



Maintaining Avaya Aura[®] Session Manager

Release 10.2.x
Issue 4
March 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

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](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.

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, 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. Unless otherwise stated, 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

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](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction	9
Purpose	9
Changes to platform support	9
Change history	10
Chapter 2: Session Manager overview	11
Chapter 3: Regulatory information and safety precautions	12
General safety information	12
Safety Inspection	13
Electrical safety rules	13
Protecting against ESD damage	15
Chapter 4: General information	16
Required equipment	16
Supported servers	16
Supported browsers	16
Session Manager Dashboard	17
Session Manager Dashboard field descriptions	17
Session Manager software version	22
Server Ethernet ports	23
Customer account commands	24
Accessing the root account	26
Session Manager backup and restore commands	27
Loading and managing site certificate	27
Restricted commands for the Security Module	28
certTool	29
Importing Identity certificate using certTool	31
Importing Trusted certificate using certTool	31
Chapter 5: Monitoring operations	33
Log Viewer	33
Viewing log details	33
Logging field descriptions	33
Searching for logs	37
Filtering logs	37
Log Harvester	38
Accessing the Log Harvester service	38
Creating a new log harvesting profile	38
Create New Profile field descriptions	39
Viewing details of a log harvesting profile	40
Filtering log harvesting profiles	40
Submitting a request for harvesting log files	41

Viewing details of a log harvesting request.....	41
Filtering log harvesting requests.....	42
Viewing the contents of harvested log files.....	42
Searching for text in a log file.....	43
Viewing the harvested log files in an archive.....	43
Downloading the harvested log files.....	44
Harvest Archives field descriptions.....	44
Profile Criteria View field descriptions.....	46
Search Archives field descriptions.....	46
Harvest - View Harvest detail field descriptions.....	47
Security Module Status.....	48
Viewing the Security Module status.....	48
Security Module Status page field descriptions.....	49
Connection Status.....	50
Session Manager SIP Entity Monitoring.....	53
Viewing the SIP Monitoring Status Summary page.....	54
SIP Entity Link Monitoring Status Summary page field descriptions.....	54
Session Manager SIP Tracing.....	55
SIP Tracer Configuration.....	56
SIP Trace Viewer.....	60
Remote logging.....	62
Managed Bandwidth Usage.....	66
Viewing Managed Bandwidth Usage.....	66
Managed Bandwidth Usage page field descriptions.....	66
Managed Bandwidth Usage errors.....	67
Log retention.....	68
logRetention command.....	68
smconfig command.....	69
Data encryption commands.....	69
encryptionPassphrase command.....	69
encryptionRemoteKey command.....	71
encryptionLocalKey command.....	73
Viewing data encryption status.....	74
Data replication	75
Viewing replica groups.....	75
Viewing replica nodes in a replica group.....	75
Repairing a replica node.....	75
Repairing all replica nodes in a replica group.....	76
Viewing replication details for a replica node.....	76
Removing a replica node.....	77
Removing a replica node from queue.....	77
Troubleshooting Replica Nodes.....	77
Replica Groups field descriptions.....	78

Replica Nodes field descriptions.....	79
Replication Node Details field descriptions.....	82
User Data Storage and Data Center management.....	84
Viewing the User Data Storage status	85
HTTP proxy commands.....	85
httpProxyAccess command.....	85
checkHttpProxy command.....	87
Chapter 6: Verification testing.....	89
Session Manager maintenance tests.....	89
Maintenance Tests field descriptions.....	89
Running maintenance tests.....	90
Maintenance Test descriptions.....	90
Verifying the System Manager and Session Manager or Branch Session Manager installation.....	92
Generating a test alarm.....	94
Call Routing Test for Session Manager.....	95
Call Routing Test page field descriptions.....	95
Setting up a Call Routing Test.....	97
Call Routing Test results.....	98
Troubleshooting Call Route Test failure.....	98
Chapter 7: Maintenance functions.....	99
Planning network outage or service maintenance.....	99
Maintenance functions.....	100
Backup and Restore.....	100
hardware_info command.....	108
Replacing server components.....	108
IP address changes.....	110
Migrating servers.....	114
Chapter 8: Call Detail Recording on Session Manager.....	116
Minimum requirements for CDR.....	117
CDR Data file naming and structure.....	117
CDR login and password.....	118
CDR record transfer.....	119
Retrieving CDR data files.....	119
CDR record deletion.....	120
CDR security provisions.....	120
Call Detail Recording alarms.....	121
Administering CDR on a new Session Manager instance.....	121
Enabling CDR for an existing Session Manager instance.....	121
Chapter 9: Resources.....	123
Session Manager documentation.....	123
Finding documents on the Avaya Support website.....	124
Accessing the port matrix document.....	124
Avaya Documentation Center navigation.....	125

Training.....	126
Viewing Avaya Mentor videos.....	126
Support.....	127
Using the Avaya InSite Knowledge Base.....	127
Appendix A: SNMP support for Session Manager.....	129
Serviceability Agents.....	129
Configuring the Session Manager Serviceability Agent.....	130
Verifying the Session Manager serviceability agent registration.....	131
Activating a serviceability agent.....	131
Managing SNMPv3 user profiles for the selected serviceability agents.....	131
Managing target profiles for the selected serviceability agents.....	132
Generating the test alarm from the web console.....	132
Repairing serviceability agents.....	132
Serviceability Agents field descriptions.....	133
Managing SNMPv3 user profiles.....	135
Creating an SNMPv3 user profile.....	135
Editing an SNMPv3 user profile.....	135
Viewing an SNMPv3 user profile.....	135
Deleting an SNMPv3 user profile.....	136
Filtering SNMPv3 user profiles.....	136
SNMPv3 user profiles field descriptions.....	136
Managing SNMP target profiles.....	138
Creating an SNMP target profile.....	138
Editing an SNMP target profile.....	138
Viewing an SNMP target profile.....	138
Deleting an SNMP target profile.....	139
Filtering target profiles.....	139
SNMP Target profile list.....	139
SNMP target profiles field descriptions.....	140
Notification Filter Profile.....	140
Creating a Notification Filter Profile.....	141
Viewing a Notification Filter Profile.....	141
Editing a Notification Filter Profile.....	141
Deleting a Notification Filter Profile.....	142
Assigning a Notification Filter Profile to a serviceability agent.....	142
Unassigning a Notification Filter Profile from a serviceability agent.....	142
Filter Profiles field descriptions.....	143
Create, View, Edit, or Delete Filter Profiles field descriptions.....	143
System Manager TrapListener service.....	144
Configuring the TrapListener service.....	144
Viewing the System Manager TrapListener Service settings.....	145
View Profile: TrapListener field descriptions.....	145
Session Manager SNMP MIB.....	146

Appendix B: Product notifications	151
Viewing Product Correction Notices and Product Support Notices.....	151
Registering for product notifications.....	152

Chapter 1: Introduction

Purpose

This document provides general maintenance information for Avaya Aura® Session Manager.

Routine maintenance includes regularly scheduled backup and restore operations, running maintenance tests, and monitoring system components.

The primary audience for this document is anyone who is involved with the maintenance of Session Manager.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Change history

Issue	Date	Summary of changes
4	March 2026	Added the section: Changes to platform support on page 9
3	February 2026	Updated the following sections: • Supported servers on page 16 • Server Ethernet ports on page 23
2	April 2025	Added the following section for R10.2.1.1: • Planning network outage or service maintenance on page 99
1	Dec 2023	10.2.x

Chapter 2: Session Manager overview

Avaya Aura® Session Manager is a SIP routing tool that integrates all SIP devices across the entire enterprise network. Session Manager simplifies the existing communication infrastructure by combining existing PBXs and other communications systems, regardless of the vendor, into a cohesive and centrally managed SIP-based communications network.

Session Manager supports the following features:

- Integration with third-party equipment and endpoints to normalize disparate networks.
- Centralized routing of calls using an enterprise-wide numbering plan.
- Centralized management through System Manager, including configuration of user profiles and deployment of enterprise-wide centralized applications.
- Interconnection with Communication Manager and Avaya Communication Server 1000 to provide multiple feature support for SIP and non-SIP endpoints.
- Interconnection with IP Office through SIP to provide feature support for SIP endpoints.
- Third-party E911 emergency call service for enterprise users.
- Centralized Presence Services for scalability and reduced network complexity with a variety of endpoints and communication servers.
- Support for converged voice and video bandwidth management.
- Application sequencing capability to incrementally deploy applications without needing to upgrade the PBX.
- Geographic redundancy.
- Mobility of SIP telephones and enterprise mobility for SIP users.
- Support for call reconstruction to allow Call Preservation for SIP calls, which provides mid-call features to be invoked after a failover.
- Support to carry Presence Information Data Format Location Object (PIDF-LO) as a Multipurpose Internet Mail Extensions (MIME) body/attachment in a SIP message. Session Manager can also pass the PIDF-LO information in the SIP message.

Chapter 3: Regulatory information and safety precautions

General safety information

Follow these rules to ensure general safety:

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

- Reinstall all covers correctly before returning the server to service.

**Warning:**

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

Safety Inspection

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

Consider these conditions and the safety hazards they present:

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

Perform the following safety checks when servicing this unit:

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

Electrical safety rules

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

Observe the following rules when working on electrical equipment.

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

If an electrical accident occurs:

- Use caution. Do not become a victim yourself.

- Turn off power.
- Send another person to get medical aid.

Protecting against ESD damage

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

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

Caution:

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

To avoid damaging ESD-sensitive components:

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

Caution:

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

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

Chapter 4: General information

Required equipment

For maintenance and troubleshooting activities, you may need:

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

Supported servers

- Avaya Solutions Platform S8300 Release 6.0 for Communication Manager and Branch Session Manager
- Avaya Solutions Platform 130 Release 6.0 Appliance: Dell PowerEdge R640 and R660xs

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

 Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Session Manager Dashboard

The Session Manager Dashboard page displays the overall status and health summary of each administered Session Manager instance. Using Session Manager Dashboard, you can also do the following:

- Change the service state of a Session Manager instance.
- Stop the Session Manager server.
- Reboot the Session Manager server.
- Enable and disable EASG for selected Session Manager.
- Clear trace and error logs on demand for selected Session Manager and Branch Session Manager

Note:

If the **License Mode** of Session Manager or Branch Session Manager displays `Restricted`, you cannot change the service state to **Accept New Service**. You cannot change the service state 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

Table continues...

Name	Description
Topology	If Enable Edge Topology is enabled on the Global Settings page, Session Manager displays the Topology column. Specifies the type of the Session Manager or Branch Session Manager edge topology configuration. The options are: • Enterprise: For Session Manager in an enterprise configuration. • Edge: If a SIP Entity is of type Edge Core or Edge Branch.
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 a 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
Region	Displays the region name with which this Session Manager instance is associated.  Note: • Dashboard populates the Region column if you enable policy-based communication feature on the Global Settings page. • Region column is not applicable for a Branch Session Manager. The region column for a Branch Session Manager is always (---).

Table continues...

Name	Description
Load Factor	The load factor of the administered Session Manager or Branch Session Manager. The field displays the current/last hour peak/last 24-hour peak load factor. Clicking the link displays the Session Manager Load Factor page.  Note: The last hour and 24-hour peak load factor for a Branch Session Manager is always unknown (---).
Entity Monitoring	The monitoring status of the administered Session Manager instances. The field displays the number of entities with connection problems/the total entities. Clicking the link displays the Session Manager Entity Link Connection Status page.  Note: 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 (---).
Active Call Count	The current number of active calls for the administered Session Manager instances. Clicking the link displays the Call Counts page.
Registrations	The current registration summary and the maximum number of registrations in the last 24 hours. Clicking the link displays the Registration Summary page.
Push Notifications	The current number of push notifications for the administered Session Manager instances. The field displays average activations per hour in the last 24 hours/notifications in last hour/notifications in last day/notification errors in last day. Clicking the link displays the Push Notification Performance page.  Note: • Dashboard populates the push notification counts if you enable the mobile push notification feature on the Global Settings page. • Push notification counts are shown only for a Core Session Manager. The push notification counts for a Branch Session Manager is shown as (---).

