Administering the Avaya Aura® Web Gateway

Release 3.9.1
Issue 2
August 2021

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“ **Hosted Service** ” 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 UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as

only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. 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

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document describes ongoing administration, management, and maintenance tasks for the Avaya Aura® Web Gateway. Use this document after deploying the Avaya Aura® Web Gateway. For more information about deployment, see *Deploying the Avaya Aura® Web Gateway*.

Note:

This document does not describe SDK developer applications.

Change history

Issue	Date	Summary of changes
Release 3.9.1, Issue 2	August 2021	• Indicated system layer commands supported in software-only deployments in System layer commands on page 27. • Added Enabling the lockout policy for Unified Portal accounts on page 63. • Added Enabling or disabling disk encryption on Avaya Aura Web Gateway on page 129. • Removed procedures related to the ClamAV antivirus tool. • Added CylancePROTECT antivirus software overview on page 140. • Updated the upgrade procedures for Release 3.9.1 under Avaya Aura Web Gateway upgrade and migration operations on page 174.
Release 3.9, Issue 1	March 2021	• Added Setting a timeout period for an SSH session on page 25. • Added the use-cases when WebRTC media adaptation must be enabled to the description of Configuring WebRTC media adaptation on page 61.

Table continues…

Issue	Date	Summary of changes
		• Added Scheduling log collection on page 73. • Added Canceling scheduled log collection on page 75. • Updated the default value and the range of values of the **Application HTTPSession Timeout** parameter in Application Properties field descriptions on page 93. • Removed information about the unsupported VP8 codec from Configuring video codecs and bandwidth on page 94. • Added Avaya Spaces Calling and Avaya Aura Web Gateway integration checklist on page 96. • Added Configuring SSO for an Avaya Spaces web-client on page 99. • Updated the name of the pre-defined configuration in Configuring mobile application settings on page 110 and Disabling specific push notifications on page 111. • Added Disabling all push notifications on page 112. • Updated the description of Communication Manager parameters in Avaya Aura Communication Manager configuration on page 113. • Indicated that Avaya Aura® Web Gateway support IWA for multiple domains in the sections under Integrated Windows Authentication administration and management on page 115. • Updated the list of parameters in firewall.pl script on page 147. • Added Characters supported for Avaya Aura Web Gateway passwords on page 149. • Added Password policy for human-user accounts on page 149. • Added Configuring password rules on page 150. • Added Avaya Aura Web Gateway entry points on page 150. • Added Viewing performance statistics on page 151. • Added Performance charts on page 152. • Updated the steps in Viewing performance logs on page 158. • Added Viewing the firewall configuration on page 164. • Added Automatic backups on page 166. • Added Configuring automatic backups on page 167.

Table continues…

Issue	Date	Summary of changes
		• Added Changing the location of automatic backups on page 167. • Added procedures for performing migration to Release 3.9 under “Migrating Avaya Aura® Web Gateway”. • Added new troubleshooting procedure Cannot log in to the Avaya Aura Web Gateway web administration portal after changing the System Manager password on page 187. • Updated the steps and command syntax in System Manager does not show Avaya Aura Web Gateway alarms on page 188. • Added new troubleshooting procedure Avaya Aura Web Gateway returns a TLS handshake error when testing the connectivity to a push notification server on page 190. • Added new troubleshooting procedure The location of automatic backups has changed after the upgrade on page 193. • Added procedures for managing Linux single-user mode under RHEL single-user mode on page 193. • Added new entries to the Glossary.

Chapter 2: Avaya Aura® Web Gateway overview

The Avaya Aura® Web Gateway server acts as a gateway to Avaya Aura® clients and applications utilizing WebRTC signaling and media. Avaya Aura® Web Gateway also provides the push notification service, enabling clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs).

You can deploy the Avaya Aura® Web Gateway through Amazon Web Services (AWS), VMware, or Avaya Virtualization Platform.

You can deploy the Avaya Aura® Web Gateway in the following environments:

- Avaya Aura® (Team Engagement)
- Avaya Aura® and Conferencing (Team Engagement and Conferencing)

To access conferencing tools, such as Avaya Meetings Server, your deployment must include Conferencing.

Note:

An Over-The-Top (OTT), or Conferencing-only, deployment option is available, but it is not described in this document. The Conferencing-only option follows a different deployment process. For more information, see *Deploying Avaya Meetings Server*.

New in this release

The following is a summary of new functionality that has been added to the Avaya Aura® Web Gateway in Release 3.9 and Feature Pack 1:

Software-only installation

Avaya Aura® Web Gateway Release 3.9 supports software-only installation. In software-only deployments, you must provide and configure the operating system for use with the Avaya Aura® Web Gateway application. Avaya Aura® Web Gateway supports VMware and AWS virtual environments for software-only installation.

Red Hat Enterprise Linux 7.6 support

Avaya Aura® Web Gateway now uses Red Hat Enterprise Linux 7.6.

Performance metrics dashboard

You can now review various performance metrics and system health indicators, such as CPU or memory usage, on the Avaya Aura® Web Gateway web administration portal.

Automatic backup

Avaya Aura® Web Gateway creates backups of configuration files and user data automatically on a weekly basis. You can modify the default automatic backup settings from the web administration portal.

Scheduled log collection

You can now enable a specific logging level on a temporary basis for a specified time period. After the specified time period expires, Avaya Aura® Device Services switches back to the original log level.

Security enhancements

To ensure the secure processing of user data and reduce security vulnerabilities, Avaya Aura® Web Gateway now supports the following features:

- The single-user mode of the RHEL operating system is now password-protected.
- Avaya Aura® Web Gateway now enforces default password policies for all human-user accounts.
- Avaya Aura® Web Gateway now supports the CylancePROTECT antivirus software.

IWA multidomain support

Avaya Aura® Web Gateway now supports IWA for multiple domains. You can now configure multiple active directories to use IWA capabilities.

Solution architecture

This section provides a graphical representation of the Avaya Aura® Web Gateway deployment architecture.

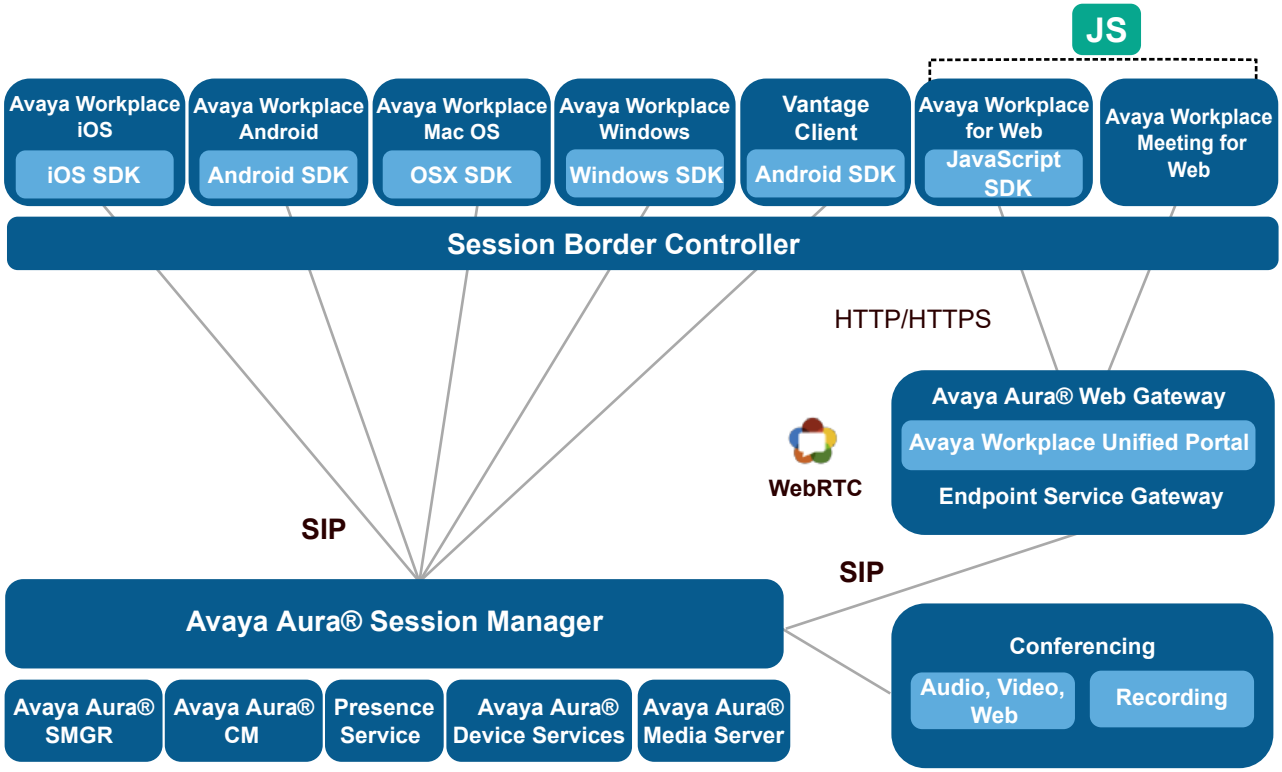
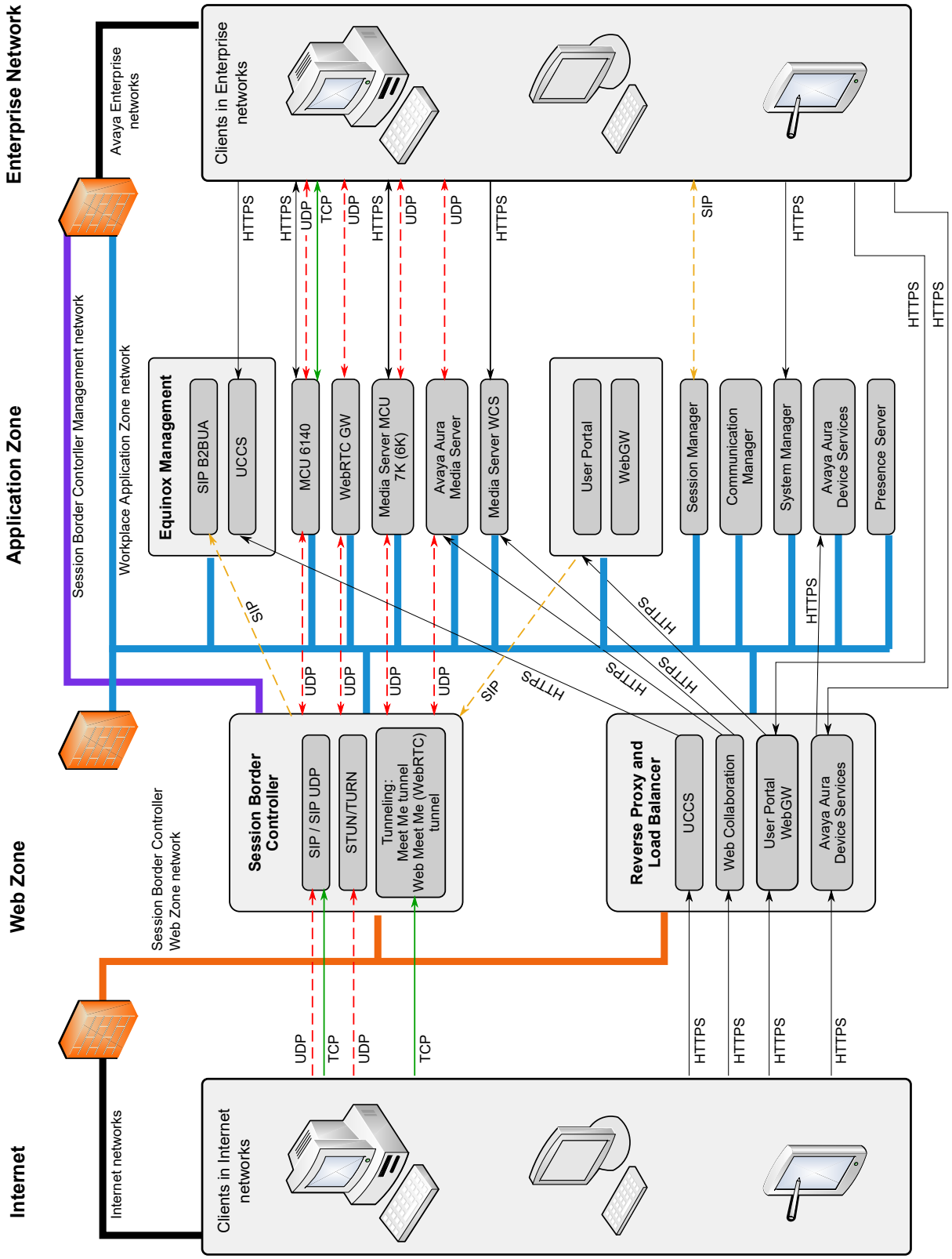


Figure 1: Avaya Workplace Client and Conferencing deployment topology

Topology diagram

This section provides a graphical representation of the Team Engagement + Conferencing deployment model topology.


Enterprise Network
Application Zone
Web Zone
Internet
Avaya Enterprise networks
Clients in Enterprise networks
Session Border Contoller Management network
Workplace Application Zone network
Equinox Management
SIP B2BUA
UCCS
MCU 6140
WebRTC GW
Media Server MCU 7K (6K)
Avaya Aura Media Server
Media Server WCS
User Portal
WebGW
Session Manager
Communication Manager
System Manager
Avaya Aura Device Services
Presence Server
HTTPS
UDP
TCP
SIP
Session Border Controller
SIP / SIP UDP
STUN/TURN
Tunneling: Meet Me tunnel Web Meet Me (WebRTC) tunnel
Session Border Controller Web Zone network
Reverse Proxy and Load Balancer
UCCS
Web Collaboration
User Portal WebGW
Avaya Aura Device Services
Internet networks
Clients in Internet networks

For detailed information about ports, go to https://support.avaya.com/security, scroll down, and click **Avaya Product Port Matrix Documents**. Navigate to the required solution component section and then click on the appropriate Port Matrix document for the release to open it.

Geographical distribution overview

In a geographically distributed system, resources are deployed in multiple data centers to reduce media delays. For this purpose, the following components are deployed in each data center:

- Avaya Aura® Media Server
- Avaya Aura® Session Border Controller
- Avaya Aura® Web Gateway
- Web Collaboration Server
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Device Services

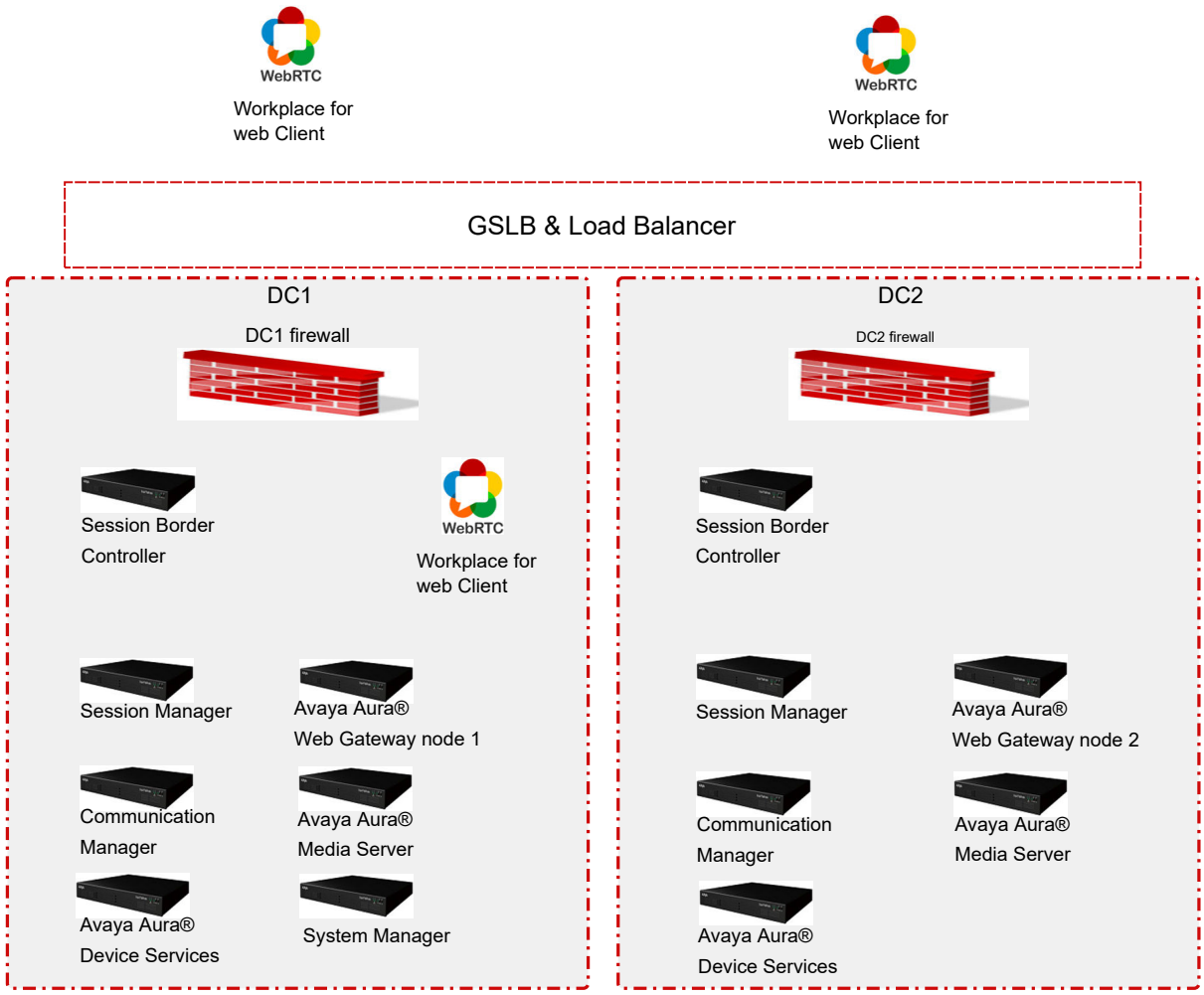
In a geographically distributed system, you must also install the following two components:

- Global Server Load Balancing (GSLB), which provides different routes and addresses based on the location of the client.
- Load balancer, which balances traffic between two or more Avaya Aura® Web Gateway nodes, which may be located in the same data center or in different data centers.

Avaya Aura® Session Manager and Avaya Aura® Communication Manager are important for call routing. To optimize media delays for point-to-point calls, deploy these components in a distributed manner across your data centers. The way in which these components are geographically distributed is outside the scope of this document. For more information about configuring Session Manager and Communication Manager, see *Administering Avaya Aura® Session Manager* and *Administering Avaya Aura® Communication Manager*.

General geographical distribution topology

In this topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. For simplicity, System Manager is deployed in Data Center 1 (DC1), while Session Manager, Communication Manager, and Avaya Aura® Device Services are deployed in all data centers.



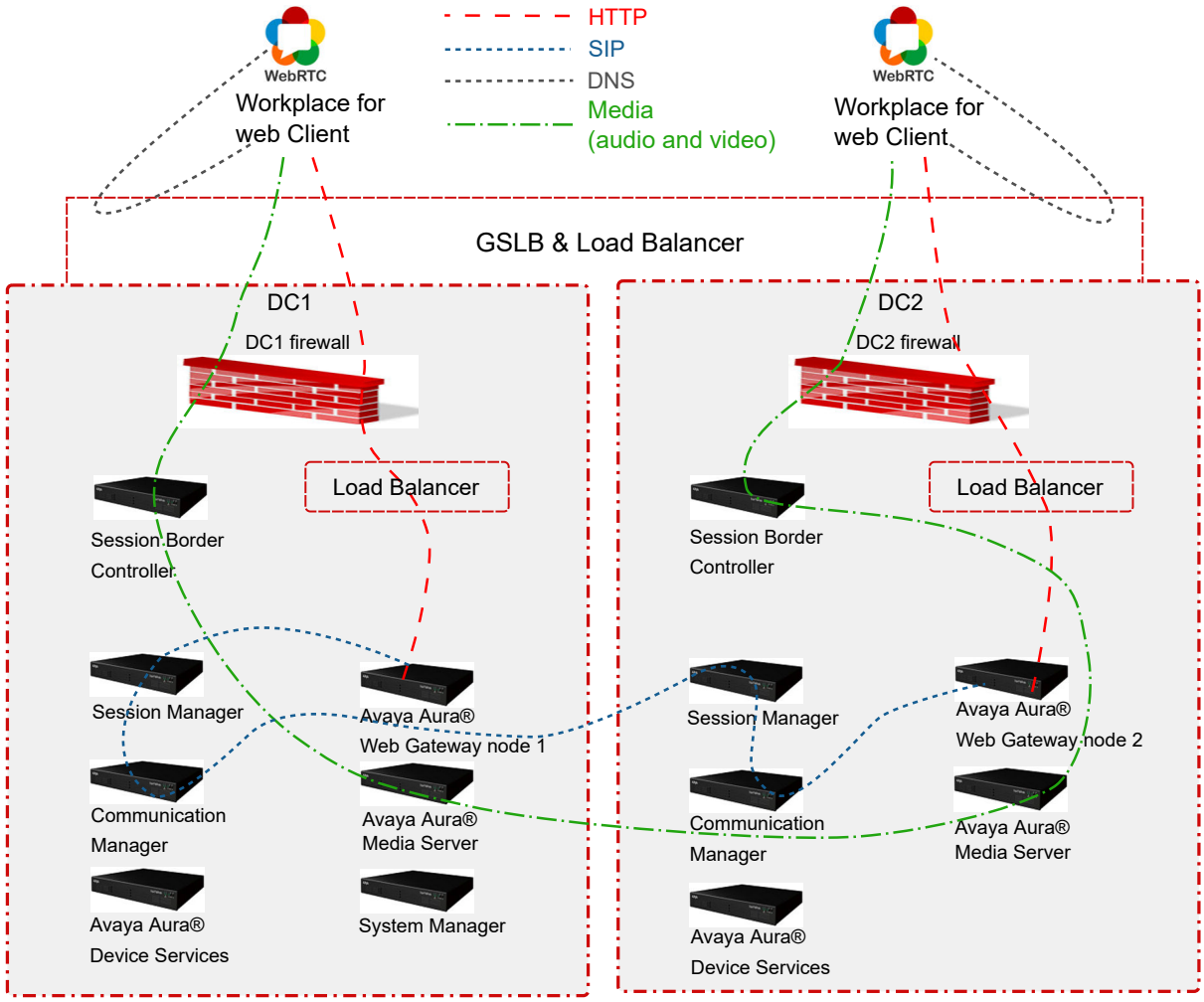
Signaling and media path topology when clients are located in or near different data centers

In the following topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. Clients are located in different data centers outside of the firewall and registered on the Avaya Aura® Web Gateway to receive calls. When one client makes a call to the other, the call follows the following flow:

1. Both clients log in to the corresponding Avaya Aura® Web Gateway and activate the call service.
    a. A client in data center 1 (DC1) gets the address of the DC1 load balancer and communicates with the Avaya Aura® Web Gateway deployed on that data center. The Avaya Aura® Web Gateway registers the client to the corresponding Session Manager deployed on DC1.

b. A client in data center 2 (DC2) gets the address of the DC2 load balancer and communicates with the Avaya Aura® Web Gateway deployed on that data center. The Avaya Aura® Web Gateway registers the client to the corresponding Session Manager deployed on DC2.

2. The DC1 Avaya Aura® Web Gateway initiates the call. To route the media, the Avaya Aura® Web Gateway uses the Session Border Controller and Avaya Aura® Media Server deployed on DC1.
3. The Avaya Aura® Web Gateway sends the SIP call to Session Manager deployed on DC1.
4. Session Manager deployed on DC1 forwards the call to Session Manager deployed on DC2.
5. Session Manager deployed on DC2 forwards the SIP invite to the Avaya Aura® Web Gateway from DC2, where the second client is logged in.
6. The Avaya Aura® Web Gateway from DC2 uses the Session Border Controller and Avaya Aura® Media Server deployed on DC2 to pass the media through the firewall to the second client.



Signalling and media path topology when both clients are located in or near the same data center

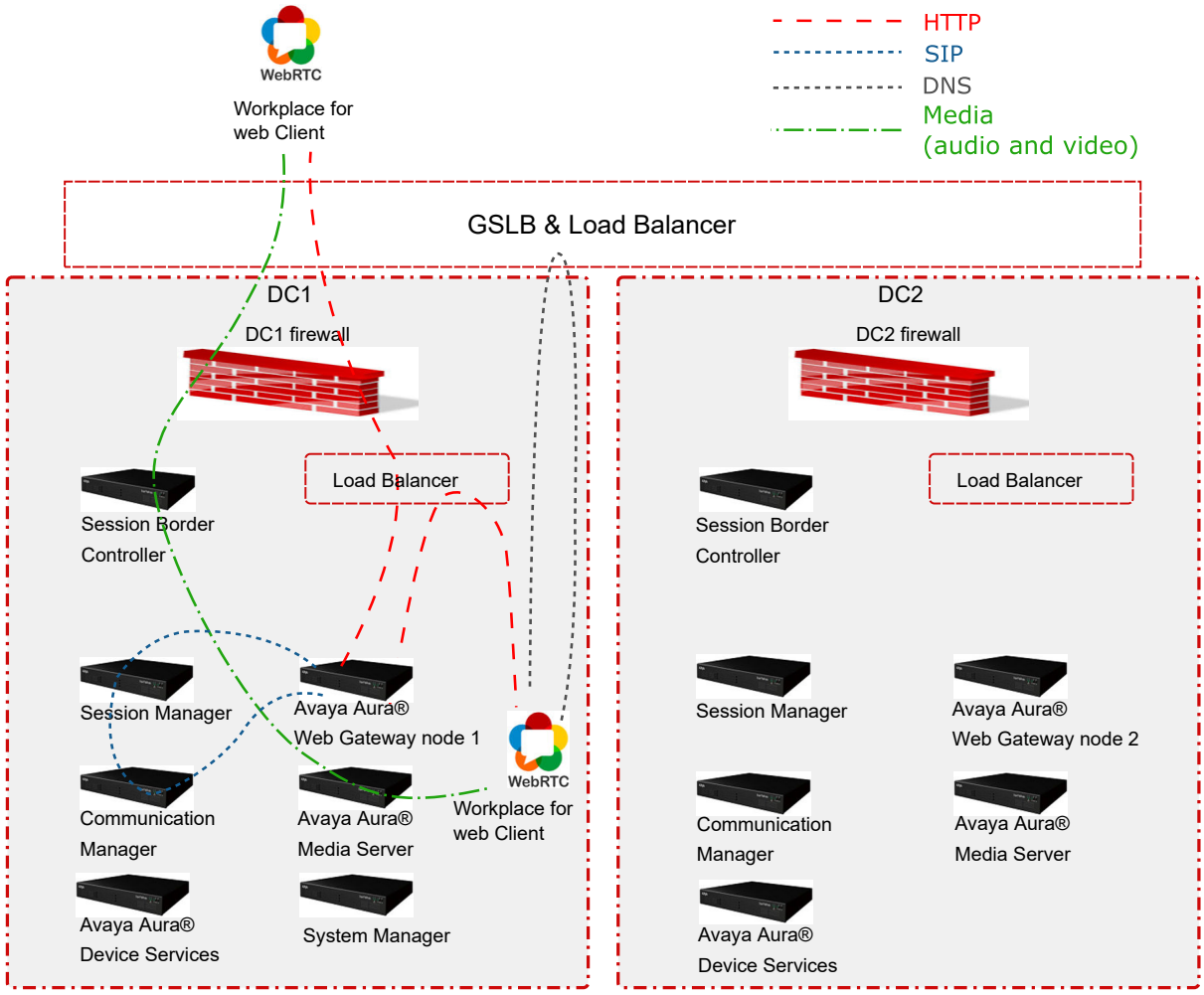
In the following topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. Two clients are located in or near the same data center (DC1):

- The first client is located outside the firewall.
- The second client is located inside the enterprise network.

Both clients are registered on the Avaya Aura® Web Gateway to receive calls. When one client makes a call to the other, the call follows the following flow:

1. Both clients log in to the Avaya Aura® Web Gateway and activate the call service.

   Both clients resolve the FQDN to the address of the load balancer deployed on DC1 and communicate with the Avaya Aura® Web Gateway deployed on DC1.
2. The external client initiates the call.
3. The Avaya Aura® Web Gateway sends the SIP call to Session Manager deployed on DC1.
4. Session Manager deployed on DC1 forwards the call to the same Avaya Aura® Web Gateway deployed on DC1, where the internal client is logged in.
5. The Avaya Aura® Web Gateway deployed on DC1 uses the Session Border Controller and Avaya Aura® Media Server deployed on DC1 to pass the media through to the internal client.



Interoperability

Product compatibility

Avaya Aura® Web Gateway interacts with the following components. For information about interoperability and supported product versions, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

Component	Description
Avaya Aura® infrastructure	The following Avaya Aura® components must be installed and configured to use TLS: • Avaya Aura® Device Services: Provides centralized contact management services using REST-based APIs. • Avaya Aura® Media Server: Supports standard media processing features. **Important:** Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC. • System Manager: Manages Avaya Aura® components, certificates, licenses, and checks log and alarm capabilities. • Session Manager: Enables applications to perform registration and telephony functions, such as call escalation.
Avaya Multimedia Messaging	A server that provides messaging services.
Conferencing	This describes the deployment for Avaya Aura® Web Gateway, but not Conferencing itself. The Avaya Meetings Server solution provides conferencing and collaboration functionality. Avaya Meetings Server is not available with the Avaya Aura® Web Gateway Avaya Workplace Client only deployment option.
Avaya SBCE	A component that provides a common element to enable secure access to the Avaya infrastructure from untrusted networks, such as the internet. In addition to SIP firewall services, this component provides the Reverse Proxy services required for HTTP signaling, media traversal, and access to other data services.

Web browser requirements

The Avaya Aura® Web Gateway administration portal supports the following web browsers:

- Internet Explorer 9, 10, or 11.
- Microsoft Edge 42 and later.
- The latest version of Mozilla Firefox or the version before it.
- Google Chrome 53 and later.

For information about supported browser versions for AWS deployments, see https://aws.amazon.com/console/faqs/#browser_support.

Data encryption

As of Release 3.8, you can enable or disable data encryption when deploying the Avaya Aura® Web Gateway OVA. When data encryption is enabled, all operational data and log files are encrypted.

You can only enable data encryption on Avaya Aura® Web Gateway if are using Appliance Virtualization Platform or a VMware Virtualized Environment. For Amazon Web Services (AWS) deployments, you must enable data encryption on AWS itself. For more information, see How to Protect Data at Rest with Amazon EC2 Instance Store Encryption.

Once data encryption is enabled, you cannot disable it using the configuration utility or the Avaya Aura® Web Gateway administration portal. To disable data encryption, you must redeploy the Avaya Aura® Web Gateway OVA.

If you enabled data encryption and selected the **Require Encryption Pass-Phrase at Boot-Time** option, then you will need to enter the data encryption passphrase after every Avaya Aura® Web Gateway reboot. If you do not select this option, Avaya Aura® Web Gateway enables the local key store to store encryption keys, so you do not need to enter the passphrase manually. However, this is a less secure solution. Alternatively, you can set up a remote key sever to store encryption keys on that server.

Encryption of Avaya Aura® Web Gateway partitions

When you enable data encryption for Avaya Aura® Web Gateway, the following partitions are encrypted:

- sdb: `/var/log/Avaya`
- sdc: `/media/data`
- sdd: `/media/cassandra`

The sda boot disk is always unencrypted.

Related links

Data encryption management on page 129

Administrator responsibilities

After the Avaya Aura® Web Gateway deployment is completed, an administrator can perform the following key management tasks:

- Manage Avaya Aura® Web Gateway services using the web administration portal.
- Set up and customize optional functionality, such as Integration Windows Authentication and multisite support.
- Adjust virtual hardware resources and disk sizes.
- Schedule repairs.
- Check logs and alarms.

- Perform backup and restore operations.
- Upgrade within an Avaya Aura® Web Gateway release or migrate to a new Avaya Aura® Web Gateway release.
- Manage system layer updates.

Chapter 3: Management tools

Setting a timeout period for an SSH session

About this task

You can set up a timeout period for idle SSH connections to Avaya Aura® Web Gateway.

The default timeout period is 10 minutes.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Open the `/etc/profile.d/999-stigs.sh` file in the vi editor with sudo privileges:

   ```
   sudo vi /etc/profile.d/999-stigs.sh
   ```

3. In the `TMOUT=<TIME>` string, replace *<TIME>* with the required timeout period in seconds.

   For example, to change the timeout period to 5 minutes, change the string to `TMOUT=300`
4. Save the file.

Usage of commands and aliases

Linux alias commands

Linux aliases are defined to make frequently used commands easier to use. When an alias is available for the required operation, you can use the alias instead of typing a long path name and using `sudo`. The path name specification and `sudo` invocation are built into the aliases that Avaya provides.

Table 1: Three categories of aliases with their functionality description

Alias	Description
`cdto`	Change to frequently used directories.
`app`	Perform application functions, such as install or backup.
`svc`	Manage the state of application related services.

Some of the alias commands are only available after the application has been installed.

You can type any of the aliases in a Linux shell to list the supported commands.

The following image provides an example of how the aliases are used:

```
[admin@aawg-ova ~]$ cdto

Syntax: cdto <target>

Available navigation targets:

    base            [/opt/Avaya]
    root            [/opt/Avaya/CallSignallingAgent]
    active          [/opt/Avaya/CallSignallingAgent/3.4.0.0.299]
    cas             [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299]
    misc            [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/misc]
    bin             [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/bin]
    config          [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/config]
    logs            [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/logs]
    ilogs           [/opt/Avaya/CallSignallingAgent/.CSAInstallLogs]
    tlogs           [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/tomcat/8.0.24/logs]

[admin@msg-esg ~]$ app

Syntax: app <command> <arguments>

Available commands:

    install         [Run application installer for installation]
    status          [statusCSA.sh]
    configure       [configureCSA.sh]
    listnodes       [clitool-csa.sh listClusterNodes]
    collectlogs     [collectLogs.sh]
    backup          [backupCSA.sh]
    restore         [restoreCSA.sh]
    upgrade         [Run application installer for upgrade]
    rollback        [rollbackCSA.sh]
    removeinactive  [removeVersion.sh (inactive instance)]
    uninstall       [uninstallCSA.sh]
```

Each alias category displays the target command, which is in square brackets. The syntax for the command is provided in the procedures outlined in this document. Arguments that you specify after an alias are passed through to the target command.

The system can simultaneously have both an active and inactive installation of the software. For example, after an upgrade, the earlier version becomes inactive, but the new version becomes active. The alias commands operate only on the active installation unless specified.

Table 2: Examples of alias commands to be used in a Linux shell

Alias example	Function provided
`cdto logs`	Changes to the log directory of the active installation on the system.
`app install`	Runs the staged application installer.
`svc telportal restart`	Restarts the telportal service.

Note:

The aliases must be used only from the command line in a Linux shell. Do not use them in a script. You must use the actual target command in a script.

System layer commands

The **sys** command line alias facilitates the use and discovery of system layer commands. Typing this command without arguments provides syntax help, and a list of supported system layer commands. The following is an example:

```
[admin@server-dev ~]$ sys

Execute system layer commands.

    -h, --help
        Command syntax (this help)

    -hh, --hhelp
        Verbose help

Available commands:

    secconfig       [Manage security settings]
    versions        [Query version information]
    volmgt          [Manage disk volume sizes]
    smcvemgt        [Manage Spectre/Meltdown patches]
    extension       [Manage system layer extensions]
  passwdrules     [Manage password rules]

  Command invocation syntax:
     sys <command> <arguments>

  Command syntax
    sys <command> -h

[admin@server-dev ~]$
```

Important:

For software-deployments, only the following system layer commands are available:

- **sys versions**
- **sys passwdrules**

Other system layer commands are unavailable.

