



# Deploying the Avaya Aura<sup>®</sup> Web Gateway

Release 10.2.x  
Issue 3  
January 2026

# Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

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

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

## Notice

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

## Documentation disclaimer

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

## Link disclaimer

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

## Warranty

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

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

## Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

## Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

## Copyright

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

## Virtualization

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

## Third Party Components

### Third Party Components

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

## Service Provider

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

## **Compliance with Laws**

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

## **Preventing Toll Fraud**

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

## **Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

## **Security Vulnerabilities**

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

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

## **Downloading Documentation**

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

## **Contact Avaya Support**

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

## **Trademarks**

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

Avaya is a registered trademark of Avaya LLC.

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

## Contents

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| <b>Chapter 1: Introduction</b>                                                                   | 9  |
| Purpose                                                                                          | 9  |
| Change history                                                                                   | 9  |
| <b>Chapter 2: Avaya Aura® Web Gateway overview</b>                                               | 10 |
| New in this release                                                                              | 10 |
| Solution architecture                                                                            | 11 |
| Topology diagram                                                                                 | 11 |
| Geographical distribution overview                                                               | 13 |
| General geographical distribution topology                                                       | 13 |
| Signaling and media path topology when clients are located in or near different data centers     | 14 |
| Signalling and media path topology when both clients are located in or near the same data center | 16 |
| Push notifications                                                                               | 17 |
| Data encryption                                                                                  | 18 |
| Interoperability                                                                                 | 19 |
| Product compatibility                                                                            | 19 |
| Web browser requirements                                                                         | 19 |
| <b>Chapter 3: Deployment process</b>                                                             | 21 |
| Configuration worksheet                                                                          | 21 |
| <b>Chapter 4: Planning and preinstallation</b>                                                   | 24 |
| Planning checklist                                                                               | 24 |
| Required skills and knowledge                                                                    | 26 |
| Required FQDNs and certificates                                                                  | 27 |
| Virtual machine requirements                                                                     | 28 |
| Software requirements                                                                            | 28 |
| Resource profile specifications                                                                  | 29 |
| Supported ESXi version                                                                           | 31 |
| Virtual disk volume specifications                                                               | 32 |
| External load balancer requirements                                                              | 33 |
| Linux alias commands                                                                             | 35 |
| System layer commands                                                                            | 37 |
| sys secconfig command                                                                            | 38 |
| sys versions command                                                                             | 38 |
| sys volmgt command                                                                               | 39 |
| sys smcvemgt command                                                                             | 42 |
| passwdrules command                                                                              | 46 |
| Data encryption commands                                                                         | 47 |
| Characters supported for Avaya Aura® Web Gateway passwords                                       | 49 |

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| <b>Chapter 5: Initial setup</b>                                          | 50  |
| OVA-based deployments                                                    | 50  |
| Deployment process checklist                                             | 51  |
| Obtaining the Avaya Aura® Web Gateway OVA file                           | 52  |
| Virtual machine deployment options                                       | 54  |
| Enabling the Enhanced Access Security Gateway from the CLI               | 62  |
| Configuring UEFI Secure Boot for OVA-based virtual machines              | 63  |
| Enabling FIPS mode                                                       | 64  |
| Enabling additional STIG hardening                                       | 65  |
| Software-only deployment in VMware-based virtualization environment      | 66  |
| Software-only installation checklist for VMware-based environment        | 67  |
| Red Hat Enterprise Linux installation                                    | 69  |
| Creating disk partitioning for software-only deployments                 | 70  |
| Creating an administrative user                                          | 72  |
| Additional packages required by Avaya Aura® Web Gateway                  | 73  |
| Enabling the Havedged service                                            | 74  |
| Enabling FIPS for software-only systems                                  | 74  |
| RHEL packages management                                                 | 76  |
| Installing the system layer                                              | 77  |
| Checking the Chrony service status                                       | 79  |
| Checking the connection to System Manager                                | 80  |
| Software-only deployment on Amazon Web Services                          | 80  |
| Software-only installation checklist for Amazon Web Services             | 80  |
| Prerequisites for software-only deployment on AWS                        | 83  |
| Creating a key pair                                                      | 83  |
| Creating and applying load balancer certificates                         | 84  |
| Creating security groups                                                 | 86  |
| Installing Red Hat Enterprise Linux 8.10 on AWS                          | 88  |
| Enabling root access                                                     | 90  |
| Prerequisites for installing the system layer on AWS                     | 90  |
| Creating target groups                                                   | 91  |
| Creating and configuring Elastic load balancers                          | 92  |
| Configuring idle timeout                                                 | 95  |
| Uninstalling the Avaya Aura® Web Gateway                                 | 95  |
| Removing a non-initial node from the cluster if the node is unavailable  | 95  |
| <b>Chapter 6: Avaya Aura® Web Gateway setup</b>                          | 98  |
| Avaya Aura® Web Gateway installation checklist                           | 98  |
| Installing the Avaya Aura® Web Gateway                                   | 98  |
| Performing a silent installation                                         | 102 |
| Seed node replacement configuration                                      | 103 |
| Installing additional nodes to create a cluster                          | 104 |
| Configuring RSA public and private keys for SSH connections in a cluster | 107 |
| Avaya Aura® Web Gateway initial configuration settings                   | 108 |

|                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------|-----|
| Front-end host, System Manager, and certificate configuration.....                                                          | 109 |
| LDAP configuration.....                                                                                                     | 112 |
| Cluster configuration.....                                                                                                  | 127 |
| Virtual IP configuration options.....                                                                                       | 128 |
| Advanced configuration.....                                                                                                 | 129 |
| Changing the Cassandra user name and password.....                                                                          | 130 |
| Changing the default password for automatic backups.....                                                                    | 131 |
| Starting services using a command line.....                                                                                 | 131 |
| Configuring OAMP to use Linux account credentials on the Avaya Aura® Web Gateway administration portal.....                 | 132 |
| Uninstalling the Avaya Aura® Web Gateway.....                                                                               | 132 |
| Removing a non-initial node from the cluster if the node is unavailable.....                                                | 133 |
| <b>Chapter 7: Deploying AAWG on ASP 130 R6.0.x (KVM on RHEL 8.10)</b> .....                                                 | 135 |
| UPDATE December, 2025.....                                                                                                  | 135 |
| <b>Chapter 8: Global FQDN configuration</b> .....                                                                           | 136 |
| DNS configuration.....                                                                                                      | 136 |
| Configuring the front-end FQDN.....                                                                                         | 136 |
| Avaya Meetings Server configuration for single FQDN deployments.....                                                        | 137 |
| Configuring Avaya Workplace Client conference control.....                                                                  | 137 |
| Configuring Web Collaboration.....                                                                                          | 137 |
| <b>Chapter 9: System Manager, Avaya Aura® Device Services, Media Server, and Avaya Meetings Server configurations</b> ..... | 139 |
| Adding the Avaya Aura® Web Gateway to System Manager.....                                                                   | 139 |
| Configuring SIP Trunks for the Avaya Aura® Web Gateway on System Manager.....                                               | 140 |
| Serviceability agents.....                                                                                                  | 141 |
| Configuring a registration expiration timer.....                                                                            | 143 |
| Configuring Avaya Aura® Media Server in System Manager.....                                                                 | 143 |
| Configuring Avaya Aura® Media Server settings.....                                                                          | 144 |
| Configuring the Avaya Aura® Web Gateway on Avaya Aura® Device Services.....                                                 | 146 |
| Uploading clients to the web deployment service.....                                                                        | 146 |
| Configuring the Avaya Aura® Web Gateway on Avaya Meetings Server.....                                                       | 147 |
| Route configuration for an external load balancer .....                                                                     | 148 |
| <b>Chapter 10: Avaya Session Border Controller configuration</b> .....                                                      | 150 |
| Avaya Session Border Controller configuration checklist.....                                                                | 150 |
| Reverse proxy configuration.....                                                                                            | 151 |
| Reverse proxy configuration checklist for a single FQDN deployment.....                                                     | 151 |
| Reverse proxy configuration checklist for a multiple FQDN deployment.....                                                   | 152 |
| Prerequisites.....                                                                                                          | 152 |
| Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment..                                 | 153 |
| Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment                                  | 154 |
| Certificate Authority configuration checklist.....                                                                          | 155 |
| Enabling web socket support.....                                                                                            | 156 |
| Configuring external traffic rules in a single FQDN for all services deployment.....                                        | 156 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Configuring internal traffic rules in a single FQDN for all services deployment.....             | 158 |
| Configuring external traffic rules in a multiple FQDN deployment.....                            | 160 |
| External client access configuration.....                                                        | 162 |
| External client access configuration checklist.....                                              | 162 |
| Checklist for creation of a TLS server profile for a management interface.....                   | 162 |
| Configuring Avaya SBC load monitoring.....                                                       | 163 |
| Adding Avaya Session Border Controller to the Avaya Aura® Web Gateway.....                       | 164 |
| Adding Avaya Session Border Controller to Avaya Meetings Server Management.....                  | 165 |
| WebRTC client side TURN configuration.....                                                       | 166 |
| External native clients media configuration.....                                                 | 171 |
| Certificate setup.....                                                                           | 178 |
| Creating a certificate signing request on Avaya Session Border Controller.....                   | 178 |
| Signing certificates with the System Manager CA.....                                             | 179 |
| Installing a certificate and a key .....                                                         | 180 |
| Installing the Avaya Meetings Management CA certificate to Avaya SBC.....                        | 182 |
| Installing a CA certificate on Avaya SBC.....                                                    | 182 |
| TLS client and server profiles setup.....                                                        | 183 |
| Creating a TLS server profile.....                                                               | 183 |
| Creating a TLS client profile.....                                                               | 183 |
| Configuring Avaya SBC network interfaces.....                                                    | 184 |
| <b>Chapter 11: Troubleshooting</b> .....                                                         | 185 |
| Unexpected characters in the /etc/hosts file on a localhost line.....                            | 185 |
| A node removed from the Cassandra cluster has the “live” status in the app listnodes output....  | 186 |
| <b>Chapter 12: Resources</b> .....                                                               | 187 |
| Documentation.....                                                                               | 187 |
| Finding documents on the Avaya Support website.....                                              | 188 |
| Avaya Documentation Center navigation.....                                                       | 189 |
| Training.....                                                                                    | 190 |
| Viewing Avaya Mentor videos.....                                                                 | 190 |
| Support.....                                                                                     | 191 |
| Using the Avaya InSite Knowledge Base.....                                                       | 191 |
| <b>Appendix A: Certificate configuration using the configuration utility</b> .....               | 192 |
| Generating Certificate Signing Requests.....                                                     | 192 |
| Getting certificates signed by the third-party CA.....                                           | 193 |
| Applying third-party signed certificates to the Avaya Aura® Web Gateway.....                     | 194 |
| Adding third-party root CA certificates to the Avaya Aura® Web Gateway.....                      | 195 |
| Creating a Certificate Signing Request (CSR) using OpenSSL.....                                  | 196 |
| Signing identity certificates for Avaya Aura® Web Gateway using third-party CA certificates..... | 197 |
| Generating an identity certificate chain.....                                                    | 198 |
| Configuring System Manager to trust third-party root CA certificates.....                        | 199 |
| Creating a client certificate.....                                                               | 200 |
| Importing client certificates into web browsers.....                                             | 201 |
| <b>Appendix B: Best Practices for VMware performance and features</b> .....                      | 203 |

|                                                                  |            |
|------------------------------------------------------------------|------------|
| Timekeeping.....                                                 | 203        |
| VMware Tools.....                                                | 204        |
| VMware networking best practices.....                            | 205        |
| Storage.....                                                     | 208        |
| Best Practices for VMware features.....                          | 208        |
| VMware High Availability.....                                    | 208        |
| VMware vMotion.....                                              | 209        |
| VMware snapshots.....                                            | 209        |
| <b>Appendix C: Creating RHEL virtual machine on Nutanix.....</b> | <b>212</b> |
| Uploading the RHEL ISO to Nutanix server.....                    | 212        |
| Installing RHEL on the Nutanix server.....                       | 213        |
| <b>Glossary.....</b>                                             | <b>216</b> |

# Chapter 1: Introduction

---

## Purpose

This document provides checklists and procedures for planning, installation, and configuration of the Avaya Aura® Web Gateway. It is intended for customer installers and administrators.

 **Note:**

This document does not describe SDK developer applications.

After you deploy Avaya Aura® Web Gateway, see *Administering the Avaya Aura® Web Gateway* for administration and maintenance information. You can also find information about managing Integrated Windows Authentication (IWA) and push notification services in *Administering the Avaya Aura® Web Gateway*.

---

## Change history

This section describes the major changes made in this document:

| Issue | Date          | Summary of changes                                                                                                                                                                                                                                                                                                                 |
|-------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3     | January 2026  | Added the following section: <ul style="list-style-type: none"><li>• <a href="#">UPDATE December, 2025</a> on page 135</li></ul> Removed the following sections: <ul style="list-style-type: none"><li>• Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)</li><li>• Supported ASP R6.0.x (KVM on RHEL 8.10) versions</li></ul> |
| 2     | January 2025  | Added the following sections: <ul style="list-style-type: none"><li>• Appendix C: Creating RHEL virtual machine on Nutanix</li><li>• <a href="#">Installing RHEL on the Nutanix server</a> on page 213</li><li>• <a href="#">Uploading the RHEL ISO to Nutanix server</a> on page 212</li></ul>                                    |
| 1     | December 2024 | Release 10.2 Initial document.                                                                                                                                                                                                                                                                                                     |

# 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 10.2:

### **Support for Software-Only Deployment on Nutanix Environment**

With Release 10.2, Avaya Aura® Web Gateway Software-Only application can be deployed on Nutanix 6.5 and later.

### **Red Hat Enterprise Linux (RHEL) 8.10 support**

With Release 10.2, Avaya Aura® Web Gateway supports Red Hat Enterprise Linux Release 8.10.

### **Kernel-based Virtual Machine (KVM) on RHEL 8.10 hypervisor support**

With Release 10.2, Avaya Aura® Web Gateway can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

## Solution architecture

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

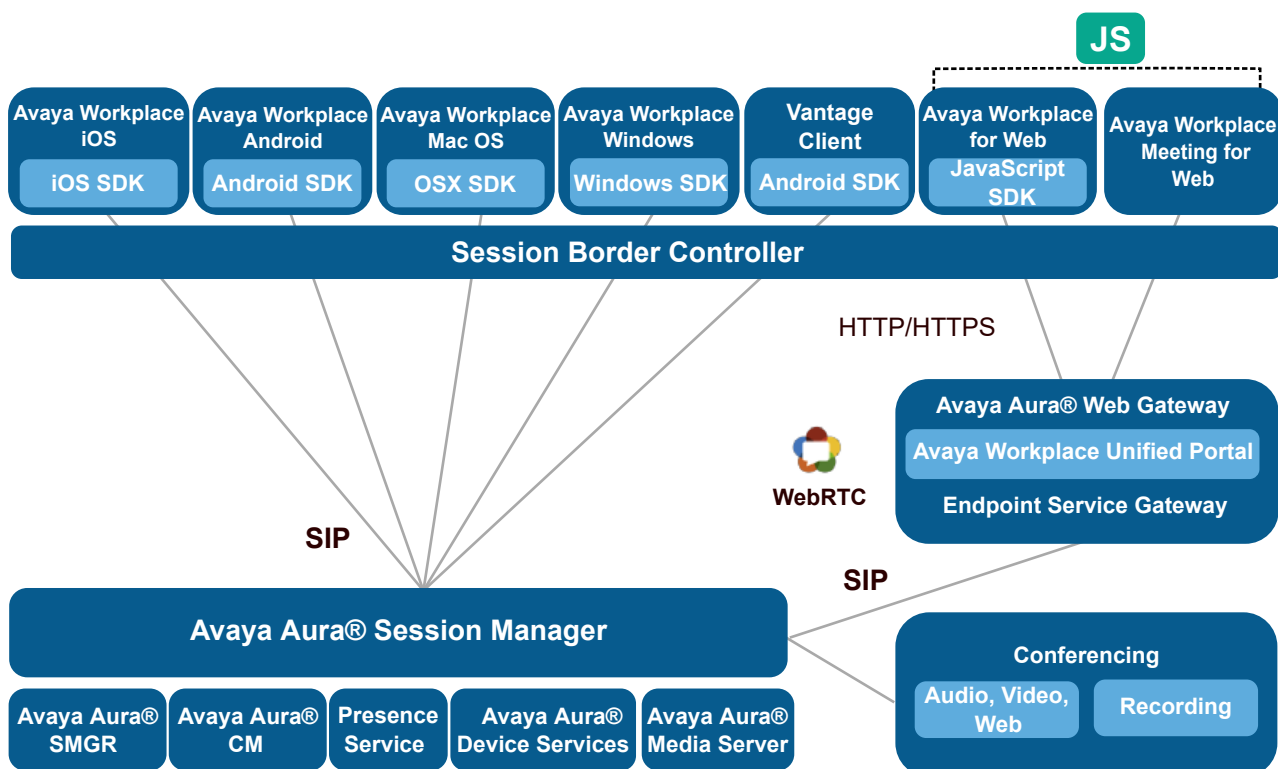
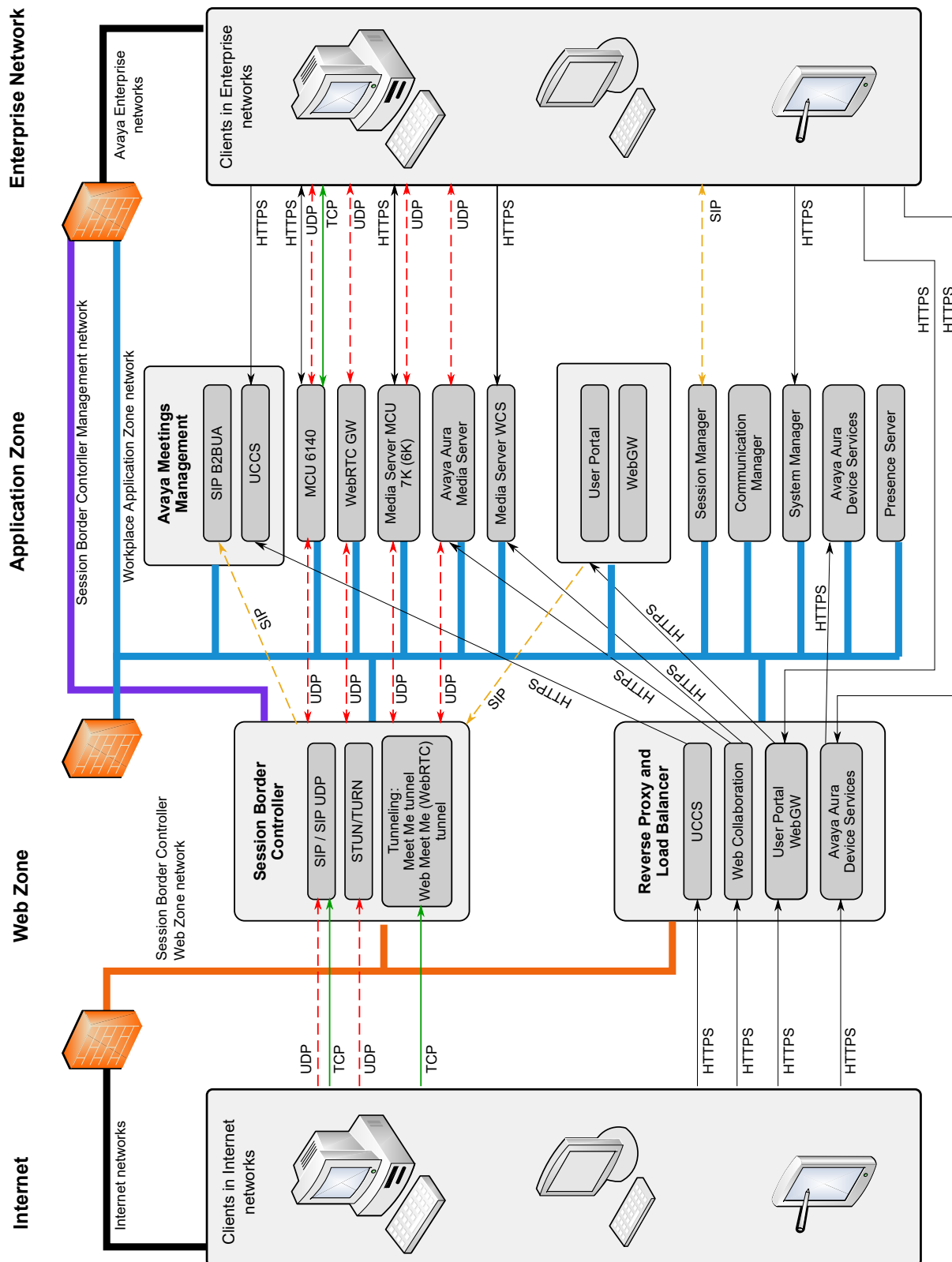


