the database of the secondary System Manager DRS denies any request from the replica node that is marked for audit until the audit is complete for the replica node.
Last Audit Time	Displays the last time and date when DRS performed the audit of data from the node that is marked for audit.

Last Error Details

Name	Description
Cause of Error	Describes why the system failed to replicate or synchronize data.
Time of Error	Displays the time when the error occurred.

Chapter 6: Alarm and Log Event IDs

Alarm Event ID descriptions

The following table contains the alarm event ID, the severity of the alarm, the reason for the alarm and a link to the troubleshooting procedure, the method for clearing the alarm, and the clear alarm event ID if one exists.

Table 1: Alarm Event ID Table

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
ARBITER_10002	Major	Session Manager does not associate with a master System Manager. See No master System Manager on page 135.	Automatic ARBITER_10003
DRS_DBG_0001	Major	Data Services Replication error. See DRS Synchronization failure on page 127.	Manual
OP_AASL10900	Major	Certificate load failure. See Certificate Status on page 123.	Automatic OP_AASL10901
OP_AASL10902	Major	Failed binding a listener, the given address is in use or an invalid interface. See Failed binding a listener on page 129.	Manual
OP_AASL10903	Warning	Connection Limit has been exceeded for remote IP using transport. See Connection limit exceeded on page 123.	Manual
OP_AFWL16002	Minor	SIP firewall configuration update failed. See SIP Firewall Configuration on page 143.	Automatic OP_AFWL15001
OP_AFWL16003	Minor	SIP firewall configuration failed schema validation. See SIP Firewall Configuration on page 143.	Manual
OP_AFWL16501	Warning	SIP firewall action matched rule. See SIP Firewall Actions on page 143.	Manual
OP_AFWL16504	Minor	SIP firewall loop detection. See SIP Call Loop Elimination on page 142.	Manual

Table continues…

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
OP_AFWL17503	Minor	SIP firewall blacklist configuration update failed. See SIP Firewall Configuration on page 143.	Automatic OP_AFWL15001
OP_AFWL17504	Minor	SIP firewall whitelist configuration update failed. See SIP Firewall Configuration on page 143.	Automatic OP_AFWL15001
OP_ANFW11001	Warning	Network firewall cannot be stopped. See Network firewall stopped on page 134.	Automatic OP_ANFW11000
OP_ANFW11002	Warning	SM100 Network Firewall critical event. See Network firewall critical event on page 134.	Manual
OP_APLM10300	Major	Failure pinholing Network Firewall. See Network Firewall Pinholing on page 134.	Manual
OP_APLM10302	Major	Failure configuring network parameters. See Network Configuration on page 133.	Manual
OP_APLM10304	Major	Ethernet interface is down. See Network Configuration on page 133.	Automatic OP_APLM10305
OP_CCAC54003	Warning	Bandwidth threshold exceeded. See Exceeding Location Bandwidth on page 128.	Automatic OP_CCAC54004
OP_CDAO50001	Minor	The database connection is down. See Database Connection on page 125.	Automatic OP_CDAO50005
OP_CDAO50002	Minor	Database query failure (SQL Exception). See Database Query on page 126.	Automatic OP_CDAO50008
OP_CDAO50003	Minor	Unexpected data. See Unexpected data on page 145.	Automatic OP_CDAO50007
OP_CDAO50009	Minor	A file I/O error occurred trying to write the local DNS server configuration or zone files. See Zone File I/O on page 147.	Automatic OP_CDAO50010
OP_CDAO50011	Major	The Session Manager Instance cannot be resolved. See Session Manager Instance Resolution on page 141.	Automatic OP_CDAO50016
OP_CDAO50012	Minor	Multiple Session Manager IP addresses map to the local Session Manager Instance. See Session Manager Instance Resolution on page 141.	Automatic OP_CDAO50015

Table continues…

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
OP_CDAO50013	Minor	SM100 Multiple IP addresses resolved by DNS. See Security Module multiple DNS resolutions on page 139.	Automatic OP_CDAO50017
OP_CDAO50018	Major	JGroups Keystore has not been replicated. This Session Manager will not be able to share bandwidth, user registration or subscription information.	Automatic OP_CDAO50019
OP_CDAO50020	Minor	Call accounting is not available. See CDR Not Operational on page 122. If the problem persists, contact Avaya Technical Support.	Automatic OP_CDAO50021
OP_CDAO50022	Warning	The direct link for Session Manager to Route Through is missing. See Route Through on page 138.	Automatic OP_CDAO50023
OP_CDAO50024	Major	BSM Entity Links to core subtended CM not administered. See BSM Entity links not administered on page 121.	Automatic OP_CDAO50025
OP_CDAO50026	Major	BSM avaya-lsp entry missing in /etc/hosts.	Automatic OP_CDAO50027
OP_CDAO50031	Minor	No entity link administered between Session Manager and the far end entity with the appropriate transport type. See No entity link with correct transport type on page 134.	Automatic OP_CDAO50032
OP_CMON55001	Warning	SIP Entity is not responding since one or more (but not all) of the connections associated with the SIP Entity are in a down state (equivalent to the SIP Monitoring state as **Partially Up**). See SIP Monitor Alarm on page 144.	Automatic OP_CMON55000
OP_CMON55002	Minor	SIP Entity is not responding since all of the connections associated with the SIP Entity are in a down state (equivalent to the SIP Monitoring state as **Down**). See SIP Monitor Alarm on page 144.	Automatic OP_CMON55000
OP_CSRE52005	Minor	Missing ELIN link. See ELIN entity link missing on page 130.	Automatic OP_CSRE52006
OP_CSVH58003 OP_CSVH58005	Minor	install.properties file errors. Contact Avaya Technical Services.	Manual
OP_CSVH58007 OP_CSVH58009	Major	install.properties file errors. Contact Avaya Technical Services.	Manual