Verbose help information

-hh is used for verbose help information, which provides a brief description of each available system layer command. The following is an example:

```
[admin@server-dev ~]$ sys -hh

The "sys" command line alias facilitates access to the following commands
related to the system layer of UCApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
with command line syntax, and "-hh" (or "--hhelp") for verbose help.
```

```
secconfig
    Manages security-related settings.

versions
    Queries the version information of various elements of the system
    layer.

volmgt
    Queries the sizes of existing disk volumes and extends their sizes.

smcvemgt
    Manages the enablement status of Linux kernel patches for the
    Spectre and Meltdown vulnerabilities.

extension
     Manages the extensions for the system layer. Supported extensions
     are currently limited to the enablement of JAR files in the
     JRE library's extensions directory to support newer application
    loads.

[admin@server-dev ~]$
```

Any arguments provided after the name of the system layer command are passed through to that command.

sys secconfig command

`sys secconfig` provides access to the **`secconfig`** command, which existed in previous releases.

This command is only available for OVA-based deployments.

The following is an example of this command:

```
[admin@server4950csa ~]$ sys secconfig --hhelp

This script is used to manage run-time security settings on this appliance.
The following command-line arguments are available:

    --help, -h
        Prints terse help (command line syntax).

    --hhelp, -hh
        Prints verbose help (this help).

    --sshCBC < --enable | --disable | --query >
    -cbc     < -e       | -d        | -q >
        Enables, disables, and queries the current state of SSH daemon
        CBC-based ciphers.

   --fips  < --enable | --disable | --query >
   Enables, disables, and queries the current state of FIPS on the system.

[admin@server4950csa ~]$
```

sys versions command

The **`sys versions`** command provides a summary of key system layer information, including the type of appliance (OVA), the version number of the system layer, the version of the current partitioning, and the OVA that was originally deployed.

```
[admin@server4889csa ~]$ sys versions
```

```
    Appliance type       : AAWG
    System layer version : 3.4.3.0.2
    Partitioning version : 2.0
    Original OVA deploy  : csa-3.5.0.0.365

[admin@server4889csa ~]$
```

sys volmgt command

Syntax help: sys volmgt --help

The **sys volmgt** command is used to query and extend disk volumes on the system.

Important:

- The **sys volmgt** command is only available if data encryption is *disabled* on Avaya Aura® Web Gateway. If data encryption is enabled, this command is unavailable and you cannot allocate free disk space to disk volumes.
- This command is only available for OVA-based deployments.

The following provides the command line syntax for this command:

```
[admin@server4889csa ~]$ sys volmgt --help

Syntax:
    --help,                  -h
    --hhelp,                 -hh
    --version,               -v
    --status,                -st
    --summary,               -s
    --monitor  [tail|less],  -m [tail|less]
    --logs,                  -l
    --scan
    --extend <volume> [ <n>m | <n>g | <n>t --remaining ]
  --extend --all
    --reset

[admin@server4889csa ~]$
```

Verbose help: sys volmgt --hhelp

The verbose help information for the scripts provides more information about what the tool is used for.

```
[admin@server4889csa ~]$ sys volmgt --hhelp

This script provides for the ability to extend the sizes of volumes on this
system. In order for a volume to be extended in size, the disk that hosts
the volume must first be increased in size using the tools that are used
to manage deployed virtual machines (VMware).

The following example illustrates how to add 20 GiB of storage to the
application log volume (/var/log/Avaya). This volume is located on the second
disk of the system and so this example assumes that disk 2 has been increased
in size by 20 GiB.

    sys volmgt --extend /var/log/Avaya 20g

The above example will do two things:

    1) It will extend the size of the LVM logical volume by 20 GiB.

    2) It will then extend the size of the Linux file system that is
```

```
       located inside that volume to the new size of the LVM logical
       volume.

Step (2) above may take several minutes to complete for larger volumes. If,
for some reason, this second operation is interrupted, it can be re-run
using the same command, but WITHOUT specifying the size argument. For example,
the following command is used to perform step (2) only for the application
log volume (/var/log/Avaya).

    sys volmgt --extend /var/log/Avaya

If in doubt as to whether or not all file systems have been fully extended in
their respective volumes, step (2) can be executed across all volumes using
a single command as follows:

    sys volmgt --extend --all

Performing step (2) on a file system that is already fully extended in its
LVM volume is a null operation (does no harm).

Note the following general points regarding this script:

- The extending of a volume cannot be undone. Make sure the correct volume
  is being extended, and by the correct size. To confirm any extend
  operation, the user is required to enter the response "confirm"
  (case insensitive).

- In order to avoid impacting system performance, avoid performing extend
  operations during periods of high traffic.

- Extend operations are performed by a background process, in order to
  avoid interference due to loss of an SSH connection. Avoid powering down
  or rebooting a server while there is a background operation in progress.
  The presence of a running background operation can be queried as follows:

    sys volmgt --status

- Logical volumes on the system are referenced using their Linux file system
  mount points, such as /var/log/Avaya and /media/data, with the exception
  of the volume containing Linux swap, which has no mount point. The Linux
  swap volume is referenced using "swap".

- Sizes are specified in base 2 units rather than base 10 (SI) units. For
  example, 1g = 1 GiB = 1024 x 1024 x 1024 bytes.

- Summary information is displayed in GiB, with a resolution of two decimal
  places. When extending the sizes of LVM volumes, units can be specified
  in mebibytes (m), gibibytes (g), or tebibytes (t).

- Due to file system overhead allocation by the Linux kernel, the size
  of a file system will never exactly match the size as reported by
  the LVM volume that contains that file system. To be certain that a file
  system is fully extended to the size of the volume that contains it,
  inspect the log file after issuing the extend operation as follows:

      sys volmgt --monitor less

  To perform such a check across all volumes:

      sys volmgt --extend --all
      sys volmgt --monitor less

The following arguments are supported by this script:

    --help, -h
```

```
    Terse help.

--hhelp, -hh
    Verbose help (this help).

--version, -v
    Prints the version of this script to stdout.

--status, -st
    Prints the current status of this tool. Use this to determine
    if there is a background operation in progress, or the results
    of the last background operation.

--summary, -s
    Prints a summary of disks, the LVM volumes contained on each disk,
    and the file system contained in each LVM volume. Disk information
    includes the size of the disk and the amount of free space
    available for allocation to volumes on the disk. LVM volume
    information includes the size of the LVM volume. File system
    information includes the size of the Linux file system and the
    current amount of space that is in use on that file system.

    Due to file system overhead allocation by the Linux kernel, the
    size of a file system will never exactly match the size as reported
    by the LVM volume that contains that file system. Refer to the top of
    this help information for more information.

--monitor [tail|less]
-m        [tail|less]
    Browse the log file for the latest extend operation. Specify "tail"
    to use the tail browser. Specify "less" to use the less
    browser, which allows scrolling and searching through the log file.
    If neither is specified, the browser defaults to the tail browser.

--logs
    Generate a zip file in the current working directory that contains
    all logs generated to date by this script.

--scan
    Scan disks for newly available storage. Do this after increasing
    the disk size of one of more disks. Once scanned, the newly
    available space appears in the "Free" column in the "--summary"
    output, and is now available for allocation to volumes on that disk.

    A summary is printed after the scan to show the updated volume
    information.

--extend <volume> [ <n>m | <n>g | <n>t --remaining ]--extend --all
    The first form of the command operates on a single volume. If a size
    is specified, then the LVM volume is extended by that size (step 1),
    and the file system it contains is extended to use the new space
    made available in that volume (step 2). If a size is not specfied,
    then the file system contained in that volume is extended (i.e.,
    step 2 only).

    The "--all" form of the command is used to perform step 2 across
    all volumes on the system.

    For more information, see the examples at the top of this help.

    If "--remaining" is specified for the size, then the specified
    volume is extended with all remaining free space on that disk.
    If a specific increment is provided, then the volume is extended
    by that amount, reducing the amount of free space on the disk
    by that amount. Specific sizes are in the form of a number
```

```
        (e.g., "10", "10.5", or ".5") and a unit. Units are "m" for
        mebibites, "g" for gibibytes", and "t" for tebibytes".

        The smallest increment that can be specified is 100 MiB.

        Example invocations:

            sys volmgt --extend /var/log/Avaya 10g
            sys volmgt --extend /var/log/Avaya 10.5g
            sys volmgt --extend /var/log/Avaya 0.5g
            sys volmgt --extend /var/log/Avaya .5g
            sys volmgt --extend /var/log/Avaya 500m
            sys volmgt --extend /var/log/Avaya --remaining
            sys volmgt --extend /var/log/Avaya

  --reset
        Resets internal tracking data. Use this if this script is blocked
        on an invalid background progress indication. This condition can
        arise if a background operation was prematurely terminated due to,
        for example, a system reboot. Verify that no background operations
        are in progress prior to executing this command, through verification
        of the process id as reported by the "--status" argument.

[admin@server4889csa ~]$
```

Partitioning examples: sys volmgt --summary

Avaya Aura® Web Gateway supports partitioning version 2.0.

The following example shows a summary of the information provided by this command for a version 2.0 partitioned system:

```
[admin@server4950csa ~]$ sys volmgt -s

                          Disk and Volume Summary

+----------- Disk ------------+------------------- Volume ---------------------+
|                              |                       LVM        File System    |
| Num  Name     Size     Free |    Name               Size      Size     Usage |
+------------------------------+-----------------------------------------------+
|  1   sda      41.78    0.00 | /                      4.00      3.81      1.26 |
|                              | /home                  4.00      3.81      0.05 |
|                              | /opt/Avaya            14.97     14.61      1.14 |
|                              | /tmp                   2.81      2.71      0.01 |
|                              | /var                   3.00      2.89      0.03 |
|                              | /var/log               2.00      1.91      0.00 |
|                              | /var/log/audit         3.00      2.89      0.00 |
|                              | swap                   8.00       n/a       n/a |
+------------------------------+-----------------------------------------------+
|  2   sdb      60.00    0.00 | /var/log/Avaya        60.00     58.93      0.05 |
+------------------------------+-----------------------------------------------+
|  3   sdc      20.00    0.00 | /media/data           20.00     19.56      0.04 |
+------------------------------+-----------------------------------------------+
|  4   sdd      10.00    0.00 | /media/cassandra      10.00      9.71      0.02 |
+------------------------------+-----------------------------------------------+
```

sys smcvemgt command

The system layer **`smcvemgt`** command is used to manage the Linux kernel patches related to the following vulnerabilities:

- Variant #2/Spectre (CVE-2017–5715)
- Variant #3/Meltdown (CVE-2017–5754)

Note:

The kernel patch for the Variant #1/Spectre (CVE-2017–5754) vulnerability is permanently enabled on the system and cannot be disabled.

This command is only available for OVA-based deployments.

The choice to enable or disable these patches is a trade-off between performance and security impact:

- If the patches are enabled, the system might experience noticeable performance losses.
- If the patches are disabled, the system is not protected against the Variant #2/Spectre and Variant #3/Meltdown vulnerabilities.

By default, Linux patches for Variant #2/Spectre and Variant #3/Meltdown are enabled. The Variant #2/Spectre patch is enabled with Linux kernel defaults. In default operation mode, the Variant #2/Spectre Linux patch selects the mitigation method that is best suited for the processor architecture of the host machine.

Note:

To be fully functional, patches for the Variant #2/Spectre vulnerability require hardware support, which is provided by VMware and hardware vendors through microcode updates.

Changes made by the **smcvemgt** command to the Linux kernel tunalbles always cause a server reboot. The script does not manage the state of application services. To ensure that the application services are stopped before the reboot, run the `svc csa stop` command before using the **smcvemgt** command. After the reboot, manually start the application services using the `svc csa start` command.

For more information about Spectre and Meltdown kernel tunables that are affected by the **smcvemgt** command, see https://access.redhat.com/articles/3311301. For more information about the Spectre and Meltdown vulnerabilities, see https://access.redhat.com/security/vulnerabilities/speculativeexecution.

Syntax help: sys smcvemgt --help

```
[admin@server-dev ~]$ sys smcvemgt --help

Version 1.2

Syntax:
    --help,     -h
    --hhelp,    -hh
    --query,    -q
    --set,      -s  enabled
    --set,      -s  disabled
    --set,      -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
        (v2-mode: disabled | default | kernel | user | both | user+retp)
        (v3-mode: disabled | enabled)
    --history
```

Verbose help: sys smcvemgt --hhelp

```
[admin@srvr-dev ~]$ sys smcvemgt --hhelp

Version 1.2

This script manages the enablement status of the Linux kernel patches for the
following Spectre and Meltdown vulnerabilities:
```

```
    Variant #2/Spectre  (CVE-2017-5715)
    Variant #3/Meltdown (CVE-2017-5754)

The kernel patch for the following related vulnerability is permanently enabled
on the system (cannot be disabled):

    Variant #1/Spectre (CVE-2017-5753)

Note that hardware support is required for Variant #2/Spectre to be fully
functional. CPU microcode updates must be applied in order for this hardware
support to be provided. The "--query" argument includes an indication as to
whether or not hardware support is provided on this server.

For more information on Spectre/Meltdown kernel tunables, refer to:

    https://access.redhat.com/articles/3311301

For additional information on the Spectre/Meltdown vulnerabilities, refer
to:

    https://access.redhat.com/security/vulnerabilities/speculativeexecution

Syntax:

    --help,    -h
        Provide terse help.

    --hhelp,   -hh
        Provide verbose help (this text).

    --query,   -q
        Query the configuration of the Variant #2/Spectre and Variant #3/
        Meltdown tunables for system reboots, as well as on the running
        system.

    --set,  -s  enabled
    --set,  -s  disabled
    --set,  -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
        Enables and disables Variant #2/Spectre ("v2") and/or Variant #3/
        Meltdown ("v3") patches.

        This immediately reboots the server. Applications on the server are
        not managed by this script. Ensure that any applications are
        disabled, as required, prior to changing kernel settings with this
        script.

        If "enabled" is specified, then both v2 and v3 are enabled,
        with v2 set to kernel default behavior. If "disabled" is specified,
        then both v2 and v3 are disabled. Otherwise, kernel patches
        are enabled or disbled as per the specified "v2" and/or "v3"
        arguments. If a "v2" or "v3" argument is not specified, the current
        system value for that item is retained.

        v2-mode:

            disabled
                Variant #2/Spectre is disabled.

            default
                The kernel decides how to set tunables for Variant #2/
                Spectre, based on the processor architecture. Note that for
                architectures prior to Skylake, the kernel selects
                retpoline ("return trampoline") over ibrs.

            kernel
```

```
                Use "ibrs" (i.e., kernel space only).

            user
                Use "ibrs_user" (i.e., userland only).

            both
                Use "ibrs_always" (i.e., kernel space and userland).

            user+retp
                Use "retpoline,ibrs_user".

        v3-mode:

            disabled
                Variant #3/Meltdown is disabled.

            enabled
                Variant #3/Meltdown is enabled.
        The following two commands are equivalent:

            sys smcvemgt enabled
            sys smcvemgt v2=default v3=enabled

        The following two commands are equivalent:

            sys smcvemgt disabled
            sys smcvemgt v2=disabled v3=disabled

    --history
        Show a history of changes made to the enablement status of the
        Spectre and Meltdown patches.
```

sys smcvemgt usage examples

Command for querying current tunable settings

The following command queries the current tunable settings for the next boot, as well as the current runtime. This command also indicates whether there is hardware support for Variant #2/Spectre.

```
sys smcvemgt --query
```

Command for enabling patches with default settings

The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is configured for default mode. In default mode, the kernel selects the Variant #2/Spectre mitigation mechanism based on the CPU architecture of the host machine.

```
sys smcvemgt --set enabled
```

Commands for enabling patches with specific settings

- The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is set to kernel space only.

  ```
  sys smcvemgt --set v2=kernel v3=enabled
  ```

- The following command enables patches for Variant #2/Spectre, which are configured for user space with “Retpoline”, or “return trampoline”. Variant#3/Meltdown retains its current settings.

  ```
  sys smcvemgt --set v2=user+retp
  ```

Command for disabling patches

The following command disables patches for Variant #2/Spectre and Variant #3/Meltdown.

```
sys smcvemgt --set disabled
```

Command for disabling patches for a specific vulnerability

The following command disables patches for Variant #3/Meltdown. Variant #2/Spectre retains its current settings.

```
sys smcvemgt --set v3=disabled
```

passwdrules command

Description

sys passwdrules allows you to review and edit complexity rules for passwords that you use to log in to the virtual machine with the Avaya Aura® Web Gateway OVA using an SSH connection.

If data encryption is enabled, these rules also apply to encryption passphrases.

Syntax

```
sys passwdrules [show] [set [options]] [set-default]
```

show	Shows the server password rule configuration, including default, minimum, and maximum values.
set	Sets server password rules. If you do not specify any options, then Avaya Aura® Web Gateway prompts you to configure each option separately. If you do not specify a certain option, Avaya Aura® Web Gateway continues to use the existing rule for this option.
set-default	Sets server password rules to their default values.

Syntax help

```
sys passwdrules [-h | --help]
```

Options

Option	Description
`--diff=`*INTEGER*	Number of characters in the new password that must not be present in the old password.
`--min-len=`*INTEGER*	Minimum length of the password.
`--min-digs=`*INTEGER*	Minimum number of digits in the password.
`-min-upper=`*INTEGER*	Minimum number of uppercase characters in the password.
`--min-lower=`*INTEGER*	Minimum number of lowercase characters in the password.

Table continues…

Option	Description
`--min-other=`*`INTEGER`*	Minimum number of special characters in the password. **Important:** Avaya Aura® Web Gateway supports the following special characters: !, @, #, %, $, ^, *, ?, and _.
`--min-class=`*`INTEGER`*	Minimum number of character classes that must be present in the password. The character classes are: • Digits • Uppercase characters • Lowercase characters • Special characters
`--max-repeat=`*`INTEGER`*	Maximum allowed number of consecutively repeated characters. For example, if you set this parameter to 3, then the following password is invalid: `paaassword`, because `a` is repeated three times.
`--max-class-repeat=`*`INTEGER`*	Maximum allowed number of consecutively repeated characters of the same class. For example, if you set this parameter to 3, then the `pas1sw2or3d` password is invalid, because the first three characters, which are `p`, `a`, and `s`, belong to the same character class.

Example

The following is an example of a command that sets the following password rules:

- At least 16 characters in total.
- At least two digits.
- At least one special character.
- Other settings are default.

```
sys passwdrules set --min-len=16 --min-digs=2 --min-other=1
```

Related links

Configuring password rules on page 150

Data encryption commands

The following sections contains command you can use to manage data encryption. These commands are available if you enabled data encryption during Avaya Aura® Web Gateway OVA deployment.

You cannot enable or disable data encryption using system layer commands.

Important:

- In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.

- These commands are only available for OVA-based deployments.

encryptionPassphrase command

Description

You can run the **sys encryptionPassphrase** command to manage the encryption passphrase.

Syntax

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

add	Enables you to set up an encryption passphrase.
change	Enables you to change the existing encryption passphrase.
remove	Removes the encryption passphrase.
list	Displays information about passphrases and slot assignments.

encryptionStatus command

Description

The **sys encryptionStatus** command displays information about data encryption on Avaya Aura® Web Gateway , including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption password is used.

Syntax

```
sys encryptionStatus
```

encryptionRemoteKey command

Description

You can use the **sys encryptionRemoteKey** command to manage the remote key server. If you run the command without any parameters, Avaya Aura® Web Gateway displays help information about the command.

Syntax

```
sys encryptionRemoteKey [add <server address> [<port>] | remove <server address> | list]
```

add	Enables you to add a remote key server.
remove	Removes the remote key server.
list	Displays general remote key server information.

encryptionLocalKey command

Description

You can use the **disk encryptionLocalKey** command to manage the local key store. If you run this command without any parameters, Avaya Aura® Web Gateway displays help information.

Syntax

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

enable	Enables the local key store.
disable	Disables the local key store.

Chapter 4: Avaya Aura® Web Gateway management with the administration portal

Creating a client certificate

About this task

Use this procedure to create a client certificate, which can be imported into a web browser for authenticating automatic login into the Avaya Aura® Web Gateway web administration portal.

Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. Run the following command to create the `oamp.csr` and `oamp.key` files:

   ```
   sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/misc/createCSR.sh
   ```

3. To generate the `.pem` file, on the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
4. Click the **Add End Entity** tab and complete the following settings:
   a. Set **End Entity Profile** to **Empty**.
   b. Type your user name and password in **Username** and **Password**.
   c. Type your user ID in **CN, Common name**.

      The user ID you provide must use the same format that you used for the **UID Attribute ID** field on the LDAP Configuration tab.

   d. Set **Certificate Profile** to **ENDUSER**.
   e. Click **Add**.

      A new end entity with the specified user name is created on the System Manager web console.
5. In the left navigation pane, click the **Public Web** tab and complete the following settings:
   a. In **Username** and **Enrollment code** , type the same user name and password that you used to create an end entity.
   b. Click **Choose File** to add the `oamp.csr` file, which you generated in step 2 on page 40.

c. Click **OK** to generate the `.pem` file .

6. In the SSH console, run the **`openssl`** command to convert the `.pem` file to a `.pfx/.p12` file.

   The following is an example of the command:

```
sudo openssl pkcs12 -export -out <.p12 file name>-in <.pem file name>.pem -inkey
oamp.key -passout pass:<password>
```

Importing client certificates into web browsers

About this task

Use this procedure to import client certificates to the Google Chrome, Internet Explorer, or Mozilla Firefox web browser. This is an optional procedure. After you perform this procedure, you will automatically be logged in to the web administration portal. The system will bypass the Login screen.

Before you begin

On the HTTP Clients tab, set **OAMP** to one of the following:

- **REQUIRED**: For certificate authentication.
- **OPTIONAL**: For certificate or password authentication.

For information on **OAMP** options, see Available certificate validation options on page 87.

Procedure

1. Navigate to the appropriate location in your web browser:
   - From Google Chrome, navigate to **Settings** > **Show advanced settings** > **Manage certificates**.
   - From Internet Explorer, navigate to **Tools** > **Internet options** > **Content** > **Certificates**.
   - From Mozzila Firefox, navigate to ≡ > **Options** > **Advanced** > **Certificates** > **View Certificates**.
2. Click **Import** to import the certificate to your browser.

   When prompted for a password, enter the same password that was used in the **`openssl`** command to convert the `.pem` file to a `.pfx` or `.p12` file.

   Tip:

   To override the certificate authentication, in the SSH console, set `com.avaya.cas.common.certificateauth` to `0` as follows:

```
CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.common.certificateauth=0"
```

Logging on to the Avaya Aura® Web Gateway administration portal

About this task

Use this procedure to log on to the Avaya Aura® Web Gateway administration portal. You can use this administration portal to configure components and update element settings anytime. You can also manage client requests from the administration portal.

The administration portal also shows the Avaya Aura® Web Gateway deployment type, which must be selected during the initial setup.

The Avaya Aura® Web Gateway administration portal supports the following web browsers:

- Internet Explorer 9, 10, or 11.
- Microsoft Edge 42 and later.
- The latest version of Mozilla Firefox or the version before it.
- Google Chrome 53 and later.

Procedure

1. In your web browser, enter the URL:

   `https://<Gateway_FQDN>:8445/admin/`

   Tip:

   To obtain your FQDN, run the `hostname` command in the Avaya Aura® Web Gateway Linux shell.

   To set up an Avaya Aura® Web Gateway cluster, use the front-end FQDN for the cluster. If you are using an external load balancer, the front-end FQDN for the cluster will be the FQDN of the load balancer. If not, it will be the FQDN of the virtual IP assigned to the Avaya Aura® Web Gateway cluster.

2. Log on to the Avaya Aura® Web Gateway administration portal using one of the following:
   - Credentials of the user that was configured as an LDAP server administrator.
   - Linux administration account credentials.

System overview settings

Reviewing Avaya Aura® Web Gateway service status information

About this task

Use this procedure to view system overview information and server settings.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **System Overview**.

   The page displays information about the deployment type, server status, and node status.

2. **(Optional)** To modify server settings, in the Solution Servers area, click a server from the Required Server column.

   The appropriate Avaya Aura® Web Gateway administration portal page for the server you selected is displayed.

Avaya Aura® Media Server connectivity status indicators

On the System Overview page, Avaya Aura® Web Gateway displays the consolidated status for all Avaya Aura® Media Servers connected to Avaya Aura® Web Gateway. The following table shows the status indicators that Avaya Aura® Web Gateway can display.

Status indicator	Description
	All servers are available and can be used for calls.
	At least one server cannot accept requests. Other servers are available.
	At least one server cannot accept requests. Other servers are inactive.
	The system cannot obtain the status of any server.

Restarting services on an Avaya Aura® Web Gateway node

About this task

Use this procedure to restart services on any Avaya Aura® Web Gateway node from the administration portal.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **System Overview**.
2. In the Service Control area, select the node you want to restart from the drop-down list.
3. Click **Restart**.

   Avaya Aura® Web Gateway displays a pop-up window informing you that the restart is in progress.

   - If you are restarting a local node, you cannot continue working with the administration portal. You must wait until the restart is completed and then click **OK** to log in.
   - If you are restarting a remote node, press **Hide** and continue working with the administration portal. You can check whether the restart is completed and the node is back online in the Node Status area.

Identifying the seed node

About this task

In a cluster environment, you must perform certain procedures, such as upgrade, on the seed node first. Use this procedure to identify the seed node.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **System Overview**.
2. Navigate to the Cluster table.

   The seed node IP address and FQDN are listed in the Initial Node row.

Configuring general network settings on the Avaya Aura® Web Gateway

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **General Network Settings**.
2. Click the appropriate tab.

   The procedures below describe the tasks you can perform on each tab.

Updating System Manager settings

About this task

Use this procedure to fetch Media Server and Location lists from System Manager.

Procedure

1. Click the **System Manager** tab.
2. In **FQDN**, type the System Manager FQDN address.
3. In **Port**, type the System Manager port number.

   The default port number is 443.
4. In **Protocol**, select **https**.
5. Type the System Manager administration account login ID and password.

   The System Manager account must have the “View access” privilege for all media server elements.
6. Click **Save**.

Configuring the Avaya Aura® Device Services host to obtain user data

Procedure

1. Click the **Device Services** tab.
2. In **FQDN**, type the Avaya Aura® Device Services FQDN address.

   Important:

   Ensure that the Avaya Aura® Device Services FQDN is resolvable from the Avaya Aura® Web Gateway server. Open the Linux shell using the Linux administrator account credentials, and type the `ping <AADS-FQDN>` command to test DNS resolution of the Avaya Aura® Device Services FQDN from the Avaya Aura® Web Gateway.
3. In **Client interface port**, type the port that is used to access Avaya Aura® Device Services.

   The port must match the port configuration on Avaya Aura® Device Services. The default value is `443`.
4. If you are upgrading or installing the Avaya Aura® Web Gateway for the first time, type `8440` in **Server-to-server interface port**.

   This port enables the Avaya Aura® Web Gateway to establish a connection with Avaya Aura® Device Services. The value in this field is automatically populated if the Avaya Aura® Device Services configuration already exists.

   Tip:

   If you need to enable port 8440 on Avaya Aura® Device Services, go to the `cdto misc` directory and run the `sudo ./dynamicconfigurations-patch.sh enable` command on every node in the cluster.

   If you need to disable this port from the firewall rule, you can use the `sudo ./dynamicconfigurations-patch.sh disable` command.
5. In **Protocol**, select **https** or **http**.

   This selection must match the configuration on Avaya Aura® Device Services.
6. Click **Save**.
7. **(Optional)** To clear the local device services data, in the Clear Local Device Services Data area, click **Clear**.

Managing location settings

Managing Avaya Aura® Web Gateway locations

Procedure

1. Click the **Location** tab.
2. In the Web Gateway Locations area, under **Address**, verify the Avaya Aura® Web Gateway FQDN.

   This value should be automatically populated.
3. In **Location**, select the appropriate location for each server FQDN from the list of locations.

   The location information is retrieved from System Manager.

   For an Avaya Aura® Web Gateway cluster setup, set the location for each node in the cluster.

   The FQDN for each node is added automatically.
4. Click **Save**.

Managing Avaya Aura® Media Server location and priority settings for the Avaya Aura® Web Gateway

About this task

Use this procedure to assign and prioritize locations for each Avaya Aura® Web Gateway location. In a location, the Avaya Aura® Web Gateway uses the available servers in the Assigned Locations area.

Procedure

1. Click the **Location** tab.
2. In the Location Assignments and Priorities area, from **Web Gateway Location**, select an Avaya Aura® Web Gateway location.
3. To add an Avaya Aura® Media Server location to the Assigned Locations list, select the location from the Input Location list and then click **Add**.

   You can click **Add All** to add all listed locations to the Assigned Locations list.
4. **(Optional)** To remove an Avaya Aura® Media Server location from the Assigned Locations list, select the location and then click **Remove**.

   The removed Avaya Aura® Media Server locations are added to the Input Location area.
5. Drag and drop the servers in the Assigned Locations to rearrange their priority.

   The order you set in the Assigned Locations list determines how the Avaya Aura® Media Server locations will serve the selected Web Gateway location.

6. Click **Save**.
7. Repeat the steps above for each location listed in **Web Gateway Location**.

Verifying the LDAP server configuration settings

About this task

Use this procedure to modify the LDAP configuration settings so that they are consistent with the Avaya Aura® Device Services settings.

Procedure

1. Click the **LDAP Configuration** tab.
2. Modify the LDAP configuration settings as needed.

   The settings are described in Enterprise LDAP Server Configuration field descriptions on page 49.
3. Ensure that **UID Attribute ID** is set to the same value that is in Avaya Aura® Device Services.
4. Modify or update other parameters related to LDAP as required and then click **Save**.
5. Click **Test Connection** to verify the connection.
6. If the connectivity test fails, check the configured LDAP address FQDN, port, and protocol, and then run the test again.

Reviewing Avaya Aura® Media Server status

About this task

Use this procedure to review the connectivity status and availability of Avaya Aura® Media Server for a specific node in a cluster.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, do one of the following:
   - On the System Overview page, click **Media Services**.
   - Navigate to **General Network Settings** > **Media Services**.
2. For a cluster environment, in the **Node Address** field, select the required node.

   Avaya Aura® Web Gateway displays a table with information about Media Servers for the selected node.
3. In the Status column, hover over the Avaya Aura® Media Server status icon to see performance information.

4. **(Optional)** To edit Avaya Aura® Media Server settings, click the required Avaya Aura® Media Server host name and do one of the following:
   - If you are redirected to the System Manager web administration portal, log in using System Manager credentials with access privileges for Avaya Aura® Media Server.
   - If you are redirected to the Avaya Aura® Media Server web administration portal, log in using Avaya Aura® Media Server credentials.

LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of the Avaya Aura® Web Gateway. The LDAP Configuration screen on the Avaya Aura® Web Gateway web administration portal displays the enterprise LDAP server that you configured during deployment.

You cannot perform all LDAP server management tasks with the configuration utility. Use the Avaya Aura® Web Gateway web administration portal to do the following:

- Configure multiple LDAP directories.
- Specify an order in which the Avaya Aura® Web Gateway accesses LDAP directories.
- Select which LDAP directories are used for authentication.
- Configure multiple base context Distinguished Names (DNs).
- Set up LDAP synchronization.
- Configure attribute mappings.

Important:

- For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. For more information, see Importing the secure LDAP certificate using the web administration portal on page 85.
- If FIPS is enabled on Avaya Aura® Web Gateway, you must use the secure LDAP (LDAPS) connection to access LDAP servers.

Adding a new enterprise LDAP server

About this task

Before you begin

If you are planning to use multiple authentication domains, configure the UID mapping attributes as specified in Configuring the UID mapping attributes when using multiple authentication domains on page 55.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   Avaya Aura® Web Gateway displays the Enterprise LDAP Server Configuration page.

2. Click the plus (+) icon.

   Avaya Aura® Web Gateway displays the New Directory tab.

3. In the **Enterprise-Directory Type** field, click the LDAP server directory that you want to add.
4. In the **Provenance Priority** field, type the priority of the enterprise LDAP server directory.
5. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP server directory.

   For more information about attributes, see Enterprise LDAP Server Configuration field descriptions on page 49.

6. If you want to use the new server for authentication and authorization, do the following:
   a. Select the **Use for Authentication** check box.
   b. Configure role-related attributes, such as **Role Filter**, **Role Attribute ID**, and **Role Context DN**.
7. Click **Save**.

Enterprise LDAP Server Configuration field descriptions

Name	Description
Enterprise-Directory Type	Specifies the name of the enterprise directory. The options are: • ActiveDirectory_2012 • ActiveDirectory_2016 • ActiveDirectory_2019 • Novell 8.8 • Domino 7.0 or 8.5.3 • LDS_2012 • OpenLDAP 2.4.44 • OracleDirectoryServer 11.1.1
Provenance Priority	Specifies the provenance priority of the enterprise directory. Provenance priority is used while merging contacts. If a value is available in more than one directory, the directory value with higher provenance priority is returned. For example, if firstName is obtained from two directories, the firstName from the source with higher provenance priority is returned. You can assign a value between 2 to 10. You cannot assign Provenance priority 1 because it is always assigned to the authorization directory. Provenance priority 1 is the highest, and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.

Server Address and Credentials

Name	Description
Secure LDAP	Indicates whether the LDAP server connection is secure or not. If FIPS is enabled, you must use the secure LDAP connection to access LDAP servers. If you are using a secure LDAP connection, you must also import the LDAP server trusted certificate to the Avaya Aura® Web Gateway.
Import Certificate	Specifies the LDAP server trusted certificate. This field is mandatory if you are using a secure LDAP server connection. This field is only displayed when the **Secure LDAP** check box is selected.
Windows Authentication	Specifies whether to use Windows Authentication. The options are: • None • Negotiate If you select the Negotiate option, the system displays the **Configuration for Windows Authentication** section. **Note:** Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.
Address	Specifies the IP address or FQDN of the LDAP server. This field is mandatory.
Port	Specifies the port of the LDAP server. This field is mandatory.
Bind DN	Specifies the Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is a mandatory setting. The format of the Bind DN depends on the configuration of the LDAP server. This field is mandatory. **Note:** Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind.