Figure 1: Avaya Workplace Client and Conferencing deployment topology

## Topology diagram

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



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:

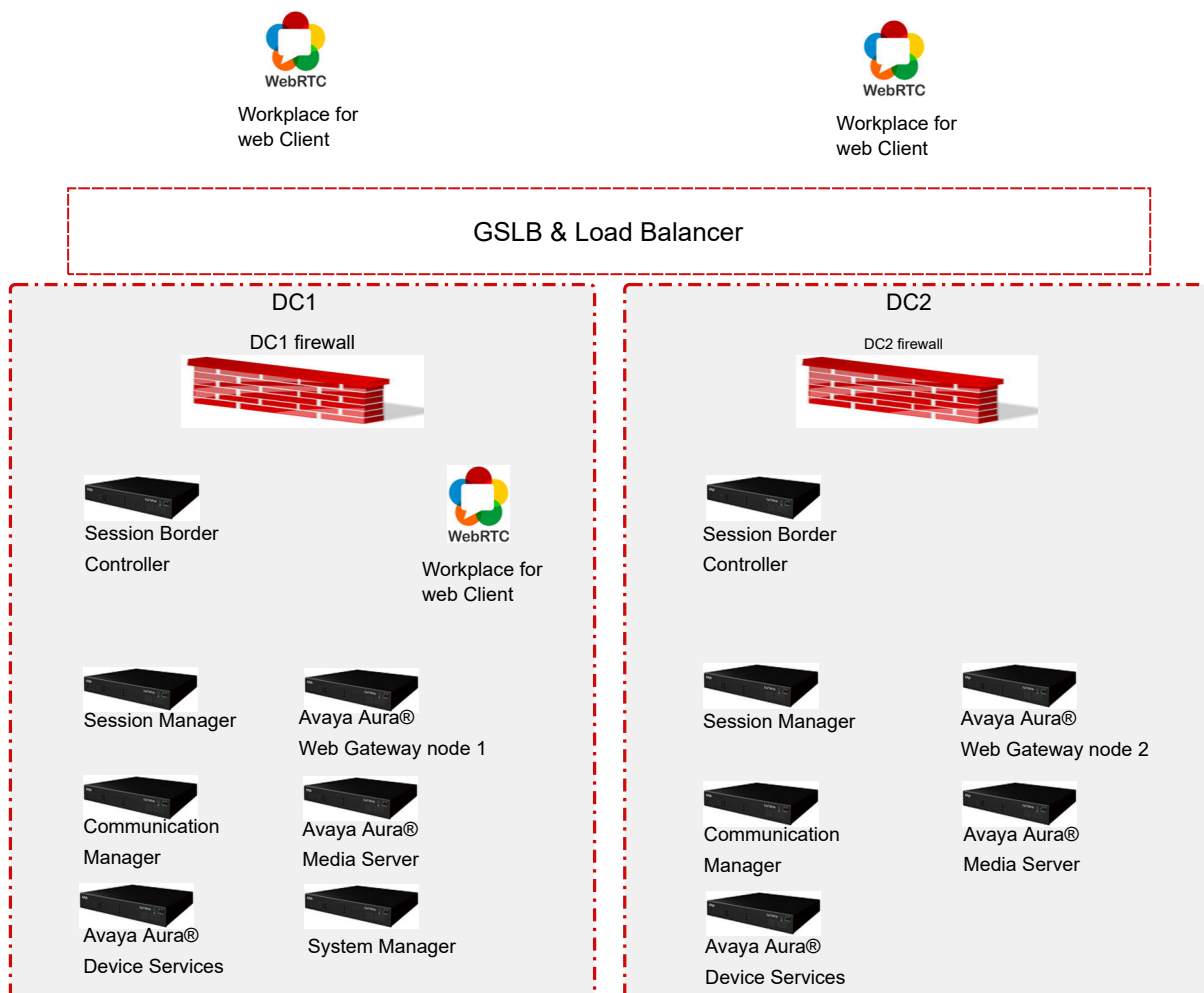
- Global Server Load Balancing (GSLB), which provides different routes and addresses based on the location of the client.
- Load balancer, which balances traffic between two or more Avaya Aura® Web Gateway nodes, which may be located in the same data center or in different data centers.

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*.

For more information about configuring a geographically distributed system, see the list of tasks for multiple data centers in [Configuration worksheet](#) on page 21.

## 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.



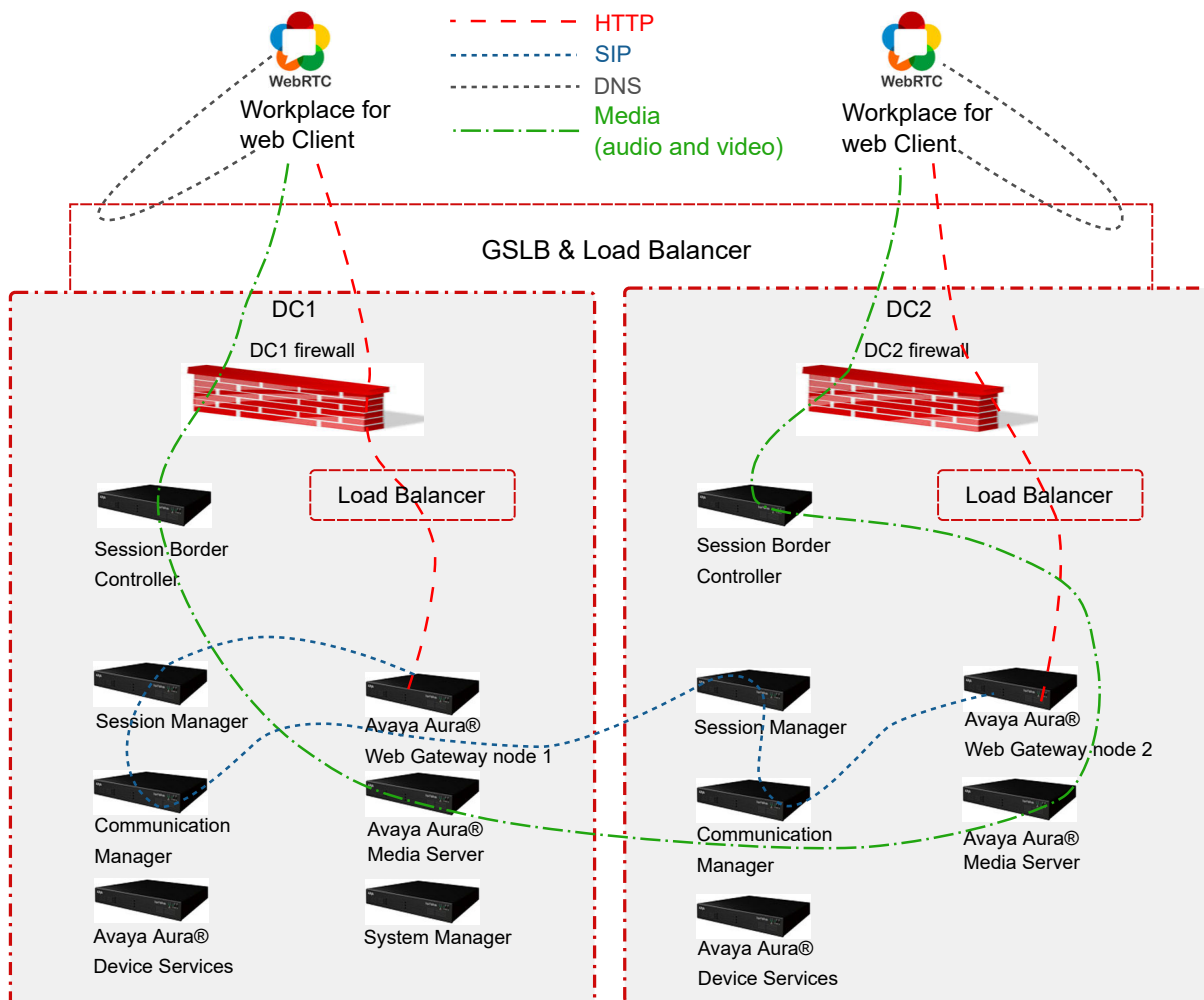
## Signaling and media path topology when clients are located in or near different data centers

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.



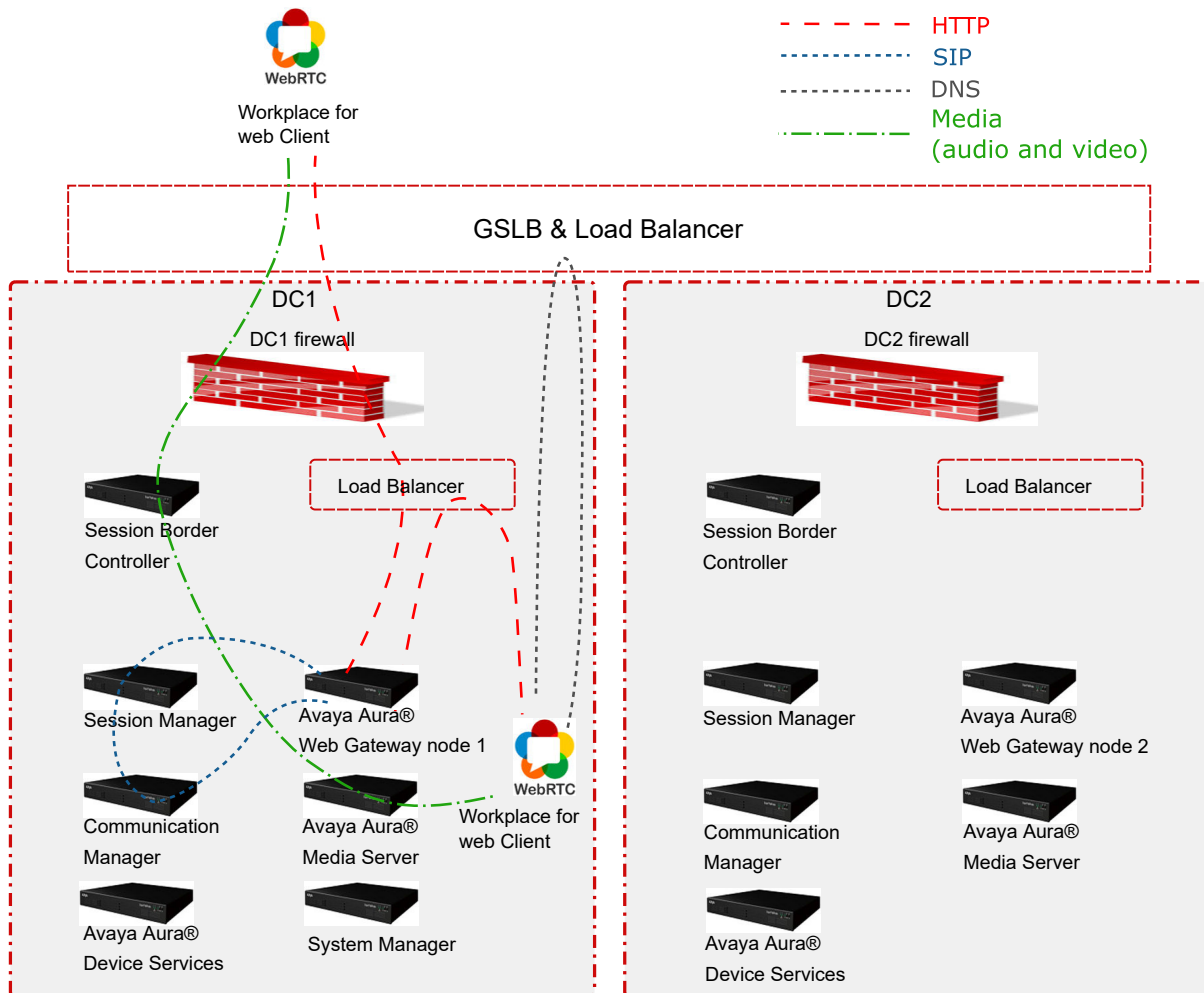
## Signalling and media path topology when both clients are located in or near the same data center

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.



## 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.

For more information about configuring and using the push notifications service, see “Avaya push notification management” in *Administering the Avaya Aura® Web Gateway*.

---

## Data encryption

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 you use Avaya Solutions Platform or a VMware Virtualized Environment. For software-only deployments, you must enable data encryption on the virtualization platform itself. For more information about enabling data encryption on Amazon Web Services, 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 server to store encryption keys.

### 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.

### Data encryption management

After deploying the Avaya Aura® Web Gateway OVA with data encryption enabled, you can manage data encryption settings using system layer commands. For information about managing data encryption settings, see the “Security options” chapter in *Administering the Avaya Aura® Web Gateway*.

# 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 | <p>The following Avaya Aura® components must be installed and configured to use TLS:</p> <ul style="list-style-type: none"> <li>Avaya Aura® Device Services: Provides centralized contact management services using REST-based APIs.</li> <li>Avaya Aura® Media Server: Supports standard media processing features.</li> </ul> <p><b>! Important:</b></p> <p>Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC.</p> <ul style="list-style-type: none"> <li>System Manager: Manages Avaya Aura® components, certificates, licenses, and checks log and alarm capabilities.</li> <li>Session Manager: Enables applications to perform registration and telephony functions, such as call escalation.</li> </ul> |
| Conferencing               | <p>This describes the deployment for Avaya Aura® Web Gateway, but not Conferencing itself.</p> <p>The Avaya Meetings Server solution provides conferencing and collaboration functionality.</p> <p>Avaya Meetings Server is not available with the Avaya Aura® Web Gateway Avaya Workplace Client only deployment option.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Avaya SBC                  | <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 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](https://aws.amazon.com/console/faqs/#browser_support).

# Chapter 3: Deployment process

The following table shows the high-level tasks for deploying the Avaya Aura® Web Gateway

| High-level tasks                             | Notes                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Perform planning and site preparation tasks. | See <a href="#">Planning checklist</a> on page 24.<br><br>As part of the site preparation, you must set up the required infrastructure components in your network. Avaya Aura® is required in Team Engagement deployments. Your deployment can also include Conferencing. |
| Complete initial setup and installation.     | You must deploy a virtual machine first and then install the Avaya Aura® Web Gateway application.<br><br>For more information, see the procedures in <a href="#">Initial setup</a> on page 50 and <a href="#">Installing the Avaya Aura Web Gateway</a> on page 98.       |
| Perform configuration.                       | Perform the appropriate configuration tasks for each deployment option. For more information, see <a href="#">Configuration worksheet</a> on page 21.                                                                                                                     |

---

## Configuration worksheet

Use this checklist to determine the configuration requirements for each deployment type. The deployment types are:

- Single FQDN, single data center.
- Multiple FQDNs, single data center.
- Multiple data centers, which is also known as geographical distribution.