Table continues...

Name	Description
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 hostname 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. • 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.
Enhanced Access Security Gateway (EASG)	Status of Session Manager EASG. The status can be: • Enabled — EASG is installed and is enabled for Avaya Service access. • Disabled — EASG is installed but is disabled for Avaya Service access. • Removed — EASG is removed from Session Manager. To enable EASG access, Session Manager must be reinstalled. • --- — EASG status for Session Manager is not retrievable or is not applicable for the current version of Session Manager.

Table continues...

Name	Description
Profile	Displays the capacity profile of a Session Manager or Branch Session Manager machine. For information about Session Manager profiles and related capacities, see <i>Avaya Aura® Session Manager Overview and Specification</i> .
Version	The version of the installed Session Manager software. Clicking a version string link displays the Session Manager Version Inventory page.
Status Last Updated	Displays the time when the Session Manager or Branch Session Manager data was last updated in the row. Hover over the time to view the full date and timestamp when the data was last updated.

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 Maintenance mode, the 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 the 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.
EASG > Enable EASG	Enables EASG for the selected Session Manager.  Note: Enable or Disable EASG is also supported when Session Manager is in Maintenance Mode , and Session Manager is currently displaying Limited Connection status.

Table continues...

Button	Description
EASG > Disable EASG	Disables EASG for the selected Session Manager.  Note: Enable or Disable EASG is also supported when Session Manager is in Maintenance Mode, and Session Manager is currently displaying Limited Connection status.
Clear Logs	Clears trace and error logs on demand for selected Session Manager and Branch Session Manager  Note: - On-demand log clearing requests will not be made to Session Managers and Branch Session Managers in maintenance mode, or are part of a Geographic Redundancy configuration and are not managed by the current System Manager. - On using this option, the administrator gets a prompt for entering the number of retention days (between 1–180) beyond which logs will be purged. The default value will be the same as given in the Log Retention (days) field on the Global Settings page. However, the administrator can change the value as needed.
As of	Displays the time when the Session Manager dashboard was last updated.
Refresh 	Refreshes the data in the table. Depending on your requirements, you can refresh all or only the required rows of the table to load the latest values. - Refresh the entire table: Without selecting any check box click the Refresh icon. - Refresh the selected rows of the table: Select the check box of the required rows and click the Refresh icon. - Refresh all rows of the current page: Select the Current Page Row check box and click the Refresh icon.

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: 10.2.0.0.xxxxxxx

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

Server Ethernet ports

Server	Eth0 / NIC1	Eth1 / NIC2	Eth2 / NIC3
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640	Management Network/ Public bridge0 (eno1)	Services eno2	Out of band management bridgeOOB (eno3)
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R660xs	Management Network/ Public bridge0 (eno8303)	Services eno8403	Out of band Management bridgeOOB (eno12399)
Avaya Solutions Platform S8300	Management Network/ Public bridge0	Services enps10	Out of band management bridgeOOB (enp3s0)

* Note:

The above table reflects a customer who has their management and security module (public) on different IP ranges. If the management and public interface are on the same IP range, use the default KVM on RHEL NIC1 bridge0 setup. If you have multiple IP ranges, you must associate the NICs with different port groups. The Avaya PLDS posted ASP 130/S8300 Release 6.0 (KVM on RHEL 8.10) qcow2 file default with NIC1 for both management and public and NIC2 for the services port. Configure NIC3 if you are using OoBM.

NIC1: Session Manager Management (public). Session Manager uses this port for HTTP/SIP (Security Module).

Eth1 / NIC1: Session Manager services port.

Eth2 / NIC2: 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.

Customer account commands

The following is the list of commands that can be run by using the *cust* or *craft* login from the shell of the Session Manager server:

- `addCustAccount`
- `aideCheck`
- `aideDBupdate`
- `arp`
- `ASP_SSH`
- `ausearch`
- `av-update-os`
- `av-version`
- `backupSM`
- `badblocks`
- `certTool`
- `changeMgmtIP`
- `custAccounts`
- `dbadapt`
- `dbdigit`
- `dbent`
- `dbuser`
- `deleteCustAccount`
- `disableSSH`
- `dnat_failover.sh`
- `EASGManage`
- `EASGSiteCert`
- `EASGStatus`
- `edgeSetup`
- `enableSSH`
- `encryptionStatus`
- `encryptionPassphrase`
- `encryptionRemoteKey`

- encryptionLocalKey
- fips_mode.sh
- generateTestAlarmSM.sh
- getlogs
- getregsub
- hardware_info
- initDRS
- initTM
- kernel_opts
- logPrune.sh
- logRetention
- mii-diag
- mii-tool
- mountiso
- patchSM
- permanentEASGRemoval.sh
- pruneAllLogs
- rebootSM
- removeCustAccount
- restart
- restoreSM
- selinux
- setup_snmp
- setBootPassword
- setLoginBanner
- setSecurityPolicy
- shutdownSM
- sipsum
- sipTrace
- sm
- sm-report

- `smconfig`
- `SMnetSetup`
- `snfw-nft.sh`
- `sshkeys`
- `start`
- `statapp`
- `status_vm`
- `swversion`
- `tshark`
- `traceDebugMon.sh`
- `traceroute`
- `traceSM`
- `updateLogRetention.sh`
- `upgradeSM`
- `was`
- `wbl`
- `wjmap`
- `wjstack`

Accessing the root account

About this task

Use this procedure to access the root account.

This procedure is not necessary for Release 8.0.1 and later.

Procedure

1. Log in to the Session Manager command line interface using the customer credentials.
2. Run the following command:

```
[cust@sm ~]$ newrole -r unconfined_r
```

Note:

You must change the SELinux roles before switching users when using the customer account.

3. Enter the customer password.
4. Run the following command:

```
[cust@sm ~]$ su - root
```

 Note:

Run this command only if the **Enable Customer Root account** check box is selected while deploying Session Manager or Branch Session Manager using Solutions Deployment Manager and the root password is set.

5. Enter the root password.

Session Manager backup and restore commands

backupSM

```
# backupSM
```

You can run this command using the customer account or the services account. This command creates the `Session_Manager_backup.tgz` file and places it in the home directory of the account running the command. For example, if the `cust` user runs the command then the backup file is placed in `/home/cust`.

restoreSM

This command requires the path to the backup file generated using the **backupSM** command.

```
# restoreSM <path to backup file>
```

Loading and managing site certificate

About this task

Site certificates are used by the onsite technicians not having access to the Avaya network to generate a response to the Enhanced Access Security Gateway (EASG) challenge. The technician will generate and provide the site certificate to the customer. The customer must load this site certificate on each server (AVP Host) and virtual machine that the technician needs to access. Once this is done the technician can use EASG Site Manager to login with the EASG challenge. After the technician is done the customer can remove the site certificate from the server or they will be removed by the EASG software after the site certificate expires (~15 days later).

You can load a site certificate using `EASGSiteCertManage --add <pkcs7_file_path>`. You will need to specify a Site Authentication Factor (SAF). The SAF must be provided to the technician and is also used by EASG Site Manager to generate a response to the EASG challenge.

Before you begin

Customers must complete the following before loading and managing site certificates:

- Have a valid login and password.
- Use a tool such as WinSCP. Log in using a customer login, for example `cust`. Copy the certificate to `/home/cust` directory (where `cust` is the customer directory).
- Use a 10 to 20 character Site Authentication Factor (SAF) for instance 12345abcwxyz.
- Be familiar with CLI type shell commands.

Procedure

1. Log in to a Linux® shell by using the customer account.

The customer account is created during the deployment procedure.

2. To manage site certificates, type the following command:

```
[cust@host ~]$ EASGSiteCertManage --add johndoe.p7b
You are about to install this site certificate into your trusted repository:
Technician Name: johndoe
Expiration Date: Nov 10 17:02:15 2016 GMT
Do you want to continue [yes/no]? yes
Please enter a site authentication factor (SAF) for the technician to use
when getting access to your machine. The SAF is alphanumeric with at least 10
characters and no more than 20 characters.
  Please enter your SAF: Site Authentication Factor
  Please confirm your SAF: Site Authentication Factor
Site Certificate installed successfully.
```

Save the Site Authentication Factor to share with the technician once on site.

3. To display information about a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --show johndoe.p7b
Subject:      CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
User Name:    johndoe
Expiration:   Nov 10 17:02:15 2016 GMT
Trust Chain:
  1. O=Avaya, OU=IT, CN=AvayaITrootCA2
  2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
  3. O=Avaya LLC, OU=EASG, CN=EASG Intermediate CA
  4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya LLC
  5. CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
```

4. To remove a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
Successfully removed Site Cert: johndoe.p7b
```

Restricted commands for the Security Module

The Security Module is also known as SM100 and ASSET.

⚠ Caution:

Only use System Manager to manage the Security Module interface. *Do not use any Linux administration tools that involve the Security Module interface, other than status commands, on the Session Manager platform.*

The following Linux commands do not work correctly or persistently, and can cause Session Manager to enter an irrecoverable state. *Do not use the following commands:*

- `systemctl start/stop/restart network`
- `ifup`
- `ifdown`
- `route`
- `ip`
- `ethtool`
- `iptables`
- `nftables`

certTool

certTool is a command line tool to manage certificates by using Session Manager. You must use certTool to install trusted certificates if System Manager is using a third-party certificate.

To access the certTool, you can use both the customer account and all service accounts. When you run the certTool as a non-root user, customer password is required to prevent unauthorized access.

certTool options

Option	Description
-i --import <certificate file>	Specifies the certificate to import. The certificate file must be in the PEM format when the -trustedca option is used, and the certificate file must be in the PKCS#12 format when adding identity certificates.
-t --trustedca	Specifies the flag to indicate that the certificate must be added to the service truststore.

Table continues...

Option	Description
-s --service	Specifies the service to which the certificate must be applied. The values are: • sip • http • mgmt • db • spirit • syslog • all • tunnel Use the <code>all</code> option only to import trusted certificates. The <code>all</code> option adds the trusted certificate to every truststore. From Release 10.2, the network interface can be used to specify the set of services to be updated. • eth0 imports the certificate in all applications that use the eth0 interface. For example, mgmt, spirit, postgres, syslog, and tunnel. • eth1 is used for security module applications. For example, securitymodule_sip and securitymodule_http.
-p --passphrase	Provides the passphrase required to import PKCS#12 identity certificates.  Warning: Passing the certificate password using the command line records the password in shell history.
-h --help	Displays the usage and options.

Error codes

Code	Description
0	Success
1	Usage
2	File does not exist
3	Importing of ID certificate failed
4	Incorrect passphrase
5	User entered <code>no</code> while importing trusted certificate
6	User aborted
7	Import of trusted certificate failed

Related links

[Importing Identity certificate using certTool](#) on page 31

[Importing Trusted certificate using certTool](#) on page 31

Importing Identity certificate using certTool

About this task

Use this procedure as an example to import Identity certificate using certTool.

Procedure

1. Log in to the certTool command line interface.

2. Run the following command:

```
certTool --import mgmt.pl2 --service mgmt
```

3. When prompted, enter the PKCS#12 passphrase to complete the import.

You can also import additional Identity certificates before running the **init**™ command.

If the PKCS #12 files do not contain the certificate chain, you must copy the trusted CAs certificates to the `/opt/jboss/server/mgmt/conf/tm/trustedcerts` directory. These certificates must be in the PEM format.

4. Run the **init**™ command for the certificates to take effect.

You must restart the Session Manager before to use newly added certificates.

Related links

[certTool](#) on page 29

Importing Trusted certificate using certTool

About this task

Use this procedure as an example to import a Trusted certificate using certTool.

Procedure

1. Log in to the certTool command line interface.

2. Run the following command:

```
certTool --import AsmDevelopmentCA.pem --trustedca -s sip
```

3. On the command line interface, type `yes` to confirm the addition of certificate as a trusted certificate.

4. To add the certificate as a Trusted certificate to all applications, run the following command:

```
certTool --import AsmDevelopmentCA.pem --trustedca -s all
```

You must restart the Session Manager before to use newly added certificates.

General information

Related links

[certTool](#) on page 29

Chapter 5: Monitoring operations

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 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 selected log details, 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 column title to sort the column data 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.