Table continues…

Name	Description
	For example: for Active Directory, you can use `domain \user`, `user@domain`, as well as the actual DN of the user object.
Bind Credential	Specifies the password of the administrative user. The password length can be from 1 to 20 characters.
Base Context DN	Specifies the complete Distinguished Name (DN) with the Organizational Unit (OU) for starting the search for users on the enterprise directory. This is the primary Base Context DN for the Avaya Aura® Web Gateway. For example, `dc=domain, dc=company, dc=com`. If you are using multiple authorization domains, Avaya recommends including a domain component to the Base Context DN. For example, `dc=avaya, dc=com`. **Note:** Some LDAP sources, such as Domino, typically do not contain the domain component in Base Context DNs. For example, `o=MyCompany`. If Base Context DNs do not contain the domain component, the Avaya Aura® Web Gateway considers them “empty” Base Context DNs when processing user login or search requests. If the Avaya Aura® Web Gateway cannot find the domain specified in the request, the search continues in “empty” Base Context DNs.
Use additional Base Context DN	Enables Avaya Aura® Web Gateway contact search and quick search. The primary Base Context DN is used for authentication. Additional Base Context DNs are used for Avaya Aura® Web Gateway contact search and quick search, and can also be used for authentication. You can configure up to 10 additional Base Context DNs. If you select this check box, you can see the **View/Edit** button. Auto-configuration will use only the primary base context DN.
View/Edit	Enables access to the Addition Base DN Configuration page, where you can add or delete additional Base Context DNs.
UID Attribute ID	Specifies the unique attribute of the user on LDAP, which is used to search for users in the LDAP server. If you are using multiple authentication domains, you must use one of the following values: • `mail` • `userPrincipalName` • Any custom attribute that uses a domain-qualified value

Table continues…

Name	Description
	If you are not using multiple authentication domains, you must use one of the following values: • `sAMAccountName` • `mail` • `userPrincipalName` This field is mandatory.
Role Filter	Specifies the search filter used to search the role of the user. For example, (&(objectClass=group) (member={1})
Role Attribute ID	Specifies that the user is a member of the groups defined by that attribute. For example, objectCategory This field is mandatory.
Roles Context DN	Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter. For example, dc=domain,dc=company,dc=com
Role Name Attribute	Specifies the name of the role attribute. This field is mandatory only if the **Role Name Attribute Is DN** field is set to true. For example, cn if the role is stored in a DN in the form of cn=admin, ou=Users, dc=company, dc=com.
Role Attribute is DN	Indicates whether the role attribute of the user contains DN. The default value is true.
Allow Empty Passwords	Indicates whether LDAP Server acknowledges the empty password. The default value is false.
Search Scope	Specifies the search level in the LDAP hierarchy. The options are: • Object: For searching only for the object. • One Level: For including one level in the LDAP hierarchy in the search. • Subtree: For including subtree in the LDAP hierarchy in the search. The default value is Subtree.
Role Recursion	Specifies whether role recursion is enabled. The options are: • true

Table continues…

Name	Description
	• false If your LDAP configuration includes nested groups, you can set the **Role Recursion** parameter to `true` so that Avaya Aura® Device ServicesAvaya Aura® Web Gateway computes role membership by searching through LDAP structures recursively. For example, the user jsmith can be in the Sales group, which can be in the AAWG users group. In this case, Role Recursion must be set to true for jsmith to be recognized as a member of the AAWG users group. If you set this parameter to `false`, Avaya Aura® Web Gateway does not compute the role membership information recursively.
Administrator Role	Specifies the administrator role in which the administrative users are assigned.
Security Administrator Role	Specifies the security administrator role in which the administrative users can manage web certificates from the web administration portal.
User Role	Specifies the user role in which the common users are assigned.
Auditor Role	Specifies the auditor role in which the users can audit the system.
Services Maintenance and Support Role	Specifies the services maintenance and support role in which users can maintain and support services.
Services Administrator Role	Specifies the services administrator role.
Language used in Directory	• Simplified Chinese (zh) • German (de) • English (en) • Spanish (es) • French (fr) • Italian (it) • Japanese (ja) • Korean (ko) • Russian (ru) • Portuguese (pt)
Active Users Search Filter	Specifies whether the user is active or inactive on LDAP Server.
Last Updated Time Attribute ID	Specifies when the user is updated on LDAP. For example, `whenChanged`

Table continues…

Name	Description
	This field is mandatory.

Configuration for Windows Authentication

Name	Description
Service Principal Name (SPN)	Specifies the service principal name UIDAttributeID must be userPrincipalName.
Import keytab file	Imports the `tomcat.keytab` file and overwrites the existing file.
Kerberos Realm	Specifies the Kerberos realm.
DNS Domain	Specifies the DNS domain of the Domain Controller.
KDC FQDN	Specifies the FQDN of the Domain Controller.
KDC Port	Specifies the port number. The default KDC port is 88.

Button	Description
Test Connection	Tests the connection changes.
Save	Saves the changes made to the enterprise directory.
Modify Attribute Mappings	Modifies the attributes of the LDAP server.

Configuring additional base context DNs

About this task

Use this procedure to add additional base context DNs. Base context DNs are used to specify sections of the LDAP directory where LDAP searches for:

- Contacts, when performing LDAP lookups. The use of multiple base context DNs ensures maximum search performance.
- Groups, when configuring and publishing settings using the Dynamic Configuration service.

When configuring additional Base Context DNs, use

You can add up to 10 base context DNs for one LDAP source.

You can also use an additional base context DN for authentication. In this case, this additional base context DN uses the role context DN that is configured in the primary LDAP server.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.
2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and then click **View/Edit**.
4. In the Additional Base Context DN Configuration window, click **+**.

5. In the table, click the **Base Context DN** field and then provide the value of the base context DN.
6. If you want to use the base context DN for authentication, select the **Use for Authentication** check box.
7. Click **Save**.
8. In the Server Address and Credentials section, click **Save**.

Modifying the provenance priority

About this task

If you configured multiple LDAP servers , use this procedure to specify the order in which Avaya Aura® Web Gateway accesses LDAP directories. For example, if a givenName attribute is defined in two LDAP servers for a given user, the value that Avaya Aura® Web Gateway uses is based on the order you define.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   Avaya Aura® Web Gateway displays the Enterprise LDAP Server Configuration page.
2. Click the **Enterprise Directory** tab that you want to use to modify the provenance priority.
3. In the **Provenance Priority** field, click **Modify**.

   Avaya Aura® Web Gateway displays the Source Priority Configuration pop-up window.
4. In the **Provenance Priority** column, type the priority level.

   You can assign a value between 2 to 10. You cannot assign Provenance priority 1 as it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.
5. Click **Save**.
6. Restart Avaya Aura® Web Gateway to apply the new priority.

Configuring the UID mapping attributes when using multiple authentication domains

About this task

If you are using multiple authentication domains, the UID mapping attribute value set for each LDAP server must be domain-qualified. Therefore, the value must include the `@domain` part. The following values are supported:

- `mail`
- `userPrincipalName`
- Any custom attribute that uses a domain-qualified value.

Note:

If you are not using multiple authentication domains, the Avaya Aura® Web Gateway supports only the following values for the UID mapping attribute:

- `sAMAccountName`
- `mail`
- `userPrincipalName`

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   The system displays the Enterprise LDAP Server Configuration page.

2. For each LDAP server configured on the Avaya Aura® Web Gateway, in the **UID Attribute ID** field, enter the appropriate value.

Administering the LDAP server configuration

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   Avaya Aura® Web Gateway displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP Server.
3. Modify the details of the enterprise directory.
4. Click **Save**.

Modifying enterprise directory attribute mappings

About this task

Each LDAP directory type includes a set of pre-defined attributes mappings, which map user attributes that Avaya Aura® Web Gateway uses to LDAP attributes defined in the default LDAP schema for the respective LDAP directory type. If you use a custom LDAP schema for your LDAP directory type, you must customize the attribute mapping accordingly.

Avaya Aura® Web Gateway search results do not include attributes that are not mapped to LDAP attributes.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   Avaya Aura® Web Gateway displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, click **Modify Attribute Mappings**.

Avaya Aura® Web Gateway displays the Enterprise Directory Mappings page. The Modify LDAP Attribute Mappings table contains the following columns:

- Application Field Name contains user attributes that Avaya Aura® Web Gateway uses.
- Directory Field Name contains pre-defined attributes from the standard LDAP schema.
- Custom Field Name enables you to enter custom attribute names.

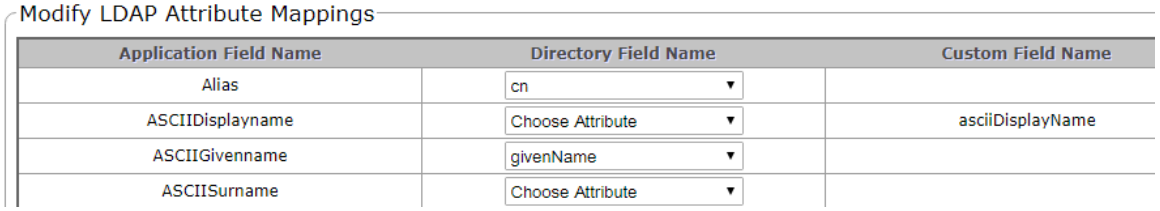
4. In the Modify LDAP Attribute Mappings section, do one of the following for the required attribute:
   - To select one of the pre-defined LDAP attributes, click the **Directory Field Name** cell and then select the required LDAP attribute from the list.
   - To use a custom LDAP attribute, click the **Custom Field Name** cell and enter the name of the required custom LDAP attribute.
   - To un-map the attribute, clear the **Custom Field Name** value and set **Directory Field Name** to **Choose Attribute**.
5. **(Optional)** If you want to reset the attribute mapping to its default settings, click **Reset**.
6. Click **Save**.

   Avaya Aura® Web Gateway restarts to apply changes.

Example

The following image shows an Active Directory 2012 attribute mapping example, where:

- Alias and ASCIIGivenname attributes use default mapping.
- ASCIIDisplayname attribute is mapped to the custom asciiDisplayName LDAP attribute.
- ASCIISurname is not mapped to any LDAP attribute



Configuring Windows Authentication for Active Directory

About this task

Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.

Before you begin

Ensure that the LDAP server you use is the Domain Controller with the appropriate Active Directory version as the server type.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

The system displays the Enterprise LDAP Server Configuration page.

2. In the Server Address and Credentials section, do the following:
   a. In the **Windows Authentication** field, click **Negotiate**.
   b. In the Confirm Action pop-up window, click **OK**.
   c. The **UIDAttributeID** must be userPrincipalName.
   d. Ensure that the other settings on the Server Address and Credentials page are appropriate for the LDAP configuration of your Domain Controller.
3. In the Configuration for Windows Authentication section, do the following:

   Tip:

   To complete the following fields, use the same values you entered when setting up the Windows Domain Controller.

   a. In **Service Principal Name**, type `HTTP` or `REST_FQDN`.

      For example, type `HTTP` or `aads.example.com`.

   b. To import the `tomcat.keytab` file transferred from the Windows Domain Controller, in **Import keytab file**, click **Import**.

      In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

      You can use the following command to generate a `tomcat.keytab` file.

      ```
      ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /
      princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass
      +rndPass /crypto all /kvno 0
      ```

      In the following example, `<Domain User Login>` is `csa_user`, `<Kerberos realm>` is `EXAMPLE.COM`, and `<FRONT—END FQDN>` is `csa.example.com`.

      ```
      ktpass /out c:\tomcat.keytab /mapuser csa_user@EXAMPLE.COM /princ HTTP/
      csa.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto
      all /kvno 0
      ```

   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in uppercase letters.

      For example, `EXAMPLE.COM`.

   d. In **DNS Domain**, type the DNS domain of the Domain Controller.

      For example, `example.com`.

   e. In **KDC FQDN**, type the FQDN of the Domain Controller.

      This value also includes the DNS domain at the end.

      For example, `ad.example.com`.

   f. In **KDC Port**, do not change the default setting , which is 88.

   g. In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file to a specific node.

This option is useful if the import to a node failed or if you add a new node to your cluster.

4. Save the settings to restart the server.

   The settings you specified are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

Configuring the internationalization parameters

About this task

The internationalization parameters specify how a user's given name and surname are stored in Microsoft Active Directory (AD), as well as the language used to store these names. Optionally, for non-Latin script languages, two of the parameters also specify how the ASCII transliteration of these names is stored.

The following procedure describes how to configure the LDAP internationalization parameters when AD is used.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.

   Avaya Aura® Web Gateway displays the Enterprise LDAP Server Configuration page.

2. Configure the language setting:

Parameter	Description	Default value
Language used in Directory	The language code of one of the languages supported by the Avaya Aura® Web Gateway.	English (en)

3. Click **Save**.
4. Click **Modify Attribute Mappings**.
5. Configure the following settings:

Parameter	Description	Default value
NativeFirstName	The attribute that stores the "given name" of the user in the language of the LDAP server.	givenName
NativeSurName	The attribute that stores the "surname" of the user in the language of the LDAP server.	sn
GivenName	This is only applicable if the language in AD is one of the non-Latin script based ones.	
SurName	This is only applicable if the language in AD is one of the non-Latin script based ones.	

The NativeFirstName and NativeSurName parameters allow the user to identify the LDAP attributes used to store the user's native language given name and surname. These are mandatory parameters with defaults of givenName and sn.

The GivenName and SurName parameters allows the user to identify the LDAP attributes used to store the ASCII transliteration of the user's given name and surname, respectively. These are optional parameters and only used only if the Language used in Directory parameter is set to one of the non-Latin script languages.

The internationalization of the names must be done using the language tags specified in RFC 3866.

To configure internationalization for Microsoft Active Directory, you must configure custom attributes for the native and the ASCII transliterations of the names, if both types of names are needed.

6. Click **Save** to apply changes and restart the Avaya Aura® Web Gateway.

Configuring Avaya Meetings Server settings on the Avaya Aura® Web Gateway

About this task

Use this procedure if your deployment includes Avaya Meetings Server.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Avaya Meetings Server** > **Avaya Meetings Management**.
2. In **Avaya Meetings Management IP**, type the Avaya Meetings Server Management server IP address.

   The system automatically populates the following SIP settings after the connection with Avaya Meetings Server is established:

   - **FQDN**
   - **SIP Port**
   - **SIP Transport**
3. Click **Save**.
4. To complete the portal settings, navigate to **Avaya Meetings Server** > **Unified Portal Settings**.
5. In the Unified Portal Settings area, configure the settings as described in Unified Portal settings field descriptions on page 61.
6. Click **Save**.

Next steps

Complete the settings on the Avaya Meetings Server Management portal as described in the Avaya Meetings Server configuration section in *Deploying the Avaya Aura® Web Gateway*.

Configuring WebRTC media adaptation

About this task

WebRTC media adaptation enables the routing of WebRTC calls to the Avaya Meetings Server server through either Avaya Aura® Media Server or Avaya Meetings Media Server. Up until solution 9.1.3, if Full Transcoded Video mode was used, you could disable media adaptation to route WebRTC calls directly to the Avaya Meetings Server. However, now, you should always enable media adaption by the AAMS (TE solution) or AEWG (OTT solution).

Starting from Avaya Aura® Web Gateway Release 3.7, WebRTC media adaptation is configured using Avaya Meetings Management. You must also ensure that WebRTC media adaptation is disabled on the Avaya Aura® Web Gateway administration portal.

Procedure

1. On Avaya Meetings Management, configure adaptation settings as described in “Configuring Avaya Meetings Media Server for WebRTC-based calls in Team Engagement deployments” in *Administering Avaya Meetings Media Server*.
2. On the Avaya Aura® Web Gateway administration portal, navigate to **Avaya Meetings Server** > **Avaya Meetings Management**.
3. Clear the **Force Media Server usage for WebRTC calls** check box.

Related links

Configuring WebRTC and presentation capabilities for the Microsoft Edge browser on page 64

Unified Portal settings field descriptions

The following table describes the options available in **Avaya Meetings Server** > **Unified Portal Settings**.

Name	Description
Conference Clients	Specifies the set of clients that can be used by the Unified Portal to join conferences. Only the **Avaya Workplace Client and Web Client** option is supported. You cannot edit the **Conference Clients** field value.
Avaya Workplace Client Aura Video Ignore	Specifies whether the Unified Portal can ignore the Avaya Workplace Client videoCapable parameter.
Allow Recording Guest Access	Specifies whether a guest user can access recordings from the Unified Portal.
Allow Portal Guest Access	Specifies whether a guest user can access any functionality on the Unified Portal.

Table continues…

Name	Description
Allow AAWG Guest Access	Specifies whether a guest user can join meetings using the Avaya Workplace Client for Web (MeetMe) that are launched by the Unified Portal.
Web MeetMe WebRTC Browser Type	Specifies which web browser types can access the Unified Portal and use the following WebRTC conferencing capabilities: • Audio • Video • Presentation. For example: screen sharing. If this field does not contain a browser name and **Web MeetMe Data Only Browser Type** contains this browser name, then you can access the Unified Portal and use Presentation Only conferencing capabilities.
Web MeetMe Data Only Browser Version Exclusion	Specifies which web browsers types and versions cannot access the Unified Portal and use Presentation Only conferencing capabilities, such as screen sharing. To provide a browser version and type, use the following format: `<browser type>:<browser version>`. Use semicolons to separate entries. Use commas to separate different versions of the same browser. For example: `Chrome:64.0,65,66,67;Firefox:60.0,61.0;Safari:9.4`.
Web MeetMe Data Only Browser Type	Specifies which web browser types can access the Unified Portal and use Presentation Only conferencing capabilities, such as screen sharing. **Note:** WebRTC features, such as audio and video, are not supported in Presentation Only mode.
Avaya Workplace Client Aura Domain	Specifies the SIP domain of enterprise users that is required for Avaya Workplace Client to join a meeting.
Web MeetMe WebRTC Browser Version Exclusion	Specifies which web browser types and versions cannot access the Unified Portal and use WebRTC conferencing capabilities. To provide a browser version and type, use the following format: `<browser type>:<browser version>`. Use semicolons to separate entries. Use commas to separate different versions of the same browser. For example: `Chrome:64.0,65,66,67;Firefox:60.0,61.0;Safari:9.4`.

Table continues…

Name	Description
Web MeetMe WebRTC Browser Min Version	Specifies the minimum browser version that can access the Unified Portal and use WebRTC capabilities, such as audio, video, and presentation. To provide a minimum browser version, use the following format: `<browser type>:<browser version>`. Use semicolons to separate entries. For example: `Chrome:55.0;Firefox:52.0;Edge:17`. If **Web MeetMe WebRTC Browser Type** does not contain a browser name but this field contains a minimum supported version for that browser, you can use WebRTC conferencing capabilities on browser versions that satisfy the minimum version requirement.
Web MeetMe Data Only Browser Min Version	Specifies the minimum browser version that can access the Unified Portal and use Presentation Only capabilities, such as screen sharing. To provide a minimum browser version, use the following format: `<browser type>:<browser version>`. Use semicolons to separate entries. For example: `Chrome:53.0;Firefox:52.0;IE:11;Safari:9.3.1;Edge:17` If **Web MeetMe Data Only Browser Type** does not contain a browser name but this field contains a minimum supported version for that browser, you can use Presentation Only conferencing capabilities on browser versions that satisfy the minimum version requirement.
Avaya Workplace Client Aura Min Version	Specifies the minimum supported Avaya Workplace Client version. The default value is 3.1
Avaya Workplace Client MeetMe Min Version	Specifies the minimum supported Avaya Workplace Client version to join a meeting in Presentation Only mode. The default value is 3.2

Enabling the lockout policy for Unified Portal accounts

About this task

By default, the Unified Portal does not lock a user account if the user enters an invalid password multiple times. You can enable the lockout policy so that Unified Portal accounts become locked after multiple consecutive failed login attempts. When the lockout policy is enabled, a user has five attempts to enter a valid password by default. You can change this value as appropriate.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI using an SSH connection.

2. Open the `/opt/Avaya/CallSignallingAgent/<version>/nginx/1.18.0-1/conf` file in a text editor.

   For example: `vi /opt/Avaya/CallSignallingAgent/<version>/nginx/1.18.0-1/conf`

3. In all `#limit_req zone=ups_login burst=5 nodelay;` strings in the file, remove the leading `#` character.

4. **(Optional)** To change the default number of login attempts, in all `limit_req zone=ups_login burst=5 nodelay;` strings in the file, replace `5` with the appropriate number of login attempts.

   For example, to allow three login attempts, update the strings as follows:

   ```
   limit_req zone=ups_login burst=3 nodelay;
   ```

5. Save the file.

Configuring WebRTC and presentation capabilities for the Microsoft Edge browser

About this task

To access WebRTC and presentation capabilities from the Microsoft Edge browser, you must configure the appropriate browser version on the Unified Portal Settings page. You must also enable Avaya Aura® Media Server adaptation to route WebRTC calls through Avaya Aura® Media Server.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Avaya Meetings Server** > **Avaya Meetings Management**.
2. Select the **Force Media Server usage for WebRTC calls** check box.
3. Click **Save**.
4. Navigate to **Avaya Meetings Server** > **Unified Portal Settings**.
5. In **Web MeetMe Data Only Browser Min Version** and **Web MeetMe Data Only Browser Min Version** fields, add the `Edge:17` entry.

   If these fields already contain another version of Microsoft Edge, then change the version to `17`.

   If you have multiple browsers, use a semicolon to separate each entry. For example: `Chrome:53.0;Firefox:52.0;Edge:17`.

6. Click **Save**.

Related links

Configuring WebRTC media adaptation on page 61

Unified Portal settings field descriptions on page 61

Configuring WebRTC and presentation capabilities for other browsers

About this task

To access WebRTC and presentation capabilities from your browser, you must configure the appropriate browser version on the Unified Portal Settings page. Use this procedure to update the default WebRTC and presentation configuration settings for other browsers, such as Internet Explorer, Firefox, or Chrome.

Note:

You cannot use Safari for audio or video calls. Safari only supports presentation capabilities, such as screen sharing.

This procedure does not describe the configuration for the Microsoft Edge browser. For more information about Microsoft Edge configuration, see Configuring WebRTC and presentation capabilities for the Microsoft Edge browser on page 64.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Avaya Meetings Server** > **Unified Portal Settings**.
2. In the **Web MeetMe WebRTC Browser Min Version** field, enter the browser type and the minimum browser version for WebRTC capabilities in the *<browser type>*:*<browser version>* format.

   If you have multiple browsers, use a semicolon to separate each entry. For example: `Chrome:53.0;Firefox:52.0;Edge:17`
3. In the **Web MeetMe Data Only Browser Min Version** field, enter the browser type and the minimum browser version for presentation-only capabilities in the *<browser type>*:*<browser version>* format.

   If you have multiple browsers, use a semicolon to separate each entry. For example: `Chrome:53.0;Firefox:52.0;Safari:11;Edge:17`
4. Click **Save**.

Related links

Configuring WebRTC and presentation capabilities for the Microsoft Edge browser on page 64
Unified Portal settings field descriptions on page 61

External access configuration

This section describes the configuration required to access the Avaya Aura® Web Gateway from outside the enterprise network through Avaya Session Border Controller for Enterprise (Avaya SBCE), which is located at the edge of the enterprise network.

Important:

Ensure that the front-end port for remote access has been enabled and set as required.

To configure the front-end port settings, see the “Front-end host, System Manager, and certificate configuration” section *Deploying the Avaya Aura® Web Gateway*.

Managing HTTP reverse proxy settings

About this task

Use this procedure if the Avaya Aura® Web Gateway is fronted by an HTTP reverse proxy that modifies any aspect of the Avaya Aura® Web Gateway service access URLs, such as the FQDN, HTTP protocol, port, or base path.

Important:

Only modify these settings if the reverse proxy serves all requests to the Avaya Aura® Web Gateway. This includes requests from clients both internal and external to the enterprise.

If the reverse proxy serves *only* external clients, ensure that the reverse proxy’s configuration accepts requests on port 443 and proxies requests to the Avaya Aura® Web Gateway on the remote access port.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access** > **HTTP Reverse Proxy**.
2. **(Optional)** If required, in **Front-end Port**, update the port value.

   The default port is 443.
3. In **Front-end Protocol**, select **http** or **https**.
4. **(Optional)** If you want to use a reverse proxy FQDN instead of the front-end FQDN set up on the Avaya Aura® Web Gateway, select the **Use Front-end Host from a client request** check box.

   If you select this check box, the certificates enabled for reverse proxy must include your FQDN in the SAN. The DNS entry for your FQDN must also point to the appropriate IP address.

   You can also select this check box if you require multiple FQDNs for the Avaya Aura® Web Gateway portal service. In this case, the reverse proxy must be configured to forward all of the IP addresses or FQDNs to the Avaya Aura® Web Gateway portal server virtual IP address. The certificate installed on the reverse proxy must include all the FQDNs that are

used in the SAN. For more information about required FQDNs and certificates, see *Deploying the Avaya Aura® Web Gateway*.

5. If you have any external clients, including WebRTC, mobile, or desktop clients outside the enterprise firewall, do the following to enable a remote port:
   a. Select the **Enable port for external access** check box.
   b. In **Front-end port for external access**, enter a value between 1024 and 65535.

      The default port value is 8444.

   This port setting must be configured in the reverse proxy so traffic for clients outside the firewall is translated from the front-end port to this remote access port.
6. To use an external load balancer, select the **Enable use of an external load balancer** check box.

   An external load balancer is mandatory for geographically distributed systems.
7. If the FQDN of the external load balancer differs from the Avaya Aura® Web Gateway front-end FQDN, provide the FQDN of the external load balancer in the **Front-end Host** field.

   Important:

   If you use an external load balancer, you must regenerate Avaya Aura® Web Gateway identity certificates so that the certificate SAN includes the external load balancer FQDN. For more information about managing identity certificates, see Managing identity certificates on page 77.
8. Click **Save**.

Related links

Geographical distribution overview on page 17

Managing STUN server settings

About this task

Use this procedure to add and prioritize STUN servers for an Avaya Aura® Web Gateway location. You must also ensure that the STUN or TURN server details have been configured on the co-located Avaya Aura® Media Server systems.

If you use client side TURN, you must add the IP address of Avaya SBCE as a STUN server. Avaya recommends using client side TURN whenever possible.

Procedure

To add a new STUN server, do the following:

1. Navigate to **External Access** > **STUN Servers**.
2. Click **Add**.

3. In **Address**, type the FQDN or IP address of the Avaya SBCE external B1 interface configured for STUN/TURN.

   Important:

   Ensure that this IP address or FQDN is accessible to the clients. These clients might use computers that are external to the enterprise and might also require a STUN server to make a call or join a meeting.

4. In **Port**, type `3478`.
5. Click **Save**.

To set the STUN priority, do the following:

6. From **Web Gateway Location**, select an Avaya Aura® Web Gateway location.
7. To add a STUN server to the Assigned STUN Servers list, select the server from the Input STUN Servers list and then click **Add**.

   You can click **Add All** to add all listed servers to the Assigned STUN Servers list.

8. **(Optional)** To remove a STUN server from the Assigned STUN Servers list, select the server and then click **Remove**.
9. In the Assigned STUN Servers area, drag and drop the servers to rearrange them.

   The order you set in the Assigned STUN Servers list determines how the STUN servers will serve the selected Web Gateway location.

10. Click **Save**.
11. Repeat the steps STUN priority steps above for each location listed in **Web Gateway Location**.

Managing Avaya Session Border Controller for Enterprise connection settings

About this task

Use this procedure to add an Avaya SBCE to the Avaya Aura® Web Gateway web administration portal. Avaya SBCE is needed for external desktop clients. Avaya SBCE Release 7.2 is required for HTTP tunneling support.

Before you begin

Perform the configuration on the Avaya SBCE administration portal as described in the “Avaya Session Border Controller for Enterprise configuration” section in *Deploying the Avaya Aura® Web Gateway*.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access** > **Session Border Controller**.

2. To enable TURN usage, select the **Enable TURN in WebRTC Client** check box.

   Avaya recommends enabling TURN in the browser client for performance reasons. For information about TURN in a WebRTC client, see TURN usage in a WebRTC client on page 69.

3. Click **Add** to add a new Avaya SBCE or click **Edit** to update the information for an existing Avaya SBCE connection.
4. Complete the following settings for the connection:
   a. In **SIP Address**, type the address of the internal interface specified for signaling on Avaya SBCE.
   b. In **SIP Port**, type `5060` if you are using TCP or `5061` if you are using TLS.
   c. In **SIP Protocol**, select **TCP** or **TLS**.
   d. In **HTTP Address**, type the internal address specified for the load monitoring entry.
   e. In **HTTP Port**, type `80` if you are using HTTP protocol or `443` if you are using HTTPS protocol.
   f. In **HTTP Protocol**, select **http** or **https**.
   g. In **Location**, specify the location of the Avaya SBCE server.

      You only need to specify the location for one node, and it is propagated to all other nodes in the cluster.
5. Click **Save**.

   After you add a new Avaya SBCE connection, the details for that connection are displayed on the screen. The connectivity status for the Avaya SBCE is also displayed.

TURN usage in a WebRTC client

Avaya's WebRTC solution is based on a TURN client residing on the Avaya Aura® Media Server or Scopia Elite MCU inside the enterprise. If the WebRTC browser is behind a restricted firewall that blocks UDP traffic, WebRTC media connections to Avaya Meetings Server or another WebRTC browser will not work. The solution for this issue is to use the WebRTC TURN client in the browser and send media to Avaya SBCE through UDP port 3478 or TCP/TLS port 443. The UDP port is preferable for Quality of Service (QoS) reasons. If you use TURN on TLS, media will be encoded back to UDP by the TURN server on Avaya SBCE.

Note:

For performance reasons, Avaya recommends enabling TURN in the browser client instead of using server-side TURN.

If you use TURN from browser, disable TURN on the Avaya Aura® Media Server and Scopia Elite MCU. If you need to place a firewall between Avaya SBCE and the Avaya Aura® Media Server or Scopia Elite MCU, enable STUN on the Avaya Aura® Media Server or Scopia Elite MCU.

Avaya SBCE must be configured to support the combination of the following ports:

- STUN UDP 3478

- TURN UDP 3478
- TURN TCP/TLS 443

For more information about Avaya SBCE configuration, see *Administering Avaya Session Border Controller for Enterprise*.

Currently, the TURN feature is supported in the following browsers:

- Google Chrome
- Mozilla Firefox

Avaya SBCE connectivity status indicators

After you add an Avaya SBCE on the Avaya Aura® Web Gateway web administration portal, the connectivity status for that Avaya SBCE is also displayed. The following table describes the status indicators:

Status indicator	Status name	Description
	Active	Indicates that the server is available and can be used for calls. When you hover over this indicator, additional details, such as audio and video session, and Avaya SBCE bandwidth, are displayed.
	Overloaded	Indicates that the server is overloaded and calls cannot be made.
	Inactive	Indicates that the load monitoring cannot be retrieved for the server.
	Unknown	Indicates that the server status has not been fetched.

Reviewing the Avaya SBCE status for a specific node

About this task

Use this procedure to review the connectivity status and availability of Avaya SBCE servers for a specific node. In geographically distributed systems, Avaya SBCE from one location might be inaccessible to Avaya Aura® Web Gateway from another location, so the connectivity status might be different for different nodes.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access** > **Session Border Controller**.
2. In a cluster environment, from the **Node address** drop-down list, select the required Avaya Aura® Web Gateway node.

Result

Avaya Aura® Web Gateway displays the connectivity status of Avaya SBCE servers for the node. For more information about the connectivity status, see Avaya SBCE connectivity status indicators on page 70.

Note:

If the Avaya Aura® Web Gateway node is inactive, then all Avaya SBCE servers have an “Unknown” status.

Providing information about guest SIP domain and SIP proxy

About this task

You must provide information about the SIP server that Avaya Oceana® clients use for SIP communication so that the Avaya Aura® Web Gateway can send SIP requests to these clients.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access** > **Guest SIP Proxy**.
2. To provide information about the guest SIP domain, do the following:
   a. In the **Default Guest SIP Domain** field, specify the domain configured for Avaya Oceana® clients on Session Manager.
   b. Click **Save**.
3. To provide information about the guest SIP proxy, do the following:
   a. In the Guest SIP Proxy section, click **Add**.
   b. In the new row of the table, provide the following information:
      - **SIP Address**: The entity IP address of the Session Manager that is used by Avaya Oceana® clients.
      - **SIP Port**: The port used for SIP connection.
      - **SIP Protocol**: The protocol used for SIP connection.
      - **Location**: The appropriate location.
      - **Weight**: Enter `100`.

Log management

Changing the logging level

About this task

The logging level that you select determines which system events Avaya Aura® Web Gateway includes in log files. Avaya support personnel can use these log files for troubleshooting purposes. If the log files that you provide do not contain enough information, support personnel will ask you to select another logging level.

Unless you are told to change the logging level, use the following recommended logging levels:

- INFO: For the Client Application Service Logs category.
- WARNING: For all other log categories.

After selecting a new logging level, you must wait until the issue reoccurs before you can send updated logs to support personnel. When the issue is resolved, you *must* switch back to the recommended logging level.

Important:

Increasing logging details results in larger log files and might also decrease the system performance.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **Logs Management**.
2. In the Adjust Service Logging Level area, in **Logger**, select a log category.
3. In **Current logging level**, select the required logging level.

   Unless support personnel ask you to change the logging level, use the recommended INFO or WARNING logging levels.
4. Click **Save**.

Related links

Important logs and alarms on page 154

Configuring log retention

About this task

Log files can contain private or sensitive information. To maximize data privacy and security, you can configure log retention and specify how long you want to keep logs. After this retention period, Avaya Aura® Web Gateway deletes log files within an hour.

The default log retention period depends on whether data encryption is enabled as follows:

- If data encryption is disabled, the default period is 1 day.
- If data encryption is enabled, the default period is 30 days.

Avaya recommends that you set the log retention period to at least 8 days, unless your organization’s policies defines another retention period.

If a log file exceeds a size limit, Avaya Aura® Web Gateway deletes this log file even if the log retention period is not expired.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, click **Logs Management**.
2. Select the **Use Log Retention** check box.
3. In **Retention period (days)**, set the period for which you want to keep log files on Avaya Aura® Web Gateway.

The range is 1 to 365 days.

4. Click **Save**.

Disabling log retention

About this task

When log retention is disabled, Avaya Aura® Web Gateway will only delete log files when they exceed a size limit.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, click **Logs Management**.
2. Clear the **Use Log Retention** check box.
3. Click **Save**.

Downloading logs

About this task

Use this procedure to download Avaya Aura® Web Gateway logs to your computer. Support personnel can use the log files you collect for troubleshooting purposes.

You can only collect and download logs for one node at a time. You cannot download logs for an entire cluster at once.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **Logs Management**.
2. In the Collect Logs area, in **Number of rotated log files to collect (1-20)**, enter the number of logs you want to download.

   This setting specifies the number of files from the log file history to include in the log collection. The range is 1 to 20. If you leave this field empty, Avaya Aura® Web Gateway collects all available logs.
3. To collect logs for a node, click **Collect** in the corresponding row.
4. Wait until Avaya Aura® Web Gateway collects the logs and then click **OK**.
5. To download the logs you collected for a node, click **Download**.

Scheduling log collection

About this task

Certain log levels, such as FINEST, provide very detailed information about events on Avaya Aura® Web Gateway. However, enabling these log levels on a constant basis might negatively

impact the Avaya Aura® Web Gateway performance. You can enable detailed logging temporarily for a specified time period. After the specified period expires, Avaya Aura® Web Gateway switches back to the original log level, which you configure in the Adjust Service Logging Level area.

Scheduled log collection cancels automatically if you change the original log level for any log category.

After enabling scheduled log collection for a log category, you cannot set up scheduled log collections for other log categories until the specified time period expires or you cancel scheduled log collection.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, go to **Logs Management**.
2. In the Log capture scheduling area, select a log category for which you want to enable scheduled log collection.
3. In the **Planned log level** field, select a log level that you want to enable on a temporary basis for the log category.
4. **(Optional)** If required, repeat steps 2 and 3 for other log categories.
5. In the **Schedule Start Time** field, select one of the following:
   - **Immediate**: To start collecting logs at the planned log level immediately.
   - **Specify Time**: To specify the date and time when you want to start collecting logs at the planned log level.
6. In the **Duration** field, select one of the following:
   - **Select Duration**: To specify the period during which Avaya Aura® Web Gateway collects logs at the planned log level.
   - **No Duration (Indefinite)**: To set the log level specified in the **Planned log level** field as the new default log level for the log category.

     Note:

     When you select **No Duration (Indefinite)**, Avaya Aura® Web Gateway does not schedule log collection at the specified log level. Instead, Avaya Aura® Web Gateway sets up the new default log level for the log category starting from the time specified in the **Schedule Start Time** field.
7. Click **Schedule**.
8. In the confirmation window, click **Save**.

Result

Avaya Aura® Web Gateway saves the configuration and displays the schedule status on the page.

Related links

Canceling scheduled log collection on page 75

Canceling scheduled log collection

About this task

You can cancel scheduled log collection at any time. If you cancel scheduled log collection when it is in progress, Avaya Aura® Web Gateway switches back to the original log level immediately.

Scheduled log collection cancels automatically if you change the original log level for any log category in the Adjust Service Logging Level area.

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, go to **Logs Management**.
2. In the Log capture scheduling section, click **Cancel Schedule**.
3. In the confirmation window, click **Save** and then click **OK**.

Related links

Scheduling log collection on page 73

Configuring licensing

About this task

Use this procedure to verify the licenses that the Avaya Aura® Web Gateway obtains from System Manager.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **Licensing**.

   The feature licensing values are automatically populated.