Table continues…

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
OP_CURE56001	Warning	Authentication failure in registration attempt.	Automatic OP_CURE56000
OP_CURE56010	Warning	Data base error. See Registration service unavailable for a given user on page 137.	Automatic OP_CURE56009
OP_CURE56018	Warning	Authentication failure in subscription attempt	Automatic OP_CURE56017
OP_CURE56021	Warning	Data Manager component failure. See Registration component failure storing subscriptions on page 137.	Automatic OP_CURE56020
OP_CURE56027	Minor	User failed over, manual failback mode. See User failed over, manual failback mode on page 145.	Automatic OP_CURE56028
OP_CURE56029	Minor	User failed over to Branch Survivable Server. See User failed over to Branch Survivability Server on page 146.	Automatic OP_CURE56030
OP_LIC20251	Warning	SIP session counts exceeded the licensed number. Verify number of sessions authorized in license file.	Automatic OP_LIC20252
OP_LIC20253	Major	Session Manager instance license in error. 30–day grace period is in effect.	Automatic OP_LIC20254
OP_LIC20255	Critical	Session Manager instance license restricted. Session Manager is in **Deny New Service** state.	Automatic OP_LIC20256
OP_MAMA20102	Major	Security Module Management Agent failure. See Security Module Management Agent unable to configure Security Module on page 138.	Automatic OP_MAMA20103
OP_MMTC20011	Major	The Postgres database is not accessible. See Postgres database sanity check failed on page 135.	Automatic OP_MMTC20012
OP_MMTC20019	Minor	Alarms are not being processed. See SAL Agent sanity check failed on page 138.	Automatic OP_MMTC20020
OP_MMTC20025	Major	Security Module failed sanity check. See Security Module Sanity Failure on page 140.	Automatic OP_MMTC20026
OP_MMTC20029	Major	Call Processing SAR is not deployed.	Automatic OP_MMTC20030
OP_MMTC20031	Minor	Data Distribution/Redundancy is down. See Data Distribution/Redundancy is down on page 124.	Automatic

Table continues…

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
			OP_MMTC20032
OP_MMTC20033	Minor	Management Instance check failed. See Management Instance check failed on page 131.	Automatic OP_MMTC20034
OP_MMTC20043	Minor	Management BSM instance check failed. See Management BSM instance check failed on page 131.	Automatic OP_MMTC20044
OP_MMTC20045	Minor	ELIN entity link is missing. See ELIN entity link missing on page 130.	Automatic OP_MMTC20046
OP_MMTC20047	Warning	Failure to install the unique authentication file during Session Manager installation. See Failure to install the unique authentication file on page 129	Automatic OP_MMTC20057
OP_MMTC20048	Warning	Certificates nearing expiration date. See Certificate Expiration on page 123.	Automatic OP_MMTC20058
OP_MMTC20049	Major	Certificates nearing expiration date. See Certificate Expiration on page 123.	Automatic OP_MMTC20058
OP_MMTC20050	Critical	Certificates nearing expiration date. See Certificate Expiration on page 123.	Automatic OP_MMTC20058
OP_MMTC20051	Major	User Store connection test failed.	Automatic OP_MMTC20052
OP_MMTC20053	Warning	Cassandra error while running compaction on SSTable files.	Automatic OP_MMTC20054
OP_MMTC20055	Minor	Cassandra backup failed.	Automatic OP_MMTC20056
OP_MMTC20059	Warning	Cassandra error while repairing data.	Automatic OP_MMTC20060
OP_MPER20226	Warning	Performance Monitoring disk space is at least 80% full. See Performance data storage disk usage on page 135.	Automatic OP_MPER20230
OP_MPER20227	Major	Performance Monitoring disk space is at least 95% full and data collection has been disabled. See Performance data storage disk usage on page 135.	Automatic OP_MPER20231
OP_MPER20228	Minor	NFS server used for performance data storage is not accessible. See Alarms for NFS Disk Space on page 120.	Automatic OP_MPER20232

Table continues…

Event ID	Severity	Alarm description/Link	How Cleared Clear Event ID
OP_MPER20229	Major	NFS server used for performance data storage is not accessible. See Alarms for NFS Disk Space on page 120.	Automatic OP_MPER20233
OP_MWD20202	Minor	Session Manager watchdog service unable to start the requested service. See Service <name of service> has totally failed on page 140.	Automatic OP_MWD20200
OP_MWD20204	Major	WebSphere does not respond to SIP requests. The Session Manager monitoring of WebSphere has failed indicating that WebSphere is no longer functioning. At this point, watchdog restarts WebSphere in an attempt to clear the condition. If the problem persists, report the problem to Avaya Professional Services.	Automatic
OP_PCFF40000	Log only	Missing configuration file. See Missing file on page 133.	Manual
OP_PCFF40002	Minor	System Manager connection timeout. See PPM Connection problem on page 135.	Automatic OP_PCFF40003
OP_TALM00100	Indeterminate	Test alarm event provided by **`generateTestAlarmSM.sh`** command.	Automatic OP_TALM00101
OP_TMAG20500	Major	A certificate change has been made that requires a restart. Session Manager should be restarted to avoid any potential outages.	Automatic OP_TMAG20501
OP_TPBR10	Minor	Postgres connection/indexing issues. See Database error on page 126.	Manual
OP_TPBR4	Minor	Postgres connection failure. See Hard disk drive data save errors on page 130.	Manual
OP_TPBR5	Minor	Postgres integrity/protocol violation. See Hard disk drive data save errors on page 130.	Manual
OP_TPBR6	Minor	Postgres invalid transaction failure. See Hard disk drive data save errors on page 130.	Manual
OP_TPBR7	Minor	Postgres insufficient resource failure. See Hard disk drive data save errors on page 130.	Manual
OP_TPBR8	Minor	Postgres resource issues failure. See Hard disk drive data save errors on page 130.	Manual
OP_TPBR9	Minor	Postgres IO/Internal errors. See Hard disk drive data save errors on page 130.	Manual

Log Event ID descriptions

The following table contains the log event IDs and a description of the issue that caused the event. These events do not generate an alarm. Most 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 instance.