Table continues...

Name	Description
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: The system is unusable. • Alert: Action must be taken immediately. • Critical: Critical conditions. • Error: Error conditions. • Warning: Warning conditions. • Notice: Normal but significant condition. • Informational: Informational messages. • Debug: Debug-level messages.  Note: The colors of severities do not indicate logging severities.
Event ID	The unique identification number assigned to the event that generated the log.
Message	A brief description of 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 generating the message, usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of several categories. These categories generally consist of the generating facility, 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	Displays 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 Wordpad or Excel.

Table continues...

Button	Description
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.
Advanced Search	The fields that you can use to specify the 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 on the previous page. This button is not available if you are on the first page.
Next	Displays the logs on 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 the 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, and service. • Severity: Severity level of the log. • Message: Brief description of the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device generating the message. • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories consist of the generating facility with the severity of the message. The second drop down list displays operators. Based on the search criteria that you select in the first drop down field, those applicable for the selected criteria 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 Calendar. 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 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 steps 4 through 6.
Click **-** to delete a search condition. You can delete a search condition if you have more than one.
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 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.

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. You can use this profile 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 must 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 for troubleshooting and diagnosing problems.

Accessing the Log Harvester service

Procedure

On the System Manager web console, click **Services > Events > Logs > Log Harvester**.

Creating a new log harvesting profile

About this task

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

Before you begin

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

- The hostname of the server on which the product is running.

If you do not see the hostname of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:

```
cd /opt/nortel/oam-logging
./configureSpiritAgentClient.sh <enrollment password>
```

The system now enrolls CS 1000 to the log harvester of System Manager.

- The product name

- The directories or the log files
- The filter text if you select one or more directories

*** Note:**

By default, harvesting is enabled for System Manager. All other products should always integrate and install their log harvesting extension packs during System Manager installation. After integration, they directly get their product type and files in System Manager in the drop down list on the Log Harvesting page.

Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, click **New**.
3. On the Create New Profile page, do the following:
 - a. In **Profile Name**, type the profile name.
 - b. In **Profile Description**, type a description of the profile.
4. Select the hostname 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 another instance of the same product running on the same server or a different server, click plus (+).
5. **(Optional)** If you select one or more directories, in the **File Name Filter** field, type a text pattern as the filter criteria.

During the harvesting operation, the system harvests those files that match the filter criteria.

6. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

Create New Profile field descriptions

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

Table continues...

Name	Description
Host Name	The host name of the servers on which products are installed. If you do not see the hostname of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command: <pre>cd /opt/nortel/oam-logging ./configureSpiritAgentClient.sh <enrollment password></pre> After typing a minimum of three characters, wait for three seconds to capture the final keyword and fetch the required results.
Product	The products for which you can harvest logs.
Directories	A list of directories that contain 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 system filters the log files present in the selected directory for harvesting. When you select the <code>/a/b/c</code> directory and type <code>com</code> in this field, the harvest operation for this profile harvests the log files in the directory <code>/a/b/c</code>. The log files contain <code>com</code> in the file name. The field does not support wild cards.

Button	Description
+	Displays 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 > Logs > Log Harvester**.
2. On the Log Harvester page, select a profile, and click **View**.

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

3. Click **Done**.

Filtering log harvesting profiles

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

Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the 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 match 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 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 > Logs > Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, type the relevant information in the **Archive Name** and **Archive Description** fields.

The system saves the harvested log files in the specified archive file.

4. Click **Run Profile** to send a request.

The table in the Harvest Criteria View section provides you the log harvesting request status. If the execution status of the request is successful, 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 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, in the Harvest Request Details section, click a request in the table.
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 those log harvesting requests that meet 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 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 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 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, in the Harvest Request Details section, click a request in the table.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.
The system lists the harvested log files.
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 product log file.

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 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, in the Harvest Request Details section, click a request in the table.
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

About this task

Use this procedure to view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
4. Click **Show Files**.
5. On the Search Archives page, navigate through the folders 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 stored in a zip file on the local server.

Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the 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, in the Harvest Request Details section, click a request in the table.
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 different servers.
 - If you select a host name of a server under a product, the system creates a zip file containing the harvested log files for the products running on the selected server.
 - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
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 compressed file.

Name	Description
Archive Name	The name of the archive file to create for storing 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 for storing harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of log harvesting requests.
Status	The status of log harvesting requests. The options are: • SUCCESS: System Manager successfully harvests the log messages. • FAILURE: System Manager fails to harvest the log messages for the product. • PARTIAL SUCCESS: 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 contains 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 log harvesting requests for selected profiles.
View	Displays the View Harvest detail page to view the details of selected log harvesting requests.
Show Files	Displays the Search Archives page to: • Search for text contained in the harvested log files. • Download log files of one or more products running on the same or different servers. • View the contents of log files.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under the column headers of the table that displays the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields to enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles 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	Displays 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	Displays the text, based on which, the log files present under a selected directory are filtered for harvesting. For example, if you select the directory <code>/a/b/c</code> and enter the text <code>com</code> in this field, the harvest operation for this profile harvests the log files that contain <code>com</code> in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and returns 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 to 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 if the contents of log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available if the contents of log files span across multiple pages.
Search	Searches for the text occurrences 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: System Manager successfully harvests the log messages. • FAILURE: System Manager fails to harvest the log messages for the product.
Request Description	Displays 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: System Manager successfully harvests the log messages. • FAILURE: 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	Displays a brief description of 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 returns to the Harvest Archives page.
Refresh	Refreshes the records in the table.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields to 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 to 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.

You can perform the following actions by using the Security Module Status page:

- **Reset** : Reset 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 being reset.

- **Synchronize**: Synchronize the administered configuration with the configuration information stored on the security module.
- **Connection Status**: Display 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 whether Session Manager must be taken out of service.
 - Determining whether links are secure or not.
 - Viewing link details and statistics.

Viewing the Security Module status

About this task

Use this procedure to view the security module status.

Possible causes for the security module status to be **Down** include:

- The security module might have recently been reset. A reset can take several minutes to complete.

- The security module might not have received security module configuration information from System Manager.

Procedure

1. On the System Manager web console, click **Elements > Session Manager**.
2. If the security module state of Session Manager does not display as **Up**:
 - a. Click the status text of the security module for Session Manager to display the Security Module Status page.
 - b. Verify that the IP address of Session Manager is correct.
 - c. Select the Session Manager instance.
 - 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

Name	Description
Session Manager	The list of administered Session Manager instances. A warning symbol after the name indicates that the Session Manager or Branch Session Manager instance is in the Maintenance Mode service state.
Type	The type of Session Manager or Branch Session Manager instance.
Status	The status of the security module for Session Manager. The options are: *up * down
Connections	The total number of connections for the security module.
IP Address	The IP address of the security module used for SIP traffic. This field must match the address administered on the SIP Entity form for the Session Manager instance.
VLAN	The VLAN ID associated with the security module.
Default Gateway	The default gateway used by the security module. This value must match the default gateway administered on the Session Manager instance form.

Table continues...

Name	Description
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 must match. If these values do not match, you must investigate the synchronization issue.
Certificate Used	The type of certificate in use.
Reset	The field to reset the selected Session Manager instance.
Synchronize	The field to synchronize the security module of the selected Session Manager.
Connections Status	The field to display the connection status information for the selected Session Manager instance.

Connection Status

Using the Connection Status page, you can 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 whether Session Manager must be taken out of service.
- Determining whether links are secured or not.
- Viewing link details and statistics.

Monitoring Connection Links

Procedure

1. On the System Manager web console, click **Elements > 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.

Table continues...

Name	Description
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.
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 54

[SIP Entity Link Monitoring Status Summary page field descriptions](#) on page 54

Viewing the SIP Monitoring Status Summary page

About this task

Use this procedure to view the status of the entity links for all the administered Session Manager instances.

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, click **Elements > Session Manager > System Status > SIP Entity Monitoring**.

Related links

[Session Manager SIP Entity Monitoring](#) on page 53

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.

Table continues...

Field	Description
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.
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 53

Session Manager SIP Tracing

SIP Tracing allows tracing of SIP messages between the Session Manager server and remote SIP entities.

SIP Tracing consists of the following 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. The SIP tracer, logs incoming and outgoing SIP messages. It also logs SIP messages that are dropped by any security component such as SIP firewall.

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 in the **Max Message Count** field so that the security module can capture packets.

SIP Tracer Configuration

From the SIP Tracer Configuration page, you can configure tracing properties for one or more security modules. You can view the output of the SIP Tracer on the System Manager web console. Session Manager overwrites the existing Tracer configuration when Session Manager receives a new Tracer configuration. Enabling SIP traces from the SIP Tracer Configuration page invokes traceSM in the background.

The SIP Tracer Configuration page contains the following sections:

- **Tracer Configuration:** Attributes that control the basic functionality of the SIP Message tracer. You can enable or disable the attributes.
- **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:** The administered Session Manager instances on which to apply the filters.

Related links

[SIP tracing and Call Processing logs](#)

Tracer Configuration field descriptions

Session Manager Instances

Name	Description
Name	Select one or more configured Session Manager instances for which the specific filters should be used.  Note: When you select a Session Manager from the list, the View button is activated. You can 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.
Syslog Server 1	Specifies the Syslog server 1 configuration, if configured.
Syslog Server 2	Specifies the Syslog server 2 configuration, if configured.
Description	Specifies the details of the Session Manager configuration.

Button	Description
View	Retrieves the current trace configuration details for the selected Session Manager and displays the details on the Trace Configuration page.
Commit	Saves the configuration changes.

Tracer Configuration

Name	Description
Tracer Enabled	Enable or disable SIP message tracing. The default is enabled. If Tracer Enabled is disabled, the system disables all the check boxes. If the syslog server configuration and SIP Tracer is enabled for the Session Manager instance, then SIP trace information is also sent to a remote syslog server.
Trace All Messages	Enable or disable SIP message tracing for all SIP messages. If Trace All Messages is disabled, the system disables all the check boxes.
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.

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

Table continues...

Name	Description
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 .@122.111.11.

Configuring SIP tracing Procedure

1. On the home page of the System Manager web console, click **Elements > Session Manager > System Tools > SIP Tracer Configuration**.

2. In the **Tracer Configuration** section of the page, enable or disable the configuration attributes.
3. Set a user filter or call filter, or delete a filter.
4. In the Session Manager Network section, select one or more of the administered Session Manager instances.

SIP Tracer applies filters to the selected Session Manager instances. SIP Tracer overwrites any previous filter configurations.
5. Click **Commit**.

Filtering by user

About this task

Use this procedure to filter messages by using the user filter. 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 or To field.

Procedure

1. On the home page of System Manager web console, click **Elements > 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 to be traced.

You must add at least a user filter or call filter in the **Max Message Count** field so that the security module can 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 System Manager web console, click **Elements > 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 System Manager web console, click **Elements > 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

About this task

Use this procedure to view trace logs. You can set filters to display trace logs within a certain time range. Due to the filter options, SIP Tracer displays trace records multiple times.

Procedure

1. On the System Manager web console, click **Elements > Session Manager > System Tools > SIP Trace Viewer**.
2. To filter trace logs for a range of hours or days, click **Filter** and enter the date, time, time zone information in the From and To areas.

Using this filter criteria, the SIP Tracer displays only the logs with a time stamp between the From and To values.
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.
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.

Table continues...

Name	Description
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. To view the file, use 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

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 syslogd (syslog server)

Configuring an unsecure UDP syslog server

Procedure

1. Configure the firewall to accept logs on UDP port 514. 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:

If you plan to send logs from more than one Session Manager, you need to add a rule for each IP address.

```
firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -s 1.2.3.4 -p udp --dport 514 -j ACCEPT
firewall-cmd --direct --permanent --add-rule ipv4 filter 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.conf` with your favorite editor.
- b. Add the following line to the end of the file:

```
local2.info -/var/log/tracer.log
```

- c. Write the file and close it.

3. Enable logging from a remote system to syslog UDP port 514:

- a. Open the `/etc/sysconfig/syslog` file 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. Run the `service syslog restart` command to restart the syslog service.
- e. Run 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 that 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
 - syslogd

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. Run the following command to configure the firewall to accept connections/logs on UDP port 514.