2. Ensure that the information is correct and that none of the licenses have expired.

   The values are obtained from System Manager. You can update these values on the Avaya Aura® Web Gateway administration portal by navigating to **General Network Settings** > **System Manager** if they are incorrect.

   For more information on WebLM license configuration on System Manager, see *Administering Avaya Aura® System Manager*.

Specifying the WebLM server for the Avaya Aura® Web Gateway

About this task

Use this procedure to select a WebLM server for the Avaya Aura® Web Gateway.

By default, the Avaya Aura® Web Gateway uses the WebLM server that is hosted on System Manager. If you use the System Manager URL for the WebLM server, then the WebLM URL is automatically changed when you:

- Modify the System Manager FQDN using the configuration utility.
- Generate certificates from the Generate Identity Certificates via System Manager area of the web administration portal. For more information, see Managing System Manager certificates on page 77.

If you use a specific WebLM URL, this URL will not be changed when the System Manager URL is changed or new identity certificates are generated.

Note:

Users with the Auditor role cannot edit WebLM settings.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Licensing**.
2. Do one of the following:
   - To use the WebLM server hosted on System Manager, select the **Use SMGR url for license server** check box.
   - To use a specific WebLM server, clear the **Use SMGR url for license server** check box, and then provide the FQDN of the WebLM server and the port for connecting to the WebLM server.
3. Click **Save**.

Security settings

Managing certificates in the Avaya Aura® Web Gateway web administration portal

About this task

You can use the Avaya Aura® Web Gateway administration portal to review and manage certificates. The management options in the administration portal do not replace the setup that you need to complete during installation. After installation is completed, use the web administration portal for management when possible. Only use the configuration utility if the administration portal is not available or for troubleshooting purposes.

Before you begin

- You must have the Security Administrator role to access certificate management options.
- In a cluster environment, ensure that all nodes in the cluster are running.

Procedure

1. On the web administration portal, navigate to **Security Settings** > **Certificate Management**.
2. Click the appropriate tab.

   The procedures below describe the tasks you can perform on each tab.

Managing System Manager certificates

About this task

Use this procedure to manage System Manager security identity certificates.

Procedure

1. Click the **SMGR Certificates** tab.
2. In the Generate Identity Certificates via System Manager area, update the following fields if they are not automatically populated:
   - **System Manager Address**: To update this setting, navigate to **General Network Settings** > **System Manager**.
   - **System Manager HTTPS Port**: To update this setting, navigate to **General Network Settings** > **System Manager**.
   - **Common Name**: To update this setting, navigate to **External Access** > **HTTP Reverse Proxy**.
3. In the **Node Address** drop-down menu, do one of the following to generate a certificate:
   - Choose a node for a cluster configuration.

     If you choose the **All Cluster Nodes** option, certificates will be generated automatically for all cluster nodes.
   - Keep the default setting for a standalone configuration.
4. In **System Manager Enrollment Password**, type the enrollment password as defined on the System Manager web console.
5. Click **Generate Certificates** to start requesting certificates from System Manager.
6. Restart the Avaya Aura® Web Gateway after the certificates are generated.

   This completes all the certificate updates. For a cluster environment, only the remote node is restarted.

Managing identity certificates

Procedure

1. Click the **Identity Certificates** tab.
2. Use the following subsections to manage CSRs, keystore data, and server identity certificates.

3. After performing the required task, when prompted, restart the Avaya Aura® Web Gateway server for the changes to take effect.

Managing CSRs

Procedure

In the Certificate Signing Requests area, do one of the following:

- To set up a new CSR, click **Create** and then follow the steps in Creating CSRs on page 78.
- To remove an existing CSR, select it and then click **Delete**.
- To process a signed CSR, click **Process Signing Request**. For more information, see Processing CA signing requests on page 79.

Creating CSRs

About this task

This procedure provides a high-level overview of how to create CSRs.

Procedure

1. If you clicked **Create** in the Certificate Signing Requests area, complete the following settings in the Create Certificate Signing dialog box and then click **Apply**.
   a. In **Alias**, type an alias using alphanumeric characters.

      An example of an alias is `ottawacrt123`.

   b. Complete the other settings as required.

      You can use the **Show Advanced Settings** button to view additional settings information. For more information about settings, see Create Certificate Signing Request screen field descriptions on page 78.
2. Ensure that the CSR file is successfully saved on your computer.

   The generated CSR is also added to the Certificate Signing Requests area.

   In a cluster configuration, the CSR list on all nodes is identical.
3. **(Optional)** In a cluster environment, if the CSR is not available on a node, click **Propagate** to synchronize requests from the current node to the cluster.

Next steps

Provide the CSR file to the CA for signing and apply the signed CSR as described in Processing CA signing requests on page 79.

Create Certificate Signing Request screen field descriptions

Name	Description
Alias	The name of the certificate
Common Name	The FQDN of the node. For example, `amm.example.com` You cannot provide wildcard (*) characters in this field.

Table continues…

Name	Description
Use Existing FQDNs for SAN	Use this option to select a particular node in a cluster for which a certificate should be generated. You can also select all cluster nodes.
Specify SAN manually	Use this option to manually specify additional FQDNs or IP addresses for which the certificate should be generated.
Subject Alternative Name	An optional text field that can be used to further identify this certificate. You can provide multiple entries in this field. You cannot provide wildcard (*) characters in this field.
Key Bit Length	The certificate key length in bits.
Signature Algorithm	The hash algorithms to be used with the RSA signature algorithm.
Organizational Unit	The group within the company or organization creating the certificate.
Organization	The name of the company or organization creating the certificate.
City/Locality Name	The city where the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Country (ISO 3166)	The name of the country within which the certificate is being created in the ISO 3166 format. For more information about the format, see ISO 3166 country codes.

Processing CA signing requests

About this task

Use this procedure to process CA signing requests and upload signed certificates to Avaya Aura® Web Gateway.

If you want to use an identity certificate signed by a third-party CA, you must import an identity certificate chain in either PEM or PKCS12 format. This chain must contain the identity certificate signed by the third-party CA, all intermediate CA certificates, and the root CA certificate.

Procedure

1. Use the appropriate CA documentation to sign the signing request with the CA.
2. In the Certificate Signing Request area, select the appropriate signing request and then click **Process Signing Requests**.
3. In the Process Signing Request dialog box, click **Choose file** to add the signed certificate and then click **Apply**.

Result

The signed certificate is removed from the Certificate Signing Requests area and added to the Keystore area.

Related links

Generating an identity certificate chain in the PEM format on page 82
Generating an identity certificate chain in the PKCS12 format on page 83

Managing keystore data

Procedure

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then import keystore data.

  For more information, see Importing keystore data on page 80.
- To export a certificate in the PKCS12 format, select a keystore file and then click **Export**.

  In the Export Certificate dialog box, you can enter a password to protect your exported file.
- To view keystore file details, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

Importing keystore data

About this task

Use this procedure to import third-party identity certificates to the Avaya Aura® Web Gateway Keystore.

Procedure

If you clicked **Import**, complete the following settings in the Import Certificate dialog box and then click **Apply**.

1. In the **Certificate Type** drop-down menu, select a format for importing the certificate.
2. From **Certificate File**, click **Choose file** to add the certificate file in the selected format.
3. If you selected the PEM format, in **Key File**, click **Choose file** to add the key file in the PEM format.
4. If you selected the PKCS12 format, in **Password**, type the password for the imported certificate.
5. In **Alias**, type an alias to be used for the imported certificate.

Managing server interface certificates

About this task

Use this procedure to manage Keystore identity certificates.

Procedure

1. Navigate to the Server Interfaces area.
2. In a cluster environment, select the node to administer from the **Node Address** list.
3. Do one of the following:
   - To assign the certificate to a specific server interface, click **Assign** and then complete the settings in the Assign Certificates dialog box as described in Certificate assignment descriptions on page 81.

If you assign a certificate only to a selected node, then you must restart the services on that node to apply the changes. If you assign a certificate to the entire cluster, you must restart all nodes in the cluster.

- To view details about the certificate, click **Details**.
- To export the certificate in the PKCS12 format, click **Export**.

Certificate assignment descriptions

Name	Description
Application	Specifies the interface for REST API to the clients.
Internal	Specifies the interface being used for server-to-server component communication.
OAM	Specifies the Operations, Administration, and Maintenance (OAM) interface.
SIP	Specifies the SIP interface.

Installing third-party CA certificates

About this task

Use this procedure if you want to use certificates signed by a third-party CA instead of certificates signed by System Manager.

Before you begin

Obtain a third-party CA-signed identity certificate, all intermediate CA certificates, and the root CA certificate. Do one of the following:

- Create a certificate signing request (CSR). For more information, see Managing CSRs on page 78.

  Note:

  If the CA provides certificates as separate PEM files, you must manually generate an identity certificate chain. For more information, see Generating an identity certificate chain in the PEM format on page 82.

- Obtain a certificate bundle in the PKCS12 format from the CA. The PKCS12 bundle must include a private key, the identity certificate, all intermediate CA certificates, and the root CA certificate. To view the bundle content and ensure that it includes a full certificate chain, run the `openssl pkcs12 -info -in <pkcs12_certificate_file_name>` command.

  If the CA provides the identity certificate as a separate `.p12` file, generate an identity certificate chain. For more information, see Generating an identity certificate chain in the PKCS12 format on page 83.

Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal.
2. Navigate to **Security Settings** > **Certificate Management** > **Identity Certificates**.
3. In the Keystore area, click **Import** and then select either the identity certificate chain in the PEM format or the PKCS12 certificate bundle.

4. In the Server Interfaces area, select the required server interface.
5. Click **Assign** and then select the certificate chain or PKCS12 bundle that you imported in step 3 on page 81.

   Avaya Aura® Web Gateway restarts to apply the changes.
6. Navigate to **Security Settings** > **Certificate Management** > **Truststore**.
7. Click **Import** and then select the third-party root CA certificate and all intermediate CA certificates.

Next steps

Install the third-party root CA certificate and all intermediate CA certificates on the clients.

Generating an identity certificate chain in the PEM format

About this task

If you want to use an identity certificate signed by a third-party certificate authority (CA), you must generate an identity certificate chain. An identity certificate chain must include the following certificates in order:

1. The third-party CA-signed identity certificate.
2. All intermediate CA certificates, if any.
3. The root CA certificate.

Assign this certificate chain to a specific Avaya Aura® Web Gateway server interface.

Use this procedure to generate an identity certificate chain in the PEM format.

Before you begin

Ensure that you have the third-party CA-signed identity certificate, root CA certificate, and all intermediate CA certificates in the PEM format. If these files are in the PKCS12 format, you can convert these certificates to the PEM format using the OpenSSL tool.

Procedure

1. Log in to the Avaya Aura® Web Gateway using your SSH credentials.
2. Navigate to the directory with the certificates.
3. Run the **`cat`** command as follows:

   ```
   cat <Identity_ertificate_file_name>
   <Intermediate_CA_certificate_file_name> <Root_CA_file_name> >
   <Certificate_chain_file_name>
   ```

   If you have several intermediate CA certificates, list all intermediate CA certificate file names, separated by a space, and then list the root CA certificate file name.

   For example, if you have the identity certificate `identity.crt`, two intermediate CA certificates (`intermediateCA1.crt` and `intermediateCA2.crt`), and root CA certificate `rootCA.crt`, run the following command to generate a certificate chain with the `identityChain.crt` file name:

```
cat identity.crt intermediateCA1.crt intermediateCA2.crt rootCA.crt
> identityChain.crt
```

Related links

Managing server interface certificates on page 80

Generating an identity certificate chain in the PKCS12 format

About this task

If you want to use an identity certificate signed by a third-party certificate authority (CA), you must generate an identity certificate chain. An identity certificate chain must include the following certificates:

1. The third-party CA-signed identity certificate.
2. All intermediate CA certificates, if any.
3. The root CA certificate.

Assign this certificate chain to a specific Avaya Aura® Web Gateway server interface.

Use this procedure to generate an identity certificate chain in the PKCS12 format. You must do this if the CA does not provide a PKCS12 certificate chain that includes all required certificates.

Tip:

The commands in this procedure must be entered as a single line even if they appear as multiple lines in the document.

Before you begin

- Ensure that the OpenSSL library is installed on Avaya Aura® Web Gateway.
- Ensure that you have the following certificate files:
  - The third-party CA-signed identity certificate in the PKCS12 format.

    Certificate files in the PKCS12 format usually have the `.p12` extension.
  - A certificate chain in the PEM format that includes all intermediate and root CA certificates.

Procedure

1. Log in to the Avaya Aura® Web Gateway using your SSH credentials.
2. Navigate to the directory with the certificates.
3. Run the following command to get a private key from the identity certificate file:

   ```
   openssl pkcs12 -in <certificate_file_name> -out <private_key_file>
   -nocerts
   ```

   In this command:

   - `<certificate_file_name>` is the file name of the identity certificate in the PKCS12 format.
   - `<private_key_file>` is a file name of the private key.

   For example: `openssl pkcs12 -in certificate.p12 -out privateKey.key -nocerts`

4. Run the following command to get the identity certificate in the PEM format from the `.p12` certificate file:

   ```
   openssl pkcs12 -in <certificate_file_name> -out
   <identity_certificate> -nokeys
   ```

   In this command:

   - `<certificate_file_name>` is the `.p12` certificate file name.
   - `<identity_certificate>` is a file name of the identity certificate in the PEM format.

   For example: `openssl pkcs12 -in certificate.p12 -out certificate.pem -nokeys`

5. Run the following command to create an identity certificate chain in the PKCS12 format:

   ```
   openssl pkcs12 -export -out <certificate_chain> -inkey
   <private_key_file> -in <identity_certficiate> -certfile
   <CA_certificate_chain>
   ```

   In this command:

   - `<certificate_chain>` is the file name of the resulting identity certificate chain in the PKCS12 format.
   - `<private_key_file>` is the file name of the private key.
   - `<identity_certificate>` is the file name of the identity certificate in the PEM format.
   - `<CA_certificate_chain>` is the file name of a certificate chain in the PEM format that includes all intermediate and root CA certificates.

   For example: `openssl pkcs12 –export -out certificateChain.p12 -inkey privateKey.key -in certificate.pem -certfile CACert.pem`

Related links

Managing server interface certificates on page 80

Managing truststore certificates

About this task

Use this procedure to manage truststore certificates available on the Avaya Aura® Web Gateway.

Procedure

1. Click the **Truststore** tab.
2. In the Truststore area, select a certificate and then click one of the following:
   - **Import**: To import a certificate in PEM or PKCS12 format.

     If the file imported into the truststore contains multiple certificates, then all CA certificates from the file will be imported. Alias names, other than the first certificate in the chain, are appended with the suffix `_<X>`, where `<X>` indicates a certificate number, such as 1, 2, or 3.

If a new certificate is imported into the truststore or if any certificate is removed from the truststore, then you must restart the system to apply the change. In a cluster environment, all nodes in the cluster must be restarted.

- **Details**: To view information about the certificate.
- **Delete**: To delete the certificate from the truststore.

  Important:

  After you remove a certificate form the truststore, restart the Avaya Aura® Web Gateway to apply certificate updates. For a cluster configuration, restart the remote node.
- **Export**: To export the certificate in the PEM format.

Importing the secure LDAP certificate using the web administration portal

About this task

For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. The following procedure describes how to import the LDAP certificate using the Avaya Aura® Web Gateway web administration portal.

Before you begin

Ensure that the FQDN that is configured as the address of the LDAP source is defined in one of the following places:

- The Common Name in the Subject field.
- Subject Alternative Name.

You can use the following **openssl** command in the Avaya Aura® Web Gateway CLI to verify the certificate content:

```
openssl s_client -connect <ldap server:port> | openssl x509 -noout -text
```

Procedure

1. On the Avaya Aura® Web Gateway web administration portal, navigate to **General Network Settings** > **LDAP Configuration**.
2. Select the **Secure LDAP** check box.
3. Click **Import Certificate**.
4. In the Import Certificate window, click **Choose File** and select the certificate from your computer.
5. Click **Save**.

   Avaya Aura® Web Gateway uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, Avaya Aura® Web Gateway overwrites the existing certificate.

Configuring HTTP clients

About this task

Use this procedure to enable communication between the Avaya Aura® Web Gateway and the clients that use HTTP-based Avaya Aura® Web Gateway services over the REST and OAMP interface.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **HTTP Clients**.
2. Set the following options:
   a. **REST** to **NONE**, which is the default value.

      This setting enables guest users to join conference calls.

   b. **OAMP** to **OPTIONAL**.

      This setting validates certificates presented by clients that are using Avaya Aura® Web Gateway services.
3. Click **Save**.

Related links

Available certificate validation options on page 87

Configuring the certificate policy for Avaya Oceana® integration

About this task

Avaya Aura® Web Gateway validates the certificates presented by servers that generate token requests. When a third-party guest access server requests a token, Avaya Aura® Web Gateway verifies the client certificate and ensures that it is trusted.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **HTTP Clients**.
2. In the Client-Device Certificate Policy section, set **REST** to **OPTIONAL**.
3. Click **Save**.

Related links

Available certificate validation options on page 87

Available certificate validation options

Name	Description
OPTIONAL	Enables the Avaya Aura® Web Gateway to validate certificates presented by the clients to establish a secure HTTP connection with the Avaya Aura® Web Gateway.
NONE	Prevents the Avaya Aura® Web Gateway from performing any validation on certificates presented by the clients. If you select this option, the client cannot perform trusted hosts-based authentication with the Avaya Aura® Web Gateway.
OPTIONAL_NO_CA	Enables the Avaya Aura® Web Gateway to validate certificates presented by the clients. However, the Avaya Aura® Web Gateway does not require such certificates to be signed or issued by a trusted Certificate Authority (CA).
REQUIRED	Ensures that the clients present a valid certificate that is signed or issued by a trusted CA to establish a secure HTTP connection with the Avaya Aura® Web Gateway.

Adding a trusted host

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **Trusted Hosts**.
2. Click **Add**.
3. In the new row, type the FQDN or IP address of the trusted host.

   If you are configuring integration with Avaya Oceana®, then you must enter the FQDN of the server that requests authorization tokens.

   When connecting to a cluster, add the IP address or FQDN of each node in the cluster and the virtual IP address of the cluster that you want Avaya Aura® Web Gateway to trust.
4. Click **Save**.

Configuring session security

About this task

Use this procedure to set SRTP security policies for SIP sessions.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **Session Security**.
2. In **SRTP Policy**, select the security policy you want to apply.

The default option is `Best Effort`.

3. From the displayed list of encoding algorithms, select the appropriate algorithms for media encryption.

   The selection of encoded algorithms is based on the media SRTP encoding algorithms that are supported by the back-end communications network and far-end endpoints.

4. Click **Save**.

Enabling Avaya Breeze® platform authorization

About this task

Use this procedure to enable Single Sign-On (SSO) capabilities for Avaya Aura® Web Gateway users that previously authenticated using the Avaya Breeze® platform Authorization application.

To enable authorization, you must import the Avaya Breeze® platform authorization certificate to Avaya Aura® Web Gateway. If the certificate is changed, then you must re-upload it to Avaya Aura® Web Gateway.

For more information about Authorization Service, see “Authorization Service” in *Administering Avaya Breeze® platform*.

Before you begin

Obtain the Avaya Breeze® platform authorization certificate file in the `.PEM` format. For more information, see *Deploying Avaya Oceana®*.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **Authorization**.
2. Click **Browse** and select the `.PEM` file that you exported from the Avaya Breeze® platform node.
3. Click **Save**.

OAuth configuration

OAuth is an authorization mechanism that enables you to authenticate using a combination of enterprise credentials and other factors that the enterprise has chosen, including enterprise Single Sign-On (SSO) and multi-factor authentication.

You can log in to Avaya Workplace Client using OAuth and have an SSO experience for the following features:

- Voice service.
- Services provided by Avaya Aura® Device Services, including automatic configuration, contacts, and enterprise search.

- Avaya Aura® Web Gateway for Apple Push Notifications on Avaya Workplace Client for iOS clients.
- Presence using SIP.
- Avaya Multimedia Messaging service on Avaya Aura® Presence Services.

When OAuth is used, Avaya Workplace Client accesses Avaya Aura® Web Gateway services using special OAuth access tokens. You must configure Avaya Aura® Web Gateway so that it:

- Provides Avaya Workplace Client with information where to obtain access tokens.
- Validates access tokens provided by Avaya Workplace Client.

Use the procedures listed in the sections below to set up OAuth on Avaya Aura® Web Gateway.

Before using OAuth on Avaya Aura® Web Gateway, you must configure OAuth on Avaya Aura® Device Services first. For general information about configuring OAuth on Avaya Aura® Device Services, see “OAuth configuration” in *Deploying Avaya Aura® Device Services*.

Creating client mapping

About this task

In the OAuth authorization flow, Avaya Aura® Web Gateway validates the access token received from a client to grant the client rights to use Avaya Aura® Web Gateway resources. To configure settings required for token validation, you must provide Avaya Aura® Web Gateway with the URL to discover authorization resources configured on Avaya Aura® Device Services.

Before you begin

Configure OAuth on Avaya Aura® Device Services.

Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal with the security administrator role.
2. Navigate to **Security Settings** > **OAuth 2.0** > **Client ID Mapping**.
3. Click **Add**.
4. In the Create new client mapping window, complete the fields as follows:
   a. In **Client ID**, enter `Equinox`.

      This value is case sensitive.

   b. In **OIDC Discovery URL**, enter `https://<AADS front-end FQDN>:<AADS PORT>/auth/realms/<Realm>/.well-known/openid-configuration`

      In this string:

      - `<AADS front-end FQDN>` is the Avaya Aura® Device Services front-end FQDN.
      - `<AADS PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
      - `<Realm>` is the Keycloak realm configured on Avaya Aura® Device Services, which is SolutionRealm by default.

5. Click **OK**.

Editing the existing client mapping

About this task

Use this procedure to review or edit identity provider mapping settings.

If you use the default OAuth configuration on Avaya Aura® Device Services, you do not need to edit the configured client mapping on Avaya Aura® Web Gateway. You only need to edit the mapping for customized configurations. An example is if access token stores the email address value in a custom attribute instead of the default `email` attribute.

Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal with the security administrator role.
2. Navigate to **Security Settings** > **OAuth 2.0** > **Client ID Mapping**.
3. Select the required client mapping and then click **Edit**.
4. Update the settings as required.

   For more information about the settings, see Client mapping field descriptions on page 90.
5. Click **OK**.

Client mapping field descriptions

The following table lists the client mapping fields.

Field	Description	Editable
Client ID	The Client ID that you provided when creating the client mapping.	✗
OIDC Discovery URL	The URL to discover the Keycloak resources you provided when creating the client mapping.	✗
Issuer	The issuer attribute that Avaya Aura® Web Gateway passes to clients in authorization tokens.	✗
Public Key	The public key that is used to sign access tokens.	✓
Access token email address attribute	The attribute in the access token that contains the email address of a user. The default value is `email`.	✓

Deleting the client mapping

About this task

After you create a client mapping, you cannot edit some mapping attributes. For example, you cannot update the discovery URL if the Avaya Aura® Device Services FQDN has changed or you

want to use another Avaya Aura® Device Services system. If you need to update these attributes, you must delete the existing mapping first and then create a new mapping.

Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal with the security administrator role.
2. Navigate to **Security Settings** > **OAuth 2.0** > **Client ID Mapping**.
3. Select the required client mapping.
4. Click **Delete**.

Related links

Client mapping field descriptions on page 90

Specifying the Avaya Aura® Device Services system used for issuing access tokens

About this task

When OAuth is configured, clients use access tokens to access Avaya Aura® Web Gateway features. Access tokens are issued by Avaya Aura® Device Services. Use this procedure to specify the Avaya Aura® Device Services system that issues access tokens for clients.

Before you begin

- Ensure that OAuth is configured on Avaya Aura® Device Services. For more information, see “OAuth configuration” in *Deploying Avaya Aura® Device Services*.
- If you want to specify an Avaya Aura® Device Services URL manually, obtain the authorization endpoint URL configured on Avaya Aura® Device Services as described in Obtaining the authorization endpoint URL configured on Avaya Aura Device Services on page 92.

Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal with the security administrator role.
2. Navigate to **Security Settings** > **OAuth 2.0** > **Client ID Mapping**.
3. Do one of the following:
   - Select the **Use AADS for OAuth Authorization** check box.

     If you select this check box, clients will obtain access tokens from the Avaya Aura® Device Services system configured in your deployment. This is the recommended option.
   - In **Authorization Endpoint URL**, enter the authorization endpoint URL configured on Avaya Aura® Device Services.

Note:

- You only need to enter the authorization endpoint URL manually for customized configurations. If you use the default OAuth configuration on Avaya Aura® Device Services, use the **Use AADS for OAuth Authorization** check box.
- If the **Authorization Endpoint URL** check box is selected, you cannot modify **Authorization Endpoint URL**.

4. Click **Save**.

Obtaining the authorization endpoint URL configured on Avaya Aura® Device Services

About this task

Use this procedure if you want to specify the authorization endpoint URL configured on Avaya Aura® Device Services manually.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the security administrator role.
2. Navigate to **Security Settings** > **Client ID Mapping**.
3. Select a client mapping configuration.
4. Click **Edit**.
5. Copy the **Authorize Endpoint** value.
6. Click **Cancel** to discard any changes.

Advanced settings

Configuring resource sharing

About this task

Use this procedure to enable Cross-Origin Resource Sharing (CORS) so that HTTP-based clients from different domains can access Avaya Aura® Web Gateway services.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **CORS Configuration**.
2. Select **Enable Cross-Origin Resource Sharing** and **Allow access from any origin**.
3. Click **Save**.

Managing application sessions

About this task

Use this procedure to:

- Set a timeout period for terminating inactive, idle, or unattended sessions.
- Manage concurrent HTTP sessions.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Application Management**.
2. In the Application Properties area, complete the required settings, which are described in Application Properties field descriptions on page 93.
3. Click **Save**.

Application Properties field descriptions

Name	Description
Admin HTTPSession Timeout (minutes)	The timeout period for the Avaya Aura® Web Gateway web administration portal. You can enter a value between 1 and 60 minutes. The default value is 10 minutes.
Application HTTPSession Timeout (minutes)	The timeout period for application components. You can enter a value between 3 and 120 minutes. The default value is 15 minutes.
Maximum Concurrent HTTP Sessions	The maximum number of active sessions that are available for application components. If the number of sessions exceeds the configured value for any component, a 503 error, which indicates that service is unavailable, is generated by that component. You can enter a value between 100 and 1,000,000. The default value is 200,000.
Concurrent HTTP Sessions per User	The number of active sessions that are available per user. If the number of sessions exceeds the configured value for any user, a 429 error, which indicates that there are too many requests, is sent as a response to the user's request. You can enter a value between 10 and 1000. The default value is 50.

Codecs and bandwidth

Use the following procedures to add, remove, or change the priority of audio and video codecs. The Avaya Aura® Web Gateway offers these codecs to HTTP-based clients and the internal telephony infrastructure while performing call signaling negotiations.

The following codec categories are available:

- WebRTC: Offered to browser-based clients through HTTP.
- SIP: Used internally when communicating through the Avaya Aura® infrastructure or Avaya Meetings Server servers.

Configuring audio codecs and bandwidth

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Media Settings** > **Audio**.
2. In the SIP Audio Codecs and WebRTC Audio Codecs areas, drag and drop the codecs as required to rearrange them.
3. To add SIP or WebRTC codecs to the list, select the codec that you want to add, and click **Add**.
4. To remove SIP or WebRTC codecs from the list, select the codecs that you want to remove, and click **Remove**.
5. In **OPUS Profile**, select a bandwidth level for the Opus codec if it is included in the WebRTC Audio Codec list.

   The Opus codec defines the audio bandwidth.
6. Click **Save**.

Configuring video codecs and bandwidth

About this task

Use this procedure to select video codecs that Avaya Aura® Web Gateway uses for SIP and WebRTC calls.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Media Settings** > **Video**.
2. In the SIP Video Codecs and WebRTC Video Codecs areas, drag and drop the codecs as required to rearrange them.
3. To add SIP or WebRTC codecs to the list, select the codec that you want to add, and click **Add**.
4. To remove SIP or WebRTC codecs from the list, select the codecs that you want to remove, and click **Remove**.

5. In **Call Maximum Video Bandwidth (kbps)**, do one of the following to disable video or modify the video bandwidth:
   - To disable video, select 0.
   - To modify the video bandwidth, select the appropriate value.

   Tip:

   For the Avaya Aura® Web Gateway to support 1020p HD video, this setting must be set to 1792 kbps or higher. You can select **Custom** to enter your own customized value.

   The bandwidth value specified will be the maximum allowed by the Avaya Aura® Web Gateway. If the bandwidth value specified in SDP or Avaya Aura® Device Services is lower than the Avaya Aura® Web Gateway value, then the system uses the lower value.
6. Click **Save**.

Configuring Avaya Aura® Media Server credentials

About this task

Use this procedure to verify and set the Avaya Aura® Media Server REST security configuration credentials.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Media Settings** > **AAMS Credentials**.
2. Select **Use Credentials for Authentication** to use the existing login credentials for authentication.

   Login and **Password** are automatically set to the same credentials that are used for the Avaya Aura® Media Server REST signaling interface. The Avaya Aura® Web Gateway uses these credentials to establish a TLS connection with the Avaya Aura® Media Server. If these credentials are updated in the Avaya Aura® Media Server, then they also need to be updated in the Avaya Aura® Web Gateway.
3. Click **Save**.

Push notification management

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). Configuring push notifications on the Avaya Aura® Web Gateway administration portal is part of the push notification configuration procedure. Before configuring push notifications on the Avaya Aura® Web Gateway administration portal, you must create and configure an Avaya Spaces account. You also need to configure settings on Avaya Aura® Session Manager and Avaya Aura® Communication Manager. For more

information about the entire configuration procedure, see the sections under Avaya push notification management on page 100.

Avaya Oceana® and Avaya Aura® Web Gateway integration checklist

Avaya Oceana® requires the Avaya Aura® Web Gateway to provide WebRTC Signaling Gateway services to video and voice-enabled SIP agents through a browser endpoint. This checklist outlines the tasks you must perform in the Avaya Aura® Web Gateway web administration portal to enable web voice and video in Avaya Oceana®.

No.	Task	Notes	Reference	✔
1	Add the FQDN of the server that requests tokens from the Avaya Aura® Web Gateway server to the trusted hosts list.	Guest clients use these tokens for authorization on the Avaya Aura® Web Gateway.	See Adding a trusted host on page 87.	
2	To enable guest access calls, set the client certificate policy to **OPTIONAL**.	This is required to verify the client certificate of the third-party guest access token server.	See Configuring the certificate policy for Avaya Oceana integration on page 86.	
3	Provide information about the SIP server that Avaya Oceana® clients use for SIP communication.	This information enables the Avaya Aura® Web Gateway to send SIP requests to the clients.	See Providing information about guest SIP domain and SIP proxy on page 71.	

Avaya Spaces Calling and Avaya Aura® Web Gateway integration checklist

Avaya Spaces Calling requires the Avaya Aura® Web Gateway to provide WebRTC Signaling Gateway services to voice-enabled SIP agents through a browser endpoint. The following checklist outlines the high-level tasks to perform in your deployment to enable web voice in Avaya Spaces. For detailed information about Avaya Spaces, see *Administering* and *Deploying* documents for Avaya Spaces.

No.	Task	Notes	✔
1	Ensure that you have deployed each of the servers that are required for WebRTC calls.	In addition to Avaya Aura® Web Gateway, you must install and configure the following servers: • Avaya Aura® System Manager • Avaya Aura® Session Manager • Avaya Aura® Communication Manager • Avaya Aura® Device Services • Avaya Aura® Media Server • LDAP directory source, such as Active Directory or other support LDAP servers. For information about the deployment and administration document, see Documentation on page 196.	
2	On Avaya Aura® Device Services, publish the COMM_ADDR_HANDLE_TYPE and COMM_ADDR_HANDLE_LENGTH parameters.	For information about publishing settings on Avaya Aura® Device Services, see Chapter “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*. For information about the parameters, see the “Avaya Aura® Device Services specific parameters” section in *Administering Avaya Aura® Device Services*.	
3	Configure Avaya Aura® Web Gateway and other servers.	Do the following: • Perform the tasks listed in “Configuration worksheet” and the procedures listed in Chapter “System Manager, Avaya Aura® Device Services, Avaya Aura® Media Server, and Avaya Meetings Server configurations” in *Deploying the Avaya Aura® Web Gateway*. • Configure the Avaya Aura® Device Services host to obtain user data as described in Configuring the Avaya Aura Device Services host to obtain user data on page 45. • Configure the Avaya Aura® Web Gateway location settings as described in Managing Avaya Aura	

Table continues…

No.	Task	Notes	✔
		Web Gateway locations on page 46 and Managing Avaya Aura Media Server location and priority settings for the Avaya Aura Web Gateway on page 46. • If the Web clients are located under a different domain than that used by Avaya Aura® Web Gateway, configure resource sharing as described in Configuring resource sharing on page 92. • Configure Single Sign-On (SSO) for Avaya Spaces as described in Configuring SSO for an Avaya Spaces web-client on page 99.	
4	Synchronize users from LDAP directories and Avaya Aura® to Avaya Spaces. To use the click-to-call functionality, you must also synchronize work phone numbers.	You can use one of the following options: • On Avaya Aura® Device Services, synchronize Avaya Spaces and Avaya Aura®. For information, see Chapter "Avaya Spaces integration" and the "Configuring data synchronization between Avaya Aura® Device Services and Avaya Spaces" procedure in *Administering Avaya Aura® Device Services*. • Import phone numbers of enterprise users to Avaya Spaces in .csv files. • Ask end-users to enter their work phone numbers to their Avaya Spaces user profiles directly. For information about managing Avaya Spaces, see documents at https://resources.avayacloud.com/aspx/Avaya_Spaces.	
5	If you have clients outside your enterprise firewall, configure Avaya Session Border Controller for Enterprise.	See the procedures in the "Avaya Session Border Controller for Enterprise configuration" chapter in *Deploying the Avaya Aura® Web Gateway*.	

Related links

Configuring SSO for an Avaya Spaces web-client on page 99

Configuring SSO for an Avaya Spaces web-client

About this task

The Avaya Spaces SSO functionality allows Avaya Spaces users to log in to Avaya Spaces web clients, such as Avaya Spaces Calling Chrome extension, using their Avaya Spaces login. These web clients use the Avaya Spaces Accounts token to log in to Avaya Aura® Web Gateway without asking the user to enter their user name and password.

This procedure applies both to Avaya-provided web clients, such as Avaya Spaces Calling Chrome extension, and to your own custom web-clients that register on Avaya Aura® Web Gateway using Avaya Spaces SSO.

Before you begin

Perform the steps listed in Avaya Spaces Calling and Avaya Aura Web Gateway integration checklist on page 96.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Spaces Configuration** > **Spaces SSO**.
2. Select the **Enable SSO** check box.
3. In **Domain**, type the name of the domain configured for your company in Avaya Spaces and then click **Add**.
4. If you have multiple domains configured for your company in Avaya Spaces, repeat the previous step for all these domains.
5. If you are configuring Avaya Spaces SSO for your own web-client, do the following:
   a. In **Client ID**, enter the ID of your web client.
   b. Click **Add**.

   This step is not required for Avaya-provided web clients. For these clients, Avaya Aura® Web Gateway already contains information about its IDs.
6. Click **Save**.

Related links

Avaya Spaces Calling and Avaya Aura Web Gateway integration checklist on page 96

Chapter 5: Avaya push notification management

Push notifications

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). The push notification service sends notifications automatically. Therefore, an application can receive notifications even when it is suspended or in Sleep mode.

The Avaya Aura® Web Gateway can send push notifications about the following telephony-related events:

- Incoming calls.
- Incoming calls on an Avaya Aura® Communication Manager bridged line appearance.
- Incoming calls on an Avaya Aura® Communication Manager enhanced pickup group.
- Incoming calls on an Avaya Aura® Communication Manager team button.
- Voicemail status updates.