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.
- INFO: informational message only.

You can view audit log events using the log viewer for tracking administration changes.

Table 2: Log Event ID Table

Event ID	Severity	Log message
ARBITER_10001	WARN	Session Manager switched to a different System Manager. See Switched Session Manager on page 141.
AU_MSEM20304	INFO	Database record has been updated. See Database UPDATE on page 127.
AU_MSEM20306	INFO	Record has been inserted into the database. See Database INSERT on page 126.
AU_MSEM20308	INFO	Database record has been deleted. See Database DELETE on page 125.
AU_MSEM20310	INFO	Request was made that affects Session Manager. See Action on Session Manager on page 119.
AU_MSEM20312	INFO	Request was made that affects the System Manager. See Action on System Manager on page 120.
OP_MWD20203	INFO	Service <service name> has totally failed again. The service fails to restart but no alarm is raised again since failure is already reported.
OP_AASL10901	INFO	Certificate load successful. See Certificate Status on page 123.
OP_AFWL15001	INFO	SIP Firewall: new configuration imposed. See SIP Firewall Configuration on page 143.
OP_AFWL15002	INFO	Busyout mode is ON or OFF. See Camp-on busyout mode on page 122.

Table continues…

Event ID	Severity	Log message
OP_AFWL16001	INFO	SIP firewall deep inspection disabled or no active rules. See SIP Firewall Configuration on page 143.
OP_AFWL16502	INFO	Too many SIP Firewall alarms. See SIP Firewall Actions on page 143.
OP_AFWL16503	INFO	SIPFW block flow action summary log. See SIP FW Block flow action summary log on page 144.
OP_AFWL16505	INFO	Log message: "SIP firewall loop detection action: %s " "Remote IP: %s Local port: %d Transport: %s, " "Req-URI: %s To: %s From: %s PAI: %s. " "This loop resulted in %d %s in the last second." See SIP Call Loop Elimination on page 142.
OP_AFWL17501	INFO	SIP firewall blacklist disabled or no active rules. See SIP Firewall Configuration on page 143.
OP_AFWL17502	INFO	SIP firewall whitelist disabled or no active rules. See SIP Firewall Configuration on page 143.
OP_ANFW11000	INFO	Network firewall started.
OP_APLM10301	INFO	Success pinholing Network Firewall. See Network Firewall Pinholing on page 134.
OP_APLM10303	INFO	Success configuring network parameters. See Network Configuration on page 133.
OP_APLM10305	INFO	Ethernet interface is up. See Network Configuration on page 133.
OP_CCAC54000	WARN	A location's bandwidth limit was exceeded and caused the denial of at least one call. See Call Admission Control Call Denial on page 122.
OP_CCAC54004	INFO	Bandwidth threshold no longer exceeded.
OP_CCAC54001	INFO	Precedes alarm OP_CCAC54000
OP_CCAC54002	INFO	A location that previously exceeded bandwidth causing call denial has not exceeded bandwidth again.
OP_CCAC54004	INFO	Bandwidth is no longer being exceeded.
OP_CCAC54500		Due to call admission control, a particular (originating or terminating) location's bandwidth would have been exceeded. As a result, the call was denied.
OP_CCAC54501	INFO	Call Admission Control reduced the bandwidth of a call to prevent exceeding the bandwidth limit. As a result, the call quality is degraded.
OP_CDAO50004	WARN	The database connection is down. See Database Connection on page 125.

Table continues…

Event ID	Severity	Log message
OP_CDAO50005	INFO	The database connection has been restored. Administration updates should be taking effect now. See Database Connection on page 125.
OP_CDAO50006	WARN	Unexpected data. See Unexpected data on page 145.
OP_CDAO50007	INFO	There was invalid data in the database, but the error has been corrected. See Unexpected data on page 145.
OP_CDAO50008	INFO	There was an SQL query error, but the error has been corrected. See Database Query on page 126.
OP_CDAO50010	INFO	There was a file I/O error, but the error has been corrected. See Zone File I/O on page 147.
OP_CDAO50014	WARN	A file I/O error occurred trying to write the local DNS server configuration or zone files. See Zone File I/O on page 147.
OP_CDAO50015	INFO	Multiple Session Manager IP addresses no longer map to the local Session Manager instance.
OP_CDAO50016	INFO	The Session Manager Instance resolution issue has been corrected. See Session Manager Instance Resolution on page 141.
OP_CDAO50017	INFO	DNS no longer resolves to multiple IP addresses for the Security Module. See Security Module multiple DNS resolutions on page 139.
OP_CDAO50019	INFO	Bandwidth threshold no longer exceeded for the <location name> location. See Exceeding Location Bandwidth on page 128.
OP_CDAO50021	INFO	The Call detail Recording (CDR) system is now operational. Call accounting is resumed. See CDR Not Operational on page 122.
OP_CDAO50023	INFO	The missing Entity Link for Session Manager to Route-Through has been inserted. See Route Through on page 138.
OP_CDAO50025	INFO	Missing BSM Entity Link has been resolved.
OP_CDAO50027	INFO	Missing BSM avaya-lsp entry has been resolved.
OP_CDAO50032	INFO	An entity link is now administered between Session Manager and the far-end entity.
OP_CMON55000	INFO	SIP monitoring state for SIP Entity has changed to the **Up** state. See SIP Monitor Alarm on page 144.
OP_CSRE52001	INFO	A call was placed that exceeded the administered bandwidth limit, but was allowed to proceed anyway because it was undeniable. A common reason for undeniability is an emergency call.
OP_CSRE52002	INFO	Restricted headers requested to be removed on ingress adaptation.