The deployment option with multiple data centers requires multiple FQDNs. With this deployment, you require at least one FQDN for each service.

| Task                                                                                                                                                                                                                                                                                                                                                                   | Single FQDN, single data center                                            | Multiple FQDNs, single data center                                                                           | Multiple data centers                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Configure a global FQDNs. See <a href="#">Global FQDN configuration</a> on page 136                                                                                                                                                                                                                                                                                    | ✓                                                                          | —                                                                                                            | ✓                                                                          |
| Configure Avaya Aura® Web Gateway certificates.<br><b>+ Tip:</b><br>When possible, perform certificate configuration in the web administration portal as described in <i>Administering the Avaya Aura® Web Gateway</i> . If the web administration portal is not available, see <a href="#">Certificate configuration using the configuration utility</a> on page 192. | ✓<br><br>For this deployment, use System Manager certificates if possible. | ✓<br><br>For this deployment, generate a Certificate Signing Request (CSR) and get it signed by a public CA. | ✓<br><br>For this deployment, use System Manager certificates if possible. |
| Configure System Manager. See <a href="#">Adding the Avaya Aura Web Gateway to System Manager</a> on page 139.                                                                                                                                                                                                                                                         | ✓                                                                          | ✓                                                                                                            | ✓                                                                          |
| Configure Avaya Aura® Media Server. See <a href="#">Configuring Avaya Aura Media Server settings</a> on page 144.                                                                                                                                                                                                                                                      | ✓                                                                          | ✓                                                                                                            | ✓                                                                          |
| Configure Avaya Aura® Device Services. See <a href="#">Configuring the Avaya Aura Web Gateway on Avaya Aura Device Services</a> on page 146.                                                                                                                                                                                                                           | ✓                                                                          | ✓                                                                                                            | ✓                                                                          |

Table continues...

| Task                                                                                                                                                                        | Single FQDN, single data center | Multiple FQDNs, single data center | Multiple data centers |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|------------------------------------|-----------------------|
| If your deployment includes Conferencing, configure Avaya Meetings Server. See <a href="#">Configuring the Avaya Aura Web Gateway on Avaya Meetings Server</a> on page 147. | ✓                               | ✓                                  | ✓                     |
| Configure the reverse proxy on Avaya Session Border Controller. See <a href="#">Reverse proxy configuration</a> on page 151.                                                | ✓                               | ✓                                  | ✓                     |
| If you are planning to use external clients outside the enterprise firewall, configure client access. See <a href="#">External client access configuration</a> on page 162. | ✓                               | ✓                                  | ✓                     |
| Configure an external load balancer. See <a href="#">Route configuration for an external load balancer</a> on page 148.                                                     | —                               | —                                  | ✓                     |

# Chapter 4: Planning and preinstallation

Review this chapter before you start installing the Avaya Aura® Web Gateway. You can either deploy the Avaya Aura® Web Gateway using Amazon Web Services (AWS) or VMware.

 **Warning:**

When you deploy Avaya Aura® Web Gateway, avoid copying and pasting commands directly from this document. This can introduce unwanted characters and errors. Double-check all inputs you copy or type them manually.

---

## Planning checklist

This checklist outlines planning requirements and tasks that you must complete before deploying the Avaya Aura® Web Gateway.

| No. | Task                                                        | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ✓ |
|-----|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that you have all required skills and knowledge.     | Before deploying Avaya Aura® Web Gateway, ensure that you have all required skills and knowledge described in this chapter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |   |
| 2   | Ensure that you have all required components and equipment. | <p>Team Engagement deployments require Avaya Aura®. Your deployment can also include Conferencing. For more information about components, see <a href="#">Product compatibility</a> on page 19.</p> <p>You must also have:</p> <ul style="list-style-type: none"><li>• A virtual machine. You can deploy Avaya Aura® Web Gateway in a VMware or Amazon Web Services environment either using either an Avaya-provided OVA or as a software-only application. Ensure your system meets the specifications outlined in <a href="#">Resource profile specifications for Avaya Aura Web Gateway on VMware</a> on page 29 and <a href="#">Resources profile</a></li></ul> |   |

*Table continues...*

| No. | Task                                                                                                                                                                                                                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|     |                                                                                                                                                                                                                                                              | <p><a href="#">specifications for Avaya Aura Web Gateway on Amazon Web Services</a> on page 30.</p> <ul style="list-style-type: none"> <li>• The Red Hat Enterprise Linux 8.10 operating system, if you are planning to install Avaya Aura® Web Gateway as a software-only application. If you are installing Avaya Aura® Web Gateway using an Avaya-provided OVA, the operating system is installed automatically.</li> <li>• An SSH tool, such as PuTTY.</li> </ul> <p><b>+ Tip:</b></p> <p>Configure your SSH tool to properly see lines in the Avaya Aura® Web Gateway configuration utility. For example, in the PuTTY Reconfiguration screen, navigate to <b>Window &gt; Translation</b> and do the following:</p> <ul style="list-style-type: none"> <li>- Set <b>Remote character set</b> to <b>Use font encoding</b>.</li> <li>- Select <b>Use Unicode line drawing code points</b>.</li> </ul> |   |
| 3   | <p>Determine the structure of your deployment. Deployment types are:</p> <ul style="list-style-type: none"> <li>• A single FQDN with a single data center.</li> <li>• Multiple FQDNs with a single data center.</li> <li>• Multiple data centers.</li> </ul> | <p>Consider the following to determine which deployment type you require:</p> <ul style="list-style-type: none"> <li>• Do you want a single FQDN for all services or a separate FQDN for each service? A single FQDN has some restrictions and requires internal traffic to be routed through the reverse proxy. However, with a single FQDN, you can use a single certificate for all services.</li> <li>• Does your system require a single data center or multiple regionally-distributed data centers?</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |   |
| 4   | <p>Ensure that you can log in to the Avaya Product Licensing and Delivery System (PLDS) to download software and to obtain licences.</p>                                                                                                                     | <p>Ensure that you have access to PLDS and can download files. Download the Avaya Aura® Web Gateway installation file from PLDS.</p> <p>Avaya Aura® Web Gateway software and enhanced user privileges are licensed capabilities.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |   |

Table continues...

| No. | Task                                                                                                               | Notes                                                                                                                                                                                                                                                                                                                                                            | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|     |                                                                                                                    | You can access PLDS at <a href="http://plds.avaya.com/">http://plds.avaya.com/</a> .                                                                                                                                                                                                                                                                             |   |
| 5   | Obtain the required IP addresses, FQDNs, and certificates.                                                         | The IP addresses are used by the interfaces of the different infrastructure components. Certificates are required to ensure secure interaction between solution components. For more information, see <a href="#">Required FQDNs and certificates</a> on page 27.                                                                                                |   |
| 6   | If you are planning to deploy a geographically distributed system, review the external load balancer requirements. | See <a href="#">External load balancer requirements</a> on page 33.                                                                                                                                                                                                                                                                                              |   |
| 7   | Open the required ports on the firewall.                                                                           | For detailed information about the ports that must be opened, go to <a href="https://support.avaya.com/security">https://support.avaya.com/security</a> , scroll down, and click <b>Avaya Product Port Matrix Documents</b> . Navigate to the Avaya Aura® Web Gateway section and then click on the appropriate Port Matrix document for the release to open it. |   |

## Required skills and knowledge

Before deploying the product, ensure that you know how to do the following:

- Manage VMware or AWS deployments.
  - For VMware deployments, you must be familiar with virtual machines using vCenter and vSphere.
  - For AWS deployments, you must be familiar with Amazon Machine Images (AMIs) and with the AWS Management console. For a list of supported browsers in AWS, see [https://aws.amazon.com/console/faqs/#browser\\_support](https://aws.amazon.com/console/faqs/#browser_support).
- Install, deploy, and use key Avaya Aura® components.
- Install, set up, and use the enterprise LDAP directory.
- Use basic Linux commands.

### Related links

[Product compatibility](#) on page 19

## Required FQDNs and certificates

| Required FQDNs                                                                                                                                                                                                                                                                                                                                                               | Required certificates                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>In a single FQDN model, you require one FQDN that represents all services. For example: webservices.company.com.</p> <p>From the internet, the FQDN resolves to the IP address of the external Avaya SBC interface. Internally, from the enterprise, it resolves to the IP address of the internal Avaya SBC interface.</p>                                               | <p>The certificate includes the FQDN and must be signed by a public CA.</p>                                                                                                                                                                                                 |
| <p>FQDN for the Avaya Meetings Server Management service. For example: conferencing_management.company.com.</p> <p>Internally the FQDN resolves to the virtual IP address of the Avaya Meetings Server Management system.</p> <p>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBC interface.</p>                      | <p>In a single FQDN deployment, the certificate is signed by the System Manager CA.</p> <p>In a multiple FQDN deployment, the certificate is signed by a public CA.</p>                                                                                                     |
| <p>FQDN for each Web Collaboration Services server IP address. For example: webconference1.company.com, webconference2.company.com and so on.</p> <p>Internally, the FQDN resolves to the IP address of the Web Collaboration Services server.</p> <p>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBC interface.</p> | <p>In a single FQDN deployment, the certificate for each Web Collaboration Services server is signed by the System Manager CA.</p> <p>In a multiple FQDN deployment, the certificate is signed by a public CA.</p>                                                          |
| <p>FQDN for the Avaya Aura® Web Gateway portal server virtual IP address. For example: webgateway.company.com.</p> <p>Internally, the FQDN resolves to the virtual IP address of the Avaya Aura® Web Gateway portal service.</p> <p>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBC interface.</p>                   | <p>The certificate must include the global services FQDN in the SAN.</p> <p>In a single FQDN deployment, the certificate for each server IP address is signed by the System Manager CA.</p> <p>In a multiple FQDN deployment, the certificate is signed by a public CA.</p> |
| <p>FQDN for TURN media tunneling. For example: turnmedia.company.com.</p> <p>The FQDN resolves to the IP address of the external Avaya SBC interface used for TURN media.</p>                                                                                                                                                                                                | <p>The certificate is signed by a public CA.</p>                                                                                                                                                                                                                            |

*Table continues...*

| Required FQDNs                                                                                                                                                                                     | Required certificates                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <p>FQDN for HTTP media tunneling. For example: media.company.com.</p> <p>The FQDN resolves to the IP address of the external Avaya SBC interface used for HTTP media tunneling.</p>                | The certificate is signed by a public CA.           |
| <p>FQDN for the Avaya SBC management interface. For example: sbce_management.company.com.</p> <p>The FQDN resolves to the IP address for the internal Avaya SBC interface used for management.</p> | The certificate is signed by the System Manager CA. |

## Virtual machine requirements

### Software requirements

Avaya Aura® supports the following software versions:

- Avaya Solutions Platform 130 (Avaya-supplied KVM on RHEL 8.10): Dell PowerEdge R660xs or R640.
- Avaya Solutions Platform S8300 (Avaya-supplied KVM on RHEL 8.10): S8300E.

**\* Note:**

Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.

- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 7.0 or 8.0
  - VMware® vCenter Server 7.0 or 8.0

To view compatibility with other solution releases, see Broadcom website (formerly VMware) and search for VMware Product Interoperability Matrix.

- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.

**\* Note:**

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
- Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
- Avaya Aura® Release 8.1.x and later supports ASP R6.0.x (KVM on RHEL 8.10) hypervisor.

## Resource profile specifications

### Resource profile specifications for Avaya Aura® Web Gateway on VMware

The following section outlines the resource profile specifications for differently sized virtual machines. The virtual machine resource requirements apply both to OVA-based and software-only deployment options.

**! Important:**

When deploying an Avaya Aura® Web Gateway cluster, you must use the same resource profile for each Avaya Aura® Web Gateway node in the cluster. Mixed profile clusters are not supported.

| Specifications             | Avaya Aura® Web Gateway Profile 1                                                                                                                                                                           | Avaya Aura® Web Gateway Profile 2                                                                                                                                                 | Avaya Aura® Web Gateway Profile 3                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vCPU</b>                | 4                                                                                                                                                                                                           | 8                                                                                                                                                                                 | 16                                                                                                                                                                                |
| <b>CPU reservation</b>     | 4600 MHz                                                                                                                                                                                                    | 9200 MHz                                                                                                                                                                          | 18400 MHz                                                                                                                                                                         |
| <b>Memory</b>              | 6 GB                                                                                                                                                                                                        | 12 GB                                                                                                                                                                             | 16 GB                                                                                                                                                                             |
| <b>Hard disk</b>           | 132 GB                                                                                                                                                                                                      |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>Minimum clock speed</b> | 2600 MHz                                                                                                                                                                                                    |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>Capacity</b>            | Both of the following:<br><ul style="list-style-type: none"> <li>• 1250 Conferencing or Avaya Workplace Client sessions</li> <li>• 1250 Portal Conferencing users</li> </ul>                                | Both of the following:<br><ul style="list-style-type: none"> <li>• 2500 Conferencing or Avaya Workplace Client sessions</li> <li>• 2500 Portal Conferencing users</li> </ul>      | Both of the following:<br><ul style="list-style-type: none"> <li>• 5000 Avaya Workplace Client or Conferencing sessions</li> <li>• 5000 Conferencing Portal users</li> </ul>      |
| <b>Server type</b>         | Dell R220 or equivalent                                                                                                                                                                                     |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>CPU</b>                 | Intel Xeon CPU E5-26700@2.60GHz                                                                                                                                                                             |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>Physical processor</b>  | 1                                                                                                                                                                                                           | 2                                                                                                                                                                                 | 4                                                                                                                                                                                 |
| <b>Physical core</b>       | 4                                                                                                                                                                                                           |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>NICs</b>                | 1GBPS                                                                                                                                                                                                       |                                                                                                                                                                                   |                                                                                                                                                                                   |
| <b>Load supported</b>      | <ul style="list-style-type: none"> <li>• 16 Conferencing calls per second.</li> <li>• 12500 Avaya Workplace Client Busy Hour Call Attempts (BHCA).</li> <li>• 20 Portal user requests per second</li> </ul> | <ul style="list-style-type: none"> <li>• 33 Conferencing calls per second.</li> <li>• 25000 Avaya Workplace Client BHCA.</li> <li>• 40 Portal user requests per second</li> </ul> | <ul style="list-style-type: none"> <li>• 50 Conferencing calls per second.</li> <li>• 50000 Avaya Workplace Client BHCA.</li> <li>• 60 Portal user requests per second</li> </ul> |

## Resource profile specifications for Avaya Aura® Web Gateway on ASP R6.0.x (KVM on RHEL 8.10)

The following table describes the resource requirements to support different profiles for Avaya Aura® Web Gateway on Avaya-supplied ASP R6.0.x:

| Specifications             | Avaya Aura® Web Gateway Profile 1                                                                                                                                                                          | Avaya Aura® Web Gateway Profile 2                                                                                                                                                | Avaya Aura® Web Gateway Profile 3                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vCPU</b>                | 4                                                                                                                                                                                                          | 8                                                                                                                                                                                | 16                                                                                                                                                                               |
| <b>CPU reservation</b>     | 4600 MHz                                                                                                                                                                                                   | 9200 MHz                                                                                                                                                                         | 18400 MHz                                                                                                                                                                        |
| <b>Memory</b>              | 6 GB                                                                                                                                                                                                       | 12 GB                                                                                                                                                                            | 16 GB                                                                                                                                                                            |
| <b>Hard Disk</b>           | 132 GB                                                                                                                                                                                                     |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>Minimum clock speed</b> | 2600 MHz                                                                                                                                                                                                   |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>Capacity</b>            | Both of the following <ul style="list-style-type: none"> <li>• 1250 Conferencing or Avaya Workplace Client sessions</li> <li>• 1250 Portal Conferencing users</li> </ul>                                   | Both of the following <ul style="list-style-type: none"> <li>• 2500 Conferencing or Avaya Workplace Client sessions</li> <li>• 2500 Portal Conferencing users</li> </ul>         | Both of the following <ul style="list-style-type: none"> <li>• 5000 Conferencing or Avaya Workplace Client sessions</li> <li>• 5000 Conferencing Portal users</li> </ul>         |
| <b>Server type</b>         | Dell R660xs or equivalent                                                                                                                                                                                  |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>CPU</b>                 | Intel Xeon CPU E5-26700@2.60GHz                                                                                                                                                                            |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>Physical core</b>       | 4                                                                                                                                                                                                          |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>NICs</b>                | 1GBPS                                                                                                                                                                                                      |                                                                                                                                                                                  |                                                                                                                                                                                  |
| <b>Load supported</b>      | <ul style="list-style-type: none"> <li>• 16 Conferencing calls per second</li> <li>• 12500 Avaya Workplace Client Busy Hour Call Attempts (BHCA).</li> <li>• 20 Portal user requests per second</li> </ul> | <ul style="list-style-type: none"> <li>• 33 Conferencing calls per second</li> <li>• 25000 Avaya Workplace Client BHCA.</li> <li>• 40 Portal user requests per second</li> </ul> | <ul style="list-style-type: none"> <li>• 50 Conferencing calls per second</li> <li>• 50000 Avaya Workplace Client BHCA.</li> <li>• 60 Portal user requests per second</li> </ul> |

## Resources profile specifications for Avaya Aura® Web Gateway on Amazon Web Services

The following table outlines the profiles created by the CloudFormation template generators. You can use the CloudFormation template generation tool to create a template for the required profile. The template contains the computing and networking resources required for the profile.

| Profile | Service size  | AWS instance type | vCPUs | Memory (GB) |
|---------|---------------|-------------------|-------|-------------|
| Small   | 1250 sessions | c4.xlarge         | 4     | 6           |
| Medium  | 2500 sessions | c4.2xlarge        | 8     | 8           |

## Networking considerations for Amazon Web Services

There are some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon VPC Limits, see the AWS documentation at <https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html>.

### ! Important:

Use a direct connection along with a private WAN connection with Service Level Agreement (SLA) measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between AWS and the customer premises.

When you deploy Avaya Aura® Web Gateway in an AWS environment, also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Aura® Web Gateway in the same AWS region.