For messaging push notifications, use Avaya Multimedia Messaging or Avaya Aura® Presence Services Release 8.0.2 or later.

Push notification provider

The Avaya Aura® Web Gateway interacts with the APNs through a push notification provider. You must register your Avaya Aura® Web Gateway system with the push notification provider before activating push notifications. The default provider is the Avaya Push Notification provider, which must be used to support push notifications for Avaya Workplace Client. If you want to use push notifications for third-party SDK-based applications, you must use a third-party push notification provider.

For the Avaya Push Notification provider, you must create and configure an account at accounts.avayacloud.com. This account is used to store the data required to authorize your Avaya Aura® Web Gateway system. This account requirement does not apply if you are working with a third-party provider.

Related links

Third-party push notification provider requirements on page 102

Checklist for push notification service configuration

Use this checklist to set up the push notification service for your iOS applications.

Depending on whether you are planning to work with the default Avaya Push Notification provider or a third-party push notification provider, the task you perform are slightly different.

No.	Task	Notes	✔
1	Set up an Avaya Spaces account.	See Avaya Cloud account configuration on page 102. This step is not required for third-party notification providers.	
2	Configure the third-party push notification provider.	See the requirements in Third-party push notification provider requirements on page 102. This step is not required if you are working with the Avaya Push Notification provider.	
3	Configure your enterprise network firewall.	See Firewall configuration on page 104.	
4	If you are using the Avaya Push Notification Provider, determine if you want to use CA certificates built-in to RHEL.	See Configuring the use of CA certificates built-in to RHEL for the Avaya Push Notifications provider on page 105. If you do not want to use built-in certificates, you must upload CA certificates to the truststore as described in Managing truststore certificates on page 84.	
5	Configure the push notification provider on the Avaya Aura® Web Gateway.	• If you are working with the Avaya Push Notification provider, see Configuring the Avaya Push Notification provider on the Avaya Aura Web Gateway on page 106. • If you are working with a third-party push notification provider, see Configuring a third-party push notification provider on the Avaya Aura Web Gateway on page 108.	
6	Configure push notifications for mobile applications.	See Configuring mobile application settings on page 110.	
7	Configure Avaya Aura® Session Manager and Avaya Aura® Communication Manager.	See Avaya Aura components configuration on page 112.	

Table continues…

No.	Task	Notes	✔
8	Set the parameters to enable push notifications on iOS applications.	See Configuration parameters for iOS applications on page 114. To enable push notifications in iOS applications, you must configure the required parameters using Avaya Aura® Device Services or a settings file. Avaya Aura® Device Services is the recommended option if it is available in your deployment.	

Third-party push notification provider requirements

By default, the Avaya Aura® Web Gateway uses the Avaya Push Notification provider for Avaya clients, such as Avaya Workplace Client for iOS. If you are planning to use push notifications for third–party Avaya™ Client SDK-based iOS applications, you must use a third-party provider, for example, developed by the iOS application developer. This provider must implement the following APIs:

- Interface with the Apple Push Notification service (APNs). Implementation of this interface ensures that the APNs trusts the third-party push notification provider to send notifications to Avaya clients. For more information about implementing the interface and the APIs required by the APNs, see APNs Overview.
- Interface with Avaya Aura® servers. The third-party push notification provider must trust the Avaya Aura® Web Gateway to receive push notifications from it. Avaya Aura® Web Gateway uses the OAuth-based API for authentication. For more information about the APIs, see Avaya™ Client SDK.

  Currently, the existing third-party push notification providers do not support Avaya APIs.

Avaya Cloud account configuration

If you are planning to use the Avaya Push Notification provider, you must create and configure an Avaya Cloud account. This account stores the parameters required to authorize your Avaya Aura® Web Gateway system.

Use the following sections to create and configure your Avaya Cloud account.

Registering an Avaya Cloud account

About this task

Use this procedure to register an Avaya Cloud account using your email address.

Procedure

1. In your web browser, enter https://accounts.avayacloud.com/.
2. In the **Email or Phone** field, type your email address.
3. Click **Yes, sign me up!**.

   Avaya Cloud sends a confirmation email to the email address you specified.
4. In your mailbox, open the confirmation email and then click the **Confirm** button.

   You are redirected to the Avaya Cloud My Account page.
5. Provide your first name, last name, password, and, optionally, a photo.
6. Click **Create an account**.

Setting up a company and domain in Avaya Cloud

About this task

You must provide the company domain associated with your Avaya Aura® Web Gateway system.

Before you begin

Ensure that your customer domain matches the email address domain for logging in to Avaya Workplace Client.

Procedure

1. Log in to https://accounts.avayacloud.com/ as an administrator.
2. If you have not set up your company or want to configure a new company, do the following:
   a. Click on your user name in the top-right area of the screen and then click **Add Company**.
   b. Type a name and description for your company.
   c. Click **Save**.
3. Click **Manage Companies** and click the existing company name.
4. Click the **Domains** tab.
5. Click **Add Domain**.
6. Enter the domain name and then click **OK**.
7. To verify ownership of the domain, next to the domain name, click **Verify**.

8. Do one of the following:
   - Follow the on-screen instructions to add the verification code to your domain account and then click **Verify**.
   - At the bottom-right area of the Verify Domain window, click **Manual Verify** to have Avaya personnel verify the ownership of the domain.

Adding the Avaya Mobile Push Notification Service to a company profile on your Avaya Cloud account

About this task

To activate the push notification service for the Avaya Aura® Web Gateway , you must add the Avaya Mobile Push Notification Service application to your company profile on the Avaya Cloud account.

Procedure

1. Log in to https://accounts.avayacloud.com/ as an administrator.
2. From the dashboard, on the left area, click **Manage Companies**.
3. Select the required company and then click the **Apps** tab.
4. Click **Configure New App**.
5. From the **Product** drop-down list, select **Avaya Mobile Push Notification Service**.
6. Click **Save**.

   Avaya Cloud creates a new Avaya Mobile Push Notification Service application.

Next steps

When you configure notifications, you provide authorization data to the Public Settings section of your new Avaya Mobile Push Notification Service application.

Related links

Configuring the Avaya Push Notification provider on the Avaya Aura Web Gateway on page 106

Firewall configuration

Avaya Aura® Web Gateway communicates with the Avaya Push Notification provider cloud service using HTTPS. To use the Avaya Push Notification provider, your enterprise network firewall and the HTTP proxy server must allow outbound HTTPS connections to the Avaya Push Notification provider address, which is `pnp.avaya.com:443`.

Important:

If you configured push notifications for Release 3.7, Avaya Aura® Web Gateway still uses the old `apnp.avaya.com` Avaya Push Notification provider address. Avaya recommends that you change this address to `pnp.avaya.com` and update your enterprise network firewall and HTTP proxy server settings to `pnp.avaya.com:443`

For applications other than Avaya Workplace Client for iOS, you must use a third-party provider. The firewall and the HTTP proxy of your enterprise must allow outbound HTTPS connections to this push notification provider.

For iOS devices running in your enterprise network, Apple push notifications rely on connectivity between iOS devices and the Apple Push Notification service network. For more information about port configuration required to receive Apple push notifications, see https://support.apple.com/en-us/ht203609

Related links

Reconfiguring the Avaya Push Notification provider after upgrade or migration on page 183

Configuring the use of CA certificates built-in to RHEL for the Avaya Push Notifications provider

About this task

By default, Avaya Aura® Web Gateway uses built-in CA certificates of RHEL to connect to the Avaya Push Notification provider and use the APNs. In this case, you do not need to upload CA certificates to the truststore manually. If you do not want to trust the built-in CA certificates, you can disable the use of these certificates for push notifications.

If you do not use built-in CA certificates of RHEL, you must upload trusted third-party CA certificates for Avaya Push Notification provider to the Avaya Aura® Web Gateway truststore.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **Certificate Management** > **Truststore**.
2. Do one of the following:
   - If you want to use built-in CA certificates of RHEL, select the **Use Operating System Trusted Root CAs for Push Notification Provider** check box.
   - If you want to use third-party CA certificates only, clear the **Use Operating System Trusted Root CAs for Push Notification Provider** check box.
3. Click **Save**.

   Avaya Aura® Web Gateway restarts to apply changes.

Configuring the Avaya Push Notification provider on the Avaya Aura® Web Gateway

About this task

To use the Avaya Push Notification provider, you must generate authorization data and export this data to your Avaya Cloud account. You cannot edit other provider data, such as the name or address, and you cannot delete the Avaya Push Notification provider from the Avaya Aura® Web Gateway.

For a cluster, perform this procedure once, regardless of the number of nodes in the cluster.

Before you begin

- Create and configure an Avaya Cloud account.
- If you do not use CA certificates built-in to RHEL, install the public certificate of the push notification provider on the Avaya Aura® Web Gateway. For more information, see Managing truststore certificates on page 84.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Provider Settings**.
2. From **Push Notification Provider**, select **Avaya Provider**.
3. In **Enter Company Domain**, enter your company domain.

   You must enter the same company domain that you provided in your Avaya Cloud account.
4. Click **Generate Key**.

   The Avaya Aura® Web Gateway generates a public and private key pair and an identifier. This data is required to authorize Avaya Aura® Web Gateway on the push notification provider. The Avaya Aura® Web Gateway also updates the following values:

   - **System Id**: A unique identifier for your system.
   - **Public Key**: A public key.
5. Click **Export**.

   Avaya Aura® Web Gateway displays a pop-up window with the authorization information in JSON format. You must provide this data to your Avaya Cloud account.

   The following is an example of the authorization data:

```
{
    "systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com",
    "description": "Avaya Aura Web Gateway Services",
    "publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCEj9wc3klayOKHYIVIeL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----",
    "alg": "ES256"
}
```

Important:

- Do *not* close the Provider Settings page on the Avaya Aura® Web Gateway administration portal until you finish exporting authorization data to your Avaya Spaces account.
- Do *not* save the data you provided on the Provider Settings page of the Avaya Aura® Web Gateway administration portal until you export authorization data to your Avaya Cloud account. Otherwise, the push notification service might not work as expected.

6. Copy the authorization data, including the surrounding curly brackets, and save it in a file on your computer.
7. In a new browser tab, log in to your Avaya Cloud account and navigate to **Manage Companies**.
8. Select the required company and navigate to the **Apps** tab.
9. From **App**, select **Avaya Mobile Push Notification Service**.
10. In Data Configuration, select the **JSON** check box.
11. Replace the content in **Public Settings** with the content of the file that you created in step 6 and then save your changes.

    You must ensure that the authorization data you enter in **Public Settings** is a valid JSON string. If the data uses an invalid format, the Avaya Cloud account displays a warning message, but still allows you to save changes.

    The Avaya Cloud account stores authorization data internally. **Public Settings** only displays the authorization data that you entered last. You will not lose any previously entered authorization data if you overwrite existing content with the new authorization data.
12. Return to the Provider Settings page on the Avaya Aura® Web Gateway administration portal.
13. Click **Test** to verify that your system can connect and authenticate with the push notification provider.
14. Do one of the following:
    - If the verification completed successfully, click **Save**.
    - If the verification failed, fix the issue as described in Avaya Aura Web Gateway cannot connect to a push notification provider on page 190 and then and re-run the connectivity test.

      If the problem persists, contact Avaya support personnel.

Related links

Avaya Aura Web Gateway does not display the default Avaya Push Notification provider or mobile application configuration on page 192

Avaya Aura Web Gateway returns a TLS handshake error when testing the connectivity to a push notification server on page 190

Configuring a third-party push notification provider on the Avaya Aura® Web Gateway

About this task

To use push notifications on third-party iOS applications, you require a third-party push notification provider. An Avaya Breeze Client SDK application developer can implement a third-party push notification provider. Use this procedure to set up or update a third-party push notification provider on the Avaya Aura® Web Gateway.

Before you begin

A third-party Avaya Breeze Client SDK application developer must implement the third-party push notification provider. For more information about push notification provider requirements, see Third-party push notification provider requirements on page 102.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Provider Settings**.
2. Do one of the following:
   - To add a new provider configuration, click **Add**.
   - To edit an existing provider, select the required provider from **Push Notification Provider** and click **Edit**.
3. In **Enter Company Domain**, enter the domain where your Avaya Aura® Web Gateway is deployed.

   For example: `mycompany.com`
4. In **Push Notification Provider Name**, enter a name for the provider.

   For example: `MyPushNotificationProvider`.

   This name is used in the Avaya Aura® Web Gateway administration portal for display purposes only.
5. In **Push Notification Provider Address**, enter the FQDN where your push notification provider is deployed.

   For example: `mypushnotifications.mycompany.com`
6. In **Push Notification Provider Port**, enter the port number for the push notification provider.

   The default port is 443.
7. Click **Generate Key**.

The Avaya Aura® Web Gateway generates a public and private key pair and an identifier. This data is required to authorize Avaya Aura® Web Gateway on the push notification provider. The Avaya Aura® Web Gateway also updates the following values:

- **System Id**: A unique identifier for your system.
- **Public Key**: A public key.

8. Click **Export**.

   Avaya Aura® Web Gateway displays a pop-up window with the authorization data in JSON format.

   The following is an example of the authorization data:

```
{
    "systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com",
    "description": "Avaya Aura Web Gateway Services",
    "publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCEj9wc3klayOKHYIVIeL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----",
    "alg": "ES256"
}
```

Important:

- Do *not* close the Provider Settings page on the Avaya Aura® Web Gateway administration portal while you are exporting authorization data to your push notification provider.
- Do *not* save the data you provided on the Provider Settings page of the Avaya Aura® Web Gateway administration portal until you export authorization data to your push notification portal. Otherwise, the push notification service might not work as expected.

9. Copy the system ID and public key data and provide it to your push notification provider.

   For example:

```
"systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com"
"publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCEj9wc3klayOKHYIVIeL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----"
```

   The steps you must perform to provide authorization data are provider-specific. For more information, contact your third-party push notification provider vendor.

10. Return to the Provider Settings page on the Avaya Aura® Web Gateway administration portal.
11. Click **Test** to verify that your system can connect and authenticate with the push notification provider.
12. Do one of the following:

    - If the verification completed successfully, click **Save**.

- If the verification failed, fix the issue as described in Avaya Aura Web Gateway cannot connect to a push notification provider on page 190 and then and re-run the connectivity test.

  If the problem persists, contact Avaya support personnel.

Related links

Removing a third-party push notification provider on page 110

Removing a third-party push notification provider

About this task

Use this procedure to remove the configuration for a third-party push notification provider from the Avaya Aura® Web Gateway. You can only remove a provider that is not used by any mobile applications. You cannot remove the default, built-in Avaya Push Notification provider.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Provider Settings**.
2. In **Push Notification Provider**, select the required provider.
3. Click **Remove** and click **Yes** in the confirmation window.

Related links

Configuring a third-party push notification provider on the Avaya Aura Web Gateway on page 108

Configuring mobile application settings

About this task

If you plan to use push notifications on a third-party CSDK-based iOS application, use this procedure to provide information about this application on Avaya Aura® Web Gateway. You can then select the required third-party push notification provider for the application.

Avaya Workplace Client for iOS configuration is pre-defined. Therefore, this procedure is not required for Avaya Workplace Client for iOS. You only need to modify the Avaya Workplace Client for iOS configuration if the default Avaya Push Notification provider configuration uses the old `apnp.avaya.com` address. For more information, see Reconfiguring the Avaya Push Notification provider after upgrade or migration on page 183.

Note:

- The name of the pre-defined Avaya Workplace Client for iOS configuration is `Avaya Workplace`.
- If you use Avaya Workplace Client for iOS, do not use other third-party iOS applications.

Before you begin

Configure a push notification provider on Avaya Aura® Web Gateway. For more information, see Configuring the Avaya Push Notification provider on the Avaya Aura Web Gateway on page 106 and Configuring a third-party push notification provider on the Avaya Aura Web Gateway on page 108.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Mobile Application Settings**.
2. Do one of the following:
   - To create a new mobile application configuration, click **Add**.
   - To edit existing configuration settings, from **Application Name**, select the required application and click **Edit**.
3. In **Application Name**, provide an appropriate application name.
4. In **Application Id**, provide the iOS application bundle identification string.

   Each application must have a unique identification string.
5. In **Push Notification Provider**, select the required push notification provider.
6. To verify that the Avaya Aura® Web Gateway can send notifications to the mobile application, click **Test**.
7. Do one of the following:
   - If the verification is completed successfully, click **Save**.
   - If the verification failed, fix the issue as described in iOS application cannot connect to a push notification provider on page 191 and re-run the connection test.

     If the problem persists, contact Avaya support personnel.

Disabling specific push notifications

About this task

Use this procedure to disable push notifications for a specific third-party application. You cannot delete the pre-defined `Avaya Workplace` configuration.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Mobile Application Settings**.
2. In the **Application** field, select the required mobile application.
3. Click **Remove** and click **Yes** to confirm.

Disabling all push notifications

About this task

Use this procedure to disable push notifications for all third-party applications, including the default applications, such as `com.avaya.AvayaCommunicator`. If you want to restore a default application, see Configuring a third-party push notification provider on the Avaya Aura Web Gateway on page 108.

Before you begin

These steps apply to the current release of Avaya Aura® Web Gateway. If you have an earlier release of Avaya Aura® Web Gateway, contact Avaya personnel to obtain the appropriate script, then copy the `disable_push.sh` script to your Avaya Aura® Web Gateway server and complete step 2 on page 112.

Procedure

1. Locate the `disable_push.sh` script on the Avaya Aura® Web Gateway server.
   a. Log in to the Avaya Aura® Web Gateway using your SSH credentials.
   b. Type `cdto CAS` to navigate to the CAS folder.
   c. Type `cd push_notifications/` to navigate to the push notifications folder.
   d. Type `cp disable_push.sh ~/disable_push.sh` to copy the script to your home directory.
   e. Type `cd ~` to navigate to your home directory.
2. Run the following command to execute the script:

   ```
   sh disable_push.sh
   ```

   Avaya Aura® Web Gateway stops providing the push notification service to all currently registered mobile devices. Mobile devices can no longer register for a push notification service on Avaya Aura® Web Gateway.
3. Restart services on all nodes of the cluster.

   For more information, see Restarting services on an Avaya Aura Web Gateway node on page 43.

Avaya Aura® components configuration

The following sections outline the settings you can modify on Avaya Aura® Session Manager and Avaya Aura® Communication Manager to improve the performance of the push notification service.

Avaya Aura® Session Manager configuration

Session Manager allows users to have multiple SIP devices associated with their accounts. The Avaya Aura® push notification solution requires that Session Manager user accounts must be configured to allow the use of multiple devices. Avaya Aura® Web Gateway counts as one additional device that registers on Session Manager to receive incoming notifications. The multiple device option is called Multiple Device Access (MDA) and is configured through a user configuration template. For more information about configuring user provisioning rules, see *Administering Avaya Aura® Session Manager*.

Avaya Aura® Communication Manager configuration

Communication Manager controls how long an incoming call alerts at a VoIP endpoint that uses SIP for call signaling. The time required to establish a call depends on various conditions, including the following:

- Call setup latency through the push notification network.
- Additional network connection steps required by iOS clients to present the incoming call notification to end users.

If you use the Apple Push Notification service in your deployment, you must change the default values of the following Communication Manager timers to provide Avaya Workplace Client for iOS users with sufficient time to answer the call. Otherwise, Communication Manager might drop the call or send it to coverage before the called party has a chance to answer the call.

Alternate route timer

By default, Communication Manager has a six second alternate router timer that expires when no 180 Ringing response is received from the called party. When the timer expires, Communication Manager drops the call. If you enable push notifications, increase this value of the **Alternate Route Timer(sec)** parameter to 10 seconds. This parameter is located in a Communication Manager SIP signaling group that is associated with the Session Manager instance used by mobile clients that are subscribed for push notifications.

Redirect on OPTIM Failure timer

The timer controls how long Communication Manager waits for a SIP 18x provisional response before canceling the call that was intended for an iOS client. The default value is 5,000 milliseconds. If you enable push notifications, increase this value to 10,000 milliseconds. The value is configured in the **Redirect on OPTIM Failure** field in a Communication Manager SIP trunk-group.

Coverage path number of ring cycles

This timer controls the number of ring cycles to alert the originally called party before directing them to the first coverage point in the coverage path. The exact duration of the wait time depends on the ring cycle length, which can be different in different countries. By default, Communication Manager waits for two ring cycles. In the **Don't Answer** field under Coverage Criteria, increase the Number of Rings to four ring cycles for the Coverage Paths that apply to users with Avaya Workplace Client running on an Apple device.

Note:

- To avoid changing coverage behavior for users who do not use Avaya Workplace Client for iOS, you can create a new coverage path with the number of rings set to four cycles for Avaya Workplace Client for iOS users. For other users, keep the existing coverage path with the number of rings set to the default two cycles.
- If an Avaya Workplace Client for iOS user already has a coverage path with the number of rings set to four cycles or higher, you do not need to edit this coverage path.
- If a user has both a deskphone and Avaya Workplace Client for iOS, the higher number of rings applies to both endpoints. That is, an incoming call rings for four cycles on the deskphone even if Avaya Workplace Client for iOS is not logged in.

For more information about Communication Manager settings, see *Administering Avaya Aura® Communication Manager*.

Configuration parameters for iOS applications

To enable the use of push notifications on iOS applications, you must provide the following configuration parameters to iOS applications:

- TELEPHONY_PUSH_NOTIFICATION_ENABLED. This parameter is used to enable or disable push notifications. To enable push notifications, set this parameter to `1`. To disable push notifications, set this parameter to `0`.
- TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL. This parameter is used to provide the Avaya Aura® Web Gateway address to iOS applications. An example is `https://avaya-aura-web-gateway-hostname.company-domain.com`. If you are using a custom HTTPS port, the parameter must include this port number. For example: `https://avaya-aura-web-gateway-hostname.company-domain.com:8443`.

You can use one of the following methods to configure these parameters:

- Import the parameters to the Dynamic Configuration service on Avaya Aura® Device Services using the `dynamicConfigUpload.txt` file. For more information, see “Administration of the Dynamic Configuration service” in *Administering Avaya Aura® Device Services*.
- Use the `46xxsettings.txt` configuration file to push the parameters to clients.

The Dynamic Configuration service is the recommended method. Use this option if Avaya Aura® Device Services is available in your deployment.

Chapter 6: Integrated Windows Authentication administration and management

Integrated Windows Authentication (IWA) enables you to log in to different services with the same credentials. To support IWA, some Avaya Aura® Web Gateway server administration is required. Users must be able to authenticate to the Avaya Aura® Web Gateway API using a preexisting authentication to a Windows domain. Avaya Aura® Web Gateway uses SPNEGO to negotiate authentication with the client and Kerberos to validate the authentication of the client user. User roles are retrieved normally through LDAP.

Use the following sections to complete IWA configuration on the Avaya Aura® Web Gateway and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting.

Avaya Aura® Web Gateway supports IWA for multiple domains. The User Principal Name (UPN) domain and the authentication domain must be the same as the root domain of the directory.

Authentication prerequisites

You must have the following to set up IWA:

- An Active Directory server.
- A DNS server for the DNS domain of Active Directory.

  For information about setting up the DNS server, see *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows*.
- A Windows client on the Active Directory domain.
- An Avaya Aura® Web Gateway server that is resolvable by the DNS.
- A domain user that is mapped to the Service Principal Name (SPN) of the Avaya Aura® Web Gateway server.
- Domain users for all individual users.
- The sAMAccountName attribute must match the user name part of the userPrincipalName attribute.

  For example, if the sAMAccountName is jdoe, then the userPrincipalName must use the following format: jdoe@<*domain.name*>.

- To log in to a computer, the user must enter the user name part of the userPrincipalName configured for that user. The domain must also match the domain part of that user userPrincipalName. The user login name format is `<domain>\<user name>`.

  For example, if the user has the “jdoe@avaya.com” userPrincipalName, where “avaya” is the domain and “jdoe” is the user name; then the user logs in to a computer using the “avaya \jdoe” account.

Important:

- Do not change the userPrincipalName attribute configured for the user. If you change the userPrincipalName after IWA is configured, IWA will not work.
- The Active Directory, Windows client, and Avaya Aura® Web Gateway server must resolve each other FQDNs. However, they do not need to use the same DNS server or belong to the same zone.

Setting up the Windows Domain Controller

About this task

Use this procedure to add the Avaya Aura® Web Gateway SPN to a domain user on the Windows Domain Controller or the Active Directory server. The SPN must be unique across the domain. To avoid issues with duplicated SPNs, track of any SPNs assigned to users.

Avaya Aura® Web Gateway supports IWA for multiple domains. To configure IWA for multiple domains that are in different Active Directories, repeat this procedure on each Active Directory.

Important:

Enter all commands exactly as shown in this procedure, and use the following guidelines:

- The hostname used to access the Tomcat server must match the host name in the SPN exactly. Otherwise, authentication fails.
- The server must be part of the local trusted intranet for the client.
- The SPN must be formatted as `HTTP/<host name>` and must be exactly the same everywhere.
- The port number must not be included in the SPN.
- Only one SPN must be mapped to a domain user.
- The Kerberos realm is always the uppercase equivalent of the DNS domain name. For example, `EXAMPLE.COM`.
- Avaya Aura® Web Gateway supports IWA for parent and child domains. However, you cannot assign an SPN and generate a `tomcat.keytab` file for the child domain because the SPN can only be mapped to a single user in a forest. Here, you need to assign the SPN and generate a `tomcat.keytab` file for the parent domain.

Procedure

1. Create a new IWA service account.

Do not select an account associated with an existing user.

2. Run the following command to attach the SPN to the domain name:

   `setspn -S HTTPS/<FRONT-END FQDN> <Domain user login>`

   In the following example, `<FRONT-END FQDN>` is `csa.example.com` and `<Domain user login>` is `csa.example.com`:

   ```
   setspn -S HTTP/csa.example.com csa_user
   ```

   Important:

   - If you are using Active Directory 2003, you must use `setspn -A` instead of `setspn -S`.
   - When you use `setspn -S`, the Active Directory server searches for other users with the same SPN assigned. If the server finds a duplicated SPN, see step 3 on page 117.

3. **(Optional)** To remove a duplicated SPN from another user, run the following command:

   `setspn -d <SPN> <old user>`

4. Run one of the following commands to generate a `tomcat.keytab` file:

   - If FIPS is disabled on Avaya Aura® Web Gateway, run the following command:

     `ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto all /kvno 0`

   - If FIPS is enabled on Avaya Aura® Web Gateway, run the following command:

     `ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto <Encryption Type> /kvno 0`

     Where *<Encryption Type>* can be one of the following:

     - `AES256-SHA1`: If you want to use the AES256-SHA1 encryption type.
     - `AES128-SHA1`: If you want to use the AES128-SHA1 encryption type.

     The encryption type must correspond to the encryption type configured for the domain user that is mapped to the Avaya Aura® Web Gateway SPN. For more information, see Enabling encryption for the domain user on page 118.

     AES256–SHA1 is the preferred encryption type.

The following example displays the command for generating a keytab file in FIPS mode. In this example, `<Domain User Login>` is `csa_user`, `<Kerberos realm>` is `EXAMPLE.COM`, and `<FRONT—END FQDN>` is `csa.example`.

```
ktpass /out c:\tomcat.keytab /mapuser csa_user@EXAMPLE.COM /princ HTTP/
csa.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto
AES256-SHA1 /kvno 0
```

5. Transfer the generated `tomcat.keytab` file to the Avaya Aura® Web Gateway server using the OAMP administration portal.

   Since this is a credentials file, handle it securely and delete the original file after this file is imported into the Avaya Aura® Web Gateway server. You can generate and re-import a new `tomcat.keytab` file anytime.

Next steps

- If you are using FIPS, enable AES encryption for the domain user as described in Enabling encryption for the domain user on page 118.
- Set up IWA on Avaya Aura® Device Services as described in Setting up IWA on the Avaya Aura Web Gateway administration portal on page 119.

Windows Domain Controller command descriptions

Setting up the Windows Domain Controller on page 116 uses the following command values:

Command	Description	Example value
<FRONT—END FQDN>	The REST front host FQDN of the Avaya Aura® Web Gateway server. This is either the FQDN of the Virtual IP assigned to the cluster (if internal load balancing is used) or the FQDN of the external load balancer, if it is used.	`csa.example.com`
<Domain user login>	The Windows login ID for the domain user you created.	`csa_user`
<Kerberos realm>	The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name.	`EXAMPLE.COM`

Enabling encryption for the domain user

About this task

In FIPS mode, Kerberos uses Advanced Encryption Standard (AES). By default, support for Kerberos AES authentication is disabled for Active Directory users. Use this procedure to enable encryption support for the domain user that is mapped to the Avaya Aura® Web Gateway SPN.

This procedure is only required if FIPS is enabled on Avaya Aura® Web Gateway.

Before you begin

Generate a keytab file as described in Setting up the Windows Domain Controller on page 116.

Procedure

1. In Active Directory, select the domain user that is mapped to the Avaya Aura® Web Gateway SPN.

   For example: aads_spn_user.
2. Open the domain user properties.
3. Click the **Account** tab.
4. In the Account options area, do one of the following:
   - If you used the AES256–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 256 bit encryption** check box.
   - If you used the AES128–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 128 bit encryption** check box.
5. Click **OK**.

Setting up IWA on the Avaya Aura® Web Gateway administration portal

About this task

This procedure describes the changes you must perform on the Avaya Aura® Web Gateway administration portal to configure IWA.

If you want to configure IWA for multiple domains, you must repeat this procedure for each active directory that requires to use IWA.

Before you begin

Generate a `tomcat.keytab` file for the active directory that you plan to use for IWA. If you want to configure IWA for multiple domains, you must generate a `tomcat.keytab` file for each active directory.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, click **LDAP Configuration**.
2. Select the required Active Directory.
3. In the Server Address and Credentials area, do the following:
   a. In the **Windows Authentication** drop-down menu, select **Negotiate**.
   b. In the Confirm Action dialog box, click **OK**.
   c. In **UID Attribute ID**, type `userPrincipalName`.

If this field is not set to `userPrincipalName`, you might encounter license issues and other unpredictable behavior.

d. Ensure that the other settings are appropriate for the LDAP configuration of your Domain Controller.

Important:

The LDAP server that you use must be the domain controller with the appropriate Active Directory version as the server type.

4. In the Configuration for Windows Authentication area, complete the following information using the same values you provided when setting up the Windows Domain Controller:

a. In **Service Principal Name (SPN)**, type `HTTP/<FRONT—END FQDN>`.

For example, `HTTP/csa.example.com`.

b. Click **Import** to import the `tomcat.keytab` file transferred from the Windows Domain Controller.

In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

c. In **Kerberos Realm**, type the Kerberos realm, which is usually in all uppercase letters. For example, `EXAMPLE.COM`.

d. In **DNS Domain**, type the DNS domain of the Domain Controller.

For example, `example.com`.

e. **(Optional)** Select the **Use SRV Record** check box.

f. **(Optional)** If **Use SRV Record** is not selected, in **KDC FQDN**, type the FQDN of the Domain Controller.

This value also includes the DNS domain at the end. For example, `ad.example.com`.

g. **(Optional)** In **KDC Port**, retain the default value of 88.

This field is only visible if **Use SRV Record** is not selected.

h. **(Optional)** In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file you imported in step 4.b on page 120 to a specific node.

This option is useful if the import to a node failed or if you add a new node to your cluster.

5. Click **Save** to retain the settings and restart the server.

The settings that you updated are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

Chapter 7: Virtual hardware adjustments

The following sections describe how to perform virtual hardware adjustments on a virtual machine.

For information about disk volume sizes, see the disk volume specifications in Virtual disk volume specifications on page 121.

Virtual disk volume specifications

The following table shows the file system layout for systems deployed using Avaya-provided OVAs.

Disk Volume	Volume size can be increased	Volume Size (GiB)			
		Disk 1	Disk 2	Disk 3	Disk 4
/boot	No	0.2			
swap	Yes	8.0			
/	Yes	4.0			
/tmp	Yes	2.8			
/var	Yes	3.0			
/var/log	Yes	2.0			
/var/log/audit	Yes	3.0			
/home	Yes	4.0			
/opt/Avaya	Yes	15.0			
/var/log/Avaya	Yes		60.0		
/media/data	Yes			20.0	
/media/cassandra	Yes				10.0
Total for disk		42.0	60.0	20.0	10.0
Total disk size		132.0			

Increasing the size of a virtual disk

About this task

Each virtual disk holds one or more disk volumes. Before you can increase the size of a disk volume, you must first increase the size of the host disk to provide the required disk space.

This procedure describes how to adjust the size of a virtual disk in the Virtualization Enabled (VE) environment. The VE environment uses the standard VMware infrastructure facilities.

Before you begin

- Ensure that the system layer on the virtual machine has been upgraded to the current release. You can verify this using the `sys versions` command.
- Delete all snapshots from the virtual machine. You cannot adjust disk sizes while snapshots exist.
- Determine the disk volume to be increased in size.
- Determine the disk number that hosts the disk volume. You can use the `sys volmgt --summary` command for more information.

Procedure

1. If the virtual machine is installed and running, log in to the system, and shut down the operating system by running the following command:

   ```
   sudo shutdown -h now
   ```

2. Stop your virtual machine if it is still running.
3. Click **Edit Settings**.
4. From the Hardware tab, select the hard disk to be enlarged.
5. In **Disk Provisioning**, enter a higher value for the disk size and select the appropriate unit of measure.
6. Click **OK**.
7. Power on the virtual machine.

Next steps

Increase the size of the disk volume.

Increasing the virtual machine disk volume size

About this task

Use this procedure to increase the size of a disk volume. The upgrade process for an OVA from a previous release requires an increase in the size of one or more disk volumes.

In rare circumstances, Avaya support might recommend specific increments in disk volume sizes to address unexpected disk engineering issues.

Important:

You can only allocate free disk space to disk volumes if data encryption is disabled on Avaya Aura® Web Gateway. If data encryption is enabled, you *cannot* allocate free disk space.

Before you begin

Increase the size of the virtual disks that host the volumes to be increased. This process makes new disk space available. For example, if the volume requires an additional 20.0 GiB of space and the host disk is currently 50.0 GiB, then you must change the size of the host disk to 70.0 GiB.

Procedure

1. If the virtual machine is not running, then power it up.
2. Scan the disks on the virtual machine to detect newly available disk space by running the following command:

   ```
   sys volmgt --scan
   ```

   Tip:

   For more information about this command, you can use the following commands:

   - For syntax help: `sys volmgt -h`
   - For verbose help: `sys volmgt -hh`

   After the scan is complete, an updated file system summary is displayed. The newly available disk space is reported in the Disk > Free column.
3. Allocate all of the unused space on the disk to the target volume by running the following command:

   ```
   sys volmgt --extend <volume> --remaining
   ```

   For `<volume>`, specify the name of the volume as it appears in the Volume > Name column.

   All `--extend` operations are run as background tasks.

   a. To monitor the status of the operation in progress or of the last completed operation, run the following command:

      ```
      sys volmgt --monitor less
      ```

   b. To gather all volume management logs into a zip file in the current working directory, run the following command:

      ```
      sys volmgt --logs
      ```

   c. If a disk has multiple volumes and more than one volume is being increased in size, use one of the following commands to allocate a specific amount of unused space to a volume:

      ```
      sys volmgt --extend <volume> <x>m
      sys volmgt --extend <volume> <x>g
      sys volmgt --extend <volume> <x>t
      ```

In these commands, `m` means megabytes, `g` means gigabytes, `t` means terabytes, and `<x>` is a decimal number. For example, the following command increments the `/var/log` volume by 10.5 GiB:

```
sys volmgt --extend /var/log 10.5g
```

4. Verify that the new space has been allocated to the volume by running the following command:

   ```
   sys volmgt --summary
   ```

   Due to disk overhead, the size of the volume reported under the Volume > LVM Size column will never exactly match the size reported under the Volume > File System > Size column.

   a. If you suspect that the file system size is not correct, verify that the operation is complete by running the following command:

      ```
      sys volmgt --status
      ```

   b. If the status is reported as “Complete”, you can correct the situation using `--extend` without an increment value:

      ```
      sys volmgt --extend /var/log
      ```

      This operation does not add more space to the volume that hosts the file system. Instead, it reissues the command to make full use of the current volume.