Table continues…

Event ID	Severity	Log message
OP_CSRE52003	INFO	Restricted headers requested to be removed on egress adaptation.
OP_CSRE52006	INFO	Previously missing ELIN link has been added.
OP_CSVH58002 OP_CSVH58004 OP_CSVH58006 OP_CSVH58008	INFO	Previous configuration file error has been resolved.
OP_CURE56000	INFO	Registration Authorizations no longer failing for user.
OP_CURE56009	INFO	Registration Service no longer failing for user and domain.
OP_CURE56017	INFO	Subscription Authorizations no longer failing for user and domain.
OP_CURE56020	INFO	No longer failing storing subscription, user and domain.
OP_CURE56024	INFO	Subscription terminated due to error response to NOTIFY. Either the subscriber or the subscriber server may be experiencing problems. Ensure that the subscriber and the server servicing the subscriber are functional.
OP_CURE56025	INFO	Application modified parameters in the route header back to the Session Manager.
OP_CURE56026	INFO	Emergency call was made. Provides the contact URI, originating location, and destination.
OP_CURE56028	INFO	No longer any failed over users or failback policy is no longer manual.
OP_CURE56030	INFO	User no longer failed over to Branch Survivable Server.
OP_CURE56031	WARN	Requests received from an untrusted host where the authentication realm does not match an authoritative domain.
OP_CURE56032	INFO	No longer receiving requests from untrusted host where the authentication realm does not match an authoritative domain.
OP_CURE57000	INFO	A user was forcibly unregistered due to administration. Provides user handle.
OP_CURE57001	INFO	A user has registered. Provides user handle.
OP_CURE57002	INFO	A user has unregistered. Provides user handle.
OP_CURE57003	INFO	A user’s registration has expired. Provides user handle.
OP_CURE57004	INFO	A user was forcibly unregistered due to duplicate user registration that overwrote it. Provides user handle.
OP_CURE57005	INFO	A user’s subscription expired. Provides user handle, domain, and event package.
OP_CURE57006	INFO	A user failed authentication. Provides user handle and domain.

Table continues…

Event ID	Severity	Log message
OP_CURE57007	INFO	Failed to compare registrations we found in database with contact address in REGISTER request. Provides user handle and domain.
OP_CURE57008	INFO	Failed to look up existing registration for user. Provides user handle and domain.
OP_CURE57009	INFO	A user asked us to remove all registrations (by supplying a '*' as the contact address) but we failed to do so. Provides user handle and domain.
OP_CURE57010	INFO	A registration was terminated due to reducing the user's simultaneous devices setting in administration. Provides user handle and domain.
OP_CURE57011	INFO	Session Manager detected a registration interruption. This suggests that the device rebooted.
OP_LIC20252	INFO	SIP session counts no longer exceed the licensed number.
OP_LIC20254	INFO	Session Manager instance license error has been resolved.
OP_LIC20256	INFO	Session Manager license is no longer restricted.
OP_MAMA20103	INFO	Security Module Management Agent is able to configure the Security Module.
OP_MMTC20012	INFO	Postgres database sanity check passed.
OP_MMTC20020	INFO	SAL Agent sanity check passed and the SAL Agent is running again.
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_MMTC20046	INFO	ELIN entity link has been administered.
OP_MMTC20052	INFO	User Store connect test passed.
OP_MMTC20054	INFO	Cassandra compaction error has been resolved.
OP_MMTC20056	INFO	Cassandra backup failure has been resolved.
OP_MMTC20057	INFO	Unique authentication file has been installed.

Table continues…

Event ID	Severity	Log message
OP_MMTC20058	INFO	Certificate is no longer nearing expiration date.
OP_MMTC20060	INFO	Cassandra repair data successfully completed.
OP_MWD20200	INFO	Service <service name> has started.
OP_MWD20203	INFO	Service <service name> has totally failed again.
OP_MPER20230	INFO	Performance Monitoring disk space used does not exceed 80%.
OP_MPER20231	INFO	Performance Monitoring disk space used does not exceed 95%.
OP_MPER20232	INFO	NFS server used for performance data storage is now accessible.
OP_MPER20233	INFO	NFS server used for performance data storage is now accessible.
OP_PCFF40001	INFO	Found [FnuFile | LabelFile | SmsConfigFile | ButtonRangesFile].
OP_PCFF40002	INFO	System Manager connection resolved.
OP_PCFF40003	INFO	System Manager connection timeout resolved.
OP_TALM00100	INFO	Test alarm generated by **`generateTestAlarmSM.sh`** has been resolved.
OP_TMAG20501	INFO	Session Manager was restarted due to a certificate change.

Action on Session Manager

This event indicates that an administrator has initiated an administrative request from System Manager Web Console using a Session Manager Element Manager Web page that affects Session Manager or Survivable Remote Session Manager (Branch Session Manager). For example, an administrator may need to change the state of the Session Manager instance to **Deny New Service** 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:<The name of the user logged into System Manager Web Console>
- ClientHost :<The IP address of the computer of the Web user>
- Action on Session Manager: <The name of Session Manager or Branch Session Manager>
- Description: <The 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 System Manager Web Console using a Session Manager Element Manager Web page that affects the System Manager server.

The log messages for this event have the following format:

- LoginID:<The name of the user logged into the System Manager Web Console>
- ClientHost :<The IP address of the computer of the Web user>
- Action on System Manager Description:<The description of the requested action>

Alarms for NFS Disk Space

Alarms are generated when Session Manager cannot read or write performance data to or from an NFS server. This can occur when the NFS server is down or when the network connection between the System Manager and the NFS server has failed.

- If the problem persists, the Session Manager Element Manager raises a *Warning Alarm* once every 24 hours until either:
  - The condition which is causing the Session Manager Element Manager to be unable to read or write the NFS storage has been resolved and the Session Manager Element Manager can once again successfully write and read data to and from the NFS server, or
  - The system has been sending NFS *Warning Alarms* for one week.
- If the NFS failure condition persists for more than one week, the Session Manager Element Manager stops sending *Warning Alarms* and begins to send *Minor Alarms* once every 24 hours until such time as the NFS error condition has been repaired and the Session Manager Element Manager can once again read and write data to the NFS server.