```
firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -i lo -p udp --dport 514 -j ACCEPT
firewall-cmd --direct --permanent --add-rule ipv4 filter 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:

```
firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -s 1.2.3.4 -p tcp --dport 50614 -j ACCEPT
firewall-cmd --direct --permanent --add-rule ipv4 filter 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. Run the command `service syslog restart` to restart the syslog service.
 - e. Run 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 -O -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 real-time managed bandwidth data. Administrators can use this data to manage networks with multimedia calls. The page displays a read-only table containing one row for each administered location. It also provides details about actual call counts and bandwidth usage for audio and video calls respectively.

You can expand each row to see 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

Procedure

1. On the home page of System Manager web console, click **Elements > Session Manager > System Status > Managed Bandwidth Usage**.
2. In the Details column, click **Show**.

The application displays the bandwidth usage information of the Session Manager instance in that location.

3. Click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

Use the Managed Bandwidth Usage page to view the system wide bandwidth usage information. If no bandwidth management is implemented, the fields in this table remain blank.

Name	Description
Details	The breakdown of usage among the administered Session Manager instances 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	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.

Table continues...

Name	Description
Multimedia BW Used	The bandwidth used for multimedia calls of Session Manager instances in a given location.
Multimedia BW Allow	The 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	The 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.

Name	Description
Session Manager	The name of the Session Manager instance. A warning symbol indicates the Session Manager instance is in the Maintenance Mode service state.
Audio Call Count	The number of audio calls terminated by the selected Session Manager for the given location.
Audio BW Used	The sum of bandwidth used by audio calls terminated by the selected Session Manager for the given location.
Multimedia Call Count	The 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 instance 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.

Log retention

You can view the number of days Session Manager has been administered to retain application and system logs.

For more information, see *Administering Avaya Aura® Session Manager* and *Avaya Aura® Session Manager Data Privacy Guidelines* from the Avaya Support website at <https://support.avaya.com>.

logRetention command

The **logRetention** utility displays the currently administered log retention time.

Syntax

```
logRetention [-a] [-c] [-d] [-h -g -l -v -h | ? ]
```

- a** Displays all log retention time settings.
- c** Displays current log retention time from database.
- d** Displays default log retention time.

- g** Displays global log retention time (blank if unavailable).
- l** Displays local log retention time (blank if unavailable).
- v** Verify current log retention configuration.
- h | ?** Displays help options.

smconfig command

The **smconfig** command will include the administered log retention time in its output.

If the Session Manager has overridden the global settings, both the local and overridden log retention values will be displayed.

Syntax

```
smconfig
```

- v** displays Branch Session Manager information.

Data encryption commands

The following CLI commands are available to make changes to the data encryption settings.

For more details on administering data encryption, refer to *Administering Avaya Aura Session Manager 8.1.x* and *Avaya Aura Session Manager Data Privacy Guidelines, Release 8.1.x*.

Related links

[Viewing data encryption status](#) on page 74

encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

Syntax

```
encryptionPassphrase [add | change | remove | list]
```

- add** Displays the prompts to add the encryption passphrase.
- change** Displays the prompts to change the encryption passphrase.
- remove** Removes the encryption passphrase.
- list** Displays the encryption passphrase and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding encryption passphrase

About this task

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase add**.
3. In **Enter existing passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

Changing encryption passphrase

About this task

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase change**.
3. At the prompt, in **Current Passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

The application displays the following message.

```
Passphrase successfully changed.
```

Removing encryption passphrase

About this task

Use the **encryptionPassphrase remove** command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

```
The last passphrase cannot be removed!
```

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase remove**.
3. At the prompt, in **Passphrase to remove**, type the existing encryption passphrase.

The application displays the following message.

```
Passphrase successfully removed.
```

Displaying encryption passphrase and slot assignment

About this task

Use the **encryptionPassphrase list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase list**.

The application displays the details based on the system configuration.

Slot	Status	Passphrase/Remote Server
Key Slot 0:	ENABLED	Passphrase
Key Slot 1:	ENABLED	Passphrase
Key Slot 2:	ENABLED	Passphrase
Key Slot 3:	ENABLED	Passphrase
Key Slot 4:	ENABLED	Passphrase
Key Slot 5:	Disabled	empty
Key Slot 6:	Disabled	empty
Key Slot 7:	Disabled	empty
.....		
.....		
.....		
Key Slot 31:	Disabled	empty

encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

Syntax

```
encryptionRemoteKey [add | remove | list]
```

- | | |
|---------------|---|
| add | Displays the prompts to add the remote key server. |
| remove | Removes the remote key server. |
| list | Displays the remote key server and slot assignment. |

Considerations

You must deploy the application with data encryption.

Adding remote key server

Before you begin

Ensure that the remote key server is configured and accessible.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey add** <Address> <Port>.

Where:

Address is the IP address or FQDN of the remote key server.

Port is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.

3. In **Enter existing passphrase**, type the existing encryption passphrase.

If the remote key server is not configured, the application displays the following message.

```
Remote key server not found
```

If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

Removing remote key server

About this task

Use the **encryptionRemoteKey remove** command to remove the existing remote key server.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey remove** <Address>.

Where:

Address is the IP address or FQDN of the remote key server.

You must use the same IP address or FQDN value that you used to add the remote key server.

3. In **Passphrase**, type the existing encryption passphrase.

The application removes the remote key server and displays the following message:

```
RemoteKey successfully removed.
```

Displaying remote key server and slot assignment

About this task

Use the **encryptionRemoteKey list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey list**.

The application displays the details based on the system configuration.

Slot	Status	Passphrase/Remote Server
Key Slot 0:	ENABLED	Passphrase
Key Slot 1:	ENABLED	<IP Address of Remote Key Server>
Key Slot 2:	ENABLED	Passphrase
Key Slot 3:	DISABLED	empty
Key Slot 4:	DISABLED	empty
Key Slot 5:	DISABLED	empty
Key Slot 6:	DISABLED	empty
Key Slot 7:	DISABLED	empty
.....		
.....		
.....		
Key Slot 31:	DISABLED	empty

encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

Syntax

```
encryptionLocalKey [enable | disable]
```

enable Enables the local key store.

disable Disables the local key store.

Considerations

You must deploy the application with data encryption.

Enabling local key store

About this task

Use the **encryptionLocalKey enable** command to enable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey enable**.

3. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.
If the local key store is already enabled, the application displays the following message.
`Local key store is already enabled.`

Disabling local key store

About this task

Use the **encryptionLocalKey disable** command to disable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey disable**.
The application displays the following message.
`Local keystore removed`
`Local Key Store is now disabled.`

Viewing data encryption status

About this task

The **encryptionStatus** command displays information about encryption on the system.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionStatus**.
3. When the system prompts, type the password.

For example, if the local key store is configured, the system displays the following status:

```
Data Encryption: enabled
Local Key Store: enabled
Encryption Passphrase Required at Boot-time: no
```

For example, if the remote key server is configured, the system displays the following status:

```
Data Encryption: enabled
Local Key Store: disabled
Encryption Passphrase Required at Boot-time: yes
remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
```

Related links

[Data encryption commands](#) on page 69

Data replication

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

About this task

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

About this task

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.

From Release 8.1, you can repair more than one replica nodes of a replica group.

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 to 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 one or more replica node, and click **Repair**.

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

Repairing all replica nodes in a replica group

About this task

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.

Table continues...

Button	Description
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.

Table continues...

Name	Description
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 Polling: 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 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

Table continues...

Name	Description
	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 Capable	Displays whether the replica node is GR-capable 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	Displays 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 selected nodes from the replica group.
Remove From Queue	Removes the selected replica node from the queue.
Show All Replica Groups	Returns to the Replica Groups page.
Advanced Search	The link to perform advance search. When you click on this link, System Manager displays the Criteria section.
Filter: Enable	The fields where you can set the filter criteria. Filter: Enable is a toggle button.
Filter: Disable	Hides the column filter fields. Filter: Disable is a toggle button.
Filter: Apply	Filters replica nodes based on the filter criteria.
Select: All	Selects all replica nodes in the table.
Select: None	Clears the selection for the users that you select.
Refresh	Refreshes the replica node information in the table.

Criteria

Name	Description
Select Search Criteria	The options are: • Replica node name • Synchronization time • Synchronization Status

Table continues...

Name	Description
Select Search Operator	The options are: • Equals • Not Equals • Starts with • Ends with • Contains
Enter Search to Text	Specify the search criteria.

Button	Description
-	Removes the additional search criteria fields. This field is enabled when the additional search criteria fields are added.
+	Adds the additional search criteria fields.
Clear	Clears the search criteria.
Search	Performs the search for the specified search criteria
Close	Closes the Criteria section.

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.

Table continues...

Name	Description
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 Capable	Displays whether the replica node is GR-capable 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 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.

Table continues...

Name	Description
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 - 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.

Button	Description
Refresh	Refreshes the Replication Node details.
Done	Returns to the Replica Nodes page.

User Data Storage and Data Center management

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

User Data Storage stores the call logs, contacts, device data, and other user-related data for users associated with the specific Session Manager instance.

* Note:

The User Data Storage backup is not related to the System Manager backup.

Related links

[Viewing the User Data Storage status](#) on page 85

Viewing the User Data Storage status

About this task

Use this procedure to view the User Data Storage status of the selected Session Manager instance.

Procedure

1. On the home page of the System Manager web console, click **Elements > Session Manager > System Status > User Data Storage**.
2. Click the Session Manager instance whose status you want to view.

If the selected Session Manager instance is in the Maintenance mode, the System Manager web console displays the following message:

No status details while in Maintenance Mode

The System Manager web console displays the User Data Storage status of the selected Session Manager instance.

Related links

[User Data Storage and Data Center management](#) on page 84

HTTP proxy commands

Under normal circumstances, Session Manager automatically enables firewall access and verifies whether the administered HTTP Proxies are accessible.

The following CLI commands are available to make changes and monitor the HTTP proxy configuration if the HTTP Proxies are not working as expected.

For more information about administering HTTP proxy, see *Administering Avaya Aura® Session Manager*.

Related links

[httpProxyAccess command](#) on page 85

[checkHttpProxy command](#) on page 87

httpProxyAccess command

Using the `httpProxyAccess` command, you can enable or disable firewall access.

Syntax

```
httpProxy proxyAddress [--enableFirewall | --disableFirewall | --checkFirewall] [--
interface <networkInterface>] [--silent | --verbose]
```

proxyAddress

<IPv4Address or FQDN>:<port>

--enableFirewall	Firewall access enabled.
--disableFirewall	Firewall access disabled.
--checkFirewall	Verify the Firewall status.
--networkinterface	eth0 or eth1 or IP address. Default value is eth0.
--silent	Suppresses output.
--verbose	Displays additional details.

Related links

[HTTP proxy commands](#) on page 85

[Enabling HTTP proxy access](#) on page 86

[Disabling HTTP proxy access](#) on page 86

[Checking HTTP proxy access](#) on page 87

Enabling HTTP proxy access

About this task

Use the command `httpProxyAccess` to enable firewall access to the specified HTTP proxy address.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type the following:

```
httpProxyAccess <proxyAddress> --enableFirewall
```

For example,

```
$ httpProxyAccess smhttpproxy.com:3128 --enableFirewall
```

Related links

[httpProxyAccess command](#) on page 85

Disabling HTTP proxy access

About this task

Use the command `httpProxyAccess` to disable firewall access to the specified HTTP proxy address.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type the following:

```
httpProxyAccess <proxyAddress> --disableFirewall
```

For example,

```
$ httpProxyAccess smhttpproxy.com:3128 --disableFirewall
```

Related links

[httpProxyAccess command](#) on page 85

Checking HTTP proxy access

About this task

Use the command `httpProxyAccess` to check firewall access to the specified HTTP proxy address.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type the following:

```
httpProxyAccess <proxyAddress> --checkFirewall
```

For example,

```
$ httpProxyAccess smhttpproxy.com:3128 --checkFirewall
```

Related links

[httpProxyAccess command](#) on page 85

checkHttpProxy command

Using the `checkHttpProxy` command, you can check whether a given HTTP proxy is accessible.

Syntax

```
checkHttpProxy proxyAddress [--auth <authType>] [--user <proxyUser>] [--password <proxyPassword>] [--interface <networkInterface>] [--timeout <proxyTimeout>] [--tries <proxyTries>] [--silent | --verbose]
```

proxyAddress	<IPv4Address or FQDN>:<port>
--auth <authType>	Authorization type is none or basic. Default value is none.
--user <proxyUser>	HTTP Proxy username for basic authentication.
--password <proxyPassword>	HTTP Proxy password for basic authentication.
--interface <networkInterface>	eth0, eth1 or IP address. Default value is eth0.
--timeout <proxyTimeout>	1 to 9999 seconds. Default value is 1.
--tries <proxyTries>	1 to 9999 tries. Default value is 1.
--silent	Suppresses output.

--verbose

Displays additional details.

Related links

[HTTP proxy commands](#) on page 85

[Checking the accessibility of the HTTP proxy](#) on page 88

Checking the accessibility of the HTTP proxy

About this task

Use the command `checkHttpProxy` to check whether the HTTP proxy is accessible.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type:

```
checkHttpProxy proxyAddress
```

Few examples:

- `$ checkHttpProxy smhttpproxy.com:3128`
- `$ checkHttpProxy 10.179.179.83:3130 --auth basic`
- `$ echo password | checkHttpProxy smhttpproxy.com:3130 --auth basic --user username`
- `$ checkHttpProxy smhttpproxy.com:3130 --auth basic -user username`
- `$ checkHttpProxy smhttpproxy.com:3128 --auth basic --user invalid --password invalid`

If the HTTP Proxy does not require authentication, the username and password are ignored.

Related links

[checkHttpProxy command](#) on page 87

Chapter 6: Verification testing

Session Manager maintenance tests

You can perform tests on the System Manager server and the administered Session Manager instances by using the Maintenance Tests page on the System Manager web console. The maintenance 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 not responding.

Maintenance Tests field descriptions

Name	Description
Select System Manager or Session Manager to test	To select the System Manager or Session Manager instance on which to perform the maintenance tests.

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

Name	Description
Test Description	The description of the test.
Test Result	The output of the test performed on System Manager or the selected Session Manager.
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..`

Running maintenance tests

About this task

Use this procedure to run maintenance tests on System Manager or any configured Session Manager or Branch Session Manager.

Procedure

1. On the System Manager web console, click **Elements > 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.
3. Do one of the following:
 - To run all the tests, select **Execute All Tests**.
 - To run specific tests, select the tests you want to run, and click **Execute Selected Tests**.
4. Verify that 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 Load Factor status

Note:

This test is applicable for Session Manager and Branch Session Manager instances running on release 10.1.x or later.

This test will generate alarms when the threshold value exceeds the value given in the **Load Factor Alarms Threshold (80 - 150)** field on the Global Settings page. The test will also generate alarms when the threshold is overridden for a particular Session Manager.

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 Push Notification provider availability

Note:

If the mobile push notification feature is enabled on the Global Settings page, you can run this test. This test is applicable only for core Session Manager instances that are running on release 8.1.3 or later.

This test verifies that Session Manager can connect with the push notification provider and sends a test notification to the application for validation. If the application receives the test notification, the test passes.

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.

Verifying the System Manager and Session Manager or Branch Session Manager installation

About this task

Use this procedure to verify that System Manager, Session Manager and Branch Session Manager are installed and configured properly and the servers and applications are communicating.

Procedure

1. On the home page of the System Manager web console, click **Elements > Session Manager > System Tools > Maintenance Tests**.

2. In the **Select System Manager or a Session Manager to test** field, select the System Manager or the administered Session Manager or Branch Session Manager that you want to test.
3. Click **Execute All Tests**.
4. Verify that all tests display `Success`.
5. On the home page of the System Manager web console, click **Elements > Session Manager > System Status > Security Module Status**.
6. Verify that the status is **Up** for the deployed Session Manager or Branch Session Manager.
7. Verify that the IP address is correct.
8. If the status is **Down**, reset the security module:
 - a. Select the appropriate Session Manager or Branch Session Manager from the table.
 - b. Click **Reset**.



Warning:

Session Manager or Branch Session Manager cannot process calls while the security module is restarted.

9. On the home page of the System Manager web console, click **Elements > Session Manager > Dashboard**.
10. On the Session Manager Dashboard page, verify that the installed software versions of all Session Managers are same.
11. On the home page of System Manager web console, click **Elements > Session Manager > System Tools > Maintenance Tests**.
12. Select the appropriate Session Manager instance that you want to test.
13. Click **Execute All Tests**.
14. Verify that all tests display **Success**. wrong tag
15. Check the replication status of the Session Managers:
 - a. On the home page of System Manager web console, click **Services > Replication**.
The **Synchronization Status** must be green and the status must be **Synchronized**.
 - b. If the status is not **Synchronized**, select the check box next to **Session Managers** and click **View Replica Nodes** to determine which Session Manager is not synchronized with System Manager.
16. On the home page of the System Manager web console, click **Services > Events > Alarms** to verify that there are no active alarms for Session Manager.
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 94.

18. For Geographic Redundant systems:

- a. On the home page of the System Manager web console, click **Services > Inventory > Managed Elements**.
- b. Verify that the managed elements in the **Managed by** column display the correct value of the managing System Manager.

Generating a test alarm

About this task

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`.
2. If using the **Generate Test Alarm** button on the Serviceability Agents screen:
 - a. On the System Manager web console, click **Services > 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, click **Services > 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.

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

SIP INVITE parameters

Name	Description
Calling Party IP Address	IP address from which the INVITE is received. The Calling Party Address field accepts: • IPv4 address • IPv6 address  Note: You can enter IPv6 addresses only if you have selected the Enable IPv6 field on the Global Settings screen.

Table continues...

Name	Description
Calling Party URI	SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. The Calling Party URI field accepts: • IPv4 address • FQDN or hostname • IPv6 address enclosed in square brackets ([]) You can enter IPv6 addresses only if you have selected the Enable IPv6 check box on the Global Settings page. • String and @ followed by a valid IPv6 address enclosed in ([]) For example, 5552000@[2001:cdba::3257:9652].
Called Party URI	SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. The Called Party URI field accepts: • IPv4 address • FQDN or Hostname • IPv6 address enclosed in square brackets ([]) You can enter IPv6 addresses only if you have selected the Enable IPv6 check box on the Global Settings page. • String and @ followed by a valid IPv6 address enclosed in ([]) For example, 5552000@[2001:cdba::3257:9652].
Day of Week	Day of the week. Call times can influence routing policies.
Time (UTC)	Time. Call times can influence routing policies.
Called Session Manager	The Session Manager instance that receives the initial INVITE from the calling party.  Note: These are core Session Manager and Branch Session Manager instances.
Transport Protocol	The transport protocol used by the calling party, which may impact routing options. The Call Routing Test uses this field to test the routing based on entity links.
Session Manager Listen Port	Port on which the called Session Manager instance receives the INVITE.

Name	Description
SIP headers	The number of SIP headers inserted into the SIP INVITE request created by the call routing test.
Attachment	The Content-Type and content of an attachment inserted into the SIP INVITE request created by the call routing test.

 Note:

SIP headers and **Attachment** fields are valid only for Session Manager Release 8.1.1 and later.

Button	Description
Execute	Carries out the routing test based on the parameters that you provide. When you perform a Call Route Test on Session Manager Release 8.1.1, Session Manager displays an invite message. The Invite Message section displays the Original invite and Modified invite tabs along with a Difference tab which highlights the changes made between the Original and Modified invite messages. Both Original and Modified invite messages have line numbers to help you evaluate the changes made to the message. The Routing Decisions section displays the result of the routing test. The result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice, and the lines are displayed in the same order that the test attempted to test the destinations. Each line displays the following information: • Destination of the invite. • The adapted digits of the invite. • The domain of the invite. The Routing Decision Process section contains information about how the Session Manager made the routing decisions. This tool allows you to test your routing administration.
Reset	Resets and clears all the SIP INVITE parameters that you provide on the screen.

Invite Message section

Name	Description
Original	Displays the original invite message.
Modified	Displays the modified invite message.
Difference	Displays the difference along with the line numbers between original invite and modified invite messages.

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.

Chapter 7: Maintenance functions

Planning network outage or service maintenance

About this task

This procedure provides the high-level steps to perform before and after a planned outage or service maintenance of Session Manager.

Procedure

1. Change the state of the Session Manager instance to **Deny New Service**.
 - a. From the System Manager web console, select **Elements > Session Manager > Dashboard**.
 - b. On the Session Manager Dashboard page, select the required Session Manager name from the table.
 - c. Click the **Service State** drop-down.
 - d. From the drop-down menu values, select **Deny New Service**.
 - e. On the confirmation page, click **confirm**.
2. Shut down the Session Manager.

Note:

Skip this step if you are planning to upgrade the Session Manager.

- a. From the System Manager web console, select **Elements > Session Manager > Dashboard**.
 - b. On the Session Manager Dashboard page, select the required Session Manager name from the table.
 - c. Click the **Shutdown System** drop-down.
 - d. From the drop-down menu values, select **Shutdown**.
 - e. On the confirmation page, click **confirm**.
3. Perform the required maintenance procedure.
4. Power on the Session Manager virtual machine from the vSphere web console.

 Note:

Perform this step if you performed step 2 of this procedure.

To start the Session Manager virtual machine, perform one of the following options:

- Right-click the virtual machine and click **Power > Power On**.
- On the Inventory menu, click **Virtual Machine > Power > Power On**.

The Session Manager virtual machine is powered on.

5. Verify if Session Manager is working as expected. Test the Session Manager and run the maintenance tests.
6. Change the state of the Session Manager instance to **Accept New Service**.
 - a. On the System Manager web console, select **Elements > Session Manager > Dashboard**.
 - b. On the Session Manager Dashboard page, select the required Session Manager name from the table.
 - c. Click the **Service State** drop-down.
 - d. From the drop-down menu values, select **Accept New Service**.
 - e. On the confirmation page, click **confirm**.

Maintenance functions

The maintenance functions for Session Manager include the following:

- Backing up data
- Restoring backed up data
- Shutting down the server
- Rebooting the server

Backup and Restore

The backup and restore functions run on System Manager.

System Manager creates one backup file that contains all the data for the entire system. You do not need to create individual backup files of all the Session Manager instances. The data and configuration files for the entire system are stored centrally on System Manager.

System Manager supports local backup and remote backup. You can transfer backup files by using the sftp or scp protocol.

You can perform either a backup or a restore operation at a specified time. The restore operation fails if a backup operation is in progress. When a restore operation is in progress, the system

ignores all backup jobs that are scheduled at that time. System Manager displays a warning if you attempt to restore a corrupted or tampered backup file.

 Note:

You can only restore a data file on the same software version on which the backup was taken. However, when you upgrade to a newer release of System Manager, the system preserves the data. If an upgrade failure occurs, System Manager rolls back to the previous configuration.

Backup and Restore field descriptions

Name	Description
Operation	The type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, the name of the backup file. • For the restore operation, the name of the backup file that was used for the restore.
Path	• For the backup operation, the path of the backup file. • For the restore operation, the path of the backup file that was used for the restore.
Status	The status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	The error details of the backup or restore operation that has failed.
Operation Time	The time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	The user who performed the operation.

Button	Description
Backup	Displays the Backup page from where you can back up the System Manager data.
Restore	Displays the Restore page from where you can restore the data to System Manager.

Schedule Backup field descriptions

Use this page to schedule a job for backing up data by specifying the date and time.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field also displays the time interval of recurrence. The options are: • Execute task one time only. • Tasks are repeated. The system generates an alarm if you do not schedule a System Manager backup every 7 days.
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

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

Creating a data backup on a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In **File name**, type the backup file that you want to create.
5. **(Optional)** To create encrypted backup using encryption password, do the following:
 - a. Clear the **Use Global Backup Encryption Password** check box.

System Manager displays the following fields:

- **Backup Encryption Password**
- **Confirm Backup Encryption Password**

- b. In **Backup Encryption Password**, type the encryption password.
- c. In **Confirm Backup Encryption Password**, retype the encryption password.

You must remember the password to restore the backup.

6. Click **Now**.

If the backup is successful, the Backup and Restore page displays the message: Backup job submitted successfully. Please check the status detail below!!

Scheduling a data backup on a local server

Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the name of the backup file that you want to create.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
 - Job name
 - Date and time when the system must run the job
 - Frequency at which the system must run the job
 - Range
7. Click **Commit**.

Viewing pending jobs

Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. In the navigation pane, click **Pending Jobs**.
3. To view the details of the job, on the Pending Jobs page, select a pending job and click **View**.

The Job Scheduling-View Job page displays the details of the selected job.

Pending Jobs field descriptions

Name	Description
Job Type	The type of job represented by a job type icon. The types of job with icons are: 1.  System scheduled job. 2.  Admin scheduled job. 3.  On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.
Element	The element name for which the job is executed. For example, Communication Manager and its IP, if the job is for some specific Communication Manager.

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

Table continues...

Button	Description
Filter: Enable	Displays fields under select columns that you can use to set 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 pending jobs based on the filter criteria.
Select: All	Selects all the pending jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	Refreshes the pending job information.

Criteria section

To view this section, click **Advanced Search**. You can find the **Advanced Search** link at the at the upper-right corner of the page.

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

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

Viewing list of backup files

Procedure

On the System Manager web console, click **Services > Backup and Restore**.

Result

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

Restoring data backup from a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

 Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you must restore.

If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

 Note:

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. **(Optional)** To restore encrypted backup using encryption password, do the following:
 - a. Clear the **Use Global Backup Encryption Password** check box.
System Manager displays the **Backup Encryption Password** field.
 - b. In **Backup Encryption Password**, type the encryption password.

6. Click **Restore**.

On the Restore Confirmation page, the system displays the following message:

The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

7. Click **Continue**.

The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Restoring data backup from source Session Manager with a different IP/FQDN

About this task

Use this procedure to restore data backup from Session Manager with a different IP address or FQDN.

Procedure

1. On a remote server, take a backup of the source Session Manager database with IP1 / FQDN1 as its address.
2. Shutdown the source Session Manager.
3. Deploy new Session Manager with IP2 / FQDN2 as its address.
4. On the new Session Manager, restore the source Session Manager database from the remote server.
 - The information of the IP1 address is not restored.
 - The information of FQDN1 is restored.
5. Change the FQDN1 value to FQDN2 on the new Session Manager as follows:
 - a. Log in to the console of the new Session Manager instance through SSH.
 - b. Type **SMnetSetup**.
 - c. Change the FQDN of new Session Manager from FQDN1 to FQDN2.

Next steps

Do the following changes on System Manager and Communication Manager consoles:

- Edit the Management IP and SIP IP of Session Manager to the new IP address on System Manager. For more information on management and SIP IP's administration, see *Administering Avaya Aura® System Manager*.
- Edit node name IP of Session Manager to new IP address on Communication Manager. For more information on node name IP administration, see *Administering Avaya Aura® Communication Manager*.

Backup data retention

When a new backup is initiated and the maximum number of files is reached, the system removes the oldest backup file to make room for the new backup file.

To perform the scheduled backup on the System Manager server, you must delete the older backup files from the system as the filename is dependent on the scheduled job.

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

Changing the Maximum Backup Files value

About this task

The new value for **Maximum Backup Files** is effective from the next backup is run.

Procedure

1. On System Manager Web Console, click **Services > Configurations > Settings > SMGR > SMGR Element Manager**
2. Click **Edit** at the top right of the page.
3. In the **Maximum Backup Files** field, enter the number of backup files you want to keep.

4. Click **Commit** to save the change.

hardware_info command

The **hardware_info** command displays detailed information about the Session Manager.

Example output:

```
[cust ~]$ hardware_info
[System Information]
  Manufacturer: VMware, Inc.
  Product Name: VMware Virtual Platform

[CPU Information]
  CPU #0
    Model:
    MHZ: 2933.437
    Cores: 1
  CPU #2
    Model:
    MHZ: 2933.437
    Cores: 1
  CPU #4
    Model:
    MHZ: 2933.437
    Cores: 1
  CPU Reservation: 3950 MHz

[Memory Information]
  Total RAM: 3145728 kB
  Memory Reservation: 3072 MB

[Disk Information]
  KNAME MOUNTPOINT TYPE FSTYPE      SIZE RO
  sr0                                46K  0
  sda                                80G  0
  sda1 /boot          part ext3        200M  0
  sda2 [SWAP]      part swap         8G  0
  sda3                                part LVM2_member 71.8G  0
  dm-0 /           lvm  ext4        21.5G  0
  dm-2 /home       lvm  ext4         7.2G  0
  dm-3 /tmp        lvm  ext4         7.2G  0
  dm-4 /var        lvm  ext4        35.8G  0
  sdb                                10G  0
  sdb1                                part LVM2_member 10G  0
  dm-1 /data       lvm  ext4         10G  0

[Network Information]
  eth0:
    IP: 10.64.22.41
    Link detected: yes
  eth1:
    IP: 10.64.22.42
    Link detected: yes
```

Replacing server components

This procedure provides the high-level steps for replacing a server component. For more information, see the documentation for the specific server.

Procedure

1. Change the state of the Session Manager instance running on a VMware ESXi host to **Deny New Service**:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
 - b. On the Session Manager Dashboard page, select the appropriate Session Manager name from the table.
 - c. Click **Maintenance Mode**.
 - d. From the drop-down menu, select **Deny New Service**.
 - e. On the Confirmation page, click **Confirm**.
2. Use the GUI to shut down or reboot the server.
3. Unplug the power cord.
4. Replace the server part or the component.
5. Power up the server by pressing the power button on the front of the server.
6. Verify the system is working properly. Test the system and run the maintenance tests.
7. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager name from the table.
 - c. Click **Service State**.
 - d. From the drop-down menu, select **Accept New Service**.
 - e. On the **Confirmation** page, click **Confirm**.

Replacing an appliance model Session Manager server

Procedure

1. Back up the system using Solution Deployment Manager.
2. Place the selected Session Manager instance in the **Maintenance Mode** state.
3. Power down the Session Manager server.
4. Replace the server with the new hardware.
5. Install Appliance Virtualization Platform on the server.
6. From Solution Deployment Manager, deploy a new Session Manager OVA.
7. Restore the backup that was taken in step 1.
8. Test the new Session Manager.
9. Place the Session Manager in the **Accept New Service** state.

IP address changes

This section describes the procedures for changing the following Session Manager attributes:

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

You can change these attributes after the initial installation if you need to move the server elsewhere on a network.

To change the IP address or host name of the System Manager hosted on VMware, see *Deploying Avaya Aura® System Manager*.

Changing the Security Module IP address

About this task

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

Procedure

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

 Note:

The 96xxsettings.txt parameter ENABLE_PPM_SOURCED_SIPPROXYSRVR should be set to 0 to prevent the phone from retaining the previous address downloaded from the Session Manager instance.

3. Change the state of the Session Manager instance to **Deny New Service**:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager name from the table.
 - c. Click **Service State**.
 - d. From the drop-down menu, select **Deny New Service**.
 - e. On the **Confirmation** page, click **Confirm**.
4. If the server is to be relocated:
 - a. Power down the server.
 - b. Relocate the server.
 - c. Power up the server.

5. Change the Security Module address of Session Manager:
 - a. On System Manager Web Console, select **Elements > Routing > SIP Entities**.
 - b. Select the appropriate Session Manager and click **Edit**.
 - c. In the **FQDN or IP Address** field, enter the new IP address for the Security Module.
This is not the management IP address.
 - d. Click **Commit**.
6. Update any associated Security Module information:
 - a. On System Manager Web Console, select **Elements**, select **Session Manager > Session Manager Administration**
 - b. Select the appropriate Session Manager instance and click **Edit**.
 - c. Change any necessary information such as the default gateway and QoS parameters for the Security Module.
 - d. Click **Commit**.
7. Change the provisioning for all SIP entities with links to the changed Session Manager Security Module address using the entity's administration.

For example, if Communication Manager communicates with the Session Manager, the Communication Manager signaling groups need to be updated in order to connect to the Session Manager at its new address.
8. After all provisioning has been changed, check the status of the Security Module:
 - a. On System Manager Web Console, select **Elements > System Status > Security Module Status**.
 - b. Ensure the **Status** for the Session Manager instance is **Up** and the IP address is correct.
9. Test the Session Manager instance:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
 - b. In the **Select Target** field, select the Session Manager instance from the drop-down menu.
 - c. Click **Execute All Tests**.
10. Change the state of the Session Manager to **Accept New Service**:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager name from the table.
 - c. Click **Service State**.
 - d. From the drop-down menu, select **Accept New Service**.
 - e. On the **Confirmation** page, click **Confirm**.

11. Perform a PPM reload to tell the phones where the Session Manager instance has moved:
 - a. On System Manager Web Console, select **Elements > Session Manager > System Status > Registration Summary**.
 - b. Select the appropriate Session Manager.
 - c. Click **Reload** and select **Reload Complete** from the drop-down menu to reload the phone with all of its data in order to use the new Session Manager IP address.
 - d. Click **Confirm**.
 - e. On the status page, verify that all SIP endpoints have registered.

Changing the Session Manager IP address or host name

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

Procedure

1. Change the state of the Session Manager instance to **Deny New Service**:
 - a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
 - b. On the **Session Manager Dashboard** page, select the appropriate Session Manager name from the table.
 - c. Click **Service State**.
 - d. From the drop-down menu, select **Deny New Service**.
 - e. On the **Confirmation** page, click **Confirm**.
2. Update the Session Manager information:
 - a. On the System Manager web console, under **Elements**, click **Session Manager > Session Manager Administration**.
 - b. Select the appropriate Session Manager and click **Edit**.
 - c. Update the information in the **Management Access Point FQDN/IP** field.

The **Management Access Point FQDN/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.
 - d. Click **Confirm**.
3. To change the IP address or FQDN of a Survivable Remote Session Manager or Branch Session Manager:
 - a. Change the IP address of the host in which a Branch Session Manager is installed using the Branch Session Manager page on the System Manager console.
 - b. Log in to the Solution Deployment Manager web console.
 - c. Select **VM Management > Show All > VMs**. Select the Session Manager from the VM list that you want to edit. Click **Edit**.

- d. Enter the new values for the IP address or FQDN or both.
- e. Submit the changes and wait for the update to finish.

 Note:

You need to make the change first in System Manager and then in Solution Deployment Manager as mentioned above. Otherwise, data is not replicated to Branch Session Manager. In such cases, you can fix the problem by running the command `initTM`.

4. To change the IP address or FQDN of a Session Manager or a Branch Session Manager:

- a. Log in to the console of the Session Manager instance using the craft or customer login.

 Note:

Use vSphere client to connect to Avaya Aura® Appliance Virtualization Platform(AVP) or VMware server (VE), and use the console application in vSphere to run the `SMnetSetup` command.

For information about installing vSphere client and the limitations of using the vSphere client in AVP configurations, see [PSN027036](#).

- b. Type `SMnetSetup`.
- c. Type the new Session Manager management IP address when you are prompted for the IP address of the server.
- d. Type the new Session Manager host name when you are prompted for the host name of the server.
- e. Enter additional information as needed.
For example, you can change information such as the netmask gateway.
- f. If the System Manager IP address changed, type the new IP address. Otherwise, press the `Enter` key.

5. Test the Session Manager instance:

- a. On the System Manager Web Console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
- b. In the **Select Target** field, select the Session Manager instance from the drop-down menu.
- c. Click **Execute All Tests**.

6. Change the state of the Session Manager to **Accept New Service**:

- a. On the System Manager Web Console, under **Elements**, select **Session Manager**.
- b. On the **Session Manager Dashboard** page, select the appropriate Session Manager name from the table.
- c. Click **Service State**.

- d. From the drop-down menu, select **Accept New Service**.
 - e. On the **Confirmation** page, click **Confirm**.
7. If the Identity Certificates contain the IP address or the host name of the Session Manager, make sure the certificates are re-initialized with the new IP address or host name or both:
 - a. On the home page, under **Elements**, click **Inventory > Manage Elements**.
 - b. Select the appropriate Session Manager.
 - c. Click **More Actions > Configure Identity Certificates**.
 - d. Select the management certificate.
 - e. Click **Replace**.
 - f. Enter the appropriate information in the fields.
 - g. Ensure **Replace this Certificate with Internal CA Signed Certificate** is selected.
 - h. Click **Commit**.
8. If a CDR adjunct is administered, you must change the adjunct to use the new Session Manager IP address.

Changing the IP address or FQDN of System Manager

About this task

After you install System Manager, you can change the IP address, hostname, or the general network settings of the machine running System Manager.

When you want to add a secondary System Manager for geographic redundancy, run the **changeMgmtIP** command from the Session Manager command line to reconfigure and to use the secondary System Manager.

For more information, see *Changing the IP address and FQDN in System Manager* in *Administering Avaya Aura® System Manager*.

Use this procedure to make changes to Session Manager and Branch Session Manager *after* you change the System Manager IP address or FQDN.

Procedure

1. Log in to the CLI of the Session Manager using the craft or customer login.
2. Run the command **changeMgmtIP**.
3. Type the new IP address for the Primary System Manager when you are prompted.
4. Submit the changes, and wait for the update to finish.

Migrating servers

Avaya no longer supports the S8510, S8800, S8300D, R610, and DL360 G7 servers. However, the servers can still be used in the virtualized configuration if the servers have the resources to deploy and run the OVA.

The following procedure describes the high-level steps for migrating the S8510, S8800, S8300D, R610, and DL360 G7 servers to the R2 Common servers.

1. To access Solution Deployment Manager, log on to the System Manager user interface and navigate to **Services> Solution Deployment Manager**
2. Perform a backup using the Solution Deployment Manager.
3. Set Session Manager in maintenance mode.
4. Turn off the server that you are migrating.
5. Replace the existing server with the new server.
6. Install VMware ESXi on the server.
7. Using the Solution Deployment Manager, deploy a new Session Manager OVA.
8. Using the Software Deployment Manager, restore the backup that you created in Step 2.
9. Test the new Session Manager server.
10. Change the service state of the Session Manager server to **Accept new service**.

Chapter 8: Call Detail Recording on Session Manager

The Call Detail Recording (CDR) feature records information on calls. When you enable CDR, the CDR records are saved in a special directory on the local hard drive of the server.

The call record contains information regarding:

- The time of the call
- The duration of the call
- The dialed number
- The calling party
- The terminating SIP entity
- The originating SIP entity
- The bandwidth indicator

For each Session Manager, you can administer CDR as either disabled or enabled. CDR records are created if you enable the CDR in at least one of two Session Manager entities.

 Note:

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

CDR records on Session Manager are created on connected calls.

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

For sequenced applications (implicit or administered for a user), only one CDR record is generated for a given call.

If the secondary Session Manager of a user receives a call, the call is routed to the primary Session Manager of the user as per user registration. In that case, the CDR is still generated on the secondary Session Manager and not on the primary Session Manager.

Minimum requirements for CDR

To support the Session Manager CDR functionality, the following minimum requirements must be met:

- IP connectivity between the CDR adjunct and the Session Manager server periodically to collect the CDR data files remotely.
- The CDR adjunct must be compatible with Session Manager CDR formats. Contact Avaya support for more information regarding the formats.

CDR Data file naming and structure

Session Manager generates and stores CDR data files in the `/CDR_User` directory on the server using the CDR feature. Whenever the CDR adjunct logs into the server, the CDR adjunct gets direct access to this directory.

 Note:

The full path of the directory is `/data/home/CDR_User/`. The CDR adjunct login is limited to accessing the files contained in this directory.

The CDR files stored in the special directory are those that the server has completed and closed. These files are ready for the CDR adjunct to collect, process, and subsequently delete from the server. CDR_User group members are assigned the rights to read and subsequently delete the CDR data files.

The file naming convention for the following CDR data file formats are:

1. Standard Flat File (default) format — `tssssss-ssss-YYMMDD-hh_mm`
2. Enhanced Flat File format — `tssssss-ssss-YYMMDD-hh_mm`
3. Enhanced XML File format — `tssssss-ssss-YYMMDD-hh_mm_n.xml`
4. IPv6 Standard Flat File — `tssssss-ssss-YYMMDD-hh_mm`
5. IPv6 Enhanced Flat File — `tssssss-ssss-YYMMDD-hh_mm`

Where:

The file name is more than 25 characters for the XML format.

For other formats, the file name is fixed at 25 alphanumeric characters, including dashes (-) and underscores (_).

`t` is populated with the character `S` in the first Session Manager release.

`ssssss-ssss` is an alphanumeric string of six characters, followed by a dash (-) and an alphanumeric string of four characters, for a total of 11 characters. This hexadecimal string uniquely identifies the Session Manager server using its IPv4 IP address.

`YY` is a two-digit number representing the year when the file was created.

MM is a two-digit number representing the month when the file was created.

DD is a two-digit number representing the day of the month when the file was created.

hh is a two-digit number representing the hour of the day when the file was created (24 hour clock server time).

mm is a two-digit number representing the number of minutes after the hour when the file was created.

_n is a number that increments by 1 if more than one file with the same timestamp is created.

.xml portion indicates that the file contains XML.

Example

For a CDR file created on January 29, 2009, at 3:24 PM from a Session Manager at IP address 142.9.147.59, the data file is named as follows:

S008e09-933b-090129-15_24

For three XML files created with the same timestamp as mentioned above, the files are named as follows:

- *S008e09-933b-090129-15_24_1.xml*
- *S008e09-933b-090129-15_24_2.xml*
- *S008e09-933b-090129-15_24_3.xml*

Note:

- CDR data files naming convention used by Session Manager is compatible with the CDR data files naming convention used by Communication Manager. Communication Manager must support the *CM Survivable CDR* functionality to ensure file name compatibility.
- CDR XML format conforms to W3 XML standard. According to the standard, whitespace between elements is optional. Hence, CDR file of XML standard displays all fields for a call in one line. Removing the extra whitespace characters from the XML CDR files reduces performance issues with disk occupancy.

CDR login and password

The CDR adjunct uses a special login, *CDR_User*. This login is restricted to reach only the directory where the CDR records are stored. The passwords are set up in the **Elements > Session Manager > Session Manager Administration** section of System Manager for each Session Manager that has CDR enabled. The Session Manager administrator creates a password for the designated login *CDR_User*. The login and password must be provided to the CDR adjunct administrator so that the adjunct can retrieve the CDR data files. The administrator should verify that this login and password work on each server on which CDR is administered.

CDR record transfer

CDR data is transferred in an encrypted manner from the Session Manager server to the CDR adjunct using a secure file transfer protocol such as SFTP. CDR records are stored and transferred in batches rather than one record at a time.

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

Retrieving CDR data files

About this task

This section provides an example of a typical CDR data file retrieval session from a single server named MyServer.MyDomain.com and provides suggestions and cautions concerning the setup and operation of the Session Manager CDR functionality.

Procedure

1. Navigate to the directory where the CDR data files are to be transferred.
2. Run the following command to begin the session:

```
sftp CDR_User@MySessionManager.MyDomain.com
```

- The command launches the SFTP program and passes the Session Manager server name and user ID to the server for enabling the session. In this example, the server name is MySessionManager.MyDomain.com and the user ID is CDR_User.
- The server responds with the standard login message and prompts for the password.

3. Enter the password.

You are placed in the CDR data files directory on the Session Manager server.

4. Run the **mget S*** command to copy all files that exist on the server with file names that begin with a capital S to the local directory.
5. Run the **ls -al** or an equivalent command to view which files were transferred.
6. To remove each transferred file, one at a time, from the server, run the command **rm <individual file name>**.

Do not use the **rm S*** command. This action removes the CDR files from the Session Manager server. See the note and caution for more information.

Note:

The files are removed individually to avoid deleting a new CDR data file added to the directory between the time the files are transferred and the time they are deleted. If a new file was added during this period and the **rm *** command was used, the new file

would be deleted without getting transferred to the CDR adjunct. Any CDR records that were contained in the “new” file would be permanently lost.

 Caution:

The CDR adjunct must perform file verification to ensure that the adjunct has accurately received the file before deleting it from the server. For example, this check could be comparing the relative file size of the received file with the file size on the server to ensure they are the same size before deleting the file on the server.

The adjunct provider may elect to design the adjunct to retrieve a group of files on one polling pass and then process those files to ensure they are in the correct format and contain valid data. If no errors are detected, the adjunct would then remove the previously retrieved files on the next polling pass. If errors are detected in a file, the adjunct could re-retrieve the errant file before removing it from the server.

7. Run the **bye** command for the adjunct to sign off from the server.

CDR record deletion

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

1. o After the CDR adjunct retrieves a data file from the server and verifies that it contains valid data, the adjunct deletes the data file from the server.
2. The server automatically removes any CDR data file stored on its local hard drive that is older than five days.
3. The onsite or remote switch administrator or technician with proper permissions can delete unwanted CDR data files.

CDR security provisions

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

If firewalls are implemented anywhere between the CDR adjunct and the various Session Manager servers, it may be necessary to *punch pinholes* in those firewalls to allow communication between the CDR adjunct and the servers.

Call Detail Recording alarms

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

The alarm must be cleared manually after the failure condition is resolved.

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

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

Administering CDR on a new Session Manager instance

Procedure

1. On System Manager Web Console, click **Elements > Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. On the Session Manager Administration page, under Session Manager instances, click **New**.
4. In the Add Session Manager page, select the **Enable CDR** check box.
5. Enter a password for *CDR_User* login.
6. Re-enter the password to confirm it.
7. In the **Data File Format** field, click the format of the CDR data file.

Additionally, you can also include CDR records for other type of calls such as user to user calls and incomplete calls.

8. Click **Commit**.

Enabling CDR for an existing Session Manager instance

Procedure

1. On System Manager Web Console, click **Elements > Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Select a Session Manager instance from the list and click **Edit**.
4. In the Edit Session Manager page, select the **Enable CDR** check box.
5. Enter a password for the *CDR_User* login.

6. Re-enter the password to confirm it.
7. Click **Commit**.

Chapter 9: Resources

Session Manager documentation

The following table lists the documents related to Session Manager. Download the documents from the Avaya Support website at <https://support.avaya.com>.

Title	Description	Audience
Overview		
<i>Avaya Aura® Session Manager Overview and Specification</i>	Describes the key features of Session Manager.	System administrators
<i>Avaya Aura® Session Manager Security Design</i>	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Implementation		
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment</i>	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment</i>	Describes how to deploy the Session Manager in the Software-Only and Infrastructure as a Service (IaaS) environment.	Services and support personnel
<i>Routing Web Service API Programming Reference</i>	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
<i>Avaya Aura® Session Manager Element Manager Web Service API Programming Reference</i>	Describes how to get programmatic access to Session Manager Dashboard and User Registration status data.	Services and support personnel
Administration		
<i>Administering Avaya Aura® Session Manager</i>	Describes the procedures to administer Session Manager using System Manager.	System administrators

Table continues...

Title	Description	Audience
<i>Avaya Aura® Session Manager Data Privacy Guidelines</i>	Describes how to administer Session Manager to fulfill Data Privacy requirements.	System administrators, Network administrators, services, and support personnel
Installation and upgrades		
<i>Upgrading Avaya Aura® Session Manager</i>	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Maintaining and Troubleshooting		
<i>Maintaining Avaya Aura® Session Manager</i>	Contains the procedures for maintaining Session Manager.	Services and support personnel
<i>Troubleshooting Avaya Aura® Session Manager</i>	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support > Documents**.
4. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
5. From the **Select Content Type** list, select one or both of the following options:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
 - Set a collection as the default or favorite collection.
 - Save a PDF of the selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive collections that others have shared with you.
- Click **Watch** () to add a topic to your watchlist so you are notified when the content is updated or removed.
 - View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
 - Unwatch the selected content or all topics.
- Send feedback for a topic.

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
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager

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.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

 Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: 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 SNMP Whitepaper* 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 145.	
2	Create an SNMP V3 user profile using the same settings as the System Manager TrapListener settings.	Creating an SNMPv3 user profile on page 135.	
3	Create an SNMP user profile and assign the System Manager user profile.	Creating an SNMP target profile on page 138. Use the following values: • Port 10162 • Domain Type UDP • Protocol V3	
4	Verify the Session Manager serviceability agent can register with System Manager.	Verifying the Session Manager serviceability agent registration on page 131.	
5	Assign the System Manager target profile.	Managing target profiles for the selected serviceability agents on page 132.	
6	Attach the user profile to the Session Manager serviceability agent.	Managing SNMPv3 user profiles for the selected serviceability agents on page 131.	
7	Verify the Session Manager serviceability agent can forward alarms to the System Manager.	Generating test alarms on page 132.	

Verifying the Session Manager serviceability agent registration

Procedure

1. On the System Manager web console, click **Services > 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 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 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 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 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 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 an alarm.

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

To view the alarm details, 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 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 field descriptions

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

Button	Description
Activate	Activates one or more Serviceability Agent.
Manage Profiles	Manages the target profiles for the selected serviceability agents.
Generate Test Alarm	Generates test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents
Repair Serviceability Agent	Repairs the serviceability agent.
Manage Profile Job Status	Manages the profile job for the serviceability agent.

Table continues...

Button	Description
Reset Table	When you perform the retry operation on the Manage Profile Job Status page, System Manager displays the list of failed agents on the Serviceability Agents page. If you need to clear the list of failed agent list and display all the available agents in the Agent List section, use the Reset Table button.
Advanced Search	The link to perform advance search. When you click on this link, System Manager displays the Criteria section.
Filter: Enable	The fields where you can set the filter criteria. Filter: Enable is a toggle button.
Filter: Disable	Hides the column filter fields. Filter: Disable is a toggle button.
Filter: Apply	Filters agents based on the filter criteria.
Select: All	Selects all agents in the table.
Select: None	Clears the selection for the agents that you select.
Refresh	Refreshes the agent information in the table.

Criteria

Name	Description
Select Search Criteria	The options are: • Hostname • IP Address • System Name • Device Type • System OID • Target Profile • User Profile
Select Search Operator	The options are: • Equals • Not Equals • Starts with • Ends with • Contains
Enter Search to Text	Specify the search criteria.

Button	Description
-	Removes the additional search criteria fields. This field is enabled when the additional search criteria fields are added.

Table continues...

Button	Description
+	Adds the additional search criteria fields.
Clear	Clears the search criteria.
Search	Performs the search for the specified search criteria
Close	Closes the Criteria section.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the 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 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 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 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 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.