      Tip:

      Similar to using `--extend` to increase volume sizes, you can also monitor the `--extend` operation and gather logs using the following commands:

      ```
      sys volmgt --monitor less
      sys volmgt --logs
      ```

Chapter 8: AWS-specific management options

If you deployed Avaya Aura® Web Gateway in an Amazon Web Services (AWS) environment, use the following sections to perform AWS-specific management operations. You can perform these management operations anytime.

Increasing the size of an AWS disk volume

About this task

Use this procedure to add additional storage to the system by increasing the size of an attached disk and then allocating the free space to volumes on the disk. You cannot decrease the size of a disk.

Procedure

1. On the Amazon Web Services console, navigate to **Services** > **Compute**, and then click **EC2**.
2. On the EC2 Management Console page, click **Instances**.
3. Select the instance to which you want to add storage.

   The system displays instance details.
4. Click the **Description** tab.
5. In the **Block devices** field, select a disk for which you want to increase the size:

   The options are:

   - disk1
   - disk2
   - disk3
   - disk4

   For more information about disk options, see Block device descriptions on page 126.
6. In the **EBS ID** field, click the ID.

   The system displays the Volumes page with only the selected device.

7. To update the storage on the EBS disk volume, click **Actions** > **Modify Volume**.
8. In the Modify Volume window, in the **Size** field, enter the required disk size.
9. Click **Modify**.
10. In the Confirmation window, click **Yes**.
11. In the status window, click **Close**.
12. Log in to the system using the SSH console or PuTTY.
13. If you added storage to disk1, restart the system for the changes to take effect.

    A restart is not required when increasing the size of the other disks.
14. To use the newly allocated space, update the file system by running the following commands:
    a. `sys volmgt --summary`: To view the current disk space allocation for each volume.

       The order of block devices shown on the EC2 management console might not match the order of the devices shown in the summary tool output. Reference the devices by name and not by their display order.
    b. `sys volmgt --scan`: To scan the disks for newly allocated space.

       Important:

       If prompted, restart your system before continuing.
    c. `sys volmgt --extend [ <n>m | <n>g | <n>t | --remaining ]`: To assign unallocated disk space to the volumes on a disk, specifying the amount of space you want to add to each volume. Repeat this step for each volume that you want to extend.

       For example, to extend the size of the `/var/log/Avaya volume` on disk1 by 10 GiB, run the `\sys volmgt --extend /var/log/Avaya 10g` command.

       For more information, run the `sys volmgt --hhelp` command.
    d. `sys volmgt --summary`: To review the disk space allocation for each volume after the changes are made.

Block device descriptions

Block device on AWS	Disk number	Description
/dev/sda1	disk1	Stores operating system and application software.
/dev/xvdb	disk2	Stores application logs.
/dev/xvdb	disk3	Stores application data.
/dev/xvdd	disk4	Stores database commit logs.

Updating an existing stack with a new CloudFormation template

About this task

You can apply changes to an existing CloudFormation stack by updating the stack with a newer CloudFormation template. Changes to the stack can include additional nodes, new resources, and new port configuration. The system updates all the objects contained in the stack to match the new settings. Existing EBS volumes and S3 buckets are preserved.

To update an existing single-node stack you must use a new single-node stack template. To update an existing cluster you must use a new multi-node stack template. If you are expanding a cluster, you must already have a cluster with two or more nodes. You cannot expand a single AWS node into an AWS cluster

Before you begin

Generate a new CloudFormation template that matches the application and profile of the existing system but includes the additional resources required. For more information, see the “Creating CloudFormation templates” section in *Deploying the Avaya Aura® Web Gateway*.

Procedure

1. Sign in to the AWS console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation**.
3. Select the stack to update.
4. Click **Actions** > **Update Stacks**.
5. Update the stack using the Update Stack pages.

   You can add an additional CIDR block when going from two to three subnets. Do not change the value of any other stack parameters.

Deleting a CloudFormation stack

Procedure

1. Sign in to the AWS console and click **Services** > **Management Tools** > **CloudFormation**.
2. On the CloudFormation page, select a stack to delete.
3. Click **Actions** > **Delete Stack**.
4. Click **Yes, Delete** when prompted.

   The AMI virtual machines and other resources that are in the stack are deleted.

Note:

The stack is not completely deleted if it includes Amazon Route 53. See the next step for information about resolving this issue.

5. **(Optional)** If deleting the stack fails due to the presence of an Amazon Route 53 DNS zone, then do the following:
   a. Navigate to **Services** > **Networking & Content Delivery** > **Route 53** > **Hosted zones**.
   b. Select the Hosted Zone that is no longer required and click **Delete Hosted Zone**.
   c. Click **Confirm**.
   d. Navigate to **Services** > **Management Tools** > **CloudFormation**.
   e. Select the stack that previously failed to delete.
   f. Click **Actions** > **Delete Stack**.
   g. Click **Yes, Delete**.

Chapter 9: Security options

Data encryption management

When you deploy the Avaya Aura® Web Gateway OVA, you can enable data encryption and configure basic settings, such as providing a passphrase or enabling the local key store. After deploying the Avaya Aura® Web Gateway OVA, you can use system layer commands to perform additional data encryption management operations, such as the following:

- Enabling a remote key server.
- Managing encryption passphrases.
- Reviewing data encryption status.

Important:

In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.

Related links

Data encryption commands on page 37

Enabling or disabling disk encryption on Avaya Aura® Web Gateway

About this task

You cannot enable or disable disk encryption by using the Avaya Aura® Web Gateway web administration portal or the configuration utility. However, you can enable or disable disk encryption when restoring Avaya Aura® Web Gateway from a backup. This procedure provides the high-level steps for enabling or disabling disk encryption.

Important:

- This procedure only applies to OVA-based deployments. You cannot enable disk encryption for software-based deployments.
- For AWS deployments, you cannot enable disk encryption on Avaya Aura® Web Gateway. You must enable disk encryption on AWS itself. For more information, see How to Protect Data at Rest with Amazon EC2 Instance Store Encryption.

This procedure applies to cluster and standalone Avaya Aura® Web Gateway deployments.

Procedure

1. Perform a full system backup:
   a. Back up each node of your Avaya Aura® Web Gateway deployment.
   b. Record configuration values from the existing Avaya Aura® Web Gateway system.
   c. Copy logs, home directory content, and backup files to an external storage.

   For more information, see Backing up Avaya Aura Web Gateway on page 165.
2. Deploy new virtual machines.

   You can enable or disable disk encryption as needed when deploying the Avaya Aura® Web Gateway OVA. For information about the deployment procedures, see “OVA deployment” in *Deploying the Avaya Aura® Web Gateway*.

   Important:

   - You must use the same OVA and the same version of the Avaya Aura® Web Gateway application that was backed up.
   - You must use the original network settings, such as host names and IP addresses, from the currently installed cluster when deploying new virtual machines.
3. Restore the Avaya Aura® Web Gateway application using the backups created in step 1.

   For information about restoring Avaya Aura® Web Gateway, see Restoring Avaya Aura Web Gateway in a standalone environment on page 168 or Restoring an entire Avaya Aura Web Gateway cluster on page 171.

Remote key server management

When configuring data encryption during the OVA deployment, if you choose not to enter a passhrapse after every reboot, Avaya Aura® Web Gateway stores encryption keys in a local key store. To enhance security, you can set up a remote key server. You can add multiple remote key servers.

Enabling a remote key server

About this task

Use this procedure to use a remote key sever to store encryption keys.

When adding a remote key server for the first time, you can choose either to continue using the local key store or to disable it. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Web Gateway uses the local key store to decrypt the encrypted disks at boot time.

If you already have a remote key server enabled, you can use this procedure to add another remote key server.

Before you begin

Configure your remote key server. The exact configuration procedure depends on the key server you are using.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   `sys encryptionRemoteKey add <server address> <port>`

   In this command:

   - `<server address>` is the IP address or FQDN of the remote key server.
   - `<port>` is a port that the remote key server uses to connect to Avaya Aura® Web Gateway. This is an optional value. If you do not enter a port number, the remote key server uses port 80 by default.
3. When prompted, enter the existing passphrase.
4. When prompted to remove the local key store, do one of the following:
   - To disable the local key store, enter `y`.
   - To continue using the local key store, enter `n`.

Disabling a remote key server

About this task

Use this procedure if you do not want to use a remote key server to store encryption keys. If you have multiple remote key stores, Avaya Aura® Web Gateway will continue using other remote key stores until you disable them.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   `sys encryptionRemoteKey remove <server address>`

   In this command, `<server address>` is the IP address or FQDN of the remote key server you want to disable. You must use the same IP address or FQDN that you used when enabling the remote key server.

Passphrase management

Avaya Aura® Web Gateway requires an encryption passphrase to access encrypted partitions.

When enabling data encryption during the Avaya Aura® Web Gateway OVA deployment, you set up a single passhprase. After the OVA is deployed, you can use system layer commands to:

- Configure up to seven additional passhprases.

- Change existing passphrases.
- Remove a passphrase.
- View status of passphrases.

Adding a passphrase

About this task

Use this procedure to set up additonal passphrases. You can have up to seven passphrases in total. If you have multiple passphrases, you can use any of them to access encrypted disk partitions.

A passphrase you add must comply with the passphrase complexity rules.

Before you begin

Ensure that you have a passphrase slot available. For more information, see Reviewing the passphrase status on page 133.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase add
   ```

3. When prompted, type one of the existing passphrases.
4. When prompted, type a new passphrase.
5. Type the new passphrase again to confirm it.

Passphrase complexity rules

All encryption passphrases you add to Avaya Aura® Web Gateway must contain at least:

- Eight characters.
- One character from each of the following character sets:
  - Uppercase letters: A to Z
  - Lowercase letters: a to z
  - Numerics: 0 to 9
  - Special characters: !, @, #, %, $, ^, *, ?, and _

Removing a passphrase

About this task

Use this task to remove an existing encryption passphrase.

Avaya Aura® Web Gateway requires at least one encryption passphrase. If you have only one passphrase, you cannot remove it.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase remove
   ```

3. When prompted, type the encryption passphrase you want to remove.

Reviewing the passphrase status

About this task

Use this procedure to view information about the number of passphrases you have on Avaya Aura® Web Gateway.

Tip:

You can use this procedure before adding a new passphrase to see if Avaya Aura® Web Gateway has a free slot for a new passphrase.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionPassphrase list
   ```

   Avaya Aura® Web Gateway displays passphrase and slot assignment information.

```
Slot        Status      Passphrase/Remote Server
-------------------------------------------------
Key Slot 0: ENABLED     Passphrase
Key Slot 1: ENABLED     Passphrase
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
```

Viewing data encryption status

About this task

Use this procedure to view information about data encryption, including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption passphrase must be entered after every reboot.
- Information about configured remote key servers.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.

2. Run the `sys encryptionStatus` command.

Local key store management

Enabling the local key store

About this task

If you do not want to enter an encryption passphrase after every Avaya Aura® Web Gateway reboot and you do not have a remote key server, you can enable the local key store. However, the local key store is less secure than a remote key store or entering a passphrase after every reboot.

You can enable the local key store even if a remote key server is enabled. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Web Gateway uses the local key store to decrypt the encrypted disks at boot time.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionLocalKey enable
   ```

3. When prompted, enter the encryption passphrase.

Disabling the local key store

About this task

When you disable the local key store and do not have a remote key server, you will need to enter your passphrase after every Avaya Aura® Web Gateway reboot. If at least one remote key server is confgured, then Avaya Aura® Web Gateway will use this remote key server to store encryption keys.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
2. Run the following command:

   ```
   sys encryptionLocalKey disable
   ```

Advanced Intrusion Detection Environment tool management

Advanced Intrusion Detection Environment (AIDE) is a tool for monitoring file system changes. AIDE creates a baseline database of system layer files and then verifies the integrity of the files by comparing the database to the actual state of the system layer files. AIDE only performs file integrity checks and does not provide other checks, such as rootkit searches.

Important:

Software-only deployments do *not* include the AIDE tool. If you want to use AIDE on Avaya Aura® Web Gateway deployed as a software-only application, you must install AIDE separately.

On Avaya Aura® Web Gateway, you can manage AIDE using the **fsit.sh** system layer script, which is located in the `/opt/Avaya/bin` directory. The **fsit.sh** script is available after you deploy the Avaya Aura® Web Gateway OVA.

Avaya recommends that you run AIDE scanning at least once a week.

Creating a baseline database

About this task

Use this procedure to create a baseline database of operational system and Avaya Aura® Web Gateway files. AIDE uses this database as a reference when performing file system integrity scans.

You must create a database before you start running AIDE scans. Do *not* create a new database before each scan. Create a new baseline after you installed Avaya Aura® Web Gateway and then create a new baseline each time after you upgraded Avaya Aura® Web Gateway.

The database creation process can take up to 50 minutes depending on the system data.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to navigate to the **fsit.sh** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to create an AIDE database as a background process:

   ```
   sudo ./fsit.sh -updateDB &
   ```

   Creating the database as a background process enables you to perform other tasks at the same time.

Result

AIDE creates the baseline database and records the results in the `/var/log/aide/aide_update_status.log` file. If the database is created successfully, the log contains the `Completed` entry and a time stamp. Otherwise, the log contains the `Failed` entry. You can view the log file content using the **cat** command.

The following is an example of the **cat** command output when the baseline database is created successfully.

```
[admin@aads68 bin]$ sudo cat /var/log/aide/aide_update_status.log
Completed (Wed Dec 11 15:27:24 IST 2019)
[admin@aads68 bin]$
```

AIDE scanning

During the scanning process, AIDE compares the actual state of the file system with the reference values stored in the baseline database and informs you if there are any differences. You can either run AIDE scanning manually or configure automatic scanning. AIDE scanning can take up to 50 minutes depending on the system data. AIDE records the scanning results to the `/var/log/aide/aide_scan_status.log` file.

You must run AIDE scans on a regular basis.

Excluding files and directories from AIDE scanning

About this task

By default, AIDE checks the integrity of all Avaya Aura® Web Gateway files and directories, except for the following:

- `/opt/spirit/LogTail*`
- `/opt/spirit/logging/`
- `/opt/spirit/persist/persisted_ids.properties`

Avaya Aura® Web Gateway regularly updates certain files and directories, such as `/opt/Avaya/CallSignallingAgent/<version>/logs/`. AIDE includes all changed files in the scanning report, regardless of the reason for the change. This might result in false positive alarms in the scan report. You can add certain files and directories you want to exclude from scanning to the `/etc/aide.conf` AIDE configuration file. AIDE will not include these files and directories in scanning reports.

Warning:

Be cautions when excluding a file or directory from scanning because an intruder might place a malicious file in a place that AIDE does not check.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Open the `/etc/aide.conf` file in a text editor.

   For example, to open the file in vi, run the `vi /etc/aide.conf` command.
3. For each file or directory you want to exclude from scanning, add an entry in the following format:

   `!<path to file or directory>`

   In this entry, `<path to file or directory>` is the absolute path to the file or directory you want to exclude. For example, enter `!/opt/Avaya/CallSignallingAgent/3.8.0.0.001/logs/` to exclude the entire directory from the report.

If you want to exclude a single file, add the `$` character at the end of the entry. For example: `!/opt/Avaya/CallSignallingAgent/3.8.0.0.001/logs/File.log$`

The entry format supports regular expressions. For example, you can enter `!/opt/Avaya/CallSignallingAgent/3.8.0.0.001/logs/File*` to exclude only files and directories that have names starting with `File`.

4. Save the `/etc/aide.conf` file.

Running AIDE scanning manually

About this task

Use this procedure to run AIDE scanning manually. Scanning can take up to 50 minutes, depending on the system data. Avaya recommends that you run AIDE scanning at least once a week.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Run AIDE scanning during the least busy periods to minimize the impact on Avaya Aura® Web Gateway performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Web Gateway release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to navigate to the **`fsit.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to run AIDE scanning as a background process:

   ```
   sudo ./fsit.sh -scanNow &
   ```

Result

AIDE checks the file system integrity and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

Creating a baseline database on page 135

Configuring automatic scanning

About this task

Use this procedure to configure automatic AIDE scanning. Automatic scanning is performed once a day. Scanning can take up to 50 minutes, depending on the system data.

Do not run or schedule AIDE scanning, ClamAV virus scanning, and ClamAV database updates at the same time. Schedule AIDE scanning for the least busy periods to minimize the impact on Avaya Aura® Web Gateway performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Web Gateway release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to navigate to the **`fsit.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command to configure automatic scanning:

   ```
   sudo ./fsit.sh -enableScan <hour> <minute>
   ```

   Replace `<hour>` and `<minute>` with the time when you want to run the scan process. Use the 24–hour time format. For 12 a.m., enter `0`.

   For example, enter `sudo ./fsit.sh -enableScan 16 00` to run scanning at 4:00 p.m.

Result

AIDE checks the file system integrity once a day and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

Creating a baseline database on page 135

Disabling automatic scanning

About this task

Use this procedure to disable automatic AIDE scanning.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./fsit.sh -disableScan
   ```

Reviewing the AIDE scanning report

About this task

Use this procedure to review the results of the latest AIDE scan. The report contains the following:

- The baseline database status.
- Information about the automatic scanning configuration.
- The last database update and scan dates.
- The number of scanned files and directories.
- The number of added, removed, or changed files.
- Information about added, removed, or changed files.
- Detailed Information about changes.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to navigate to the **`fsit.sh`** script location:

   ```
   cd /opt/Avaya/bin
   ```

3. Run the following command:

   ```
   sudo ./fsit.sh -status
   ```

   The scan results are displayed in the terminal window.

Example

The following example shows a scan report with differences between the baseline database and the actual system state found:

```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-12-11 15:26:52

Summary:
  Total number of files:        55724
  Added files:                  0
  Removed files:                0
  Changed files:                1


---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /opt/Avaya/bin/fsit.sh

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


File: /opt/Avaya/bin/fsit.sh
 SHA512   : 7v0sOtK9erPSw8dw8GLTCacbvdHO28qj , bdxUm2J38kb/1yfDVO/KiA+55CeJ1hfX
```

The following example shows a scan report with no differences found:

```
AIDE, version 0.15.1

### All files match AIDE database. Looks okay!
```

CylancePROTECT antivirus software overview

Avaya Aura® Web Gateway supports the CylancePROTECT antivirus software. CylancePROTECT is an antivirus tool that uses mathematical models and machine learning algorithms instead of reactive signatures and databases to detect and neutralize malicious software. CylancePROTECT can identify threat on the operating system and memory layers.

To use CylancePROTECT, you must install the CylancePROTECT Agent on each Avaya Aura® Web Gateway node in your deployment. For information about installation, configuration, and usage of CylancePROTECT, see the CylancePROTECT Administration Guide.

Avaya Aura® Web Gateway supports CylancePROTECT version 2.1.1570 (Agent version 1570) or higher.

Out-of-band management

By default, Avaya Aura® Web Gateway uses a single network interface for all traffic types. For additional security, you can use the out-of-band management functionality to isolate client traffic from system management traffic by using different network interfaces for these traffic types.

When you enable out-of-band management on Avaya Aura® Web Gateway, the management access on the public interface is disabled. You can administer Avaya Aura® Web Gateway using the configured management interface. End users cannot access the management interface. This prevents unauthorized login attempts from the end user network.

You can configure out-of-band management after installing or upgrading Avaya Aura® Web Gateway.

Out-of-band management configuration checklist

No.	Task	Notes	✔
1	Add and configure a second network interface.	See Configuring a second network interface on page 141.	
2	Configure out-of-band management settings on the Avaya Aura® Web Gateway administration portal.	See Configuring out-of-band management settings on page 144.	
3	If you configure out-of-band management in a cluster deployment, update internode SSH communication settings.	See Configuring RSA public and private keys for SSH connections in a cluster on page 172.	
4	Generate identity certificates for the new interface.	See Generating identity certificates for the second network interface on page 145.	

Configuring a second network interface

About this task

You can add a second network interface by editing your virtual machine settings. Then you can configure this interface using RHEL CLI commands.

In a cluster deployment, perform this procedure on all nodes in the cluster.

Before you begin

Prepare the following data for the second network interface:

- IP address. In a cluster deployment, you must use a unique IP address for each node.
- Network mask

- Gateway address

Procedure

1. Log in to Avaya Aura® Web Gateway using an SSH connection.
2. Run the `ip address show` command to ensure that you have only one network interface.

   For example:

   ```
   [admin@aawg ~]$ ip address show
   1: lo:  <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
       link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
          valid_lft forever preferred_lft forever
       inet6 ::1/128 scope host
          valid_lft forever preferred_lft forever
   2: eth0:  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
       link/ether 00:0C:29:a8:86:79 brd ff:ff:ff:ff:ff:ff
       inet 192.0.2.26/24 brd 192.0.2.255 scope global eth0
          valid_lft forever preferred_lft forever
       inet6 2001:db8::fea8:8679/64 scope link
          valid_lft forever preferred_lft forever
   ```

   In this example, `lo` is the loopback interface and `eth0` is the only network interface.
3. Do the following to enable Avaya Aura® Web Gateway to process packets from any network:
   a. Open the `/etc/sysctl.conf` file in a text editor with sudo privileges.

      For example: `sudo vi /etc/sysctl.conf`
   b. Find the `net.ipv4.conf.all.rp_filter` parameter and change its value to `2`.

      ```
      net.ipv4.conf.all.rp_filter = 2
      ```
   c. Save the file.
   d. Run the `sudo reboot` command to restart Avaya Aura® Web Gateway.
   e. Run the following command to verify the updated configuration:

      ```
      sysctl -a 2>/dev/null | grep "\.rp_filter"
      ```

      The following is an example of the command output:

      ```
      [admin@aawg ~]$ sysctl -a 2>/dev/null | grep "\.rp_filter"
      net.ipv4.conf.all.rp_filter = 2
      net.ipv4.conf.default.rp_filter = 1
      net.ipv4.conf.eth0.rp_filter = 1
      net.ipv4.conf.lo.rp_filter = 0
      ```
4. On the VMware virtual machine where Avaya Aura® Web Gateway is deployed, add a new network interface.

   For information about adding network interfaces on VMware, see the documentation for the VMware version you used to deploy Avaya Aura® Web Gateway.
5. Run the `ip address show` command to ensure that you added a second network interface.

For example:

```
[admin@aawg ~]$ ip address show
1: lo:  <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0:  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0C:29:a8:86:79 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.26/24 brd 192.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:db8::fea8:8679/64 scope link
       valid_lft forever preferred_lft forever
3: eth1:  <BROADCAST,MULTICAST> mtu 1500 noop state DOWN qlen 1000
    link/ether 00:0C:29:a8:86:80 brd ff:ff:ff:ff:ff:ff
```

In this example, `eth0` is the existing network interface and `eth1` is the second network interface you added in the previous step.

6. Run the following command to copy the configuration file for the second network interface from the configuration file for the existing network interface:

   `sudo cp /etc/sysconfig/network-scipts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth1`

   The following is an example of the configuration file for the existing network interface:

   ```
   [admin@aawg ~]$ sudo cat /etc/sysconfig/network-scripts/ifcfg-eth0
   DEVICE=eth0
   BOOTPRO=static
   ONBOOT=yes
   TYPE=Ethernet
   IPADDR=192.0.2.26
   NETMASK=255.255.255.0
   GATEWAY=192.0.2.1
   ```

7. Open the `/etc/sysconfig/network-scripts/ifcfg-eth1` configuration file for the second network interface in a text editor with sudo privileges.

   For example: `sudo vi /etc/sysconfig/network-scripts/ifcfg-eht1`

8. Modify the following parameters:

   a. DEVICE: Enter `eth1`.

   b. IPADDR: Enter the IP address of the second network interface.

   c. NETMASK: Enter the subnetwork mask of the second network interface IP address.

   d. GATEWAY: Enter the gateway address.

   The following is an example of the updated configuration file for the second network interface:

   ```
   [admin@aawg ~]$ sudo cat /etc/sysconfig/network-scripts/ifcfg-eth1
   DEVICE=eth1
   BOOTPRO=static
   ONBOOT=yes
   TYPE=Ethernet
   IPADDR=198.51.100.29
   ```

```
NETMASK=255.255.255.0
GATEWAY=198.51.100.1
```

9. Save the file.
10. Run the `sudo systemctl restart network` command to apply changes.
11. Run the `ip address show` command to verify that the second network interface is configured.

    For example:

```
[admin@aawg ~]$ ip address show
1: lo:  <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0:  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0C:29:a8:86:79 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.26/24 brd 192.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:db8::fea8:8679/64 scope link
       valid_lft forever preferred_lft forever
3: eth1:  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0C:29:a8:86:80 brd ff:ff:ff:ff:ff:ff
    inet 198.51.100.29/24 brd 198.51.100.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:db8::fea8:8680/64 scope link
       valid_lft forever preferred_lft forever
```

12. From another computer, run the `ping` command to ensure that both network interfaces are accessible:

    `ping <FIRST NETWORK INETRFACE IP ADDRESS>`

    `ping <SECOND NETWORK INTERFACE IP ADDRESS>`

    For example:

```
ping 192.0.2.26
ping 198.51.100.29
```

Configuring out-of-band management settings

About this task

After configuring a second network interface, you can configure out-of-band management settings on the Avaya Aura® Web Gateway administration portal. Out-of-band management enables you to isolate client traffic from system management traffic.

Before you begin

Ensure that you have two network interfaces configured on the Avaya Aura® Web Gateway.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **OOB Management**.

2. From **Portal and AAWG Services**, select the network interface that you want to use for client traffic.
3. From **OAM**, select the network interface that you want to use for system management traffic.
4. **(Optional)** To block SSH connections to the network interface you use for client traffic, select the **Block ssh traffic on the in-band (Portal and AAWG Services) network** check box.
5. Click **Save**.
6. In the Confirm Action window, click **Yes** and then wait until the configuration process is completed.
7. Click **OK**.
8. **(Optional)** To verify the changes, do the following:
    a. Log out from the Avaya Aura® Web Gateway administration portal.
    b. In a new browser window, try to open the Avaya Aura® Web Gateway administration portal using the IP address of the network interface you configured for client traffic.
    c. Ensure that the browser displays the `Site cannot be reached` message.
    d. In a new browser window, open the Avaya Aura® Web Gateway administration portal using the IP address of the network interface you configured for system management traffic.
    e. Log in to the Avaya Aura® Web Gateway administration portal.
    f. If you selected the **Block ssh traffic on the in-band (Portal and AAWG Services) network** check box, log in to the Avaya Aura® Web Gateway CLI using SSH with the IP address of the network interface you configured for client traffic.
    g. Ensure that you cannot log in to the Avaya Aura® Web Gateway CLI using SSH.

Next steps

In a cluster deployment, update internode SSH communication settings as described in Configuring RSA public and private keys for SSH connections in a cluster on page 172.

Related links

Configuring a second network interface on page 141

Generating identity certificates for the second network interface

About this task

When out-of-band management is configured, Avaya Aura® Web Gateway uses two network interfaces to access the Avaya Aura® Web Gateway administration portal. You must generate new identity certificates so your browser can trust the Avaya Aura® Web Gateway administration portal.

By default, all new generated certificates contain the IP address of the second interface in their Subject Alternative Name (SAN) property. Therefore, you do not need to add DNS records for this interface.

Before you begin

- Configure out-of-band management on the Avaya Aura® Web Gateway administration portal.
- In a cluster environment, update internode SSH communication settings as described in Configuring RSA public and private keys for SSH connections in a cluster on page 172.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Security Settings** > **Certificate Management** > **SMGR Certificates**.
2. If you have a cluster or a single node and you do not plan to use an FQDN to access the Avaya Aura® Web Gateway administration portal, do the following:
   a. In a cluster environment, ensure that **Node Address** is set to **All Cluster Nodes**.
   b. In **System Manager Enrollment Password**, enter the System Manager enrollment password.
   c. Click **Generate Certificates**.
   d. Accept all default settings and wait until System Manager generates new certificates.

   Avaya Aura® Web Gateway applies the changes by restarting its nodes. After the restart, the identity certificate of each node contains the IP address of the second network interface in the SAN field.
3. If you have a cluster or a single node and you plan to use an FQDN for accessing the Avaya Aura® Web Gateway administration portal, do the following:
   a. In **Node Address**, select the required node.
   b. Select the **Show settings** check box.
   c. In **New Subject Alternative Name**, enter the FQDN that is mapped to the IP address of the secondary interface of the node and then click **Add**.
   d. In **System Manager Enrollment Password**, enter the System Manager enrollment password.
   e. Click **Generate Certificates**.
   f. Accept all default settings and wait until System Manager generates new certificates.

      Avaya Aura® Web Gateway applies the changes by restarting its nodes. After the restart, the identity certificate of each node contains the following new entries in its SAN field:

      - The FQDN address that you provided.
      - The IP address, which is assigned automatically.
   g. In a cluster environment, repeat these substeps for all remaining nodes.

Restoring the default out-of-band management settings

About this task

You can restore the default out-of-band management settings if the network interface that you assigned for system management traffic is not reachable. With the default settings, services are accessible on all network interfaces.

Procedure

1. Log in to an Avaya Aura® Web Gateway node using an SSH connection.
2. Run the `cdto cas` command.
3. Run the `sudo ./os/securty/firewall.pl` command.
4. Enter the administrator password and then wait until the process is complete.

firewall.pl script

The **`firewall.pl`** script enables you to specify which network interfaces are used for the system management and client traffic types.

If you run the command without arguments, the out-of-band management settings are reset to the default configuration, where all traffic types use all network interfaces. This can be helpful if the network interface you selected for system management traffic is not reachable.

The script is located in the `/opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/os/security/` directory.

Syntax

```
sudo firewall.pl [--oam={<OAM_interface>|all}] [--custom={<Client_interface>|all]} [--block_ssh={y|n}] [--print_ports]
```

--oam Sets a network interface for system management traffic. For example, `eth1`. If you want to use all interfaces for system management traffic, enter `all`.

--custom Sets a network interface for client traffic. For example, `eth0`. If you want to use all interfaces for client traffic, enter `all`.

--block_ssh Specifies whether Avaya Aura® Web Gateway blocks SSH traffic on the network interface that is used for client traffic. To allow SSH traffic, enter `y`. To block SSH traffic, enter `n`.

--print_ports Prints the current firewall configuration.

Example

The following command enables client traffic on all configured network interfaces, sets the eth1 network interface for system management traffic, and allows SSH traffic on the system interface that is used for client traffic.