Filtering displayed alarms

You can filter alarms displayed on the alarm screen based on certain criteria. You can use more than one filter criterion on the selected alarms.

Procedure

1. On System Manager Web Console, select **Services** > **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 that contain a particular alarm code.

5. Click **Filter: Apply**.

   Note:

   The system displays a message if no matching records are found for the specified filter criteria.

   The page displays the alarms matching the filter criteria.

BSM Entity links not administered

This event indicates that you have not administered the mandatory entity links from the Survivable Remote Session Manager (BSM). 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 System Manager. The BSM instance was probably installed before the links were administered on System Manager. The events will resolve after administration is completed.

There should be one or two links administered, depending on the Communication Manager configuration in the core. The links must use the same ports administered between the core Communication Manager and the primary core Session Manager. This event can 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 links between the BSM instance and the core Communication Manager to which the entity link 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 Step 1 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 the problem does not resolve, contact Avaya Technical Support.

Call Admission Control Call Denial

This alarm occurs when there are multiple call failures due to the lack of bandwidth for a call on a particular location. While the alarm is active, the system checks the number of calls denied through a particular location within a particular interval, with a one hour default. The alarm is cleared when no calls were denied for the location within the last interval.

This event may be caused by one of the following:

- 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.
- Inappropriate bandwidth limitations.
- Network issues.

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. Split the location into two or more different locations, and route traffic accordingly.

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.

Certificate Expiration

Session Manager requires certificates for securing SIP and HTTP (for Personal Profile Manager) connections, and for communication between the Session Manager and System Manager. If a certificate has expired, the Session Manager may be unable to establish any new connections and security might be compromised. In many cases, TCP and UDP are not options, so certificate lifetime must be monitored.

When a certificate is approaching its expiration:

- A warning message is periodically logged, starting 60 days before expiration.
- In most cases, a major alarm is logged daily if the certificate is within 30 days of expiring.
- A critical alarm is generated when the certificate is within 15 days of expiring

It is important, therefore, that the warning expiration alarms be resolved without delay before the major and critical alarms are raised.

Troubleshooting certificate expiration alarms

Procedure

To fix the alarm, install new certificates. For the procedure to obtain a new certificate, see *Administering Avaya Aura® Session Manager*.

Certificate status

The Security Module identity certificate and CA (trusted) certificate must be present for SIP TLS. An alarm is raised if one of the certificates cannot be loaded because it is invalid, expired, or revoked.

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 123 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 system displays the following information:

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

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 or redundancy down alarm

Procedure

1. On System Manager Web Console, select **Elements** > **Session Manager** > **System Tools** > **Maintenance Tests**.
2. Select the affected Session Manager instance 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 instance, using either the Avaya craft login or an established customer login.
7. Run **statapp** to verify the status of the **WebSphere** and **mgmt** processes.
8. If the status of **WebSphere** is **Down**, run **restart WebSphere** and wait for the WebSphere SIP Container to restart.
9. If the status of **WebSphere** is **Partially Up**, wait for the status to change to completely **Up**.
10. Run **statapp** and verify that the status of **WebSphere** is **Up**.
11. Re-run the **Test data distribution and redundancy link** test.
12. If the test fails, run **restart mgmt** and wait for the Management Jboss service to restart.
13. If the problem persists, reboot the Session Manager instance, using the **Session Manager > Dashboard** page.
14. If the reboot does not solve the problem, re-install the affected Session Manager.

Database connection

This alarm indicates a problem with the connection to the database that contains the administered data for routing and users. The connection to the database is either timing out or has been lost. During this outage, the running system does not recognize any new administration.

The possible causes include:

- The database might not be running.
- The connection to the database was 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 might not be running on the Session Manager instance or is on a different IP address than expected.

To resolve this issue, go to Avaya Support site.

Troubleshooting Database Connection Alarms

Procedure

1. Ensure the database process is running on the Session Manager instance. Log in to the Session Manager system and run one or all of the following commands:
   a. Enter **statapp -s postgres -db**.

      The output is similar to **postgres-db 18/ 18 UP**.

   b. If none of these conditions are true, enter `restart postgres–db`.
2. Ensure there is a connection to the database. Verify the connection is stable and is not experiencing outages.
3. If the problem continues after performing the above steps, contact Avaya Technical Support.

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:<The name of user logged into System Manager Web Console>
- ClientHost :<The IP address of the web user 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 error

This event indicates a connection or indexing error with the postgres database. For Session Manager servers, a reinstall may be required. For System Manager servers, a restore from back up may be required. Contact Avaya Technical Support.

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 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, assetIPAdress:<NULL>, assetInterfaceName:<NULL>, assetNetMask:255.255.255.0...`

Database Query

This event occurs when a database query cannot complete or fails, usually after an upgrade indicating that the upgrade had problems. As a result, Session Manager might not operate correctly.

This event can occur if the database schemas do not match, indicating that variable types are different or fields are nonexistent.

Go to Avaya Support site to check the database versions and ensure the version are correct and compatible. In particular, the table **schemaversion** in the System Manager and Session Manager databases must have appropriate and matching version entries for major, minor, revision and schemaname.

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:<The name of user logged into System Manager Web Console>
- ClientHost :<The IP address of the web user computer>
- Action: Database UPDATE into table <The name of the database table> 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`

DRS failure due to reinstallation of System Manager

After reinstalling System Manager, run the **`initTM -f`** command on the Session Manager and Branch Session Manager instances that System Manager manages. This command re-establishes the trust relationship with the reinstalled System Manager database.

Use this procedure to resolve any DRS and trust relationship issues.

Warning:

This command removes any administered third-party certificates. You must re-administer any administered third-party certificates.

DRS Synchronization failure

About this task

Data Replication Service (DRS) replication error: The Session Manager instance is out of sync with the System Manager database.

A sync failure indicates a critical failure in the functioning of the node. The failure is not a configuration issue. Based on the error description, the administrator or support technician should analyze the problem on the element node before initiating a repair.