### Connection types

You can connect applications in a hybrid network on the Amazon VPC in the following ways:

| Connection type   | Resource                                                                                                                                          |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| VPN connection    | For information about VPN connections, see:<br><a href="https://docs.aws.amazon.com/vpc/">https://docs.aws.amazon.com/vpc/</a>                    |
| Direct connection | For information about AWS direct connections, see:<br><a href="https://aws.amazon.com/directconnect/">https://aws.amazon.com/directconnect/</a> . |

## Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

| ESXi version | Avaya Aura® Release |       |                                   |        |        |
|--------------|---------------------|-------|-----------------------------------|--------|--------|
|              | 7.1.x               | 8.0.x | 8.1.x                             | 10.1.x | 10.2.x |
| ESXi 5.0     | N                   | N     | N                                 | N      | N      |
| ESXi 5.1     | N                   | N     | N                                 | N      | N      |
| ESXi 5.5     | Y                   | N     | N                                 | N      | N      |
| ESXi 6.0     | Y                   | Y     | Y                                 | N      | N      |
| ESXi 6.5     | Y                   | Y     | Y                                 | N      | N      |
| ESXi 6.7     | N                   | Y     | Y                                 | Y      | N      |
| ESXi 7.0     | N                   | N     | Starting from Release 8.1.3:<br>Y | Y      | Y      |
| ESXi 8.0     | N                   | N     | N                                 | N      | Y      |

**\* Note:**

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.  
Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).
- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.  
For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

**Related links**

[Planning and preinstallation](#) on page 24

## 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               |        |        |        |

*Table continues...*

| Disk Volume      | Volume size can be increased | Volume Size (GiB) |        |        |        |
|------------------|------------------------------|-------------------|--------|--------|--------|
|                  |                              | Disk 1            | Disk 2 | Disk 3 | Disk 4 |
| 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             |        |        |        |

## External load balancer requirements

In a geographically distributed deployment, the Avaya Aura® Web Gateway requires an external load balancer that must comply with the following requirements:

| Requirement                                                                                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The HTTP Global Server Load Balancing (GSLB) must route requests basing on the user's location.                                                      | The GSLB functionality can be part of the DNS server and not the load balancer. In this case, however, the DNS server must be able to route requests to different locations based on the location of the browser that initiated the request.                                                                                                                                                                                    |
| The HTTP Load balancer must support session affinity. Session affinity means that all requests from the client are always routed to the same server. | <ul style="list-style-type: none"> <li>• Session affinity is based on cookies.</li> <li>• The reverse proxy inserts a cookie to responses for incoming HTTP requests and routes subsequent requests that contain the same cookie to the same Avaya Aura® Web Gateway server.</li> <li>• This feature is also known as sticky sessions. Do not use IP-based sticky sessions because this might affect load balancing.</li> </ul> |

*Table continues...*

| Requirement                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The HTTP load balancer must support web sockets.                                                                                                       | <ul style="list-style-type: none"> <li>The load balancer must not block web socket requests and must relay the web socket connections between the client and the server.</li> <li>HTTP request timeout must be configurable. You must be able to configure the timeout value to the maximum duration of the conference to prevent it from timing out the web socket session.</li> </ul>                                                  |
| The HTTP load balancer must support URL routing.                                                                                                       | The load balancer must be able to route requests to different backends based on the request URL.                                                                                                                                                                                                                                                                                                                                         |
| The HTTP load balancer must support URL rewrite.                                                                                                       | The load balancer must be able to modify the URL path of the request based on simple rules to remove or rename parts of the path.                                                                                                                                                                                                                                                                                                        |
| The HTTP load balancer must support TLS 1.2 or TLS 1.3.                                                                                                | Avaya Aura® Web Gateway supports TLS versions 1.2 and 1.3. The load balancer must support the TLS version that you plan to use in your deployment. Some services might not support TLS versions other than 1.2.                                                                                                                                                                                                                          |
| The HTTP load balancer must support at least some of the listed ciphers when interacting with back-end services.                                       | <ul style="list-style-type: none"> <li>ECDHE-RSA-AES128-GCM-SHA256</li> <li>ECDHE-ECDSA-AES128-GCM-SHA256</li> <li>ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>ECDHE-RSA-AES128-SHA256</li> <li>ECDHE-ECDSA-AES128-SHA256</li> <li>ECDHE-RSA-AES128-SHA</li> <li>ECDHE-ECDSA-AES128-SHA</li> <li>AES128-GCM-SHA256</li> <li>AES256-GCM-SHA384</li> <li>AES128-SHA</li> </ul>                                                                  |
| The HTTP load balancer must be able to use TCP health checks.                                                                                          | The load balancer must be able to perform health checks of Avaya Aura® Web Gateway servers using TCP responses. To avoid leaving multiple TCP sockets opened, you must be able to configure TCP health checks to half-opened connections.                                                                                                                                                                                                |
| The external HTTP load balancer must be able to use standard headers to determine the FQDN from the original request that is used to reach the system. | <p>Avaya Aura® Web Gateway uses the “Host” header to identify the FQDN that is used by the client to reach the system.</p> <p> <b>Note:</b></p> <p>This behavior is required if the customer requires different FQDNs per location or uses different FQDNs to reach the system. If a single global FQDN is used, you can ignore this requirement.</p> |
| The external HTTP load balancer must relay the client certificates.                                                                                    | This requirement is only needed for authenticating clients using a client certificate.                                                                                                                                                                                                                                                                                                                                                   |

*Table continues...*

| Requirement                                                                    | Description |
|--------------------------------------------------------------------------------|-------------|
| The HTTP load balancer must be able to insert custom headers to HTTP requests. |             |

## 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                                               |
|-------------------|-----------------------------------------------------------|
| <code>cdto</code> | Change to frequently used directories.                    |
| <code>app</code>  | Perform application functions, such as install or backup. |
| <code>svc</code>  | 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, --hhhelp
        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 UCAApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
with command line syntax, and "-hh" (or "--hhhelp") 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.

smcvmgmt
    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
--hhhelp,              -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 --hhhelp

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

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

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 specified,
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
mebibytes, "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           |          |                  |       |
| Num                     | Name | Size  | Free | Name             | LVM Size | File System 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 smcvmgt command

The system layer **smcvmgt** 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 tunables 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 disabled 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= <i>INTEGER</i>      | Number of characters in the new password that must not be present in the old password.                                                                                                                                                                                                                     |
| --min-len= <i>INTEGER</i>   | Minimum length of the password.<br>The default minimum length is 15 characters.                                                                                                                                                                                                                            |
| --min-digs= <i>INTEGER</i>  | Minimum number of digits in the password.                                                                                                                                                                                                                                                                  |
| --min-upper= <i>INTEGER</i> | Minimum number of uppercase characters in the password.                                                                                                                                                                                                                                                    |
| --min-lower= <i>INTEGER</i> | Minimum number of lowercase characters in the password.                                                                                                                                                                                                                                                    |
| --min-other= <i>INTEGER</i> | Minimum number of special characters in the password.<br><br><div>  <b>Important:</b><br/>           Avaya Aura® Web Gateway supports the following special characters: !, @, #, %, \$, ^, *, ?, and _ .         </div> |

*Table continues...*

| Option                                                   | Description                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--min-class</code><br><code>=INTEGER</code>        | Minimum number of character classes that must be present in the password. The character classes are: <ul style="list-style-type: none"> <li>• Digits</li> <li>• Uppercase characters</li> <li>• Lowercase characters</li> <li>• Special characters</li> </ul>                                                                  |
| <code>--max-repeat</code><br><code>=INTEGER</code>       | Maximum allowed number of consecutively repeated characters.<br>For example, if you set this parameter to 3, then the following password is invalid: <code>paaassword</code> , because <code>a</code> is repeated three times.                                                                                                 |
| <code>--max-class-repeat</code><br><code>=INTEGER</code> | Maximum allowed number of consecutively repeated characters of the same class.<br>For example, if you set this parameter to 3, then the <code>pas1sw2or3d</code> password is invalid, because the first three characters, which are <code>p</code> , <code>a</code> , and <code>s</code> , 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
```

## 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.

## 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.

## 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
```

---

## 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.

# Chapter 5: Initial setup

You can use the following options to deploy Avaya Aura® Web Gateway:

- As a software-only application that you can install on your own Red Hat Enterprise Linux (RHEL) 8.10 physical servers or virtual machines.

For software-only deployments, Avaya Aura® Web Gateway supports the following virtual environments:

- VMware
- Amazon Web Services (AWS)
- In a VMware environment using an Avaya-provided, application-specific RHEL 8.10 OVA. This option includes installing Avaya Aura® Web Gateway on Avaya Solutions Platform 130.

## **Note:**

Starting from Release 10.2.0, Avaya Aura® Web Gateway does not support OVA-based deployments in an AWS environment.

Use the following sections to perform the initial virtual machine setup.

### Related links

[Virtual machine deployment options](#) on page 54

[Software-only deployment in VMware-based virtualization environment](#) on page 66

[Software-only deployment on Amazon Web Services](#) on page 80

---

## OVA-based deployments

The following section describes deploying a virtual machine in a VMware and KVM environment using an Avaya-provided, application-specific RHEL 8.10 OVA. The components of the Avaya Aura® Web Gateway, Endpoint Service Gateway, and Unified Portal are provided in a single OVA file.

You can use the following options to deploy an OVA:

- VMware vSphere Client
- VMware Host Client, which connects directly to an ESXi host.
- Solution Deployment Manager from System Manager
- KVM

After deploying a virtual machine, install the Avaya Aura® Web Gateway application.

## Deployment process checklist

The following checklist describes the high-level deployment steps you must perform to deploy a virtual machine using an Avaya-provided OVA. This checklist also contains steps you must perform to prepare the virtual machine for Avaya Aura® Web Gateway application installation:

| No. | Task                                                                                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ✓ |
|-----|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that virtual machines you plan to use to deploy Avaya Aura® Web Gateway comply with the virtual machine requirements. | See the requirements in <a href="#">Software requirements</a> on page 28.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |   |
| 2   | Download the latest Avaya Aura® Web Gateway OVA from PLDS.                                                                   | See <a href="#">Obtaining the Avaya Aura Web Gateway OVA file</a> on page 52.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |   |
| 3   | Deploy a virtual machine or KVM using the OVA.                                                                               | <p>Avaya Aura® Web Gateway supports the following deployment options:</p> <ul style="list-style-type: none"> <li>• VMware vCenter</li> <li>• VMware vSphere</li> <li>• Solution Deployment Manager from System Manager</li> <li>• KVM</li> </ul> <p>For more information about the deployment process, see the appropriate procedure in <a href="#">Virtual machine deployment options</a> on page 54.</p> <p>The Avaya Aura® Web Gateway OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk.</p> |   |
| 4   | Optional: Enable the Enhanced Access Security Gateway (EASG).                                                                | <p>EASG enables Avaya support engineers to access your Avaya Aura® Web Gateway and resolve product issues in real-time.</p> <p>If you use VMware vCenter or Solution Deployment Manager, you can enable EASG when deploying a virtual machine. If you use vSphere, you can enable EASG from the CLI. For more information about enabling EASG, see <a href="#">Enabling the Enhanced Access Security Gateway from the CLI</a> on page 62.</p>                                                                                                       |   |
| 5   | Optional: Configure UEFI Secure Boot settings.                                                                               | For security reasons, Avaya Aura® Web Gateway uses the UEFI Secure Boot feature by default. If required, you can                                                                                                                                                                                                                                                                                                                                                                                                                                    |   |

*Table continues...*

| No. | Task                                                                                                              | Notes                                                                                                                                                                                                                                                                                       | ✓ |
|-----|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|     |                                                                                                                   | configure the Secure Boot settings as described in <a href="#">Configuring UEFI Secure Boot for OVA-based virtual machines</a> on page 63.                                                                                                                                                  |   |
| 6   | Optional: Enable FIPS mode.                                                                                       | You can only enable FIPS mode before installing the application layer. For information about enabling FIPS, see <a href="#">Enabling FIPS mode</a> on page 64.                                                                                                                              |   |
| 7   | Enable additional STIG hardening.                                                                                 | You only need to enable additional hardening if your organization policies require full Security Technical Implementation Guide (STIG) compliance.<br><br>For more information about enabling additional STIG hardening, see <a href="#">Enabling additional STIG hardening</a> on page 65. |   |
| 8   | Install or restore the application layer as required.                                                             | For information about installing the initial node, see <a href="#">Installing the Avaya Aura Web Gateway</a> on page 98.<br><br>For information about installing additional nodes, see <a href="#">Installing additional nodes to create a cluster</a> on page 104.                         |   |
| 9   | If you are installing a cluster, configure RSA keys for SSH connections after all additional nodes are installed. | See <a href="#">Configuring RSA public and private keys for SSH connections in a cluster</a> on page 107.                                                                                                                                                                                   |   |

After deploying a virtual machine, install the Avaya Aura® Web Gateway application as described in the “Avaya Aura® Web Gateway setup” chapter.

## Obtaining the Avaya Aura® Web Gateway OVA file

### Procedure

Do one of the following:

- Download the Avaya Aura® Web Gateway OVA from the Avaya Product Licensing and Delivery System (Avaya PLDS) at <https://plds.avaya.com>.
- Place an order for the DVDs containing the OVA file using the Material Code ID or description.

For more information about the material ID, see “Product Order Codes and Pricing” in *Avaya Aura® Web Gateway Offer Definition*.

## Downloading software from PLDS

### About this task

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS.

After downloading an Avaya Aura® Web Gateway OVA, you must verify that the SHA256 checksum of the OVA file matches the SHA256 checksum value provided on PLDS. To calculate the SHA256 checksum, you can use any SHA256 hash calculation tool, such as sha256sum.

Along with PLDS, you can download the product software from <https://support.avaya.com> using the Downloads and Documents tab at the top of the page.

#### \* Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

### Procedure

1. On your web browser, type <https://plds.avaya.com> to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.
4. Click **View Downloads**.
5. Click the search icon  for Company Name.
6. In the Search Companies dialog box, do the following:
  - a. In the **%Name** field, type *Avaya* or the Partner company name.
  - b. Click **Search Companies**.
  - c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
  - In **Download Pub ID**, type the download pub ID.
  - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. In the **Download Manager** box, click the appropriate **Download** link.

#### \* Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location to save the file, and click **Save**.

12. **(Optional)** When the system displays the security warning, click **Install**.

When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

## Virtual machine deployment options

Use one of the following procedures to deploy the OVA. You can use vSphere Client, Host Client, Solution Development Manager (SDM) or KVM.

### Important:

When deploying an Avaya Aura® Web Gateway cluster, you must use the same resource profile for each Avaya Aura® Web Gateway node in the cluster. Mixed profile clusters are not supported.

### Related links

[Resource profile specifications for Avaya Aura Web Gateway on VMware](#) on page 29

## Supported vSphere clients

The following table lists vSphere clients that you can use to deploy the Avaya Aura® Web Gateway OVA, depending on the VMware ESXi version:

| Client type                | Launched from                                                | Is supported on |                   |
|----------------------------|--------------------------------------------------------------|-----------------|-------------------|
|                            |                                                              | ESXi 6.7        | ESXi 7.0 or later |
| vSphere client application | Application installed on your computer.                      | ✗               | ✗                 |
| vSphere Client for vCenter | Web client launched with the IP of vCenter.                  | ✓               | ✓                 |
| ESXi Host Client           | Web client launched with the IP of the individual ESXi host. | ✓               | ✓                 |

## Deploying the Avaya Aura® Web Gateway OVA using the vSphere Client

### About this task

Use this procedure to deploy the Avaya Aura® Web Gateway OVA on vCenter using the vSphere Client.

This procedure applies to vSphere Client Release 7.0.3. If you use another version of the vSphere Client, the steps might differ from the steps described in this procedure.

### Procedure

- Log in to the vSphere Client at `https://<VCENTER>/UI`.  
In this URL, <VCENTER> is the IP address or FQDN of the vCenter server.
- Right-click an appropriate cluster or ESXi host where you want to deploy the OVA and select **Deploy OVF Template**.

The vSphere Client displays the Deploy OVF Template window.

3. To download the OVA file, on the Select an OVF template page, do one of the following:
  - To download the OVA file from a web location, select **URL** and provide the complete network path to the OVA file.
  - To download the OVA file from the local computer, select **Local file** and click **Upload files** and select the OVA file.
4. Click **Next**.
5. On the Select a name and folder page, do the following:
  - a. In **Virtual machine name**, type a name for the virtual machine.
  - b. In **Select a location for the virtual machine**, select an appropriate location for the virtual machine.  
By default, this is the location that you select in step 2.
  - c. Click **Next**.
6. On the Select a compute resource page, do the following:
  - a. In **Select the destination compute resource**, select an appropriate ESXi host for the virtual machine.  
By default, this is the location that you select in step 2.
  - b. Ensure that the Compatibility area displays the `Compatibility check succeeded` message.
  - c. Click **Next**.
7. On the Review details page, do the following:
  - a. Ensure that the **Publisher** field contains the `Entrust Code Signing CA - OVCS1 (Trusted certificate)` entry.
  - b. Verify the OVA template details.
  - c. Click **Next**.
8. On the License agreements page, do the following:
  - a. Read the End User License Agreement (EULA).
  - b. To accept the EULA, select the **I accept all license agreements** check box.
  - c. Click **Next**.
9. On the Configuration page, select an Avaya Aura® Web Gateway profile that matches your deployment requirements.

 **Important:**

If you deploy the OVA for a non-seed node in a cluster, you must use the same resource profile that you use for the seed node.

For more information about resource profile specifications, see [Resource profile specifications for Avaya Aura Web Gateway on VMware](#) on page 29. The vSphere Client also displays the basic system requirements for the profile in the Description area.

10. Click **Next**.
11. On the Select storage page, do the following:
  - a. In **Select virtual disk format**, select the appropriate disk format.  
 If you select **Thick provision**, the entire disk space required for the virtual machine is reserved and unavailable for other virtual machines to use. If you select **Thin provision**, unused space is available for other virtual machines.
  - b. In the Datastore table, select an appropriate data store for the virtual machine.
  - c. Ensure that the Compatibility area displays the *Compatibility check succeeded* message.
  - d. Click **Next**.
12. On the Select networks page, for each source network, select an appropriate destination network.
13. Click **Next**.
14. On the Customize template page, configure the following parameters:
  - a. In **Enhanced Access Security Gateway (EASG)**, configure EASG settings.
  - b. In **Disk Encryption Settings**, configure disk encryption settings.
  - c. In **Management Network Settings**, configure network settings, such as the IP address, FQDN, network mask, and DNS.
  - d. In **Account login Details**, configure credentials for a Linux administrator user, including the user name, password, and group.

For more information about the disk encryption and EASG fields, see [Data encryption field descriptions](#) on page 57 and [Enhanced Access Security Gateway field descriptions](#) on page 58.

 **Note:**

- If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful. The vSphere Client displays the number of remaining mandatory settings that you must configure at the top of the Customize template page.
  - The vSphere Client validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the virtual machine console.
15. Click **Next**.
  16. On the Ready to complete page, review the configuration details and then click **Finish** to complete the virtual machine deployment.

## Next steps

Install the Avaya Aura® Web Gateway.