```
sudo firewall.pl --oam=eth1 --custom=all --block_ssh=n
```

Enabling additional STIG hardening

About this task

The Security Technical Implementation Guides (STIGs) are the requirements that, when implemented, enhance application security and monitoring capabilities. By default, Avaya Aura® Web Gateway enables essential STIG hardening options during the system layer installation or upgrade. These default settings are appropriate for most deployments. If your organization requires stricter STIG compliance, use this procedure to enable additional Linux STIG security hardening options.

Important:

You *cannot* enable additional STIG hardening in software-only deployments.

Procedure

1. Log in to the virtual machine with the Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to enable additional STIG hardening options:

   ```
   sys secconfig --stig --enable
   ```

3. When prompted, press `c` to apply new password rules.
4. **(Optional)** To review the STIG hardening status, run the following command:

   ```
   sys secconfig --stig --query
   ```

Disabling additional STIG hardening

About this task

Use this procedure to disable additional STIG hardening. The default STIG hardening options, which are enabled during the system layer installation or upgrade process, will still be available. Avaya Aura® Web Gateway also continues to use the password complexity rules that were set up when you enabled additional STIG hardening.

Procedure

1. Log in to the virtual machine with the Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to disable additional STIG hardening:

   ```
   sys secconfig --stig --disable
   ```

3. **(Optional)** To review the STIG hardening status, run the following command:

```
sys secconfig --stig --query
```

Characters supported for Avaya Aura® Web Gateway passwords

You can use the following characters for Avaya Aura® Web Gateway passwords:

- Uppercase letters: A to Z
- Lowercase letters: a to z
- Numerics: 0 to 9
- Special characters: !, @, #, %, $, ^, *, ?, and _

These rules apply to all passwords that you enter manually to access resources and for Keystore passwords.

Note:

The web administration portal supports Active Directory-based authentication. Therefore, you can use other special characters, such as double quotes ("), for web administration portal passwords.

Password policy for human-user accounts

Human-user accounts are accounts that require you to enter a password manually to access Avaya Aura® Web Gateway resources. To protect data and prevent unauthorized access to the system, Avaya Aura® Web Gateway provides default complexity rules for human-user accounts. Each password you create for human-user accounts must meet these requirements.

Avaya Aura® Web Gateway enforces the default complexity rules for the following human-user accounts:

- SSH administration access to Avaya Aura® Web Gateway CLI
- Keepalived authentication
- Cassandra database administrator

If your organization requires a different password policy, you can modify the default complexity rules by using the **`sys passwdrules`** command.

Note:

- Avaya Aura® Web Gateway does not enforce complexity rules for the following passwords because they are not configured on Avaya Aura® Web Gateway:
  - Avaya Aura® Web Gateway web administration portal password.

  - System Manager enrollment password.
- Avaya Aura® Web Gateway does not apply complexity rules for the Keystore password because it is not considered to be a human-user account.

Related links

Configuring password rules on page 150

Configuring password rules

About this task

You can modify the default password complexity policy for human-user accounts.

Procedure

1. Log in to Avaya Aura® Web Gateway using an SSH connection.
2. Run the `sys passwdrules` command with appropriate arguments.

Related links

Password policy for human-user accounts on page 149
passwdrules command on page 36
passwdrules command on page 36

Avaya Aura® Web Gateway entry points

The following table shows accounts that you can use to access various Avaya Aura® Web Gateway resources.

Login name	Accessible resources	Password change method
SSH administration user	• Virtual machine resources. • Avaya Aura® Web Gateway web administration portal, if additional STIG hardening is disabled.	Using the **passwd** command in the Avaya Aura® Web Gateway CLI.
Cassandra database administration user	CLI-based Cassandra database administration.	Using the Avaya Aura® Web Gateway configuration utility.
Keepalived account	In a cluster environment, this account is used for IP takeover and to ensure High Availability.	Using the Avaya Aura® Web Gateway configuration utility.

Chapter 10: Monitoring and maintenance options

Monitoring services

Procedure

Run the following command to view the status of individual Avaya Aura® Web Gateway services:

```
svc csa status
```

Viewing performance statistics

About this task

You can review various performance metrics and system health indicators, such as CPU or memory usage, on the Avaya Aura® Web Gateway web administration portal. You can review performance metrics for specific nodes from logs currently available on Avaya Aura® Web Gateway or from an external performance log file.

Note:

Avaya Aura® Web Gateway stores performance logs a maximum of 30 days. You can collect logs for the future use as described in Downloading logs on page 73. Performance logs have the `perf_CLF.log` file name format and they are located in the `/opt/Avaya/CallSignallingAgent/<build_number>/logs` directory. Each log file contains metrics for a specific day.

Procedure

1. On the Avaya Aura® Web Gateway portal, go to **System Information** > **Performance Metrics**.
2. View performance data for a node for a specific day as follows:
   a. Select **Choose Performance log from node by date**.
   b. In **Nodes**, select the required node.
   c. In **Date**, select the required date.
3. View performance metrics from an external performance log file as follows:
   a. Select **Choose Performance Log file**.

b. From **File**, select a log file

4. Click **Retrieve**.

   Avaya Aura® Web Gateway displays performance metrics in the Performance Metrics area. By default, Avaya Aura® Web Gateway displays the Summary tab.

   If Avaya Aura® Web Gateway does not contain performance logs for the selected date, it displays a warning message.

   Retrieving logs from an external file might take several seconds depending on the log file size and network bandwidth.

5. In the Performance Metrics area, click the tab that contains performance metrics you want to review.

   For more information about performance metrics, see Performance charts on page 152.

6. **(Optional)** If you review performance metrics for the current date, click **Refresh** to update the metrics.

Related links

Performance charts on page 152

Performance charts

The following table lists the performance charts that you can see on the Performance Metrics page.

Chart	Description
Summary	Displays smaller versions of all available charts.
System load	Displays CPU information, such as CPUs load, time spent waiting for input or output operations, or time used by user space processes. For example, you can use this chart to monitor whether the system load average threshold is exceeded due to spikes.
Java memory usage	Displays information about the Java virtual machine (JVM) memory usage.
HTTP Session Number	Displays the number of active HTTP sessions over time.
Servers Request Latency/Count	Displays statistics related to requests to other solution components, such as System Manager, Avaya Meetings Server, or Session Manager. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.

Table continues…

Chart	Description
Call Resource Request Latency/ Count	Displays statistics related to requests to the Call service API, such as creating or updating a call, or getting information about a call. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
Clients Resource Request Latency/Count	Displays statistics related to requests to the Clients service API, such as keepalive messages or getting information about clients. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
Presence Session Resource Request Latency/Count	Displays statistics related to requests to the Presence service API, such as creating, deleting, updating, or getting information about Presence sessions. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
Service Resource Request Latency/Count	Displays statistics related to requests to activate or deactivate call requests. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
Token Resource Request Latency/Count	Displays statistics related to requests to the IView Token service. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
Root Resource Request Latency/ Count	Displays statistics related to requests to the root API, such as getting information about available resources. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.

Table continues…

Chart	Description
Configuration Resource Request Latency/Count	Displays statistics related to requests to the Configuration API, such as getting information about the Avaya Aura® Web Gateway configuration. • The Servers Request Count chart displays the number of requests per 30 seconds. • The Servers Request Latency chart displays the average latency for a single request.
SIP Status Counter	Displays the number of failures for SIP requests. This chart displays statistics for various SIP request types, such as INVITE, NOTIFY, BYE, REFER, REGISTER, OPTIONS. PUBLISH, and SUBSCRIBE.

Related links

Viewing performance statistics on page 151

Log management

Use the Avaya Aura® Web Gateway web administration portal to adjust logging levels, manage log retention, and collect logs for troubleshooting purposes. You can also use the perfLogViewer tool to view performance logs.

Related links

Changing the logging level on page 71
Viewing performance logs on page 158
Downloading logs on page 73
Configuring log retention on page 72

Important logs and alarms

Log descriptions

Code	Description
AUD_CSA-00012	The database has been manually stopped.
AUD_CSA-00014	The Tomcat server has been manually stopped.
AUD_CSA-00016	The Sip relay server has been manually stopped.
AUD_CSA-00018	Nginx has been manually stopped.
AUD_CSA-00022	Recovery Manager has been manually stopped.
AUD_CSA-00023	The SNMP IP address and product ID have been updated.

Table continues…

Code	Description
AUD_CSA-00032	The maximum rate of requests or responses within a given time period has been exceeded.
AUD_CSA-00041	Recovery Manager monitoring has been disabled.
AUD_CSA-00043	Recovery Manager Watchdog restart has been disabled.
AUD_CSA-00060	ESG Telportal has been manually stopped.
AUD_CSA-00107	The Keepalived service has been manually stopped.
AUD_CSA-00109	Overload controls have been disabled.

Alarm descriptions

Code	Description
1.3.6.1.4.1.6889.2.94.0.20 1.3.6.1.4.1.6889.2.94.0.21	Failed to reach the LDAP server.
1.3.6.1.4.1.6889.2.94.0.24 1.3.6.1.4.1.6889.2.94.0.25	Some Cassandra nodes are down or unreachable.
1.3.6.1.4.1.6889.2.94.0.26 1.3.6.1.4.1.6889.2.94.0.27	Failed to reach Avaya Meetings Server Management.
1.3.6.1.4.1.6889.2.94.0.28 1.3.6.1.4.1.6889.2.94.0.29	Failed to reach Session Manager because the signalling request timed out.
1.3.6.1.4.1.6889.2.94.0.34 1.3.6.1.4.1.6889.2.94.0.35	Failed to reach Avaya Aura® Device Services.
1.3.6.1.4.1.6889.2.94.0.38 1.3.6.1.4.1.6889.2.94.0.39	Failed to reach all Avaya Media Server services.
1.3.6.1.4.1.6889.2.94.0.56 1.3.6.1.4.1.6889.2.94.0.57	Approaching full capacity of memory usage.
1.3.6.1.4.1.6889.2.94.0.62 1.3.6.1.4.1.6889.2.94.0.63	REST certificate alarm.
1.3.6.1.4.1.6889.2.94.0.64 1.3.6.1.4.1.6889.2.94.0.65	OAMP certificate alarm.
1.3.6.1.4.1.6889.2.94.0.66 1.3.6.1.4.1.6889.2.94.0.67	Tomcat certificate alarm.
1.3.6.1.4.1.6889.2.94.0.76 1.3.6.1.4.1.6889.2.94.0.77	The system is operating in License Error Mode (major).
1.3.6.1.4.1.6889.2.94.0.78 1.3.6.1.4.1.6889.2.94.0.79	The system is operating in License Restricted Mode (critical).

Table continues…

Code	Description
1.3.6.1.4.1.6889.2.94.0.80 1.3.6.1.4.1.6889.2.94.0.81	No audio licenses are available.
1.3.6.1.4.1.6889.2.94.0.82 1.3.6.1.4.1.6889.2.94.0.83	Audio licenses are at a critical threshold.
1.3.6.1.4.1.6889.2.94.0.86 1.3.6.1.4.1.6889.2.94.0.87	Time server synchronization.
1.3.6.1.4.1.6889.2.94.0.92	The average CPU usage has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.94	The average CPU usage has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.104	The request latency for Session Manager has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.106	The request latency for Session Manager has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.110	The request latency for Avaya Meetings Server Management has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.112	The request latency for Avaya Meetings Server Management has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.122	The request latency call resource for all calls has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.124	The request latency call resource for all calls has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.128	The request latency call resource for getting calls has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.130	The request latency call resource for getting calls has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.134	The request latency call resource for getting call capabilities has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.136	The request latency call resource for getting call capabilities has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.140	The request latency call resource for creating calls has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.142	The request latency call resource for creating calls has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.146	The request latency call resource for updating calls has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.148	The request latency call resource for updating calls has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.152	The request latency call resource for activated or deactivated calls has exceeded the major threshold.

Table continues…

Code	Description
1.3.6.1.4.1.6889.2.94.0.154	The request latency call resource for activated or deactivated calls has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.158	The request latency for getting Avaya Meetings Server Management tokens has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.160	The request latency for getting Avaya Meetings Server Management tokens has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.164	The request latency for getting resources from the root resource has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.166	The request latency for getting resource from the root resource has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.170	The request latency for getting all clients from the client resource has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.172	The request latency for getting all clients from the client resource has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.176	The request latency for getting clients from the client resource has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.178	The request latency for getting clients from the client resource has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.182	The request latency for the KeepAlive server from the resource has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.184	The request latency for the KeepAlive server from the resource has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.188	The request latency for the configuration resource has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.190	The request latency for the configuration resource has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.194	The request latency for creating presence session has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.196	The request latency for creating presence session has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.200	The request latency for getting presence session has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.202	The request latency for getting presence session has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.206	The request latency for updating presence session has exceeded the major threshold.
1.3.6.1.4.1.6889.2.94.0.208	The request latency for updating presence session has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.212	The request latency for deleting presence session has exceeded the major threshold.

Table continues…

Code	Description
1.3.6.1.4.1.6889.2.94.0.214	The request latency for deleting presence session has exceeded the critical threshold.
1.3.6.1.4.1.6889.2.94.0.216	Avaya Media Server is down or unreachable.
1.3.6.1.4.1.6889.2.94.0.218	Avaya Media Server is not provided.
1.3.6.1.4.1.6889.2.94.0.220	Avaya Media Server is overloaded.
1.3.6.1.4.1.6889.2.94.0.222	Connection to Avaya Media Server has failed.
1.3.6.1.4.1.6889.2.94.0.224	Avaya Media Server is not found.
1.3.6.1.4.1.6889.2.94.0.230	The video licenses are unavailable.
1.3.6.1.4.1.6889.2.94.0.232	The video licenses are in the critical state.
1.3.6.1.4.1.6889.2.94.0.234	The server node licenses are unavailable.
1.3.6.1.4.1.6889.2.94.0.236	The server node is at a critical threshold.

Viewing performance logs

About this task

Use this procedure to view performance logs using the perfLogViewer tool. This tool processes special performance logs that track system performance. Avaya Aura® Web Gateway creates performance log on a daily basis.

You can view the following data using the perfLogViewer tool:

- Calls Resource Request Latency
- Clients Resource Request Latency
- Configuration Resource Request Latency
- HTTP Session Number
- Presence Session Resource Request Latency
- Root Resource Request Latency
- Server Request Latency
- Service Resource Request Latency
- SIP Status Counter
- System Average Load
- Token Resource Request Latency

Procedure

1. From the Avaya Aura® Web Gateway web administration portal, download an archive with Avaya Aura® Web Gateway logs on your computer.

   For more information, see Downloading logs on page 73.

2. Extract performance logs from the archive with Avaya Aura® Web Gateway logs.

Performance logs have the `perf_CLF.log.<LOG_FILE_NUMBER>` file name format. In the log archive, performance logs are located in the `/opt/Avaya/CallSignallingAgent/<build_number>/logs` directory.

3. Copy the perfLogViewer tool on your computer from the following location on Avaya Aura® Web Gateway:

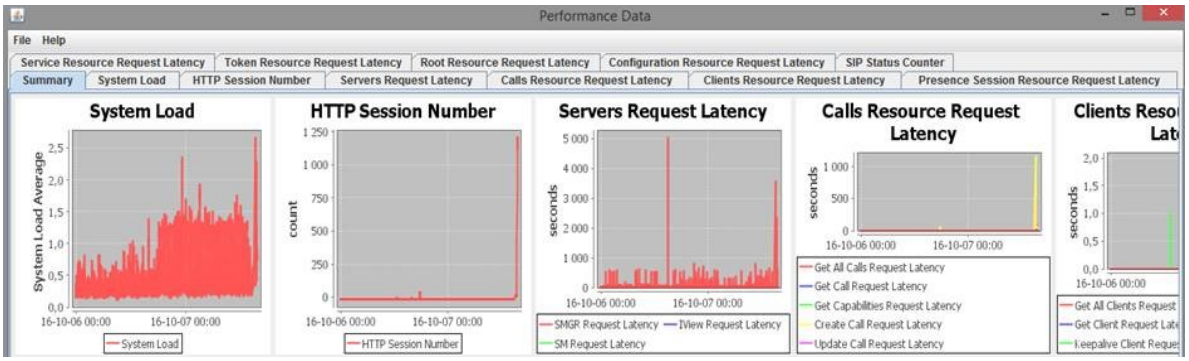
   `/opt/Avaya/CallSignallingAgent/<build_number>/CAS/<build_number>/lib/perfLogViewer-<version_number>.jar`

   You can use any file transfer utility, such as SFTP or SCP.

4. Double-click the `.jar` file to run the perfLogViewer tool.

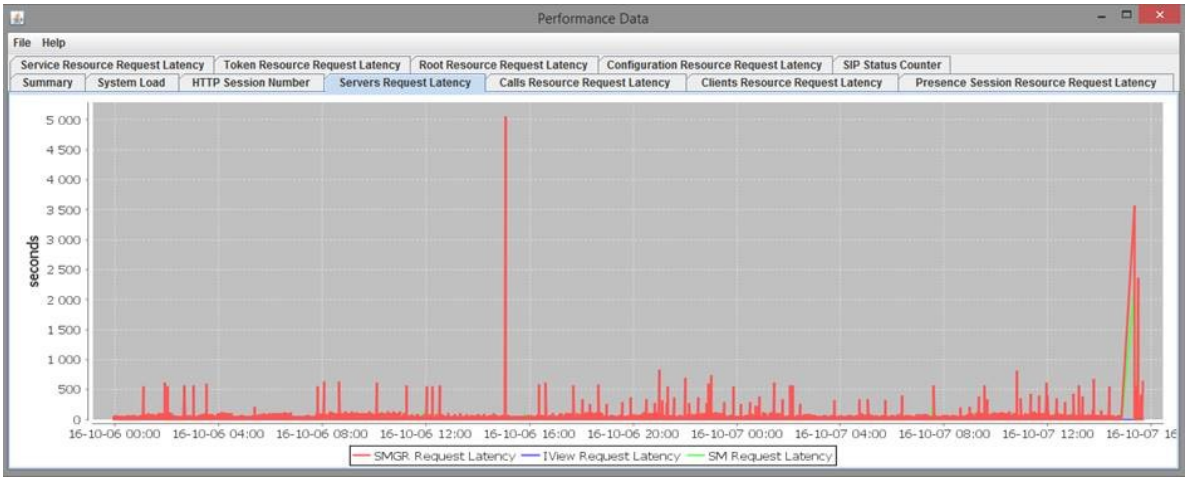
5. In the perfLogViewer tool, click **File** > **Open** and then select the required performance file.

   The following image provides an example of the summary page displaying some of the performance metrics:



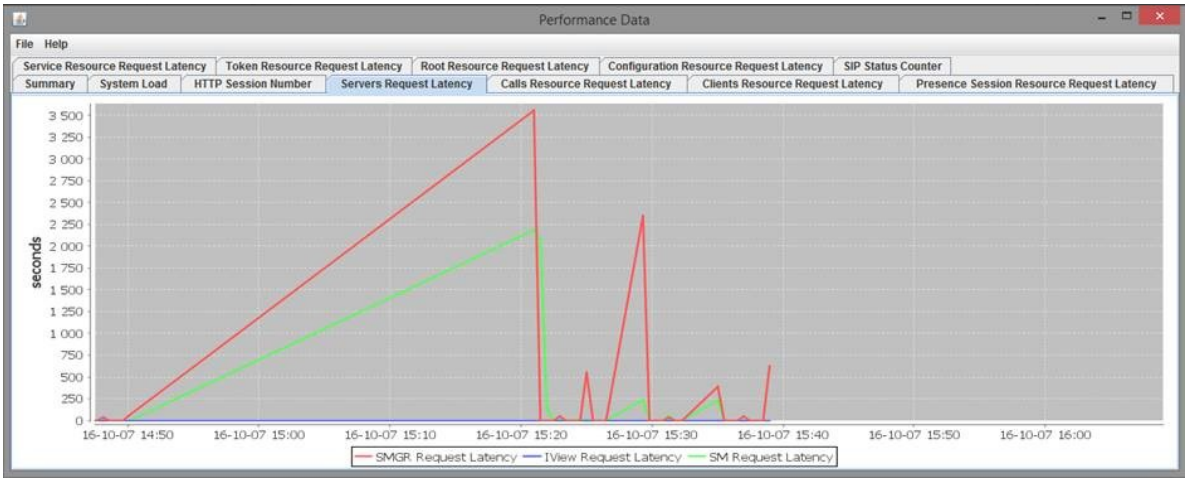
6. To investigate a metric in detail, click the required data tab.

   The following image provides an example of the server request latency over time:



7. To investigate an area of the graph in more detail, press and hold the left mouse button to select the area of interest.

The following image displays the maximized portion of a graph using the zoom in functionality:



Note:

If perfLogViewer cannot load a log because the system and log locales are different, then close the `.jar` file and run the following command in the Windows command prompt:

```
java -Duser.language.format=en -Duser.country.format=US -jar
perfLogViewer-<version_number>.jar.
```

Managing Cassandra repairs

About this task

The repair process synchronizes the data between nodes to provide consistency. Use this procedure to set up the date and time for the Cassandra repair process. You can run the repair on a weekly or monthly basis. You can also disable the repair.

The Avaya Aura® Web Gateway performs the repair on one node at a time. By default, the Avaya Aura® Web Gateway performs the repair once a week on Sunday at 01:20 a.m.

Tip:

Set the time when the system usage is low to minimize impact on system performance.

Cassandra repair results are stored in the `CAS.log` file.

Procedure

1. Log in to the seed node as an administrator by using an SSH connection.

2. Run the following commands to open the `catalina.properties` file in the vi editor:

```
cdto active
sudo vi mss/<tomcat_version>/conf/catalina.properties
```

3. To run the repair on a weekly basis, do the following:

   a. Edit the `com.avaya.cas.cassandra.repair.time.hour=<hour>` string to set the hour when the procedure starts.

      This parameter uses a 24-hour notation. For example, if you want to start the procedure at 4 p.m., enter `16`.

   b. Edit the `com.avaya.cas.cassandra.repair.time.minute=<minute>` string to set the minute when the procedure starts.

   c. Edit the `com.avaya.cas.cassandra.repair.time.weekday=<day_of_week>` string to set the required day of the week.

      The week starts from Sunday. For example, for Sunday, enter `1`, for Monday, enter `2`, and so on.

   d. In the `com.avaya.cas.cassandra.repair.time.monthday=<day_of_month>` string, set `<day_of_month>` to `0`.

   For example, to run the repair procedure on Wednesdays at 8:30 p.m., edit the entries as follows:

```
com.avaya.cas.cassandra.repair.time.hour=8
com.avaya.cas.cassandra.repair.time.minute=30
com.avaya.cas.cassandra.repair.time.weekday=4
com.avaya.cas.cassandra.repair.time.monthday=0
```

4. To run the repair on a monthly basis, do the following:

   a. Edit the `com.avaya.cas.cassandra.repair.time.hour=<hour>` string to set the hour when the procedure starts.

      This parameter uses a 24-hour notation. For example, if you want to start the procedure at 4 p.m., enter `16`.

   b. Edit the `com.avaya.cas.cassandra.repair.time.minute=<minute>` string to set the minute when the procedure starts.

   c. In the `com.avaya.cas.cassandra.repair.time.weekday=<day_of_week>` string, set `<day_of_week>` to `0`.

   d. Edit the `com.avaya.cas.cassandra.repair.time.monthday=<day_of_month>` string to set the required day of the month.

   For example, to run the repair procedure on the second day of each month at 2:40 p.m., edit the entries as follows:

```
com.avaya.cas.cassandra.repair.time.hour=14
com.avaya.cas.cassandra.repair.time.minute=40
com.avaya.cas.cassandra.repair.time.weekday=0
com.avaya.cas.cassandra.repair.time.monthday=2
```

5. To disable the repair, set both `com.avaya.cas.cassandra.repair.time.weekday` and `com.avaya.cas.cassandra.repair.time.weekday` to `0` or to any other valid non-zero value.

   For example:

   ```
   com.avaya.cas.cassandra.repair.time.weekday=0
   com.avaya.cas.cassandra.repair.time.monthday=0
   ```

6. Save the file.
7. Run the `svc telportal restart` command to restart services.
8. In a cluster environment, repeat the previous steps on all non-seed nodes in the cluster.

Enhanced Access Security Gateway support for the Avaya Aura® Web Gateway

Enabling the Enhanced Access Security Gateway after Avaya-provided OVA deployment

About this task

Use this procedure to enable Enhanced Access Security Gateway (EASG) functionality in Avaya Aura® Web Gateway. Avaya support engineers can use this functionality to access your computer and resolve product issues in real time.

The EASG is installed automatically when you deploy the Avaya Aura® Web Gateway OVA on a VMware standalone host or on vCenter.

Procedure

1. Open the SSH console as an administrator.
2. Run the following command to check the EASG status:

   ```
   EASGStatus
   ```

   By default, the EASG status is disabled.

3. Run the following command to enable EASG:

   ```
   sudo /usr/sbin/EASGManage --enableEASG
   ```

4. Run the following command to verify the product certificate:

   ```
   sudo EASGProductCert --certInfo
   ```

   Avaya Aura® Web Gateway displays the product certificate details.

   For example:

```
[admin@amm-ova-test ~]$ EASGStatus
EASG is disabled
[admin@amm-ova-test ~]$ sudo /usr/sbin/EASGManage --enableEASG

By enabling Avaya Services Logins you are granting Avaya access to
your system.  This is required to maximize the performance and value
of your Avaya support entitlements, allowing Avaya to resolve product
issues in a timely manner.

The product must be registered using the Avaya Global Registration
Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote
connectivity.  Please see the Avaya support site (https://support.avaya.com/
registration) for additional information for registering products and
establishing remote access and alarming.

Do you want to continue [yes/no]? yes

EASG Access is enabled. Performed by user ID: 'admin', on Oct 19 2016 - 12:28
[admin@amm-ova-test ~]$ EASGProductCert --certInfo
Subject:        CN=                              , OU=EASG, O=Avaya Inc.
Serial Number:  10005
Expiration:     Aug  6 04:00:00 2031 GMT
Trust Chain:
   1. O=Avaya, OU=IT, CN=AvayaITrootCA2
   2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
   3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
   4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
   5. CN=                              .0, OU=EASG, O=Avaya Inc.
[admin@amm-ova-test ~]$
```

If the certificate expires within 360, 180, 30, or 0 days, Avaya Aura® Web Gateway writes a certificate expiry notification to the `/var/log/messages` log file.

Removing EASG

About this task

Use this procedure to remove EASG permanently. You can use the Avaya-provided OVA deployment process to reinstall EASG.

Procedure

In the SSH console, run the following command to remove EASG:

```
sudo /opt/Avaya/permanentEASGRemoval.sh
```

Managing the Avaya Aura® Web Gateway server firewall

About this task

Use this procedure to reset the firewall settings back to the defaults, or to allow additional ports through the server firewall.

For detailed information about the ports that must be opened, go to http://support.avaya.com/security, scroll down, and click **Avaya Product Port Matrix Documents**. Navigate to the Avaya Aura® Web Gateway section and then click on the appropriate Port Matrix document for the release to open it.

Procedure

1. **(Optional)** Add the required ports to the firewall configuration file `/opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/os/security/firewall.conf`.
2. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
3. Select **Advanced Configuration** > **OS Security Utility** > **Run the firewall configuration script**.

   The firewall is configured automatically.

Viewing the firewall configuration

About this task

You can use the **`firewall.pl`** command to view the current Avaya Aura® Web Gateway firewall configuration.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator using an SSH connection.
2. Run the following command:

```
firewall.pl --print_ports
```

Chapter 11: Backup and restore

This section describes how to perform backups and restore the backed up configuration files. You can back up existing configuration files, certificates from System Manager, and other certificates that you might have applied. Do not save backup files in the application installation directory.

Note:

A backup file can only be used to restore data to the same software version that created it.

Backing up Avaya Aura® Web Gateway

About this task

Use this procedure to back up Avaya Aura® Web Gateway database and configuration files. This procedure applies to both standalone and cluster environments. In a cluster environment, you must back up files from all nodes in the cluster.

Before you begin

- Log in to the CLI as a non-root user with sudo privileges.

Procedure

1. To create a backup in a `.tar.zip` file, run one of the following commands:

   - `app backup -t`
   - `app backup -t -P '<PASSWORD>'`

   In the second command, `<PASSWORD>` is a password for protecting backup files. You must enclose the password with single quotation marks ('). If you do not enter a password or if the password does not comply with the password rules, Avaya Aura® Web Gateway prompts you to provide a password later. For information about supported characters, see Characters supported for Avaya Aura Web Gateway passwords on page 149.

   In a cluster environment, you can run this command on any node. It creates a backup for all nodes in the cluster.

   For example, to set the `Password1234#` password for your backups, run the following command:

   ```
   app backup -t -P 'Password1234#'
   ```

2. If you did not enter a password for backups, then enter it when prompted.

If the password does not comply with the password rules, Avaya Aura® Web Gateway prompts you to enter a new password.

3. Re-enter the password to confirm it.
4. Wait until the backup process is completed.
5. Ensure that the backup file with the name `<DateTimestamp>_<node_short-hostname>.tar.zip` is present in the administration directory, which is located at `/home/admin`.
6. To avoid losing backed up files on the server, save a copy of them.

   You can add these files back to the server before restoring Avaya Aura® Web Gateway.
7. Store the password that you used for backup files in a safe place.

   Avaya Aura® Web Gateway requires this password when you restore the backups.

Automatic backups

Avaya Aura® Web Gateway creates backups of configuration files and user data automatically on a weekly basis. Avaya Aura® Web Gateway uses the following default settings for automatic backups:

Setting	Value
Date and time	Each Sunday at 12:00 a.m.
Backup file location	`/var/log/Avaya/backup/`
Number of backups stored	Three rotating backups
Password	RAPtor@WELcomE

If required, you can update the default automatic backup settings using the Avaya Aura® Web Gateway web administration portal.

Important:

- Avaya Aura® Web Gateway recommends that you change the default password for automatic backups immediately after installing or upgrading Avaya Aura® Web Gateway.
- In cluster deployments, if any Avaya Aura® Web Gateway node is down, then the automatic backup creation process fails.

If the backup creation process fails, Avaya Aura® Web Gateway generates an alarm on System Manager.

Configuring automatic backups

About this task

Use this procedure to modify the default automatic backup settings. By default, Avaya Aura® Web Gateway starts creating automatic backups each Sunday at 12:00 a.m.

The backup process requires significant system resources. Therefore, schedule automatic backups during the least busy periods to minimize the impact on Avaya Aura® Web Gateway performance.

Important:

Avaya Aura® Web Gateway recommends that you change the default password.

Procedure

1. Log in to the Avaya Aura® Web Gateway administration portal.
2. Go to **Automatic Backup Configuration**.
3. In **Backup Time**, specify the time and date to start creating automatic backups.
4. Select the **Repeat every** check box and then specify the time interval between two consecutive automatic backup operations.
5. In **Max Backup**, specify how many backups you want to store on Avaya Aura® Web Gateway.
6. Change the password that is currently used for automatic backups as follows:
   a. Select the **Change Password** check box.
   b. In **Backup File Password**, type a password of your choice for backups.

      The password must comply with the password complexity rules. You can view the rules by pointing the cursor to the **Backup File Password** field.

   c. In **Re-Enter Password**, type the password again.
7. Click **Save**.

Changing the location of automatic backups

About this task

By default, Avaya Aura® Web Gateway stores automatic backups in the `/var/log/Avaya/backup/` directory. You can change the location of backup files by modifying the `tomcat.start.sh` file. You cannot change the location from the Avaya Aura® Web Gateway web administration portal.

Existing automatic backup files remain in the location where they were created. does not move these files to the new location.

Note:

- Avaya recommends that you use the default location for automatic backups.
- After the Avaya Aura® Web Gateway upgrade, the location of automatic backups is changed back to the default location. You must repeat this procedure if you want to store automatic backups in another directory.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator using an SSH connection.
2. Run the following command to navigate to the directory that contains the `tomcat.start.sh` file:

   `cd /opt/CallSignallingAgent/<version>/CAS/<version>/service.d/`
3. Open the `tomcat.start.sh` in a text editor of your choice with sudo privileges.

   For example: `sudo vi ./tomcat.start.sh`
4. In the `CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.autobackup.dir=<DIRECTORY_NAME>"` string, replace the existing *<DIRECTORY_NAME>* entry with the path to the directory where you want to store automatic backups.

   For example, if you want to store automatic backups in the `home/admin/automatic_backups/` directory, modify the string as follows:

   `CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.autobackup.dir=/home/admin/automatic_backups/"`
5. Save the file.
6. Run the following command to restart Tomcat:

   `svc tomcat restart`

Restoring options for standalone and cluster environments

Restoring Avaya Aura® Web Gateway in a standalone environment

Before you begin

- Ensure that you have the password that was used to create backup files.
- Log in to the CLI as a non-root user with sudo privileges.

Procedure

1. Reinstall the same version of the Avaya Aura® Web Gateway that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.
   b. Run the following command:
      ```
      app install
      ```
   c. Select **Advanced Configuration** and set **Enable Cassandra DB initialization** to `n` (no).
   d. To return to the previous menu, select **Return to Main Menu** and press `Enter`.
   e. Select **Continue** and press `Enter`.

      The basic load of the Avaya Aura® Web Gateway, without System Manager and LDAP options, is installed.
2. Change the ownership of the backup file to `<admin_user:admin_grp>` by running the following command:
   ```
   sudo chown <admin_user:admin_grp> <full_path_to_backup_tar_zip_file>
   ```
3. To restore the backed-up configuration files, run one of the following commands:
   - `app restore <full_path_to_backup_tar_zip_file>`
   - `app restore <full_path_to_backup_tar_zip_file> -P <PASSWORD>`

   In the second command, `<PASSWORD>` is the password you used to create the backup. If you do not enter a password, Avaya Aura® Web Gateway prompts you to enter it later.
4. If you did not enter the password for backups, then enter it when prompted.

   If the password is wrong, Avaya Aura® Web Gateway prompts you to re-enter the password. After three failed attempts, Avaya Aura® Web Gateway aborts the restore process. In this case, you will need to run the `app restore` command again.

   The restore utility applies the configuration in the backup file and automatically restarts the service.

Restoring a node in an Avaya Aura® Web Gateway cluster

About this task

Use this procedure if you only need to restore a specific node in a cluster, and not the entire cluster.

Before you begin

- Ensure that you have the password that was used to create backup files.
- Log in to the CLI as a non-root user with sudo privileges.

Procedure

1. Reinstall the same version of the Avaya Aura® Web Gateway that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.
   b. Run the following command:

      ```
      app install
      ```

   c. Select **Advanced Configuration** and set **Enable Cassandra DB initialization** to `n` (no).
   d. To return to the previous menu, select **Return to Main Menu** and press `Enter`.
   e. Select **Continue** and press `Enter`.

      The basic load of the Avaya Aura® Web Gateway, without System Manager and LDAP options, is installed.
2. Change the ownership of the backup file to `<admin_user:admin_grp>` by running the following command:

   ```
   sudo chown <admin_user:admin_grp> <full_path_to_backup_tar_zip_file>
   ```

3. To restore the backed-up files, run one of the following commands:
   - `app restore <full_path_to_backup_tar_zip_file>`
   - `app restore <full_path_to_backup_tar_zip_file> -P <PASSWORD>`

   In the second command, `<PASSWORD>` is the password you used to create the backup. If you do not enter a password, Avaya Aura® Web Gateway prompts you to enter it later.
4. If you did not enter the password for backups, then enter it when prompted.

   If the password is wrong, Avaya Aura® Web Gateway prompts you to re-enter the password. After three failed attempts, Avaya Aura® Web Gateway aborts the restore process. In this case, you will need to run the `app restore` command again.

   The restore utility applies the configuration in the backup file and automatically restarts the service.
5. From another node in the cluster, set up the RSA public and private keys as described in the “Configuring RSA public and private keys for SSH connections in a cluster” procedure.
6. Run the following command to restart the Avaya Aura® Web Gateway service:

   ```
   svc csa restart
   ```

7. Run the following Cassandra repair command:

   ```
   sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/cassandra/
   cassandraRepair.sh -M
   ```

Related links

[Configuring RSA public and private keys for SSH connections in a cluster](#) on page 172

Restoring an entire Avaya Aura® Web Gateway cluster

About this task

Use this procedure to restore an entire cluster. Restoring a cluster is useful if a failure occurs that results in the loss of all nodes.

To restore an Avaya Aura® Web Gateway node, you must install the Avaya Aura® Web Gateway software first and then restore the configuration and data files from a previously made backup.

Before you begin

- Ensure that you have the password that was used to create backup files.
- Log in to the CLI as a non-root user with sudo privileges.

Procedure

1. Reinstall the same version of the Avaya Aura® Web Gateway that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.
   b. Run the following command:

      ```
      app install
      ```

   c. Select **Advanced Configuration** and set **Enable Cassandra DB initialization** to `n` (no).
   d. To return to the previous menu, select **Return to Main Menu** and press `Enter`.
   e. Select **Continue** and press `Enter`.

      The basic load of the Avaya Aura® Web Gateway, without System Manager and LDAP options, is installed.
2. Change the ownership of the backup file to `<admin_user:admin_grp>` by running the following command:

   ```
   sudo chown <admin_user:admin_grp> <full_path_to_backup_tar_zip_file>
   ```

3. To restore the backed-up data, do the following on the seed node first and then on all non-seed nodes, one node at a time:
   a. Run one of the following command to restore the backed-up data:

      - `app restore <full_path_to_backup_tar_zip_file>`
      - `app restore <full_path_to_backup_tar_zip_file> -P <PASSWORD>`

      In these commands, `<full_path_to_backup_tar_zip_file>` is the absolute path to the `.tar.zip` backup file. In the second command, `<PASSWORD>` is the password you used to create the backup. If you do not enter a password, Avaya Aura® Web Gateway prompts you to enter it later.
   b. If you did not enter the password for backups, enter it when prompted.

If the password is wrong, Avaya Aura® Web Gateway prompts you to re-enter the password. After three failed attempts, Avaya Aura® Web Gateway aborts the restore process. In this case, you will need to run the `app restore` command again.

You must wait until the restore process is completed on the current node before restoring data on another node.

4. On the seed node, set up the RSA public and private keys as described in the “Configuring RSA public and private keys for SSH connections in a cluster” procedure.
5. Run the following command on the seed node first and then on other nodes to restart the Avaya Aura® Web Gateway:

```
svc csa restart
```

6. Run the following repair command from one of the nodes:

```
sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/cassandra/
cassandraRepair.sh -M
```

Related links

Configuring RSA public and private keys for SSH connections in a cluster on page 172

Configuring RSA public and private keys for SSH connections in a cluster

About this task

After nodes are added to a cluster, you must configure the RSA public and private keys to enable internode SSH communications.

Use this procedure to configure the RSA public and private keys on the initial node for the entire cluster.

Before you begin

Install all of the required nodes for the cluster.

Procedure

1. Log in to the Linux shell on the initial Avaya Aura® Web Gateway node as an administrator.
2. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
3. Navigate to **Clustering Configuration** > **Cluster Utilities** > **Configure SSH RSA Public/ Private Keys**.

   Avaya Aura® Web Gateway displays the RSA Public and Private key configuration tool.
4. When the system displays the `Add additional hosts to the list? (y/n)` prompt, enter `y` (yes) if you are generating keys for the first time or if you need to generate keys for a new node in the cluster.

   Otherwise, enter `n` (no).

5. If you chose to update the node list in the previous step, when Avaya Aura® Web Gateway prompts you, enter the IP address of the non-seed node in the cluster you want to generate keys for and then press `Enter`.
6. Repeat the previous step for all remaining non-seed nodes.
7. When Avaya Aura® Web Gateway prompts you to enter a user name for a node, enter the username for the Linux administrator account that you used to perform the Avaya Aura® Web Gateway installation.
8. If Avaya Aura® Web Gateway prompts you to replace the existing keys, enter `y` (yes).
9. When Avaya Aura® Web Gateway prompts you to enter a password, enter the password for the Linux administrator account that you used to perform the installation.
10. When the configuration is complete, press `Enter`.
11. Return to the main menu.
12. From the main menu, select **Continue** and then select **Yes** to restart services and apply the changes.

Chapter 12: Avaya Aura® Web Gateway upgrade and migration operations

The migration or upgrade path can flow through one or more prior releases, depending on the currently installed release. The following table shows the specific release upgrades along the migration or upgrade path.

The migration or upgrade path can flow through one or more prior releases, depending on the currently installed release.

Upgrade or migration path number	From	To
1	3.8.0.x	3.8.1
2	3.8.1	3.9
3	3.9	3.9.1

Depending on the release you are currently using, you might need to perform several upgrade or migration procedures. For example, to upgrade Avaya Aura® Web Gateway Release 3.8.0 to 3.9.1, follow paths 1, 2, and 3.

This document focuses on the upgrade process for Release 3.9.1. For information about upgrade procedures for previous releases, see the following documents:

- For Release 3.8.1, see Avaya Aura® Web Gateway upgrade and migration operations.

  If you use Avaya Aura® Web Gateway Release 3.8.0.x or earlier, you must upgrade to Release 3.8.1 before performing the migration to Release 3.9.

- For Release 3.9, see Avaya Aura® Web Gateway upgrade and migration operations.

  Avaya Aura® Web Gateway Release 3.9 and Release 3.8.1 use different operating system versions. Therefore, you cannot upgrade from Release 3.8.1 to 3.9. You must perform a migration as described in the specified document.

Important:

- Perform the system layer update before you upgrade Avaya Aura® Web Gateway.
- Avaya Aura® Web Gateway is FIPS 140-2 compliant. You can install Avaya Aura® Web Gateway in either FIPS or non-FIPS mode. You *cannot* enable FIPS mode when you are upgrading or migrating your Avaya Aura® Web Gateway to the latest release. If you need to enable FIPS, you must uninstall Avaya Aura® Web Gateway first, enable FIPS at the system layer, and then install the latest Avaya Aura® Web Gateway version. For

information about installing Avaya Aura® Web Gateway, see *Deploying the Avaya Aura® Web Gateway*.

Avaya Aura® Web Gateway upgrade checklist

Perform the tasks in this checklist to upgrade or migrate Avaya Aura® Web Gateway to Release 3.9.1. This checklist applies both to OVA-based and to software-only deployment types.

No.	Task	Description	✔
1	Back up Avaya Aura® Web Gateway.	See Backing up Avaya Aura Web Gateway on page 165.	
2	Update the system layer, if required.	For OVA-based deployments, see the procedures in Checklist for updating the system layer on page 176. For software-only deployments, see Updating the system layer for software-only deployments on page 179. In a cluster environment, update the system layer on all cluster nodes before upgrading the application layer.	
3	Upgrade the application layer.	For upgrade steps, see Upgrading Avaya Aura Web Gateway to a new version or release on page 180.	

System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs

Each VMware or AWS virtual machine that is created by deploying the Avaya Aura® Web Gateway OVA file has a system layer (operating system). The system later is updated with system layer updates provided by Avaya.

Important:

Do not apply updates obtained from sources other than Avaya to the system layer of Avaya Aura® Web Gateway virtual machines. Only use update artifacts provided by Avaya.

This section applies to systems deployed in VMware or AWS virtual environments using Avaya-provided OVAs. For information about updating the system layer in software-only deployments, see Updating the system layer for software-only deployments on page 179.

Checklist for updating the system layer

Use this checklist to update the system layer. This checklist apples to OVA-based deployments.

No.	Task	Notes	✔
1	Determine if the system layer update is applicable to the given virtual machine.	See Determining if a system update is applicable on page 176. Skip the remaining steps if the update is not applicable.	
2	Download, extract, and stage the update.	See Downloading, extracting, and staging a system layer update on page 177.	
3	Install the update during a maintenance window.	See Installing a staged system layer update on page 178.	

Determining if a system update is applicable

About this task

Before installing a system update for a virtual machine, query the version of the currently installed system. Use the current version to determine if the system layer requires an update. The virtual machine might be installed using an OVA that was already built with the latest system layer version.

Procedure

1. Log in to the virtual machine using the administrative user ID.
2. Query the version number of the system version by running the `sys versions` command.

   Note:

   Ignore the patch level reported by the above command.

Next steps

- If the above system version is already on the recommended system update, then no further action is required.
- If the system version is lower than the recommended system update version, then continue with the process to download and stage the update.

Downloading, extracting, and staging a system layer update

About this task

Before installing a system layer update, you must first download the update from the Avaya Support website, and then extract and stage the update on the system. The staging process places the update into a system area, which prepares the system for the installation of the update.

Tip:

Avaya recommends cleaning up the downloaded and extracted artifacts after staging. The staging operation copies the content to an internal system area. The downloaded and extracted content are no longer required.

Procedure

1. Download the update from the Avaya Support website.

   `ucapp-system-3.4.3.0.7.tgz` is an example of a system layer update artifact.

2. Transfer the update to the administrative account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.
3. Log in to the administrative account of the server using SSH.
4. To extract the update, run the following command:

   ```
   tar -zxf ucapp-system-<version>.tgz
   ```

   For example:

   ```
   tar -zxf ucapp-system-3.4.3.0.7.tgz
   ```

5. To stage the update, change to the required directory and perform the following staging command:

   ```
   cd ucapp-system-<version>
   sudo ./update.sh --stage
   ```

   For example:

   ```
   cd ucapp-system-3.4.3.0.7
   sudo ./update.sh --stage
   ```

6. **(Optional)** To free up disk space, clean up the downloaded and extracted files using the following commands:

   ```
   cd..
   rm ucapp-system-<version>.tgz
   rm -rf ucapp-system-<version>
   ```

   For example:

   ```
   rm ucapp-system-3.4.3.0.7.tgz
   rm -rf ucapp-system-3.4.3.0.7
   ```

7. To verify that the update has been staged, query the status:

   ```
   sysUpdate --status
   ```

The **sysUpdate** command is added to the system the first time a system update is staged. After staging, if the command is not recognized, you must exit the current session and establish a new session. Establishing a new session creates the **sysUpdate** command (alias) for the new session.

8. **(Optional)** If a system update is staged in error, run the following command to delete this staged update:

   ```
   sysUpdate --delete
   ```

   You cannot delete a staged update once the installation of the update has started.

9. **(Optional)** For more information about the **sysUpdate** command, run one of the following commands:

   ```
   sysUpdate --help
   sysUpdate --hhelp
   ```

   The **--help** option provides the command line syntax. The **--hhelp** option provides verbose help.

Next steps

Install the staged update during a maintenance window.

Installing a staged system layer update

About this task

After a system update is staged, you can install it. The installation runs in the background in order to minimize the possibility of interference, such as the loss of an SSH session. The background installation process follows these steps:

- A login warning message is created so users logging into the system know that a system update is in progress.
- If the application is running, it is shut down.
- The update is installed onto the system.
- The server is rebooted.
- Post-reboot cleanup actions are performed.
- The application is started.
- The login warning message is removed.

Important:

Do not perform any system maintenance actions, such as starting, stopping, or upgrading the application, while the system update is in progress.

Procedure

1. Log in to the administrative account using SSH.
2. Type `sysUpdate --install` to start the installation.

Avaya Aura® Web Gateway reboots after the installation process completes.

3. **(Optional)** Run one of the following commands to monitor the progress of the update:

```
sysUpdate --monitor
sysUpdate --monitor less
```

The **--monitor** option uses the Linux tail browser. The **-- monitor less** option uses the Linux less browser.

4. **(Optional)** Run the following command to review the status of the update:

```
sysUpdate --status
```

5. **(Optional)** Run the following command to obtain logs of the current and previous system layer update installations:

```
sysUpdate --logs
```

This command gathers log files into an archive in ZIP format and places this archive in the current working directory.

Next steps

If your organization requires stricter STIG compliance, re-enable additional STIG hardening after you finish installing the system layer update. For more information, see Enabling additional STIG hardening on page 148.

Updating the system layer for software-only deployments

About this task

The system layer is low-level software that provides the required operational environment for the Avaya Aura® Web Gateway application. You must update the system layer before upgrading your Avaya Aura® Web Gateway application.

For software-only deployments, Avaya provides a system layer installer in a package, which also contains an Avaya Aura® Web Gateway application installer.

For information about installing system layer updates for OVA-based deployments, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 175.

Before you begin

Download the latest `csa-swonly-<AAWG_VERSION>.tgz` software-only installation package from PLDS.

Procedure

1. Upload the software-only installation package on the virtual machine to the `/root` directory.

   Use a file transfer program of your choice, such as SFTP, SCP or WinSCP.

2. Log in to the virtual machine as the root user.

3. To extract the content of the installation package, run the following command:

   `tar -xzf csa-swonly-<AAWG_VERSION>.tgz`

   For example: `tar -xzf csa-swonly-3.9.1.0.x.tgz`

   The `/root/csa-swonly-AAWG_RELEASE/` directory contains the following files:

   - The system layer package in TGZ archive `ucapp-swonly-system-<VERSION>.tgz`.
   - The Avaya Aura® Web Gateway application binary `csa-<AAWG_RELEASE>.bin`.

4. Go to the directory with the extracted installation package:

   `cd csa-swonly-<AAWG_VERSION>`

5. To extract the content of the archive with the system layer installation files, run the following command:

   `tar -xzf ucapp-swonly-system-<SYSTEM_LAYER_VERSION>.tgz`

   For example: `tar - xzf ucapp-swonly-system-1.0.0.0.8.tgz`

6. Go to the directory with the extracted system layer package:

   `cd ucapp-swonly-system-<SYSTEM_LAYER_VERSION>`

7. Run the following command to install the latest system layer:

   `./swOnlyUpdate.sh --patch`

Upgrading Avaya Aura® Web Gateway to a new version or release

About this task

Use this procedure to upgrade Avaya Aura® Web Gateway within the same major version. Avaya Aura® Web Gateway is automatically stopped for the upgrade and remains out of service until you restart it after the upgrade is completed.

Important:

- When upgrading an Avaya Aura® Web Gateway cluster, you can upgrade cluster nodes in any order. After the first node is upgraded, you can upgrade other nodes at the same time.
- You can upgrade an Avaya Aura® Web Gateway cluster even if some nodes are turned off. You can upgrade these nodes later.

Before you begin

- For systems deployed in VMware or AWS virtual environments using Avaya-provided OVAs, update the system layer (operating system). For more information, see System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs on page 175.

Important:

In a cluster environment, update the system layer on all nodes before upgrading Avaya Aura® Web Gateway to a new version.

- For software-only deployments, update the system layer as described in Updating the system layer for software-only deployments on page 179.
- Download the required upgrade file from the Avaya support site. `csa-3.9.1.0.001.bin` is an example of an application layer upgrade file.
- Ensure that the Avaya Aura® Web Gateway application is installed. Otherwise, the `app upgrade` command will not work. For more information about Avaya Aura® Web Gateway installation, see *Deploying the Avaya Aura® Web Gateway*.
- Ensure that you know the enrollment password. Avaya Aura® Web Gateway does not store the enrollment password, so you must enter it during the upgrade.
- Open the Linux shell using the Linux administrator account credentials.

Procedure

1. Transfer the upgrade file to the administrator home folder on the Avaya Aura® Web Gateway server using a file transfer tool of your choice.
2. Set executable permissions on the upgrade file by using the following command:

   ```
   chmod 770 <filename>
   ```

   For example:

   ```
   chmod 770 csa-3.9.1.0.001.bin
   ```

3. Run the following command to start the upgrade:

   ```
   app upgrade <filename>
   ```

   For example:

   ```
   app upgrade csa-3.9.1.0.001.bin
   ```

4. Follow the prompts to complete the upgrade.
5. Restart services by running the `svc csa restart` command.

   If you are upgrading a cluster, you can restart an upgraded node before the upgrade is completed on other nodes.

Next steps

- If WebRTC media adaptation was enabled in the previous Avaya Aura® Web Gateway release and if you are using Avaya Meetings Server Release 9.1.9 or later, configure WebRTC media adaptation as described in Configuring WebRTC media adaptation on page 61.
- If the push notifications feature was enabled in the previous Avaya Aura® Web Gateway release and if you use the Avaya Push Notification provider, configure the Avaya Push Notification provider with the “pnp.avaya.com” provider address. For more information, see Reconfiguring the Avaya Push Notification provider after upgrade or migration on page 183.
- Optionally, configure AIDE scanning as described in Advanced Intrusion Detection Environment tool management on page 134.

Rolling back to the earlier version

About this task

If you have performed at least one upgrade on your system, then you can roll back to the earlier installed version. Avaya Aura® Web Gateway is stopped while the rollback is in progress.

Before you begin

You must verify that it is possible to roll back a cluster by ensuring that all the nodes in the cluster have the same inactive version available. Do not attempt a cluster rollback if all nodes cannot rollback to the same inactive version. Run the following command to display the inactive version on each node:

```
sudo cat /etc/ucapp.properties | grep UCAPP_CAS_INACTIVE
```

Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. To roll back to the earlier version, run the `app rollback` command.

   In a cluster, roll back each node one at a time. Roll back the seed node last.
3. After the rollback is completed, restart services by running the `svc csa restart` command.

   If the node is part of a cluster, complete the rollback on the other nodes, one at a time, before restarting any of the cluster nodes.

Removing an inactive version

About this task

If you have performed at least one upgrade or rollback on your system, then the earlier version is retained on the system. Earlier versions are retained so that you can roll back when needed. Use this procedure if you would like to remove the inactive version to free disk space.

Important:

After you remove the inactive version from your system, you cannot perform any rollbacks.

Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. To remove the inactive version from the system, run the `app removeinactive` command.

Reconfiguring the Avaya Push Notification provider after upgrade or migration

About this task

After you upgrade or migrate to Release 3.8, Avaya Aura® Web Gateway continues to use “apnp.avaya.com” as the default provider address for the Avaya Push Notification provider. Avaya recommends that you use the “pnp.avaya.com” domain instead. Since you cannot update or delete the default Avaya Push Notification provider, you can configure a new provider with the “pnp.avaya.com” provider address.

This procedure only applies if you are upgrading or migrating to Release 3.8. If you are performing a fresh installation, Avaya Aura® Web Gateway will use “pnp.avaya.com” as the default provider address for the Avaya Push Notification provider.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Provider Settings**.
2. Click **Add** to add a new provider configuration.
3. In **Enter Company Domain**, enter the domain where your Avaya Aura® Web Gateway is deployed.

   For example: `mycompany.com`
4. In **Push Notification Provider Name**, enter a name for the provider.

   For example: `AvayaProviderUpdated`.

   This name is used in the Avaya Aura® Web Gateway administration portal for display purposes only.
5. In **Push Notification Provider Address**, enter `pnp.avaya.com`.
6. In **Push Notification Provider Port**, enter the port number for the push notification provider.

   The default port is 443.
7. Click **Generate Key**.

   The Avaya Aura® Web Gateway generates a public and private key pair and an identifier. This data is required to authorize Avaya Aura® Web Gateway on the push notification provider. The Avaya Aura® Web Gateway also updates the following values:

   - **System Id**: A unique identifier for your system.
   - **Public Key**: A public key.
8. Click **Export**.

   Avaya Aura® Web Gateway displays a pop-up window with the authorization information in JSON format. You must provide this data to your Avaya Cloud account.

The following is an example of the authorization data:

```
{
    "systemId": "9bf8f4ab-99b1-452b-9b7f-e75aacf31d19.mycompany.com",
    "description": "Avaya Aura Web Gateway Services",
    "publicKey": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9rtz4fuYhGm2JlvnI6lZmate8eEX
\na4wvmklSdHGYZHos7y8xNBNCEj9wc3klayOKHYIVIeL0ryVFgM16Ud5FDQ==\n-----END PUBLIC
KEY-----",
    "alg": "ES256"
}
```

Important:

- Do *not* close the Provider Settings page on the Avaya Aura® Web Gateway administration portal until you finish exporting authorization data to your Avaya Spaces account.
- Do *not* save the data you provided on the Provider Settings page of the Avaya Aura® Web Gateway administration portal until you export authorization data to your Avaya Cloud account. Otherwise, the push notification service might not work as expected.

9. Copy the authorization data, including the surrounding curly brackets, and save it in a file on your computer.
10. In a new browser tab, log in to your Avaya Cloud account and navigate to **Manage Companies**.
11. Select the required company and navigate to the **Apps** tab.
12. From **App**, select **Avaya Mobile Push Notification Service**.
13. In Data Configuration, select the **JSON** check box.
14. Replace the content in **Public Settings** with the content of the file that you created and then save your changes.

    You must ensure that the authorization data you enter in **Public Settings** is a valid JSON string. If the data uses an invalid format, the Avaya Spaces account displays a warning message, but still allows you to save changes.

    The Avaya Spaces account stores authorization data internally. **Public Settings** only displays the authorization data that you entered last. You will not lose any previously entered authorization data if you overwrite existing content with the new authorization data.
15. Return to the Provider Settings page on the Avaya Aura® Web Gateway administration portal.
16. Click **Test** to verify that your system can connect and authenticate with the push notification provider.
17. Do one of the following:
    - If the verification completed successfully, click **Save**.

- If the verification failed, fix the issue as described in Avaya Aura Web Gateway cannot connect to a push notification provider on page 190 and then and re-run the connectivity test.

  If the problem persists, contact Avaya support personnel.

Next steps

- Update the firewall rules for the “pnp.avaya.com” domain.
- Update push notification configurations for mobile applications.

Related links

Firewall configuration on page 104
Updating mobile application settings on page 185

Updating mobile application settings

About this task

After configuring a new Avaya Push Notification provider, you must select this provider for all iOS applications that currently use the default Avaya Push Notification provider.

Before you begin

Configure a new Avaya Push Notification provider that uses “pnp.avaya.com” as the domain name. For more information, see Reconfiguring the Avaya Push Notification provider after upgrade or migration on page 183.

Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **Advanced** > **Push Notification Settings** > **Mobile Application Settings**.
2. In **Application Name**, select an application that uses the default Avaya Push Notification provider.

   The name of the Avaya Push Notification Provider is “Avaya Provider”.
3. Click **Edit**.
4. In **Push Notification Provider**, select the new Avaya Push Notification provider.

   For example: **AvayaProviderUpdated**.
5. Click **Save**.
6. To verify that the Avaya Aura® Web Gateway can send notifications to the mobile application, click **Test**.
7. Do one of the following:
   - If the verification completed successfully, click **Save**.

- If the verification failed, fix the issue as described in iOS application cannot connect to a push notification provider on page 191 and then re-run the connection test.

  If the problem persists, contact Avaya support personnel.

8. Repeat the steps above for all mobile applications that use the default Avaya Push Notification provider.

Chapter 13: Troubleshooting

Avaya Aura® Web Gateway administration portal is not accessible when the primary node is not working

Condition

In a cluster, when the primary Avaya Aura® Web Gateway node is down, you cannot access the Avaya Aura® Web Gateway administration portal.

Solution

You can use the second node to access the Avaya Aura® Web Gateway administration portal.

Cannot log in to the Avaya Aura® Web Gateway web administration portal after changing the System Manager password

Condition

You cannot access the Avaya Aura® Web Gateway web administration portal after changing the System Manager administration password or migrating System Manager.

Cause

Avaya Aura® Web Gateway sends requests to System Manager approximately once per minute. These requests contain the System Manager password. When the System Manager password changes, Avaya Aura® Web Gateway continues to use the old password in requests. After multiple consecutive failed login attempts, System Manager locks out the administrative account used for Avaya Aura® Web Gateway authentication.

Solution

1. On the System Manager web administration portal, create a separate administrative account for Avaya Aura® Web Gateway.

   If you use a separate administrative account for Avaya Aura® Web Gateway and this account gets locked, it will only affect Avaya Aura® Web Gateway and no other solution components. For information about configuring administrative accounts on System Manager, see *Administering Avaya Aura® System Manager*.

Note:

If you already use a separate administrative account for Avaya Aura® Web Gateway, skip this step and continue with step 2.

2. To unlock the administrative account, on the System Manager web administration portal, disable the password lockout functionality.

   For information about disabling the password lockout functionality, see *Administering Avaya Aura® System Manager*.
3. Log in to the Avaya Aura® Web Gateway web administration portal.
4. On the **General Network Settings** > **System Manager** page, type the current System Manager password.
5. Navigate to the **System Overview** page and wait until the status indicator for System Manager becomes green.
6. On the System Manager web administration portal, enable the password lockout functionality as appropriate.

System Manager does not show Avaya Aura® Web Gateway alarms

Condition

Alarms are generated on the Avaya Aura® Web Gateway, and user profiles are appropriately created and assigned, but System Manager does not show these alarms.

Solution

1. Log in to the Avaya Aura® Web Gateway.
2. Go to the `/var/net-snmp` directory.
3. Memorize the timestamp of the `snmpd.conf` file.
4. Log in to the System Manager web console and navigate to **Home** > **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
5. From the agents list, select the Avaya Aura® Web Gateway node for which alarms are not displayed on System Manager.
6. On the Serviceability Agents page, select Avaya Aura® Web Gateway and click **Manage Profiles**.
7. On the next page, click **Commit**.

   The timestamp of the `snmpd.conf` file should be updated.
8. If the timestamp of the `snmpd.conf` file was not updated, perform the remaining steps.

   If the timestamp was updated, then you do not need to do anything else.
9. Log in to System Manager as the root user using SSH.

10. Run the `locate recoverAgent.sh` command to obtain the full path to the `recoverAgent.sh` script.

    For example:

    ```
    >locate recoverAgent.sh
    >/opt/Avaya/Mgmt/7.1.11/remoteSnmpConfig/utility/recoverAgent.sh
    ```

11. Run the `service jboss restart` command to restart JBoss on System Manager.
12. Run the following command to remove the Avaya Aura® Web Gateway entry from System Manager:

    ```
    sh <path_to_recoverAgent.sh> <AAWG_IP_address>
    ```

    Where, `<path_to_recoverAgent.sh>` is the full path to `recoverAgent.sh` and `<AAWG_IP_address>` is the IP address of the Avaya Aura® Web Gateway.
13. Log in to the Avaya Aura® Web Gateway.
14. Run the following command:

    ```
    sudo -E $SPIRIT_HOME/scripts/utils/reinitilizeSnmpdConfiguration.sh
    ```

    Note:

    The command might fail when restarting snmpd. This is the expected behavior.

    ```
    Stopping existing snmpd service...
    Stopping snmpd (via systemctl): [ OK ]
    Restarting snmpd (via systemctl): Job for snmpd.service failed because the
    control process exited with error code. See "systemctl status snmpd.service"
    and "journalctl -xe" for details.
     [FAILED]
    Setting the reinitialized property to true
    ```

15. Run the following command:

    ```
    systemctl restart CSASpiritAgent.service
    ```

Clients cannot connect to the Avaya Aura® Web Gateway

Condition

Clients cannot connect to the Avaya Aura® Web Gateway if the Avaya Aura® Web Gateway does not use the default front-end port.

Cause

If the port number is not specified in the service URLs that are used to connect to the Avaya Aura® Web Gateway, clients continue to use the default 443 front-end port.

Solution

Include the actual Avaya Aura® Web Gateway front-end port number in all service URLs.

For example: If you are using the `aawg_server.company.com` service URL to access the Avaya Aura® Web Gateway and the Avaya Aura® Web Gateway front-end port is 1000, set the service URL to `aawg_server.company.com:1000`.

Avaya Aura® Web Gateway cannot connect to a push notification provider

Condition

When you test the connectivity to the push notification server, it fails.

Solution

1. Ensure that the enterprise firewall is configured as described in Firewall configuration on page 104.
2. Do one of the following:
   - If you are testing the connectivity to the Avaya Push Notification provider, ensure that the authorization data, which you entered in **Public Settings** on your Avaya Cloud account, is a valid JSON string with the correct Avaya Aura® Web Gateway data.
   - If you are testing the connectivity to a third-party push notification provider, ensure that you correctly entered the system ID and public key information on your push notification provider.
3. If the problem persists, contact Avaya support.

Avaya Aura® Web Gateway returns a TLS handshake error when testing the connectivity to a push notification server

Condition

When you test the connectivity to the push notification server, it fails with a TLS handshake error.

Cause

The issue might occur when your company uses an outgoing TLS inspector, such as ZScaler. The TLS inspector uses its own self-signed certificates to connect to the `pnp.avaya.com` Avaya Push Notification provider address.

Solution

1. From the Avaya Aura® Web Gateway CLI, run the following command to ensure that a TLS inspector is used:

   ```
   openssl s_client -connect pnp.avaya.com:443
   ```

   If the command output does not display an Entrust certificate in the certificate chain, it means that the certificate is provided by a third-party.

   The following example shows a command output when Avaya Aura® Web Gateway uses built-in RHEL certificates for Avaya Push Notification service:

   ```
   Certificate chain
    0 s:C = US, ST = New Jersey, L = Morristown, O = "Avaya, Inc.", CN =
   pnp.avaya.com
      i:C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c)
   2012 Entrust, Inc. - for authorized use only", CN = Entrust Certification
   ```

```
Authority - L1K
 1 s:C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c)
2012 Entrust, Inc. - for authorized use only", CN = Entrust Certification
Authority - L1K
   i:C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c)
2009 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification
Authority - G2
 2 s:C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c)
2009 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification
Authority - G2
   i:C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c)
2009 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification
Authority - G2
```

`apnp.avaya.com` uses a different CA certificate, so if that FQDN is used, you should see the AvayaITserverCA2 certificate in the chain. For example:

```
openssl s_client -connect apnp.avaya.com:443
CONNECTED(00000005)
depth=2 O = Avaya, OU = IT, CN = AvayaITrootCA2
verify return:1
depth=1 DC = com, DC = avaya, DC = global, CN = AvayaITserverCA2
verify return:1
depth=0 C = US, ST = NJ, O = Avaya, CN = apnp.avaya.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = NJ, O = Avaya, CN = apnp.avaya.com
   i:DC = com, DC = avaya, DC = global, CN = AvayaITserverCA2
 1 s:DC = com, DC = avaya, DC = global, CN = AvayaITserverCA2
   i:O = Avaya, OU = IT, CN = AvayaITrootCA2
 2 s:O = Avaya, OU = IT, CN = AvayaITrootCA2
   i:O = Avaya, OU = IT, CN = AvayaITrootCA2
```

2. If a third-party certificate is used, import the TLS inspector CA certificates into the Avaya Aura® Web Gateway truststore.

   For more information, see Managing truststore certificates on page 84.

iOS application cannot connect to a push notification provider

Condition

When you test the connectivity, the result indicates that the Avaya Aura® Web Gateway cannot send push notifications to the iOS application.

Cause

- Your system cannot connect with the push notification provider.
- Your mobile application is incorrectly configured on the push notification provider.

Solution

1. On the Provider Settings page of the Avaya Aura® Web Gateway administration portal, click **Test** to verify that your system can connect and authenticate with the push notification provider.

2. After successfully completing the previous step, if the problem persists, do the following:
   - For Avaya applications, such as Avaya Workplace Client for iOS, contact Avaya support.
   - For third-party iOS applications, verify that the application is correctly configured on the third-party provider.

Avaya Aura® Web Gateway displays a warning about SSH configuration during the upgrade process

Condition

After checking the configuration during an upgrade, Avaya Aura® Web Gateway displays a warning that the SSH protocol version is not defined in the `sshd_config` file. For example:

```
Checking SSH Configuration ..........................  [WARNING]
Avaya Aura Web Gateway Services uses EASG for Avaya Services access,
and requires certain sshd_config parameters.
Expected values are:
    Protocol 2
    PermitRootLogin no
    ChallengeResponseAuthentication yes
Actual values are:
    -not defined-
    PermitRootLogin no
    ChallengeResponseAuthentication yes
```

Solution

Ignore the warning.

Avaya Aura® Web Gateway does not display the default Avaya Push Notification provider or mobile application configuration

Condition

The Avaya Aura® Web Gateway administration portal does not display any of the following default configurations:

- Avaya Push Notification provider configuration. The configuration name is “Avaya Provider”.
- Mobile application configuration. The configuration name is “Avaya Workplace”.

You also cannot add your own push notification provider or mobile application configurations.

Solution

1. Log in to the Avaya Aura® Web Gateway as an administrator.

2. Run the `svc cassandra status` command and ensure that the Cassandra status is “Running”.
3. If the Cassandra status is not “Running”, run the `svc csa start` command.
4. Repeat the steps above for all remaining nodes in the cluster.
5. From any node in the cluster, run the following command:

```
sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/cassandra/
cassandraRepair.sh -M
```

The location of automatic backups has changed after the upgrade

Condition

After the upgrade, Avaya Aura® Web Gateway uses the default location for automatic backup files instead of the location that you defined.

Cause

This is the expected behavior.

Solution

Configure the required location for automatic backups as described in Changing the location of automatic backups on page 167.

RHEL single-user mode

Single-user mode is a maintenance mode available on Linux-based operating systems. In single-user mode, the operating system only starts certain services for troubleshooting and maintenance operations. In the single-user mode, you can perform operating system-level troubleshooting operations, such as repairing the file system or starting or stopping services. For more information about the use of the single-user mode, refer to the official RHEL documentation.

In single-user mode, network services are not available. Therefore, you cannot use Avaya Aura® Web Gateway functionality on a node that operates in single-user mode.

Avaya Aura® Web Gateway supports single-user mode only in a VMware-based environment for both OVA-based and software-only deployment types. You cannot enable single-user mode on AWS because you cannot change the boot sequence of the operating system in Cloud environments.

Booting the RHEL into single-user mode

About this task

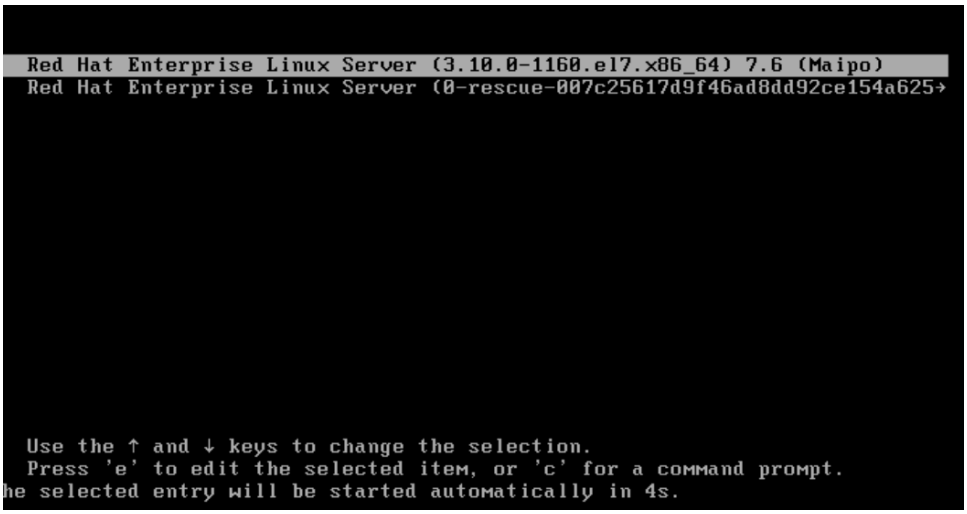
You can use single-user mode of the RHEL operating system to perform operating system-level troubleshooting and maintenance tasks. The Avaya Aura® Web Gateway functionality is unavailable in single-user mode.

You can only enable single-user mode in VMware-based environments.

In VMware OVA-based deployments, single-user mode is password-protected. The default password is the administrator password that you configure when installing Avaya Aura® Web Gateway. When you enable single-user mode for the first time, you must change the default password.

Procedure

1. From vCenter, select your Avaya Aura® Web Gateway virtual machine.
2. On the Summary tab, click **Launch Web Console**.
3. Reboot your virtual machine.
4. When vCenter displays the GRUB boot menu, select the appropriate kernel version and then press `e`.



5. When prompted to enter the user name, enter `root`.
6. When prompted to enter the password, do one of the following:
   - If you boot into single-user mode for the first time, type the administration password that you configured when installing Avaya Aura® Web Gateway, and then configure a password for single-user mode.

     Avaya Aura® Web Gateway does not enforce complexity rules for single-user mode passwords.

- If you have already used single-user mode, type the password that you configured for single-user mode.

7. When Avaya Aura® Web Gateway displays the Setparams window, navigate to the line that starts with `linux16` using the navigational keys.
8. At the end of the line, type the Space character (" ") and then type the following entry:

   ```
   rd.break console=tty1
   ```

9. Press `Ctrl`+`X`.

   After the reboot, RHEL boots into the single-user mode.

Changing the password for single-user mode

About this task

You can change the password for single-user mode from the Avaya Aura® Web Gateway CLI. You do not need to log in to single-user mode to change the single-user mode password.

Avaya Aura® Web Gateway does not enforce any complexity rules for single-user mode passwords, therefore you can use any password that you want.

Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as an administrator using an SSH connection.
2. Run the following command:

   ```
   sudo /opt/Avaya/bin/manageOSPassword.sh -p
   ```

3. Follow the system prompts to change the single-user mode password.

Exiting the single-user mode

About this task

After performing maintenance tasks in single-user mode, switch back to normal Avaya Aura® Web Gateway operational mode.

Procedure

When in the single-user mode, run the following command:

```
reboot -f
```

After the reboot, Avaya Aura® Web Gateway starts in normal mode.

Chapter 14: Resources

Documentation

The following table lists related documentation. All Avaya documentation is available at https://support.avaya.com. Many documents are also available at https://documentation.avaya.com/.

Title	Use this document to:	Audience
Overview and planning		
Avaya Aura® Core Solution Description	Understand the strategic, enterprise, and functional views of the Avaya Aura® architecture.	• Customers • Sales, services, and support personnel
Avaya Aura® Communication Manager Feature Description and Implementation	Understand the features of Avaya Aura® Communication Manager.	
What's New in Avaya Aura® Release 8.1.x	Understand the new and enhanced features of Avaya Aura® components.	• Contractors • Employees • Channel associates • Sales, services, and support personnel • Avaya Business Partners
Using		
Avaya Scopia® Desktop Client User Guide	Use the Avaya Scopia® desktop client. This document also provides usage information for the user portal.	End users
Deploying		
Deploying the Avaya Aura® Web Gateway	Install, configure, and administer the Avaya Aura® Web Gateway.	Implementation personnel
Deploying Avaya Aura® Device Services	Install, administer, configure, and maintain Avaya Aura® Device Services.	
Deploying Avaya Multimedia Messaging	Install, configure, and administer Avaya Multimedia Messaging.	

Table continues…

Title	Use this document to:	Audience
Deploying Avaya Meetings Server	Install, configure, and maintain the Avaya Meetings Server.	
Administering		
Administering Avaya Aura® Device Services	Use management tools, manage data and security, and perform periodic maintenance tasks in Avaya Aura® Device Services.	• System administrators • Implementation personnel • Services and support personnel
Administering Avaya Aura® Communication Manager	Administer Avaya Aura® Communication Manager on the following servers: • Avaya media gateways • Avaya S8XXX Servers	
Administering Network Connectivity on Avaya Aura® Communication Manager	Understand the network components of Avaya Aura® Communication Manager.	

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a 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 collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

Avaya Workplace Client solution courses and credentials, such as ACCS-7240, also include information about Avaya Aura® Web Gateway. You can access training courses at http://www.avaya-learning.com.

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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **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 key word or key words 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 the topic. 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 http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Glossary

Avaya Aura® Media Server	Avaya Aura® Media Server (Avaya Aura® MS) is a software-based media platform. Communication Manager uses Avaya Aura® MS to provide IP audio, tone generation and detection, and announcement capabilities similar to legacy H.248 media gateways or port networks with media processors.
Avaya Aura® Web Gateway	The Avaya Aura® Web Gateway server acts as a gateway to Avaya Aura® clients and applications utilizing WebRTC signaling and media. Avaya Aura® Web Gateway also provides the push notification service, enabling clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs).
Avaya Meetings Management	Avaya Meetings Management sits at the core of your Avaya Meetings Server deployment. System administrators use Avaya Meetings Management to control video network devices, such as gateways, media servers, and endpoints. Avaya Meetings Server is positioned for organizations which need robust collaboration capabilities, including industry leading HD video, plus audio and web conferencing. The Avaya Meetings Management is specially tailored to fit this Unified Communications (UC) offering, along with other video infrastructure devices of the Avaya Meetings Server.
Avaya Meetings Server	Avaya Meetings Server is an audio, video and web conferencing offer converging on a single platform the best of Avaya capabilities for scalable audio conferencing and rich web collaboration with the best of Avaya capabilities for video processing and transcoding, standards-based video room system integration, and the broad range of remote access capabilities for desktop and mobile devices.
Cassandra	Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see https://cassandra.apache.org/.
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.
Fully Qualified Domain Name (FQDN)	A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).

Network Time Protocol (NTP)	A protocol used to synchronize the real-time clock in a computer.
Secure Shell (SSH)	Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.
Simple Network Management Protocol (SNMP)	A protocol for managing devices on IP networks.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security
UDP	User Datagram Protocol. This is a communication method, similar to TCP.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W