Procedure

1. On System Manager Web Console, select **Services** > **Replication**.
2. Select the affected **Replica Group**.
3. Select the affected Session Manager.

4. Click **Repair**.
5. Manually resolve any inconsistencies.

Exceeding Location Bandwidth

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

The used bandwidth for a specific location has exceeded an allotment threshold. Additionally, the alarm indicates which multimedia pools are being exceeded.

You can configure the thresholds to be configured for each location and for each pool as well as the duration for which the threshold must be exceeded before the alarm is generated on System Manager. The default threshold for each pool is set to 80%.

The alarm is centralized and is only seen from one Session Manager instance. If the alarming Session Manager goes down, another Session Manager takes over the alarming role.

When the bandwidth is at 100% capacity for a particular location, new calls are not allowed on that location and are denied.

This alarm 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. If this is an undesired location from which to alarm, the location can be disabled from alarming in one of two ways:
   a. Set the thresholds to **Disabled** - this only applies to a single location.
   b. On the Session Manager Administration screen, check the **Disable Call Admission Control Threshold Alarms** box - this applies to all locations.
2. Check the bandwidth threshold values for the pools to ensure they are appropriate. Also ensure the **Latency before Alarm Trigger** time is appropriate.
3. Ensure the traffic is consistent with the bandwidth capacity.
4. Consider rerouting part of the traffic through a different, under-utilized location.
5. Increase bandwidth provisioning if allowed by the network.
6. Consider splitting the location into two or more different locations and route traffic accordingly.

Failed binding a listener

This event indicates that the specified address is in use or is an invalid interface.

A port conflict possibly exists with another Session Manager application on the server.

Troubleshooting failed binding listener

Procedure

1. Check the administration of the specified port to make sure that it is not already in use and that it is available for the Security Module.
2. If you cannot resolve the conflict and cannot establish a listener, contact Avaya Technical Support.

Failure to install the unique authentication file

Services can login to Session Manager in the field using Access Security Gateway (ASG) challenged authentication method. During Session Manager installation process, the default authentication file must be replaced by the unique authentication file. This alarm is related to the failure to install the unique authentication file during the Session Manager installation.

The alarm is raised when the system fails to validate the unique authentication file.

Troubleshooting unique authentication file failure

About this task

The unique authentication file can be created using Authentication File System (AFS) and loaded as shown below.

Procedure

1. Generation of unique authentication file using AFS. You can either:
   - Download the authentication file directly from AFS.
   - Receive the authentication file in an email.
2. Load the authentication file using the command "loadpwd" which validates the authenticity of authentication file.

   For further details, see the book *Implementing Avaya Aura® Session Manager Release 6.2, 03-603473*.

Hard disk drive data save errors

This event indicates that the database software is having problems persisting data to the hard disk drive. Check that there is space left on the disk drive. If not, contact Avaya Technical Support. If there is sufficient disk space, try rebooting the system. If the problem persists, contact Avaya Technical Support.

Host name resolution failed

The on-demand or periodic maintenance test run on System Manager has detected connection problems while resolving the host name of a Session Manager or Branch Session Manager instance.

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. Ensure the host name of the Session Manager instance and the survivable remote Session Manager (BSM) is administered properly on the DNS servers.
3. If the DNS server is not administered, ensure the host name-to-IP address map of the Session Manager and/or survivable remote Session Manager (BSM) instance is included in the **/etc/hosts** file on System Manager.

ELIN entity link missing

This event indicates there is no entity link between some Session Manager instances and the Emergency Location Identification Number (ELIN) server.

The ELIN server is administered as a SIP Entity of type **ELIN** server, user registrations are occurring, but the entity link between the ELIN server and a Session Manager server does not exist.

This event can occur on several Session Manager instances at the same time. The alarm can be generated on a per Session Manager basis.

To fix this problem, add the correct Entity Link between the Session Manager server and the ELIN Server.

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 System Manager Web Console, select **Elements** > **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. On System Manager Web Console, select **Elements** > **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 previously failing Branch Session Managers pass the demand tests, clear this alarm to indicate that the problem no longer exists and no further action is required.
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. Re-run the demand Maintenance Tests for the failing Branch Session Manager.
9. If the tests are still failing, run **initTM** on the Branch Session Manager to clear possible trust relationship problems.
10. 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 fail the ping test, a network problem may be the cause of the alarms.

Procedure

1. On System Manager Web Console, select **Elements** > **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. Select **Elements** > **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 instance, 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:
        a. Establish an SSH connection to the Session Manager instance, using either the Avaya craft login or an established customer login.
        b. Enter **statapp** to verify the status of **mgmt**.
        c. If the status of **mgmt** is **Down**, enter **restart mgmt** and wait for the Management JBoss server to restart.
        d. If the status of **mgmt** is **Partially Up**, wait for the status to change to completely **Up**.
        e. Enter **statapp** to verify that the status of **mgmt** is **Up**.
        f. Re-run the **Test network connections to each Session Manager** test.
        g. If the test fails, enter **initTM** on the Session Manager to clear possible trust relationship problems.
        h. Re-run the **Test network connections to each Session Manager** test.
        i. 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 System Manager Web Console, select **Elements** > **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 instance. If you cannot reboot using the**Session Manager > Dashboard** page or cannot establish an SSH connection, gain physical access to the server to reboot Session Manager.

Missing file

One of the following files is missing:

- ButtonDataType
- LabelFile

The system displays the name of the missing file.

Clearing a missing file alarm

Procedure

Redeploy the Session Manager.

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 is not configured, an alarm is raised.

When the Security Module stops or restarts, the system displays the change in state of the Security Module interface. During normal operation, the interface should only display as **Up**. Failure to properly configure the Security Module network may be due to incorrect settings.

Network firewall critical event

This alarm indicates there is a problem with the Linux network firewall iptables.

Contact Avaya Global Services.

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 that is available when you log in to the support website and use the InSite Knowledge Management Database at http://support.avaya.com.