Table continues...

Name	Description
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 SHA.
Authentication Password	The password used to authenticate the user.  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	Cancel the action and returns 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 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 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 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 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 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.

Table continues...

Button	Description
View	To go to the View Target Details page where you can view an existing SNMP target profile.
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 returns 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 System Manager web console, click **Services > 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.*
 - Do the following:
 - 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 System Manager web console, click **Services > Inventory > Manage Serviceability Agents > Notification Filter Profile**.
2. Select a filter profile.
3. Click **View**.

Editing a Notification Filter Profile

Procedure

1. On the System Manager web console, click **Services > 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 System Manager web console, click **Services > 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 System Manager web console, click **Services > 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 System Manager web console, click **Services > 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 filter 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.

View Profile: TrapListener 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.
Email Forward	The option to forward the emails to the user. The default is false . If set to true , the system forwards the emails to the user.
Email to addresses	A list of e-mail addresses, which are comma separated, to which alarms are forwarded.
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::hrProcessorFwID
- 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::snmpInTooBig
- 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

Appendix B: 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 Product Correction Notices and Product Support Notices

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

A

access log harvesting	38
accessing	
root account	26
accessing log harvest	38
accessing port matrix	124
activating agent	131
activating serviceability agent	131
adding	
encryption passphrase	70
remote key server	72
adding an SNMP target profile	138
administering	
CDR on a new Session Manager instance	121
alarm test	94
appliance model	109
assigning	
notification filter profile to a serviceability agent	142
Avaya InSite Knowledge Base	127
Avaya support website	127

B

backup and restore commands	27
Backup and Restore page	101
backup data	100
backup data retention	107
backup files; view	105
browser requirements	16

C

Call Route Test	
troubleshooting a test failure	98
Call Routing Test	95
results	98
setting up	97
CDR	116
administering on a new Session Manager instance ...	121
data file name	117
enabling for existing Session Manager instance	121
login and password	118
minimum requirements	117
record deletion	120
record transfer	119
retrieving data files	119
security provisions	120
certTool	29
error codes	29
changes to platform support	9
changing	114
encryption passphrase	70

changing (<i>continued</i>)	
Maximum Backup Files value	107
Security Module IP address	110
System Manager IP address	114
changing attributes	
post-installation	110
collection	
delete	125
edit	125
generating PDF	125
sharing content	125
command	
logRetention	68
smconfig	69
commands, customer account	24
configuring	
SIP tracing	58
configuring trap listener	144
content	
publishing PDF output	125
searching	125
sharing	125
sort by last updated	125
watching for updates	125
create filter profiles	143
creating	
notification filter profile	141
creating an SNMP target profile	138
creating an SNMPv3 user profile	135
creating log harvesting profile	38
creating system data backup on a local server	102
customer account commands	24

D

data backup from local server	105
data backup; schedule	103
data distribution test	90
data encryption	69
data retention	107
delete filter profiles	143
delete SNMPv3 user profiles	136
deleting an SNMP target profile	139
deleting an SNMPv3 user profile	136
deleting SNMP target profiles	139
disabling	
local key store	74
displaying	
slots assignment and remote key server	73
document changes	10
documentation	
Session Manager	123
documentation center	125

documentation center (<i>continued</i>)		harvested log files; download	44
finding content	125	host name resolution test	90
navigation	125	HTTP proxy	85
documentation portal	125	HTTP proxy access	
download		check	87
harvested log files	44	enabling	86
downloading harvested log files	44	HTTP proxy accessible	88
		HTTP proxy firewall access	
		disabling	86
E			
edit filter profiles	143	I	
editing an SNMP target profile	138	Identity certificate	
editing an SNMPv3 user profile	135	importing	31
editing SNMPv3 user profiles	135	importing	
enabling		Identity certificate using certTool	31
local key store	73	Trusted certificate using certTool	31
enabling CDR for existing Session Manager instance	121	installation	
encryptionLocalKey	73	verification testing	92
encryptionPassphrase	69	IP address	
encryptionRemoteKey	71	changing for the Security Module	110
Export Trace Viewer	62		
		K	
F		KB	
field description		Support site	127
TrapListener service	145		
field descriptions		L	
Agent List	133	listing	
Create New Profile	39	slots assignment and encryption passphrase	71
Filter Profiles	143	slots assignment and remote key server	73
Harvest Archives	44	slots assignment and remote server	71
Notification Filter Profiles	143	load factor status test	91
Replica Nodes	79	Loading and managing site certificate	27
Replication Node Details	82	local data backup	
Serviceability Agents	133	create	102
Filter Profiles		log details; view	33
field descriptions	143	log file; search for text	43
filtering		log harvest requests; filter	42
SIP messages	59	log harvest; access	38
filtering log harvesting profiles	40	log harvester	38
Filtering log harvesting requests	42	log harvesting profiles; filter	40
filtering logs	37	log retention	68
filtering SNMPv3 user profiles	136	Logging page	33
filtering target profiles	139	login and password, CDR	118
finding content on documentation center	125	logs; search	37
finding port matrix	124		
		M	
G		maintenance	
generate an alarm	94	session manager	99
generating test alarms	132	maintenance tests	
		secure access link agent	91
H		Managed Bandwidth Usage	66
hardware_info	108	Managed Bandwidth Usage errors	67
Harvest Archives page	47		

managing SNMPv3 user profiles	131 , 132	repairing a replica node	75
managing target profiles	132	replacing appliance	114
managing user profiles	131	replica group; remove nodes	77
Maximum Backup Files value, changing	107	replica group; removing replica node from queue	77
MIB	146	Replica Groups page	78
modifying SNMPv3 user profiles	135	replica groups; view	75
N		required equipment	16
network connections test	92	requirements	
nodes; remove	77	minimum for CDR	117
notification filter profile		restore backup	
assigning to serviceability agent	142	from with different IP/FQDN	106
creating	141	restore data	100
unassigning from serviceability agent	142	restore data backup	105
Notification Filter Profiles		restore system backup from local server	105
field descriptions	143	root account	26
notification IDs	143	S	
notifications	151	safety	12 , 13 , 15
O		electrical	13
overview		ESD	15
Session Manager	11	inspection	13
P		Schedule Backup page	101
PCN updates	151	scheduling a data backup on a local server	103
PCNs		Search Archives page	46
viewing	151	searching for a text in a log file	43
Pending Jobs page	104	searching for content	125
pending jobs; view	103	searching for logs	37
port matrix	124	searching logs	37
post-installation		security provisions, CDR	120
changing attributes	110	serviceability agent	
postgres database sanity test	91	activate	131
product notification enrollment	152	Serviceability agents	
product notifications		repair	132
e-notifications	152	Session Manager	
Profile Criteria View page	46	overview	11
PSN updates	151	SIP Entity Monitoring	53
PSNs		session manager server	109
viewing	151	setting up a Call Routing Test	97
push notification provider availability test	91	sharing content	125
R		SIP	
record deletion, CDR	120	tracing	55
record transfer, CDR	119	SIP Entity Monitoring Status Summary	54
redundancy link test	90	SIP monitoring	54
remote SIP logging	62	SIP trace logs	
removing		viewing	60
encryption passphrase	70	SIP Tracer Configuration	56
remote key server	72	SIP tracing	
removing a node	77	configuring	58
removing replica node from queue	77	SNMP MIB	146
		SNMP target profile	
		add	138
		edit	138
		SNMP target profile list	139
		SNMP target profile; view	138
		SNMP target profiles field descriptions	140
		SNMP target profiles; delete	139

SNMP traps	144	videos	126
SNMPv3 user profile; add	135	view backup files	105
SNMPv3 user profile; create	135	view contents; log harvested files	42
SNMPv3 user profile; delete	136	view details; log harvesting request	41
SNMPv3 user profile; edit	135	view filter profiles	143
SNMPv3 user profile; filter	136	view log details	33
SNMPv3 user profile; view	135	view replica groups	75
SNMPv3 user profiles		viewing	
assign	131	data encryption status	74
manage	131	PCNs	151
SNMPv3 user profiles field description	136	PSNs	151
sort documents	125	Security Module status	48
submitting a request for harvesting log files	41	User Data Storage status	85
support	127	viewing an SNMP target profile	138
supported browsers	16	viewing an SNMPv3 user profile	135
synchronizing System Manager master database and replica computer database	75 , 76	viewing details of a log harvesting profile	40
T		viewing details of a log harvesting request	41
target profile; manage	132	viewing harvested log files in an archive	43
target profiles		viewing list of backup files	105
edit	138	viewing log details	33
target profiles field descriptions	140	viewing pending jobs	103
target profiles; delete	139	viewing replica groups	75
target profiles; filter	139	viewing replica node details	76
test alarms from web console		viewing replica nodes in a replica group	75
generate	132	viewing replication details for a replica node	76
Trace viewer		viewing the contents of harvested log files	42
buttons	61	viewing trace logs	60
output	61	W	
Trace Viewer		watchlist	125
file options	62		
tracing	55		
TrapListener	144		
Traplistener service; alarming UI	144		
TrapListener service; configure	144		
troubleshooting			
Call Route Test failure	98		
Trusted certificate			
importing	31		
U			
unassigning			
filter profile from serviceability agent	142		
User Data Storage and Data Center management	84		
user data storage sanity test	92		
User Data Storage status			
viewing	85		
V			
verify alarm configuration	94		
verifying			
system communication	92		