However, the pinhole mechanism permits applications to make on-demand requests to open or close temporary “pinholes” through the network firewall.

Failure of an application to open a pinhole indicates an internal Session Manager problem. If the problem persists, contact Avaya Technical Support.

Network firewall stopped

This alarm indicates that the network firewall has been manually turned off.

Contact Avaya Global Services.

No entity link with correct transport type

This event indicates there is no entity link administered between the Session Manager and the far-end entity with the appropriate transport type. An entity link might be present, but the link does not match the transport required for the call to complete.

1. In the **Local Host Name Resolution** Table, verify the entry for the FQDN of the far-end entity has the correct transport type.
2. If the transport type is correct, verify an entity link exists and is administered correctly between the far-end entity and the Session Manager.
3. If the entity link does not exist, create an entity link between the far-end entity and the Session Manager.

No master System Manager

About this task

Session Manager could not locate any System Manager as its Management System.

Procedure

1. Check the Geographic Redundancy mode of the System Managers. If none of the System Managers are active, check System Manager Web Console for trouble shooting.
2. Verify whether or not the Session Manager instance has network connectivity to the System Managers. Check the network connectivity or SSL settings between Session Managers and System Managers.

PPM Connection problem

The connection between the Session Manager and the System Manager is down.

This alarm is raised when a PPM command fails due to a connection problem.

This can happen when:

- PPM is trying to update the System Manager database due to an endpoint request to add, update, or delete a contact from the phone.
- PPM is trying to update the System Manager database due to an endpoint request to add or update Device Data from the phone.

The alarm is resolved when the PPM successfully contacts the System Manager to update the database.

Performance data storage disk usage

Performance data storage disk usage is low or critically low.

Contact Avaya Technical Support to resize the data setup for the collection storage space.

Postgres database sanity check failed

The periodic maintenance operation 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 System Manager Web Console, select **Elements** > **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 instance 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 System Manager Web Console, select **Elements** > **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 the problem persists, contact Avaya Technical Support.

Registration authorization failure

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

The credentials provided by the user for the attempted registration are invalid.

Ensure the provided credentials being provided by the user are correct.

Registration component failure storing subscriptions

This event is related to the Eventing Handler functionality for the Registration component in Session Manager. Due to this event, subscription based functionality stops working for the affected users. For example, affected users fail to receive the Message Waiting Indicator (MWI) event for the Voicemails. 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 database inconsistency or error condition.

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

Registration service unavailable for a given user

This event is related to the endpoint processing function in the Registration component in Session Manager. This event means that the system experienced a problem or failure while processing the resolution of a SIP domain 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 a user is attempting to register to a Session Manager which does not have the user marked as a local user. A local user in this context refers to one having the Session Manager as either the Primary and Secondary Session Manager on the Communication Profile section of the Manage Users administration screen.

The problem may be related to a Replication failure on one of the Session Managers, or to the Personal Profile Management download to the endpoint itself. If the problem persists or reoccurs, contact Avaya Technical Support.

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

Route Through

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

SAL Agent sanity check failed

The periodic maintenance sanity check of the SAL Agent (Serviceability Agent) has failed. The Session Manager alarming service may not be running.

This alarm is raised only after the SAL is running again.

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

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 System Manager Web Console, select **Elements** > **Session Manager** > **System Tools** > **Maintenance Tests**.

2. Run the **Test Security Module Status** maintenance test for the failing Session Manager to verify the sanity of the Security Module.
3. Select **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
4. If the test passes and the **Status** for the Session Manager instance 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 instance from the System Name list.
   b. Select the Security Module **Reset** button.

      Warning:

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

   c. Click **Refresh** to display the current status.
   d. Rerun the **Test Security Module Status** maintenance test in Step 2 for this Session Manager instance.

Security Module multiple DNS resolutions

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 the address is correct or not. While the system may work just fine, the situation is highly dangerous in terms of not having a reliable system.

Troubleshooting Security Module multiple DNS resolution alarms

Procedure

1. Check the IP address in the Session Manager 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 Web Console, select **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
2. Select **Refresh** to display the current status.
3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.
5. If the status is selected as **Down**, reset the security module:
   a. Select the appropriate Session Manager instance from the table.
   b. Click **Reset**.

   Warning:

   Session Manager cannot process calls while the system resets the security module.
6. 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 management interface. During this failure, the Session Manager instance does not service any calls.

Possible causes are:

- The IP address specified in the Session Manager Administration configuration does not match the IP Address of the Session Manager in the Management Access Point field.
- The IP address of the Security Module was entered instead of the IP address of the Session Manager Management interface.
- The DNS name resolves to multiple IP addresses or to no IP address.

Troubleshooting Session Manager Resolution Alarms

Procedure

1. Check the IP address in the Management Access Point Host Name/IP field on Session Manager Administration page:
   a. Enter **/sbin/ifconfig**
   b. The IP address should match the eth0 IP address of the Session Manager instance.
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>**.

Switched Session Manager

About this task

Session Manager has switched to a different System Manager.

Procedure

1. Find out the System Manager Geographic Redundancy mode.
2. Verify whether the switch over was due to a manual process using the System Manager web console.
3. Verify that the failed over System Manager is in Active mode.
4. Verify that the failed from System manager is not in Active mode. Then, this might have caused the alarm.
5. Verify whether or not the Session Manager has network connectivity with the switching from System Manager.

SIP Call Loop elimination

Session Manager can sometimes receive identical INVITE requests within a short interval.

Session Manager sets up separate sessions for each INVITE. Multiple identical INVITE requests can initiate SIP call loops and deplete network resources. Session Manager provides administration features to track and terminate call looping instances in the network.

Loop Administration

You administer loop parameters when you create a SIP entity that is not of **Type** Session Manager on the SIP Entity Details page under **Elements** > **Routing** > **SIP Entities**.

Session Manager rejects requests if the number of incoming requests that have the same combination of the **R-URI**, **To**, **From**, and **PAI** header values reaches the administered **Loop Count Threshold** value within the **Loop Detection Interval** time. The frequency of the call loops is a function of the latency and the number of network elements in the loop path. An administrator must set the Loop Detection parameters based on the customer network configuration. Setting improper values of **Loop Count Threshold** and **Loop Detection Interval** can result in:

- System performance overhead.
- Non-detection of call looping scenarios in the network.

For example, if the successive loop call arrives at Session Manager after 40 milliseconds (because of the propagation delay of the intermediate hops) and the administrator needs to break the loop on the fifth loop call instance, the recommended Firewall configuration must have **Loop Count Threshold** set to 5 and **Loop Detection Interval** set to 200 milliseconds.

Alarm Generation

The Session Manager SIP Firewall generates a minor-level alarm for a call loop detection event based on the Loop Detection parameters settings. You can administer Loop Detection alarms on the Session Manager Administration page.

When an alarm is generated for the Loop Detection event, Session Manager does not generate any more alarms for the administered **Loop Detection Alarm Threshold** interval after the event. For example, if the **Loop Detection Alarm Threshold** is set to 24 hours and a Loop Detection alarm is generated, the SIP Firewall does not generate any new Loop Detection alarms for the next 24

hours. During this interval, the SIP Firewall continues to detect and break loops without generating any new alarms, but continues to log loop detection summary events.

SIP Firewall actions

If administration has configured SIP firewall rules with logs or alarms, all received SIP messages matching that rule will cause an alarm notification trap to be sent if the alarm option is set.

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 or port.
- Destination host address or port.

For rules with track operation, the system displays the concrete track value. You can use these logging details to further analyze and mitigate threats to the system.

Troubleshooting SIP Firewall actions alarms

About this task

Complete the following steps if the system displays too many *matched-rule* log or alarm messages.

Procedure

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

   See SIP Firewall Configuration section of *Administering Avaya Aura® Session Manager*, 03-603324.

SIP firewall configuration

Configuration failures are serious and cause alarms. When the system generates alarms, the system displays information about the failure: 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 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

The system generates a summary log whenever the SIPFW is stopping a block attack. For example, when the system detects an attack that must be stopped or goes below the predefined threshold. This log contains information on the packet dropped during the blocking period.

SIP Monitor Alarm

The alarmed SIP entity is not successfully responding to SIP OPTIONS requests.

A SIP entity can be reachable through 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 addresses respond to OPTIONS requests successfully.

If the state of the entity is **partially up**, at least one of the entity addresses is responding successfully and at least one address is not responding successfully.

The SIP Monitoring Status page on the System Manager provides 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.

Troubleshooting SIP Monitoring alarms

Procedure

1. Check the SIP Monitoring Status page for more details.
2. Verify network connectivity exists between 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. A typical response is *200 OK*.

Subscription authorization failure for a given user

This event is related to the Eventing Handler functionality of the Subscription processing component. This alarm means that a user has attempted to subscribe with Session Manager and failed to provide a valid authorization credential. The system logs a warning after five subscription attempts fail in one minute.

The credentials provided by the user for the attempted subscription are invalid.

Ensure the provided credentials being provided by the user are correct.

Troubleshooting alarms

Starting with 7.0 Release, the system automatically clears specific alarms. Some alarms do not have an event code that clears the event.

For more information on alarms that have associated auto clear events, see Alarm Event ID descriptions.

Use the corrective actions associated with an alarm as guidelines for troubleshooting the alarm.

Unexpected data

The system detects unexpected data the database. During this period, the invalid data will not be actualized in the running Session Manager.

Possible causes are:

- Administration data that was not properly checked for errors by the system.
- Incorrect data that was written directly into the database. For example, if you enter a digit pattern that is 5555 and set the minimum and maximum limits to 3. The limit must be set to at least 4.

To correct the problem:

1. Check any recent administration relating to the suggested configuration pages of the alarm.
2. If the problem persists, contact Avaya Global Services.

User failed over, manual failback mode

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

Manual failback policy means that without manual intervention, the failed over users stays on this nonprimary Session Manager forever. This event reflects a notification of a potential problem and not loss in service.

You can find the primary Session Manager defined on the User administration page in **Communication Profile** and **Session Manager Profile** section as the first drop-down menu.

The possible causes for this event are:

- The primary Session Manager is not running.
- The user lost connectivity with the primary Session Manager due to network issues or any other reason.
- 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 with their core Session Managers. Users active on the Survivable Remote Session Manager (BSM) do 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. To place calls from a branch SIP user to a user outside the branch, dial the call using the public number of the user. To place calls to a branch SIP user from outside the branch, dial the public number.

The possible causes are:

- Lost connectivity between the branch and core.
- The Session Manager experienced partial network outages.
- 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 Managers are operational.
2. Restore network connectivity between the branch and core.
3. Verify the Session Managers are in the **`Accept New Service`** state.
4. Check the **SIP Entity Monitoring** page to see if there are any network connectivity problems with 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. For ways to administer failback and activate failback on a system, see Communication Manager documentation.
6. If none of these steps work, call Avaya Technical Support.

Zone File I/O

Zone files are written to the local file system to reflect the host name resolution data administered on the **Local Host Name Resolution** page. The 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 that cause failure in the attempt to read or write to the zone files.

Troubleshooting Zone File I/O Alarms

About this task

To troubleshoot the error, you must log on using the **root** user.

Procedure

1. Verify that 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 such as 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.

      First check the log files in **/var/log/Avaya/sm** and ensure their size is not too large more than 100 MB.
4. Ensure that 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 the file 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.

Chapter 7: Resources

Documentation

The following documents are available at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 7.0.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.0.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel

Table continues…

Title	Description	Audience
Upgrading and Migrating Avaya Aura® applications to Release 7.0.1 from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel

Table continues…

Title	Description	Audience
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Related links

Finding documents on the Avaya Support website on page 151

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 149

Training

The following table contains courses that are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration
5U00082R	Session Manager and System Manager Administration
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Index

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z