## Data encryption field descriptions

Data encryption is only supported with AVP and the VMware Virtualized Environment.

| Name                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Encryption</b>                             | <p>Specifies whether data encryption is enabled or disabled on Avaya Aura® Web Gateway. The options are the following:</p> <ul style="list-style-type: none"> <li>• <b>1</b>: To enable data encryption.</li> <li>• <b>2</b>: To disable data encryption.</li> </ul> <p> <b>Important:</b></p> <p>You cannot change encrypted Avaya Aura® Web Gateway to non-encrypted or vice versa without a new OVA installation.</p> <ul style="list-style-type: none"> <li>• On Solution Deployment Manager: When the <b>Data Encryption</b> field is set to 1, Avaya Aura® Web Gateway enables the <b>Encryption Pass-Phrase</b> and <b>Re-enter Encryption Pass-Phrase</b> fields to enter the encryption passphrase.</li> <li>• On vCenter or ESXi: When the <b>Data Encryption</b> field is set to 1, enter the encryption passphrase in the <b>Password</b> and <b>Confirm Password</b> fields.</li> </ul> |
| <b>Encryption Pass-Phrase</b>                      | <p>The passphrase for data encryption. This field is applicable when data encryption is enabled.</p> <p>When you deploy Avaya Aura® Web Gateway using Solution Deployment Manager, Avaya Aura® Web Gateway applies the password complexity rules.</p> <p>When you deploy Avaya Aura® Web Gateway using vCenter or ESXi, Avaya Aura® Web Gateway does not apply password complexity rules.</p> <p> <b>Important:</b></p> <p>While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to a vCenter limitation. Therefore, ensure that you enter the encryption passphrase if data encryption is enabled.</p>                                                                                                                                                                                                    |
| <b>Re-enter Encryption Pass-Phrase</b>             | The password for data encryption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Require Encryption Pass-Phrase at Boot-Time</b> | When this check box is selected, you must type the encryption passphrase whenever Avaya Aura® Web Gateway reboots. By default, the <b>Require Encryption Pass-Phrase at Boot-Time</b> check box is selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

*Table continues...*

| Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p><b>! Important:</b></p> <p>Remember the data encryption passphrase. If you lose the data encryption password, the only option to access Avaya Aura® Web Gateway is to reinstall the OVA.</p> <p>If the check box is not selected, Avaya Aura® Web Gateway creates a local key store, and you do not need to type the encryption passphrase when Avaya Aura® Web Gateway reboots. However, this makes the system less secure.</p> <p>You can also set up and use a remote key server to store encryption keys. To start using a remote key server, run the <b>sys encryptionRemoteKey</b> command after Avaya Aura® Web Gateway is installed. The remote key server provides more security than the local key store.</p> |

### Enhanced Access Security Gateway field descriptions

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EASG User Access</b> | <p>Use this option to enable or disable AVAYA remote access to your system.</p> <p>If you select 1, you enable EASG User Access, and AVAYA support engineers can log in to your system and help to resolve issues.</p> <p>For EASG User Access, you must also register Avaya Aura® Web Gateway and configure remote connectivity and alarming. For more information about EASG User Access, see the <a href="#">Avaya support site</a>.</p> <p>If you select 2, you disable EASG User Access, and AVAYA support engineers cannot log in to your system.</p> |

## Deploying the Avaya Aura® Web Gateway OVA using the Host Client connected directly to the ESXi host

### About this task

Use this procedure to deploy Avaya Aura® Web Gateway OVA on vCenter using the Host Client. This procedure also applies to deploying Avaya Aura® Web Gateway on Avaya Solutions Platform 130 or an equivalent server.

### Procedure

1. Log in to the Host Client at `https://<ESXI_HOST>/UI`.

In this URL, <ESXI\_HOST> is the IP address or FQDN of the ESXi host where you want to deploy your virtual machine.

2. Right-click the ESXi host and select **Create/Register VM**.

The Host Client displays the New Virtual Machine window.

3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK files page, do the following:
  - a. In **Name for the virtual machine**, type a name for the virtual machine.
  - b. In **Click to select files or drag/drop**, upload the OVA file to the Host Client.
  - c. Click **Next**.
6. On the Select storage page, select an appropriate data storage for your virtual machine and click **Next**.
7. On the License agreements page, do the following:
  - a. Read the End User License Agreement (EULA).
  - b. To accept the EULA, click **I agree**.
  - c. Click **Next**.
8. On the Deployment options page, do the following:
  - a. In **Network mappings**, select an appropriate network.
  - b. In **Deployment type**, select an Avaya Aura® Web Gateway profile that matches your deployment requirements.

 **Important:**

If you deploy the OVA for a non-seed node in a cluster, you must use the same resource profile that you used for the seed node.

For more information about resource profile specifications, see [Resource profile specifications for Avaya Aura Web Gateway on VMware](#) on page 29. The vSphere Client also displays basic system requirements for the profile below the field.

  - c. In **Disk provisioning**, select the appropriate disk format.

If you select the **Thick** option, the entire disk space required for the virtual machine is reserved and unavailable for other virtual machines to use. If you select the **Thin** option, unused space is available for other virtual machines.

  - d. Clear the **Power on automatically** check box.
  - e. Click **Next**.
9. On the Additional Settings page, keep the default values and click **Next**.
10. On the Ready to complete page, review the virtual machine settings and click **Finish**.
11. Wait until the virtual machine is deployed.

 **Important:**

Do not refresh the browser page while deployment is in progress.

12. To ensure that the virtual machine automatically starts after a hypervisor reboot, right-click your virtual machine and select **Autostart > Enable**.

If you do not enable autostart, you must manually start the virtual machine when the hypervisor reboots.

 **Note:**

You must enable the autostart functionality on the ESXi host for the virtual machine autostart to function.

13. To start the virtual machine, right-click the virtual machine and select **Power > Power On**.
14. Access the virtual machine console.
15. Follow the system prompts to configure the remaining OVA settings as appropriate.

You must configure data encryption settings, network settings, and Linux administration account settings.

 **Note:**

When configuring the Default Search List, ensure that the list includes the domains for:

- Avaya Aura® Web Gateway
- Avaya Meetings Server Management
- System Manager and LDAP

### Next steps

- Optionally, enable the Enhanced Access Security Gateway as described in [Enabling the Enhanced Access Security Gateway from the CLI](#) on page 62. The EASG functionality enables Avaya support personnel to access your Avaya Aura® Web Gateway system and resolve product issues in real-time. Avaya recommends that you enable EASG during installation.
- Install the Avaya Aura® Web Gateway application.

## Deploying the Avaya Aura® Web Gateway OVA through Solution Deployment Manager from System Manager

### About this task

Use this procedure to create a virtual machine on the ESXi host and deploy the Avaya Aura® Web Gateway OVA on the virtual machine. You can also use this procedure to deploy the Avaya Aura® Web Gateway OVA on Avaya Solutions Platform (ASP).

### Before you begin

- Ensure that you are familiar with the “Deployment checklist” section in *Deploying Avaya Aura® applications from System Manager*.
- Add ASP or an ESXi host to the location. For more information, see “Adding an Appliance Virtualization Platform or ESXi host” in *Deploying Avaya Aura® applications from System Manager*.

## Procedure

1. Upload the required OVA file to System Manager.

For information about uploading a file to the software library, see “Downloading the OVA file to System Manager” in *Deploying Avaya Aura® applications from System Manager*.

2. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

The system displays the VM Deployment window.

5. In the Select Location and Platform section, do the following:

- a. In **Select Location**, select a location.
- b. In **Select Platform**, select a platform.

The system displays the hostname in the **Platform FQDN** field.

6. In **Data Store**, select a data store.

7. Click **Next**.

8. On the OVA tab, do the following:

- a. In **Select Software Library**, select **Select OVA from software library**.
- b. In **Select Software Library**, select the local or remote library where the OVA file is located.
- c. In **Select OVAs**, select the OVA that you want to deploy.
- d. In **Flexi Footprint**, select the footprint size that the application supports.

9. On the Enhanced Access Security Gateway page, in **EASG User Access**, do one of the following:

- Select **1** to enable EASG. The EASG functionality enables Avaya support personnel to access your Avaya Aura® Web Gateway system and resolve product issues in real time. Avaya recommends that you enable EASG during installation.
- Select **2** to disable EASG.

If you select to disable EASG, you can enable it later from the Avaya Aura® Web Gateway CLI.

10. On the Configuration Parameters page, specify the following:

- Management network settings
- Public network settings
- Admin user details

11. On the Network Parameters page, choose any application.

12. Click **Deploy**.
13. Click **Accept the license terms**.

In the Hosts for Selected Location <location name> section, the system displays the deployment status in the Current Action Status column.

The system displays the virtual machine on the VMs for Selected Location <location name> page.

14. To view details, click **Status Details**.

## Enabling the Enhanced Access Security Gateway from the CLI

### 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.

### 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.

## Configuring UEFI Secure Boot for OVA-based virtual machines

### About this task

Unified Extensible Firmware Interface (UEFI) is an interface between the operating system and the platform firmware that replaces the legacy BIOS interface. Secure Boot is an UEFI feature that secures the operating system boot-up process by preventing the loading of boot loaders and drivers that are not signed with a trusted digital signature.

By default, Avaya Aura® Web Gateway Release 10.2.x OVA-based deployments have UEFI and Secure Boot enabled. For security reasons, Avaya recommends that you use Secure Boot whenever possible.

For more information about managing Secure Boot settings on VMware virtual machines, see [UEFI Secure Boot](#) in the VMware product documentation.

### Before you begin

Deploy a virtual machine.

## Procedure

1. Log in to the vSphere Client.
2. Navigate to a Avaya Aura® Web Gateway virtual machine.
3. Right-click the virtual machine and select **Edit Settings**.
4. Click the **VM Options** tab.
5. Click **Boot Options**.
6. Ensure that **Firmware** is set to **EFI (recommended)**.
7. Do one of the following:
  - To enable Secure Boot, select the **Secure Boot** check box.
  - To disable Secure Boot, clear the **Secure Boot** check box.
8. Click **OK**.

## Checking the UEFI Secure Boot status

### About this task

You can check whether the UEFI Secure Boot is enabled on a virtual machine.

### Procedure

1. Log in to a virtual machine using an SSH connection.
2. To check the status, run the following command:

```
mokutil --sb-state
```

- If the command output is `SecureBoot enabled`, UEFI Secure Boot is enabled.
- If the command output is `Failed to read SecureBoot`, UEFI Secure Boot is disabled.

## Enabling FIPS mode

### About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS compliance.

FIPS mode is enabled at the operating system level before starting the Avaya Aura® Web Gateway installation. If FIPS is enabled for the operating system, then Avaya Aura® Web Gateway will be installed in FIPS mode. Otherwise, Avaya Aura® Web Gateway will be installed in non-FIPS mode. FIPS installation is only supported for new installations. You cannot upgrade a non-FIPS system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Web Gateway application first, change FIPS mode, and then install Avaya Aura® Web Gateway.

**\* Note:**

- This procedure applies to OVA-based deployments. If you deploy Avaya Aura® Web Gateway as a software-only application, you must enable FIPS mode using the procedure for software-only deployments.
- If FIPS mode is enabled, you must use the Secure LDAP (LDAPS) protocol to configure LDAP.
- In cluster deployments, if FIPS mode is enabled, SSL encryption for internode communication between the database servers on the Avaya Aura® Web Gateway nodes is enabled by default.
- OAuth authorization is unavailable in FIPS mode.

## 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 FIPS mode:

```
sys seconfig --fips --enable
```

3. **(Optional)** To review the FIPS status, run the following command:

```
sys seconfig --fips --query
```

## Related links

[Enabling FIPS for software-only systems](#) on page 74

## Disabling FIPS mode

### About this task

After Avaya Aura® Web Gateway is installed with FIPS mode enabled, you *cannot* switch back to non-FIPS mode. You must uninstall the Avaya Aura® Web Gateway application layer first, disable FIPS mode, and then reinstall Avaya Aura® Web Gateway.

### Procedure

1. Uninstall Avaya Aura® Web Gateway.

For more information, see [Uninstalling the Avaya Aura Web Gateway](#) on page 95.

2. Run the following command:

```
sys seconfig --fips --disable
```

## 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.

**\* Note:**

After you enable additional STIG hardening, ensure that the length of the automatic backup password is at least 15 characters.

### 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 seconfig --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 seconfig --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 seconfig --stig --disable
```

3. **(Optional)** To review the STIG hardening status, run the following command:

```
sys seconfig --stig --query
```

---

## Software-only deployment in VMware-based virtualization environment

You can deploy Avaya Aura® Web Gateway as a software-only application using your own virtual or physical machines and Red Hat Enterprise Linux 8.10. For software-only deployments, Avaya Aura® Web Gateway supports the following VMware platforms:

- ESXi: Releases 6.7, 7.0 or later
- Avaya Solutions Platform (ASP)

The following section describes how to deploy and configure a virtual machine in a VMware environment for software-only deployments. After configuring a virtual machine, use the common

installation, configuration, and administration tasks to complete the Avaya Aura® Web Gateway deployment.

## Software-only installation checklist for VMware-based environment

The following checklist describes the high-level deployment steps that you must perform when deploying Avaya Aura® Web Gateway as a software-only application on your own physical servers or in VMware-based environment.

| No. | Task                                                                                                                                             | Notes                                                                                                                                                                                                                                                                                                                         | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that virtual machines that you plan to use to deploy Avaya Aura® Web Gateway comply with the requirements for software-only installation. | See the requirements in <a href="#">Software requirements</a> on page 28 and <a href="#">Resource profile specifications for Avaya Aura Web Gateway on VMware</a> on page 29.                                                                                                                                                 |   |
| 2   | Download the Avaya Aura® Web Gateway software-only installation package from PLDS.                                                               | <p>The software-only installation package includes the following files:</p> <ul style="list-style-type: none"> <li>• Software-only system layer installer.</li> <li>• Avaya Aura® Web Gateway application installer.</li> </ul> <p>The package file name has the <code>csa-swonly-&lt;AAWG_VERSION&gt;.tgz</code> format.</p> |   |
| 3   | Install Red Hat Enterprise Linux (RHEL) 8.10.                                                                                                    | Avaya Aura® Web Gateway Release 10.2.x requires RHEL 8.10. For more information about installation, see the official Red hat documentation. Avaya also recommends that you install the latest security updates on RHEL.                                                                                                       |   |
| 4   | Create disk partitioning on RHEL.                                                                                                                | Avaya Aura® Web Gateway requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see <a href="#">Creating disk partitioning for software-only deployments</a> on page 70 and <a href="#">Disk partitions for software-only deployments</a> on page 69.            |   |
| 5   | Create a non-root Linux user.                                                                                                                    | The installation and administration of the Avaya Aura® Web Gateway server is more secure when performed by non-root users with sudo privileges. For more information, see <a href="#">Creating an administrative user</a> on page 72.                                                                                         |   |

*Table continues...*

| No. | Task                                                                                                                                                                                                                                       | Notes                                                                                                                                                                                                                                                                                                                                              | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 6   | Enable the YUM package manager on RHEL.                                                                                                                                                                                                    | The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.                                                                                                                                                                                                      |   |
| 7   | Install additional packages required by Avaya Aura® Web Gateway.                                                                                                                                                                           | By default, RHEL 8.10 does not contain certain packages that Avaya Aura® Web Gateway requires. You must install these packages manually. For more information, see <a href="#">Additional packages required by Avaya Aura Web Gateway</a> on page 73 and <a href="#">Installing additional RHEL 8.4 or RHEL 8.10 packages manually</a> on page 73. |   |
| 8   | Enable the Haveged service.                                                                                                                                                                                                                | See <a href="#">Enabling the Haveged service</a> on page 74.                                                                                                                                                                                                                                                                                       |   |
| 9   | Optional: Enable FIPS mode.                                                                                                                                                                                                                | For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see <a href="#">Enabling FIPS for software-only systems</a> on page 74.                                                                                                                                 |   |
| 10  | Do one of the following to manage additional RHEL packages: <ul style="list-style-type: none"> <li>Register your RHEL instance to the Red Hat subscription.</li> <li>Create a local repository for RPM installation or updates.</li> </ul> | For more information, see <a href="#">RHEL packages management</a> on page 76.<br><br>Registering your RHEL instance to the Red Hat subscription is the preferred option.                                                                                                                                                                          |   |
| 11  | Install the software-only system layer on your RHEL.                                                                                                                                                                                       | The system layer is low-level software that forms the required operational environment for Avaya Aura® Web Gateway.<br><br>For more information, see <a href="#">Installing the system layer</a> on page 77.                                                                                                                                       |   |
| 12  | Ensure that: <ul style="list-style-type: none"> <li>Chrony service is up and running.</li> <li>System Manager is reachable from your virtual machine.</li> </ul>                                                                           | Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Web Gateway application.<br><br>For more information, see <a href="#">Checking the Chrony service status</a> on page 79 and <a href="#">Checking the connection to System Manager</a> on page 80.                                |   |

Table continues...

| No. | Task                                           | Notes                                                                                                                                                                                                                                                       | ✓ |
|-----|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 13  | Optional: Configure UEFI Secure Boot settings. | For security reasons, Avaya Aura® Web Gateway uses the UEFI Secure Boot feature by default. If required, you can configure the Secure Boot settings as described in <a href="#">Configuring UEFI Secure Boot for OVA-based virtual machines</a> on page 63. |   |

After deploying a virtual machine, install the Avaya Aura® Web Gateway application as described in the “Avaya Aura® Web Gateway setup” chapter.

## Red Hat Enterprise Linux installation

When you deploy Avaya Aura® Web Gateway as a software-only solution, you must use the RHEL 8.4 or RHEL 8.10. For details about obtaining and installing RHEL 8.4 or RHEL 8.10, see the Red Hat website <https://www.redhat.com>.

After obtaining RHEL 8.4 or RHEL 8.10, do the following:

1. Install the RHEL 8.4 or RHEL 8.10 operating system by using the Red Hat installation procedures.

### ! Important:

Avaya Aura® Web Gateway requires specific disk partitioning. You can create the required data disks and physical volumes for data disks during or after RHEL 8.4 or RHEL 8.10 installation using the values provided in [Disk partitions for software-only deployments](#) on page 69.

2. Install the latest critical security updates.

For update procedures, see Red Hat documentation. You can install security updates by using the YUM package manager.

## Disk partitions for software-only deployments

The following table shows Avaya Aura® Web Gateway disk partitions and their logical volumes with appropriate sizes:

| Disk                                                    | Disk size (GB) | Mount Point    |
|---------------------------------------------------------|----------------|----------------|
| Disk 1:<br>• /dev/sda for VMware<br>• /dev/xvda for AWS | 42             | —              |
| Disk 2:<br>• /dev/sdb for VMware<br>• /dev/xvdb for AWS | 60             | /var/log/Avaya |

*Table continues...*

| Disk                                                                                                                | Disk size (GB) | Mount Point      |
|---------------------------------------------------------------------------------------------------------------------|----------------|------------------|
| <b>Disk 3:</b> <ul style="list-style-type: none"> <li>• /dev/sdc for VMware</li> <li>• /dev/xvdc for AWS</li> </ul> | 20             | /media/data      |
| <b>Disk 4:</b> <ul style="list-style-type: none"> <li>• /dev/sdd for VMware</li> <li>• /dev/xvdd for AWS</li> </ul> | 10             | /media/cassandra |

## Creating disk partitioning for software-only deployments

### About this task

Avaya Aura® Web Gateway requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

### Before you begin

- Install RHEL.
- Create volumes with the required disk size values. For more information, see [Disk partitions for software-only deployments](#) on page 69.

### Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Run the following commands to create the required directories:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. If you are deploying Avaya Aura® Web Gateway in a virtual AWS environment that uses c5, c5a or c5n instances, run the following command to determine the name and size of each volume in your deployment:

```
lsblk
```

The following is an example of the command output:

```
[aawgadmin ~]$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme3n1             259:0   0   20G  0 disk
nvme2n1             259:1   0   60G  0 disk
nvme1n1             259:2   0   10G  0 disk
nvme0n1             259:3   0   42G  0 disk
-nvme0n1p1          259:4   0   42G  0 part /
-nvme0n1p128        259:5   0    1M  0 part
```

In this example, the RHEL volumes have the following names and sizes:

- /dev/nvme0n1: 42 Gb
- /dev/nvme1n1: 10 Gb

- /dev/nvme2n1: 60 Gb
- /dev/nvme3n1: 20 Gb

4. Depending on your virtual environment, do one of the following to create the required physical volumes and volume groups for these volumes:

- In a VMware virtual environment, run the following commands:

```
pvccreate -f /dev/sdb
vgcreate disk2_vg /dev/sdb
pvccreate -f /dev/sdc
vgcreate disk3_vg /dev/sdc
pvccreate -f /dev/sdd
vgcreate disk4_vg /dev/sdd
```

- In a virtual AWS environment that uses c4 instances, run the following commands:

```
pvccreate -f /dev/xvdb
vgcreate disk2_vg /dev/xvdb
pvccreate -f /dev/xvdc
vgcreate disk3_vg /dev/xvdc
pvccreate -f /dev/xvdd
vgcreate disk4_vg /dev/xvdd
```

- In a virtual AWS environment that uses either c5, c5a, or c5n instances, run the following commands:

```
pvccreate -f <name of 60 Gb volume>
vgcreate disk2_vg <name of 60 Gb volume>
pvccreate -f <name of 20 Gb volume>
vgcreate disk3_vg <name of 20 Gb volume>
pvccreate -f <name of 10 Gb volume>
vgcreate disk4_vg <name of 10 Gb volume>
```

For example:

```
pvccreate -f /dev/nvme2n1
vgcreate disk2_vg /dev/nvme2n1
pvccreate -f /dev/nvme3n1
vgcreate disk3_vg /dev/nvme3n1
pvccreate -f /dev/nvme1n1
vgcreate disk4_vg /dev/nvme1n1
```

5. Run the following commands to create logical volumes in the volume groups:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

6. Run the following commands to create a file system for the /dev/sdb partition and mount the file system:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

7. Run the following commands to create file systems for the /dev/sdc partition and mount the file system:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

8. Run the following commands to create file systems for the `/dev/sdd` partition and mount the file system:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

## Creating an administrative user

### About this task

You must use a non-root Linux user with sudo privileges to install the Avaya Aura® Web Gateway application. The User ID (UID) of the Linux user that performs the installation must be the same on all nodes in the cluster.

This procedure describes how to add a user and an administrative group. For a clustered deployment of Avaya Aura® Web Gateway, perform the steps described in this procedure on every node in the cluster.

### Important:

You must create only one administrative user on each virtual machine.

### Before you begin

Deploy RHEL 8.4 or RHEL 8.10 on virtual machines.

### Procedure

1. Log in to the virtual machine with deployed RHEL 8.4 or RHEL 8.10 as the root user using an SSH connection.
2. Run the following command to create a group for the administrative user:

```
groupadd -g 4001 <admin_group>
```

In this command, `<admin_group>` is one of the following:

- If you fresh install Release 10.2.x, this is a group name of your choice.
- If you migrate from a previous Avaya Aura® Web Gateway release, this is the same administrative group that you use in that release.

For example:

```
groupadd -g 4001 admingrp
```

### Important:

For Group ID (GID), you must use 4001.

3. Run the following command to add an administrative user in the new administrative group:

```
usermod -g <admin_group> -u 4001 <admin_name>
```

In this command, `<admin_group>` is the name of the group you created in the previous step, and `<admin_name>` is one of the following:

- If you fresh install Release 10.2.x, this is the name of the administrative user that you created when deploying the virtual machine.

- If you migrate from a previous Avaya Aura® Web Gateway release, this is the same administrative user that you use in that release.

For example:

```
usermod -g admingrp -u 4001 aawgadmin
```

### Important:

For User ID (UID), you must use 4001.

4. Run the following command to create a password for the new administrative user and then enter the password:

```
passwd <admin_name>
```

In this command, <admin\_name> is the administrative user name. For example:

```
passwd aawgadmin
```

5. Run the following command to provide sudo privileges for the new administrative user:

```
usermod -aG wheel <admin_name>
```

For example:

```
usermod -aG wheel aawgadmin
```

## Additional packages required by Avaya Aura® Web Gateway

In software-only deployments, Avaya Aura® Web Gateway requires certain packages that RHEL 8.4 or RHEL 8.10 does not include by default. You must manually install the following packages:

- haveged-1.9.14-1.el8.x86\_64.rpm or later.
- tomcat-native-1.2.23-1.el8.x86\_64.rpm or later. This package is only required if you want to use Avaya Aura® Web Gateway in FIPS mode.

These packages are available from the Extra Packages for Enterprise Linux (EPEL) Fedora Special Interest Group.

For information about installing packages from the EPEL repository see the [EPEL FAQ](#). You must only install these packages if you deploy Avaya Aura® Web Gateway as a software-only application.

## Installing additional RHEL 8.4 or RHEL 8.10 packages manually

### About this task

If you do not have the EPEL repository on your RHEL 8.4 or RHEL 8.10, you can install the additional packages required by Avaya Aura® Web Gateway manually.

### Before you begin

Download the appropriate package or packages on your local machine.

### Procedure

1. Log in to the virtual machine as the root user using an SSH connection.

2. Upload packages to the virtual machine to the `/root` directory.

Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

3. To install a package, run the following command:

```
rpm -ivh /root/<PACKAGE_NAME>
```

For example, to install Haveged package `haveged-1.9.14-1.el8.x86_64.rpm`, run the following command:

```
rpm -ivh /root/haveged-1.9.14-1.el8.x86_64.rpm
```

4. Repeat the previous step for all packages you need to install.

### Next steps

Enable the Haveged service on RHEL.

## Enabling the Haveged service

### About this task

Haveged is a random number generator based on the HAVEGE algorithm designed for the use on Linux systems.

This procedure applies to software-only deployments and is not required for OVA-based deployments.

### Before you begin

Install the Haveged package.

### Procedure

1. Log in to the virtual machine as an administrator using an SSH connection.
2. Run the following command to start the Haveged service:

```
systemctl start haveged
```

3. Run the following command to start Haveged automatically after each system restart:

```
systemctl enable haveged
```

## Enabling FIPS for software-only systems

### About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS-compliant cryptographic algorithms only.

For software-only installations, FIPS mode is enabled at the operating system level before installing the system layer. If FIPS is enabled in the operating system, Avaya Aura® Web Gateway are installed in FIPS mode. If not, they are installed in non-FIPS mode. FIPS installation is supported for new installations only. You cannot upgrade a non-FIPS system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Web Gateway application first, change FIPS mode, and then re-install Avaya Aura® Web Gateway.

**! Important:**

- You must enable FIPS before installing the system layer.
- OAuth authorization is unavailable in FIPS mode.

**\* Note:**

- If FIPS mode is enabled, use the Secure LDAP (LDAPS) protocol to configure LDAP.
- If FIPS mode is enabled in cluster deployments, SSL encryption for internode communication between the database servers on the Avaya Aura® Web Gateway nodes is enabled by default.

**Before you begin**

Download and install package `tomcat-native-1.2.23-1.el8.x86_64.rpm` or later.

**Procedure**

1. Log in to the virtual machine as the root user using an SSH connection.
2. Open the `/etc/ssh/sshd_config` file in a text editor.

For example, to open the file in `vi`, run the `vi /etc/ssh/sshd_config` command.

3. Add the following three entries to the file:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1
Kexalgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha1
```

4. Save the `/etc/ssh/sshd_config` file.
5. Open the `/etc/ssh/ssh_config` file in a text editor.

For example, to open the file in `vi`, run the `vi /etc/ssh/ssh_config` command.

6. Add the following two entries to the file:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256
```

7. Save the `/etc/ssh/ssh_config` file.
8. Open `/usr/share/crypto-policies/back-ends/FIPS/opensshserver.config` file in a text editor.
  - a. Remove the existing line.
  - b. Add the line: `CRYPTO_POLICY='-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr -oMACS=hmac-sha2-512,hmac-sha2-256'`.
9. Save `/usr/share/crypto-policies/back-ends/FIPS/opensshserver.config`.
10. Restart `sshd` service using `systemctl restart sshd`.
11. Complete the steps listed in the [Federal standards and regulations](#) section of the Red Hat documentation.

## Related links

[Enabling FIPS mode](#) on page 64

## RHEL packages management

The system layer requires additional RHEL packages, which are not available by default. To obtain these packages, you can do one of the following:

- Subscribe to the Red Hat subscription.

Avaya recommends this option. For more information about the subscription process, see the Red Hat website <https://www.redhat.com>.

### Important:

- If you use the Red Hat Network subscription, you must enable additional RPMs from the RHEL CLI as described in [Enabling required RHEL repositories](#) on page 76.
  - For AWS software-only deployments, if you use the Red Hat Network subscription, you must assign a public IP address to each of your AWS instances using the AWS Elastic IP service.
- Create a local repository for RPM installation or updates.

## Enabling required RHEL repositories

### About this task

If you subscribe to the Red Hat subscription, you must enable the following RHEL repositories before installing the system layer:

- rhel-8-for-x86\_64-baseos-rpms
- rhel-8-for-x86\_64-appstream-rpms

These repositories contain RPMs that are required for system layer installation.

### Before you begin

Subscribe to the Red Hat subscription.

### Procedure

1. Log in to the RHEL virtual machine as the root user using an SSH connection.
2. Run the following command to view the enabled repositories:

```
yum repolist
```

3. Ensure that the command output contains the following entries in the “repo id” column:

- rhel-8-for-x86\_64-baseos-rpms for rhel-8-for-x86\_64-baseos-rpms.
- rhel-8-for-x86\_64-appstream-rpms for rhel-8-for-x86\_64-appstream-rpms

4. If the command output does not contain the required entries, do the following:

- To enable the rhel-8-for-x86\_64-baseos-rpms repository, run the following command:

```
subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms
```

- To enable the rhel-8-for-x86\_64-appstream-rpms repository, run the following command:

```
subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms
```

## Installing the system layer

### About this task

The system layer is a low-level software that provides the required operational environment for the Avaya Aura® Web Gateway application.

During installation, the system downloads the required packages from the remote repository. The package installation might take up to 10 minutes depending on your network bandwidth.

### Before you begin

- Install RHEL 8.4 or RHEL 8.10 on virtual machines.
- Create disk partitioning for the virtual machine.
- Enable the YUM package management on RHEL. For more information, see Red Hat documentation on the <https://www.redhat.com> website.
- Create at least one non-root administrative user as described in [Creating an administrative user](#) on page 72.
- Download the `csa-swonly-<AAWG_VERSION>.tgz` software-only installation package from PLDS.
- Obtain the FQDN of the IP address of a Network Time Protocol (NTP) server.

The system will be in **Permissive** mode by default. When you install SELinux in the system, **Enforcing** mode is enabled in RHEL. You must change SELinux to enforcing mode to update the system layer.

- Verify if SELinux is enforcing.

```
# getenforce
```

- Open the file `/etc/selinux/config` in a text editor of your choice.

```
For example:# vi /etc/selinux/config
```

- Configure the **SELINUX=enforcing** option:

```
# This file controls the state of SELinux on the system.
```

```
# SELINUX= accepts one of the following values:
```

- `# enforcing` - SELinux security policy is enforced.
- `# permissive` - SELinux prints warnings instead of enforcing.
- `# disabled` - No SELinux policy is loaded.

- SELINUX=enforcing

- `# SELINUXTYPE=` can take one of these two values:
- `# targeted` - Targeted processes are protected

- # mls - Multi Level Security protection
- SELINUXTYPE=targeted
- Save the change, and restart the system:

```
# reboot
```

 **Note:**

Avaya recommends using the NTP servers of your organization instead of public NTP servers.

- If you are planning to use FIPS, enable it as described in [Enabling FIPS for software-only systems](#) on page 74. You cannot enable FIPS mode during or after Avaya Aura® Web Gateway installation.

## 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-3.9.0.0.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-1.0.0.0.1.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 system layer:

```
./swOnlyUpdate.sh --install
```

8. When the system prompts you to enable the Enhanced Access Security Gateway (EASG) functionality, do one of the following:
  - Enter `yes` to enable EASG.

The EASG functionality enables Avaya support personnel to access your Avaya Aura® Web Gateway system and resolve product issues in real time. Avaya recommends that you enable EASG during installation.

- Enter `no` if you do not want to enable the EASG functionality.

If you select `no`, you can enable it later if required.

9. When the system prompts you, provide the IP address or FQDN of the NTP server.
10. After the system reboots, run one of the following commands to ensure that system layer is installed:

- `sys versions`
- `/root/csa-swonly-<AAWG_RELEASE>/ucapp-swonly-system-<SYSTEM_LAYER_VERSION>/swOnlyUpdate.sh --status`

### Next steps

- Ensure that:
  - The Chrony service is running.
  - System Manager and Session Manager are reachable.
- Install the Avaya Aura® Web Gateway application.

## Checking the Chrony service status

### About this task

For the optimal functioning of the Avaya Aura® Web Gateway server, the local system clock must have an accuracy of 100 milliseconds or less. You must ensure that the Chrony service is running on the virtual machine before installing the Avaya Aura® Web Gateway application.

### Procedure

1. Log in to the virtual machine CLI as the root user using an SSH connection.
2. To verify that the Chrony service is running, run the following command:

```
systemctl status chronyd
```

Ensure that the system displays `active (running)`.

3. If the Chrony service is not running, run the following command:

```
systemctl start chronyd
```

4. To verify that the system clock is synchronized, run the following command:

```
ntpstat
```

5. Ensure that the system displays `synchronized to NTP server`.

## Checking the connection to System Manager

### About this task

You must ensure that System Manager is reachable before installing the Avaya Aura® Web Gateway application.

### Procedure

1. Log in to the virtual machine CLI as an administrator using an SSH connection.
2. Run the following command:

```
ping -c 10 <SMGR_ADDRESS>
```

In this command, <SMGR\_ADDRESS> is the FQDN of System Manager.

If System Manager is reachable, the system displays the following output for the command:

```
10 packets transmitted, 10 received, 0% packet loss
```

### Next steps

---

## Software-only deployment on Amazon Web Services

You can deploy Avaya Aura® Web Gateway as a software-only application using your own virtual or physical machines and Red Hat Enterprise Linux 8.10 in the Amazon Web Services virtual environment.

The following section describes how to deploy and configure a virtual machine in the Amazon Web Services environment for software-only deployments. After configuring a virtual machine, use the common installation, configuration, and administration tasks to complete the Avaya Aura® Web Gateway deployment.

## Software-only installation checklist for Amazon Web Services

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Web Gateway as a software-only application in an AWS environment.

| No. | Task                                                                                                                                                 | Notes                                                                                                                                                                                                                  | ✓ |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that the virtual machines that you plan to use to deploy Avaya Aura® Web Gateway comply with the requirements for software-only installation. | Avaya Aura® Web Gateway supports c4.xlarge and c4.2xlarge AWS instance types. For more information, see <a href="#">Resources profile specifications for Avaya Aura Web Gateway on Amazon Web Services</a> on page 30. |   |

*Table continues...*

| No. | Task                                                                               | Notes                                                                                                                                                                                                                                                                                                                         | ✓ |
|-----|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 2   | Prepare your AWS instance for software-only installation.                          | See <a href="#">Prerequisites for software-only deployment on AWS</a> on page 83.                                                                                                                                                                                                                                             |   |
| 3   | Download the Avaya Aura® Web Gateway software-only installation package from PLDS. | <p>The software-only installation package includes the following files:</p> <ul style="list-style-type: none"> <li>• Software-only system layer installer.</li> <li>• Avaya Aura® Web Gateway application installer.</li> </ul> <p>The package file name has the <code>csa-swonly-&lt;AAWG_VERSION&gt;.tgz</code> format.</p> |   |
| 4   | Create security groups on AWS.                                                     | See <a href="#">Creating security groups</a> on page 86.                                                                                                                                                                                                                                                                      |   |
| 5   | Install Red Hat Enterprise Linux (RHEL) 8.10 on AWS.                               | Avaya Aura® Web Gateway Release 10.2.x requires RHEL 8.10. For more information about installation, see <a href="#">Installing Red Hat Enterprise Linux 8.10 on AWS</a> on page 88.                                                                                                                                           |   |
| 6   | Create disk partitioning on RHEL.                                                  | Avaya Aura® Web Gateway requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see <a href="#">Creating disk partitioning for software-only deployments</a> on page 70 and <a href="#">Disk partitions for software-only deployments</a> on page 69.            |   |
| 7   | Enable root access to RHEL.                                                        | RHEL deployed on AWS does not have the root user enabled by default. For more information, see <a href="#">Enabling root access</a> on page 90.                                                                                                                                                                               |   |
| 8   | Create a non-root Linux user.                                                      | The installation and administration of the Avaya Aura® Web Gateway server is more secure when performed by non-root users with sudo privileges. For more information, see <a href="#">Creating an administrative user</a> on page 72.                                                                                         |   |
| 9   | Enable the YUM package manager on RHEL.                                            | The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation.                                                                                                                                                                                 |   |

*Table continues...*

| No. | Task                                                                                                                                                                                                                                       | Notes                                                                                                                                                                                                                                                                                                                                              | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 10  | Install additional packages required by Avaya Aura® Web Gateway.                                                                                                                                                                           | By default, RHEL 8.10 does not contain certain packages that Avaya Aura® Web Gateway requires. You must install these packages manually. For more information, see <a href="#">Additional packages required by Avaya Aura Web Gateway</a> on page 73 and <a href="#">Installing additional RHEL 8.4 or RHEL 8.10 packages manually</a> on page 73. |   |
| 11  | Enable the Haveged service.                                                                                                                                                                                                                | See <a href="#">Enabling the Haveged service</a> on page 74.                                                                                                                                                                                                                                                                                       |   |
| 12  | Optional: Enable FIPS mode.                                                                                                                                                                                                                | For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information about enabling FIPS, see <a href="#">Enabling FIPS for software-only systems</a> on page 74.                                                                                                                                 |   |
| 13  | Do one of the following to manage additional RHEL packages: <ul style="list-style-type: none"> <li>Register your RHEL instance to the Red Hat subscription.</li> <li>Create a local repository for RPM installation or updates.</li> </ul> | For more information, see <a href="#">RHEL packages management</a> on page 76.<br><br>Registering your RHEL instance to the Red Hat subscription is the preferred option.                                                                                                                                                                          |   |
| 14  | Prepare your RHEL system for installing the software-only system layer.                                                                                                                                                                    | See <a href="#">Prerequisites for installing the system layer on AWS</a> on page 90.                                                                                                                                                                                                                                                               |   |
| 15  | Install the software-only system layer on your RHEL.                                                                                                                                                                                       | The system layer is low-level software that forms the required operational environment for Avaya Aura® Web Gateway.<br><br>For more information, see <a href="#">Installing the system layer</a> on page 77.                                                                                                                                       |   |
| 16  | In cluster deployments, create target groups for the load balancer.                                                                                                                                                                        | See <a href="#">Creating target groups</a> on page 91.                                                                                                                                                                                                                                                                                             |   |
| 17  | In cluster deployments, configure Elastic load balancers.                                                                                                                                                                                  | See <a href="#">Creating and configuring Elastic load balancers</a> on page 92.                                                                                                                                                                                                                                                                    |   |
| 18  | Ensure that: <ul style="list-style-type: none"> <li>The Chrony service is up and running.</li> <li>System Manager is reachable from your virtual machine.</li> </ul>                                                                       | Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Web Gateway application.<br><br>For more information, see <a href="#">Checking the Chrony service status</a> on page 79 and <a href="#">Checking the connection to System Manager</a> on page 80.                                |   |

Table continues...

| No. | Task                                           | Notes                                                                                                                                                                                                                                                       | ✓ |
|-----|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 19  | Optional: Configure UEFI Secure Boot settings. | For security reasons, Avaya Aura® Web Gateway uses the UEFI Secure Boot feature by default. If required, you can configure the Secure Boot settings as described in <a href="#">Configuring UEFI Secure Boot for OVA-based virtual machines</a> on page 63. |   |

After deploying a virtual machine, install the Avaya Aura® Web Gateway application as described in the “Avaya Aura® Web Gateway setup” chapter.

## Prerequisites for software-only deployment on AWS

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud and subnet settings.
- Add records with the Avaya Aura® Web Gateway front-end FQDN to your DNS or AWS Route 53 hosted zone.
- Ensure that you have an NTP server. You can deploy your own NTP server or use the NTP server provided by AWS.
- Create key pairs. For more information, see [Creating a key pair](#) on page 83.
- If you are deploying an Avaya Aura® Web Gateway cluster, create load balancer certificates for the Avaya Aura® Web Gateway virtual FQDN.

For more information, see [Creating and applying load balancer certificates](#) on page 84.

## Creating a key pair

### About this task

A key pair consists of a public key and a private key. The public key encrypts data, such as login credentials, and the private key decrypts it. You provide the key pair when creating a CloudFormation stack and use it to access Amazon Machine Instances through SSH.

For more information, see the following website: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

The system generates a \*.pem file and prompts you to save the file to your computer. You can also view the key pair name in the Key pair name column.

6. Save the \*.pem file.

 **Important:**

When you create a key pair, save it. If you lose the key, you cannot retrieve it, and you cannot access the instance.

## Creating and applying load balancer certificates

### About this task

Load balancers only appear in the private DNS within AWS. Therefore, certificates generated by external certificate authorities might not work. Use this procedure to obtain a certificate from System Manager within AWS.

 **Important:**

Avaya recommends that you perform this procedure on the System Manager that you later connect to Avaya Aura® Device Services when installing the Avaya Aura® Device Services application. If you perform this procedure on another System Manager, you must import that System Manager CA to Avaya Aura® Device Services as described in “Managing truststore certificates” in *Administering Avaya Aura® Device Services*.

### Procedure

1. On the System Manager web console, navigate to **Home > Services > Security > Certificates > Authority**.
2. Click **Add End Entity** and complete the settings in the following fields:
  - a. **End Entity Profile:** Type `<INBOUND_OUTBOUND_TLS>`.
  - b. **Username:** Type `<FQDN of the load balancer>`.

The FQDN of the load balancer is the service FQDN of the cluster. This domain name portion of the FQDN represents the domain name that clients use to access service. The FQDN must be the combination of the stack name followed by the domain. For example, if the stack name is `yourStack` and the domain is `your.domain.com`, then the FQDN is `yourStack.your.domain.com`.

 **Note:**

The stack name must start with a letter and must contain only letters, numbers, or dashes. This stack name must be used during multi-node CloudFormation.

- c. **Password:** Type your password.
- d. **Confirm Password:** Retype your password.
- e. **CN, Common name:** Type `<FQDN of the load balancer>`.
- f. **Token:** Select the PEM file.

 **Note:**

The remaining fields are optional. For more information, see *Administering Avaya Aura® System Manager*.

3. Click **Add**.
4. Navigate to **Home > Services > Security > Certificates > Authority > Public Web**.  
The system displays the EJBCA public page.
5. Click **Create Keystore**.
6. In **Username**, type the FQDN of the load balancer.
7. In **Password**, type the End Entity password that you created earlier.
8. Click **OK**.

The system displays the EJBCA Token Certificate Enrollment page.

9. In **Key length**, select the required key length.  
A length of 2048 bits is recommended.
10. Click **Enroll** and select a text editor to view the certificate.
11. Save the PEM file to your computer.
12. Sign in to the AWS console and navigate to **Services > Security, Identity & Compliance > Certificate Manager**.
13. Click **Import a certificate**.  
The system displays a form with three fields: **Certificate Body**, **Certificate private key**, and **Certificate chain**.
14. Open the PEM file you saved earlier with a text editor and do the following:

 **Note:**

You must include the BEGIN and END labels for each section that you paste into the form.

- a. In the Private Key section, copy the string from -----BEGIN PRIVATE KEY----- to -----END PRIVATE KEY----- and paste it into the **Certificate private key** field.
  - b. In the Certificate section, copy the first certificate string from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE----- and paste it into the **Certificate body** field.
  - c. In the Certificate section, copy the second certificate string from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE----- and paste it into the **Certificate chain** field.
15. Click **Review and import**.

16. Click **Import**.

The system imports the certificate and displays the status and details of the certificate.

## 17. Copy and save the ARN value in the Details section.

The ARN is required for the **Load balancer certificate ARN** field during the multi-node CloudFormation deployment.

## Creating security groups

### About this task

AWS uses security groups to control inbound and outbound traffic. For software-only installation, you must create the following security groups:

- Avaya Aura® Web Gateway security group.

This security group uses the primary eth0 interface.

- Avaya Aura® Web Gateway load balance security group.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Security group**.

2. Click **Create Security Group**.

3. In **Security group name**, type a name of your choice.

For example: AAWG security group eth0

4. **(Optional)** In **Description**, type a description for the group.

5. From **VPC**, select the Virtual Private Cloud that you plan to use for Avaya Aura® Web Gateway.

6. Configure the inbound and outbound traffic rules for the group.

For more information, see the “Traffic rules” section for the appropriate group.

7. Repeat steps [2](#) on page 86 to [6](#) on page 86 to create the additional required security groups.

## Traffic rules for the Avaya Aura® Web Gateway security group

### Inbound rules

| Type       | Protocol | Port range | Source    |
|------------|----------|------------|-----------|
| Custom TCP | TCP      | 31415      | 0.0.0.0/0 |
| Custom TCP | TCP      | 8447       | 0.0.0.0/0 |
| Custom TCP | TCP      | 7001       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8468       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8543       | 0.0.0.0/0 |

*Table continues...*

| Type       | Protocol | Port range | Source    |
|------------|----------|------------|-----------|
| Custom TCP | TCP      | 7000       | 0.0.0.0/0 |
| HTTPS      | TCP      | 443        | 0.0.0.0/0 |
| Custom TCP | TCP      | 8457       | 0.0.0.0/0 |
| Custom TCP | TCP      | 3268       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8448       | 0.0.0.0/0 |
| Custom TCP | TCP      | 21000      | 0.0.0.0/0 |
| Custom TCP | TCP      | 9999       | 0.0.0.0/0 |
| SSH        | TCP      | 22         | 0.0.0.0/0 |
| Custom TCP | TCP      | 8440       | 0.0.0.0/0 |
| Custom TCP | TCP      | 2009       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8458       | 0.0.0.0/0 |
| Custom TCP | TCP      | 3269       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8445       | 0.0.0.0/0 |
| Custom TCP | UDP      | 161        | 0.0.0.0/0 |
| Custom TCP | TCP      | 8442       | 0.0.0.0/0 |

### Outbound rules

| Type        | Protocol | Port range | Source    |
|-------------|----------|------------|-----------|
| All traffic | All      | All        | 0.0.0.0/0 |
| All traffic | All      | All        | ::/0      |

## Traffic rules for the Avaya Aura® Web Gateway load balancer security group

### Inbound rules

| Type       | Protocol | Port range | Source    |
|------------|----------|------------|-----------|
| Custom TCP | TCP      | 8440       | 0.0.0.0/0 |
| Custom TCP | TCP      | 8443       | 0.0.0.0/0 |
| HTTPS      | TCP      | 443        | 0.0.0.0/0 |
| Custom TCP | TCP      | 8445       | 0.0.0.0/0 |

### Outbound rules

| Type        | Protocol | Port range | Source    |
|-------------|----------|------------|-----------|
| All traffic | All      | All        | 0.0.0.0/0 |
| All traffic | All      | All        | ::/0      |

## Installing Red Hat Enterprise Linux 8.10 on AWS

### About this task

Use this procedure to deploy the RHEL 8.10 operating system on your AWS instance. If you are deploying a cluster, repeat this procedure for each Avaya Aura® Web Gateway node.

### Before you begin

Create security groups.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2**.
2. Click **Launch instance**.
3. On the Choose an Amazon Machine Image page, in the left pane, click **Community AMIs** and then click the **Red Hat** check box.
4. From the list of operating systems, select **RHEL 8.10** and then click **Select**.

The following is an example of the RHEL 8.10 name: **RHEL-8.10\_HVM-GA-20211017-X86\_64-0-hOURLY2-gp2**

5. On the Choose an Instance Type page, select either the **c4.xlarge** or **c4.2xlarge** type depending on your deployment and then click **Next**.
6. On the Configure Instance Details page, configure the settings as follows:
  - a. In **Network**, select the VPC that you configured for your deployment.
  - b. In **Subnet**, select the subnet that you configured for your deployment.
  - c. In **Domain join directory**, select one of the following:
    - If you plan to use your own DNS server, select **No directory**.
    - If you plan to use the AWS Route 53 for DNS, select an appropriate domain from Route 53.
  - d. In the Network interfaces area, create the ethernet network interface with the `eth0` name and the IP address of the Avaya Aura® Web Gateway node.
  - e. For other parameters, keep the default values.
7. On the Add Storage page, create four EBS volumes using the values provided in [Disk partitions for software-only deployments](#) on page 69.

For **Volume type**, use **General Purpose SSD (gp2)** for all volumes.

The following image shows the configured volumes:

**Step 4: Add Storage**

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Volume Type ⓘ  | Device ⓘ  | Snapshot ⓘ             | Size (GiB) ⓘ | Volume Type ⓘ             | IOPS ⓘ     | Throughput (MB/s) ⓘ | Delete on Termination ⓘ             |
|----------------|-----------|------------------------|--------------|---------------------------|------------|---------------------|-------------------------------------|
| Root           | /dev/sda1 | snap-0f9a46653a138be40 | 125          | General Purpose SSD (gp2) | 375 / 3000 | N/A                 | <input checked="" type="checkbox"/> |
| EBS            | /dev/sdb  | Search (case-insensit  | 70           | General Purpose SSD (gp2) | 210 / 3000 | N/A                 | <input checked="" type="checkbox"/> |
| EBS            | /dev/sdc  | Search (case-insensit  | 40           | General Purpose SSD (gp2) | 120 / 3000 | N/A                 | <input checked="" type="checkbox"/> |
| EBS            | /dev/sdd  | Search (case-insensit  | 10           | General Purpose SSD (gp2) | 100 / 3000 | N/A                 | <input checked="" type="checkbox"/> |
| Add New Volume |           |                        |              |                           |            |                     |                                     |

8. **(Optional)** On the Add Tags page, add tags for the management instance and volumes.
9. On the Configure Security Group page, do the following:
  - a. In **Assign a security group**, select **Select an existing security group**.
  - b. Select the Avaya Aura® Web Gateway security group that you created when configuring security groups.
10. On the Review Instance Launch page, verify the instance settings and then click **Launch**.

**Next steps**

If you are using your own DNS server or a public DNS server, configure DNS settings as described in [Configuring DNS settings on RHEL](#) on page 89.

**Configuring DNS settings on RHEL****About this task**

If you do not use the Route 53 DNS service, you must provide the IP address of a DNS server that you plan to use on RHEL.

**Before you begin**

Install RHEL on AWS.

**Procedure**

1. Log in to the RHEL as the root user using an SSH connection.
2. Open the `/etc/resolv.conf` file in a text editor.

For example: `vi /etc/resolv.conf`

3. Add the following entry to the file:

```
nameserver <DNS_ADDRESS>
```

In this entry, `<DNS_ADDRESS>` is the IP address of the DNS server that you plan to use in your deployment.

4. **(Optional)** Do one of the following:

- If the file does not contain the `search` entry, add the following entry:

```
search <DOMAIN_NAME>
```

In this entry, `<DOMAIN_NAME>` is your domain name. For example: `search mycompany.com`

- If the file contains the `search` entry, enter your domain name at the end of the entry.

Domain names must be separated with space characters. For example: `search example.com mydomain.com`

5. Save the file.

## Enabling root access

### About this task

You must use the root user to install the system layer. On RHEL installed on AWS, the root user is disabled by default, therefore you must enable it.

### Procedure

1. Log in to your AWS instance using the AWS CLI as the `ec2-user`.  
This is the default administration user, which does not require a login password.
2. Run the following command to edit the `/etc/ssh/sshd_config` file:  

```
sudo vi /etc/ssh/sshd_config
```
3. Add the following line to the file:  

```
PermitRootLogin yes
```
4. Save the file.
5. Run the following command to apply the changes:  

```
sudo service sshd restart
```
6. Set a password for the root user using the following command:  

```
sudo passwd root
```

## Prerequisites for installing the system layer on AWS

In addition to the prerequisites for the software-only system layer installation that are common for all deployment types, AWS has the following specific prerequisites:

- Ensure that you configured the Avaya Aura® Web Gateway front-end FQDN in the AWS Route 53 service or the DNS service that you use.
- On all Avaya Aura® Web Gateway nodes in your deployment, add information about each Avaya Aura® Web Gateway node to the `/etc/hosts` file in the following format:

`<IP_Address> <Corresponding_FQDN> <hostname>`

For example:

```
195.51.100.5 aawg1.mycompany.com aawg1
195.51.100.6 aawg2.mycompany.com aawg2
```

- Enable root access to RHEL. For more information, see [Enabling root access](#) on page 90.
- Create a non-root user on RHEL. For more information, see [Creating an administrative user](#) on page 72.
- If you are using a Red Hat subscription for RHEL package management, you must configure a public IP address on each of your AWS instances using the AWS Elastic IP service. For more information about setting up public IP addresses, see [Elastic IP addresses](#).

## Creating target groups

### About this task

In cluster deployments, target groups forward traffic from the load balancer to a specific node of the Avaya Aura® Web Gateway cluster when certain conditions are met.

You must configure two target groups for Avaya Aura® Web Gateway node IP addresses with the following parameters:

| Group                                             | Protocol | Port | IP to register                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|----------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target group for Avaya Aura® Web Gateway nodes #1 | HTTPS    | 8448 | IP addresses of all Avaya Aura® Web Gateway nodes in the cluster.<br><br>These are the IP addresses of the primary eth0 interface of cluster nodes.<br><br>On the Avaya Aura® Web Gateway administration portal, you <i>must</i> enable the use of an external load balancer. For details, see <i>Administering the Avaya Aura® Web Gateway</i> . |
| Target group for Avaya Aura® Web Gateway nodes #2 | HTTPS    | 8445 | IP addresses of all Avaya Aura® Web Gateway nodes in the cluster.<br><br>These are the IP addresses of the primary eth0 interface of cluster nodes.                                                                                                                                                                                               |

Only perform this procedure if you have an Avaya Aura® Web Gateway cluster.

### Procedure

Repeat the following steps for each target group:

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Target Groups**.
2. Click **Create target group**.

The Amazon Web Services Management displays the Specify group details page.

3. In the Basic configuration area, configure settings as follows:
  - a. In **Choose a target type**, select **IP addresses**.
  - b. In **Target group name**, type a name of your choice for the group.
  - c. In **Protocol**, select the protocol specified for the group in the “Protocol” column of the table.

- d. In **Port**, type the port number specified for the group in the “Port” column of the table.
  - e. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
  - f. In **Protocol version**, select **HTTP1**.
4. In the Health checks area, configure the settings as follows:
  - a. In **Health check protocol**, select **HTTP**.
  - b. In **Health check path**, type `/health`.
5. Click **Next**.
6. On the Register targets page, configure IP addresses for the group as follows:
  - a. In **IP**, type the IP address of a node as specified in the “IP to register” column of the table for the group you are configuring.
  - b. In **Port**, type the port number specified for the group in the “Port” column of the table.
  - c. Click **Include as pending below**.
  - d. Repeat substeps a to c for all remaining IP addresses that you must include in the group.
7. Click **Create target group**.
8. After creating all target groups, do the following:
  - a. Navigate to **Services > EC2 > Target Groups** and select the target group that you have created.
  - b. Select the target group for port 8445 that you have just created.
  - c. In the Attributes area, click **Edit**.
  - d. On the Edit attributes page, select the **Stickiness** check box.
  - e. Click **Save changes**.

## Creating and configuring Elastic load balancers

### About this task

The Elastic load balancer distributes incoming traffic between Avaya Aura® Web Gateway nodes. In cluster deployments, you must create one Elastic load balancer for Avaya Aura® Web Gateway nodes.

### Before you begin

- Create two target groups as described in [Creating target groups](#) on page 91.
- Ensure that you have the load balancer certificates for the Avaya Aura® Web Gateway front-end FQDN. For more information about creating certificates, see [Creating and applying load balancer certificates](#) on page 84.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services > EC2 > Load Balancers**.

2. Click **Create Load Balancer**.
3. On the Configure Load Balancer page, configure the settings as follows:
  - a. In **Name**, type a name of your choice.
  - b. In **Scheme**, select **Internal**.
  - c. In **IP address type**, select **ipv4**.
  - d. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
  - e. In **Listener**, add listeners for the load balancer as follows:

| Load balancer                         | Protocol | Port |
|---------------------------------------|----------|------|
| Avaya Aura® Web Gateway load balancer | HTTPS    | 443  |
|                                       | HTTPS    | 8440 |
|                                       | HTTPS    | 8443 |
|                                       | HTTPS    | 8445 |

- f. In **Availability Zones**, select the subnet that you configured for all nodes in the cluster.
4. On the Configure Security Settings page, in **Certificate Type**, select **Choose a certificate from ACM** and then select the certificates that you prepared for the Avaya Aura® Web Gateway FQDN.
5. On the Configure Security Groups page, in **Assign a security group**, select **Select an existing security group** and then select the Avaya Aura® Web Gateway load balancer security group that you created.

For more information about security groups, see [Creating security groups](#) on page 86.

6. On the Configure Routing page, configure routing as follows:
  - a. In **Target**, select **Existing target group**.
  - b. In **Name**, select the target groups related to Avaya Aura® Web Gateway nodes.

For more information about the target groups, see [Creating target groups](#) on page 91.

7. On the **Register Targets** page, click **Next: Review**.
8. Click **Create**.
- 9.
10. On the Amazon Web Services Management console, navigate to **Services > EC2 > Load Balancers**.
11. Click **Create Application Load Balancer**.
12. On the Configure Load Balancer page, configure the settings as follows:
  - a. In **Name**, type a name of your choice.
  - b. In **Scheme**, select **Internal**.

- c. In **IP address type**, select **ipv4**.
- d. In **Listener**, add listeners for the balancer as follows:

| Load balancer                         | Protocol | Port |
|---------------------------------------|----------|------|
| Avaya Aura® Web Gateway load balancer | HTTPS    | 443  |
|                                       | HTTPS    | 8440 |
|                                       | HTTPS    | 8443 |
|                                       | HTTPS    | 8445 |

- e. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
  - f. In **Availability Zones**, select the subnet that you configured for all nodes in the cluster.
13. On the Configure Security Settings page, do the following:
    - a. In **Certificate Type**, select **Choose a certificate from ACM** and then select the certificates that you prepared for the Avaya Aura® Web Gateway FQDN.
    - b. In **Security Policy**, select **ELBSecurityPolicy-TLS-1-2-2017-01**.
  14. On the Configure Security Groups page, in **Assign a security group**, select **Select an existing security group** and then select the Avaya Aura® Web Gateway load balancer security group that you created.

For more information about security groups, see [Creating security groups](#) on page 86.

15. On the Configure Routing page, configure routing as follows:
  - a. In **Target**, select **Existing target group**.
  - b. In **Name**, select the target group for Avaya Aura® Web Gateway nodes for port 8448.  
In [Creating target groups](#) on page 91, this is the “Target group for Avaya Aura® Web Gateway nodes #1” group.
16. On the **Register Targets** page, click **Next: Review**.
17. Click **Create**.
18. On the Load Balancers page, select the load balancer for Avaya Aura® Web Gateway nodes that you have just created and then do the following:

- a. In the Listeners table, select a listener with the “HTTPS : 8445” listener ID and then click **Edit**.

Amazon Web Services displays the Settings page for the listener.

- b. In Default Actions, click the **Edit** icon for the “Forward to” action.
- c. In **Select a target group**, select the target group for Avaya Aura® Web Gateway nodes for port 8445.

In [Creating target groups](#) on page 91, this is the “Target group for Avaya Aura® Web Gateway nodes #2” group.

- d. Click **Update**.

## Configuring idle timeout

### About this task

By default, the AWS environment sets the idle timeout for the Elastic load balancer to 60 seconds. Set this value to 150 seconds to provide Avaya Aura® Web Gateway enough time for cluster wide operations like generating certificates, collecting logs, and restarting services.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Load Balancers**.
2. Select the created load balancer.
3. On the **Destination** tab, click **Edit idle timeout**.
4. In **Idle timeout**, enter 150.
5. Click **Save**.

---

## Uninstalling the Avaya Aura® Web Gateway

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. To remove the Avaya Aura® Web Gateway from the system, run the following command:

```
app uninstall
```

3. When prompted, type the following:
  - a. **uninstall** and press **Enter**.
  - b. **yes** and press **Enter**.

## Removing a non-initial node from the cluster if the node is unavailable

### About this task

Use this procedure to remove an unavailable non-initial cluster node, which cannot be removed using the standard node uninstallation procedure. For example, use this procedure if you cannot log in to the node using an SSH connection or if the Cassandra service is not running on the node.

Do not use this procedure to remove the initial cluster node.

**! Important:**

After performing this procedure, do *not* start the removed node. If you start the node, it will re-appear in the list of cluster nodes.

**Before you begin**

Enable EASG functionality. EASG is required to obtain the sroot privileges, which you must use to perform commands in this procedure.

**Procedure**

1. If the virtual machine with the node that you want to remove is still running, stop the virtual machine.
2. Log in to the initial node as an administrator using an SSH connection.
3. Run the following command to obtain the sroot privileges:

```
su - sroot
```

4. Run the following commands:

```
cdto cassandra
cd bin
```

5. Run the following command to obtain the UUID of the unavailable node in the Cassandra cluster:

```
./nodetool status
```

The unavailable node has the “DN” status. The node UUID is displayed in the Host ID column. The following is an example of the command output:

```
[root@aawg bin]$ ./nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load          Tokens         Owns (effective)  Host
ID
UN  233.252.0.2   5.07 MiB      256            100.0%            d1e8b3dc-
f116-4bbc-851d-122c9e400bc3 rack1
DN  233.252.0.3   5.07 MiB      256            100.0%            e2e779ae-
d34d-2a10-23de-5ac14c4af783 rack1
UN  233.252.0.4   5.07 MiB      256            100.0%
12cc1379-5164-8e74-81c0-bc8da8d09341 rack1
```

In this example, the unavailable node has UUID e2e779ae-d34d-2a10-23de-5ac14c4af783.

6. Run the following command:

```
./nodetool removenode <UUID>
```

In this command, UUID is the UUID of the unavailable Cassandra database node. For example:

```
./nodetool removenode e2e779ae-d34d-2a10-23de-5ac14c4af783
```

7. Run the `./nodetool status` command again and ensure that the Cassandra cluster does not contain the unavailable node.

8. Run the following command:

```
cdto misc
```

9. Run the following command to obtain the UUID of the unavailable Avaya Aura® Web Gateway node:

```
app listnodes
```

The unavailable node has the “down” status. The node UUID is displayed in the Server identifier column. The following is an example of the command output:

```
[root@aawg misc]$ app listnodes
Node IP address      Status  Server identifier      Singleton  Version
233.252.0.2          live    2523a75a-11a2-45ff-ba39-e23af17c316d  master
3.11.0.0
233.252.0.3          down    3edfc879-b374-1c12-a045-a1456cfc277a
3.11.0.0
233.252.0.4          live    6e430dff-7411-f2c4-9a5a-beec23916707
3.11.0.0
```

In this example, the unavailable node has UUID 3edfc879-b374-1c12-a045-a1456cfc277a.

10. Run the following command:

```
./clitool-csa.sh removeClusterNode <UUID>
```

In this command, UUID is the UUID of the unavailable Avaya Aura® Web Gateway node. For example:

```
./clitool-csa.sh removeClusterNode 3edfc879-b374-1c12-a045-a1456cfc277a
```

11. Run the `app listnodes` command again and ensure that the Avaya Aura® Web Gateway cluster does not contain the node.

## Related links

[A node removed from the Cassandra cluster has the “live” status in the app listnodes output on page 186](#)

# Chapter 6: Avaya Aura® Web Gateway setup

---

## Avaya Aura® Web Gateway installation checklist

The following checklist describes the high-level deployment steps you must perform to the Avaya Aura® Web Gateway application on virtual machines:

| No. | Task                                                                                                              | Notes                                                                                                                                                                                                                                                                                                                                            | ✓ |
|-----|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Install or restore the application layer as required.                                                             | For information about installing standalone Avaya Aura® Web Gateway or the initial node for an Avaya Aura® Web Gateway cluster, see <a href="#">Installing the Avaya Aura Web Gateway</a> on page 98.<br><br>For information about installing additional nodes, see <a href="#">Installing additional nodes to create a cluster</a> on page 104. |   |
| 2   | If you are installing a cluster, configure RSA keys for SSH connections after all additional nodes are installed. | See <a href="#">Configuring RSA public and private keys for SSH connections in a cluster</a> on page 107.                                                                                                                                                                                                                                        |   |
| 3   | Change the default Cassandra database password.                                                                   | See <a href="#">Changing the Cassandra user name and password</a> on page 130.                                                                                                                                                                                                                                                                   |   |
| 4   | Change the default password for automatic backups.                                                                | See <a href="#">Changing the default password for automatic backups</a> on page 131.                                                                                                                                                                                                                                                             |   |

---

## Installing the Avaya Aura® Web Gateway

### About this task

Use this procedure to install a standalone Avaya Aura® Web Gateway or the initial node for an Avaya Aura® Web Gateway cluster.

**! Important:**

Do not use this procedure to install additional nodes to a cluster. For more information on installing additional nodes, see [Installing additional nodes to create a cluster](#) on page 104.

**Before you begin**

- Deploy the Avaya Aura® Web Gateway OVA.
- Start the virtual machine.
- If you are planning to use FIPS, enable it as described in [Enabling FIPS mode](#) on page 64. You *cannot* enable FIPS mode during or after Avaya Aura® Web Gateway installation. You cannot use the OAuth authentication feature when FIPS mode is enabled.

**Procedure**

1. Open the Linux shell using your Linux administrator account credentials.

The Linux administrator account is created during the deployment process.

2. Do one of the following:

- If you install Avaya Aura® Web Gateway using the OVA, run the following command:

```
app install
```

When you run the `app install` command without specifying a build, then the system automatically picks up the current build in `opt/Avaya`. If you do specify a build by running `app install csa-<version>.bin`, then the system looks for that build first in your current working directory and then in `opt/Avaya`.

- If you install Avaya Aura® Web Gateway as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, `<PATH>` is the full path to the directory where you extracted the application binary when installing the system layer, and `<INSTALLER>` is the Avaya Aura® Web Gateway application binary. For example:

```
app install /root/csa-swonly-10.1.0.0/csa-10.1.0.0.bin
```

The system displays the installation screen.

**! Important:**

During the installation, do not resize the screen or the SSH console.

3. If you are installing the initial node for a new cluster, then do the following:

- a. Select **Cluster Configuration**.
- b. Ensure that **Initial cluster node** is set to `y` (yes) and **Local Node IP address** is set to the IP address of the node.

These are the default values.

To return to the previous menu, select **Return to Main Menu** and press `Enter`.

- c. **(Optional)** In the **Cassandra Encryption** menu, enable SSL encryption to secure Cassandra database communications between nodes in a cluster.

 **Important:**

- If you want to enable Cassandra internode encryption, you must enable it during the initial installation. This setting cannot be changed after the initial installation.
- If you enabled FIPS mode, ensure that Cassandra internode encryption remains enabled. If you disable Cassandra internode encryption, installation will fail.

4. Select **Front-end host, System Manager and Certificate Configuration** and do the following:

- a. For a standalone node, select **Front-end IP or FQDN** and enter the FQDN that clients use to access services.

The default value is the FQDN assigned to the local server.

For a cluster deployment that uses the internal load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the virtual IP address of the internal load balancer.

For a cluster deployment that uses an external load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the external load balancer.

- b. Select **System Manager FQDN** and enter the FQDN of the Avaya Aura® System Manager that signs the certificates for Avaya Aura® Web Gateway services.
- c. **(Optional)** Select **System Manager web admin username (o)** and **System Manager web admin password** and provide the credentials.
- d. Select **System Manager HTTPS Port** and type the port for contacting the REST interface of Avaya Aura® System Manager.

The default port is 443.

- e. Select **System Manager Enrollment Password** and type the Avaya Aura® System Manager enrollment password.
- f. Select **Keystore password** and type a password to use for the local keystore.

 **Important:**

You must remember the Keystore password for future references. You need this password for any certificate management tasks.

- g. Configure additional settings that are required for your system as described in [Front-end host, System Manager, and certificate configuration](#) on page 109.

To return to the previous menu, select **Return to Main Menu** and press `Enter`.

5. Select **Deployment settings** and then press the `Spacebar` to select the deployment option that corresponds to the solution that you are installing.

If you have conferencing in your solution, then select **Team Engagement + Conferencing**. Otherwise, you must select **Team Engagement**. Do not select **Conferencing only**.

6. To review the settings, select **Continue** and then select **Accept and continue**.

The system runs pre-install configuration checks.

7. To install the software, select **Continue** and then accept the license agreement.

Wait for several minutes while the installation proceeds.

8. Select **Continue** to start the configuration utility.

 **Important:**

Do not change the settings in **Front-end host, System Manager and Certificate Configuration** without reentering the System Manager enrollment and keystore passwords before applying the changes.

9. Select **LDAP Configuration**, and then configure each of the LDAP settings using the LDAP configuration information for your network.

For more information on LDAP configuration, see [LDAP configuration](#) on page 112.

10. **(Optional)** If this is an initial node for a cluster, and you want to use internal load balancing, do the following:

 **Important:**

- The virtual IP address is used for redundancy management of the internal load balancer in a cluster.
- To avoid performance degradation of the cluster, an external load balancer is recommended for clusters with four or more nodes.
- For a cluster deployment that uses an external load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the external load balancer.
- If you use an external load balancer, do not configure the virtual IP settings that enable the internal load balancer.

- a. Select **Clustering Configuration > Virtual IP Configuration**.

- b. Select **Enable virtual IP** and set the value to **y** (yes).

The system displays additional Virtual IP configuration.

- c. Configure all of the Virtual IP settings as described in [Virtual IP configuration options](#) on page 128.

You must configure the initial node as the Virtual IP master node. In a cluster, you must configure one additional node as the Virtual IP backup node.

 **Important:**

You must save the Virtual IP authentication password. You need this password when configuring the second node in the cluster as the virtual IP backup node.

- d. To save the changes on the system, select **Apply** and then select **Continue**.
  - e. Select **Return to Main Menu** and press `Enter`.
11. To apply the changes, from the main menu, select **Continue** and then select **Yes** to start the services.
- The system starts the services.
12. To exit the configuration tool, select **Continue**.

### Next steps

- Set up the required certificates as described in [Certificate configuration using the configuration utility](#) on page 192.
- Install additional nodes to create a cluster.
- Change the following default passwords:
  - The default Cassandra database password as described in [Changing the Cassandra user name and password](#) on page 130. If you install a cluster, install all required additional nodes before changing the password.
  - The default password for automatic backups. For more information, see [Changing the default password for automatic backups](#) on page 131.

### Related links

[Unexpected characters in the /etc/hosts file on a localhost line](#) on page 185

---

## Performing a silent installation

### About this task

Use this procedure to perform a silent installation of the Avaya Aura® Web Gateway server.

The silent installation consists of configuring most of the settings in a properties file, instead of using the installation and the configuration menu for every item.

The properties file is called `installation.properties`. It contains the same settings that you configure during the interactive installation. The settings are grouped, and the file contains comments that describe the settings.

#### **Note:**

The properties file does not contain settings for the following elements:

- The Avaya Aura® Web Gateway cluster
- The SSH RSA configuration

You must configure these settings using the configuration utility after the silent installation is complete.

If errors occur after the installation, you can use the configuration utility to re-configure some of the settings.

## Procedure

1. From the Avaya Aura® Web Gateway binary file, extract the template file.

```
./csa-<version>.bin --tar xf -- ./installation.properties
```

2. Configure the settings in the `installation.properties` file.

The settings are the same as the interactive installation. For more information about the settings, see [Avaya Aura Web Gateway initial configuration settings](#) on page 108.

You can leave some of the settings blank and then configure them manually after the installation is complete.

3. Run the Avaya Aura® Web Gateway binary with a parameter that represents the full path to the properties file.

For example:

```
app install /home/avaya/installation.properties
```

4. **(Optional)** To start the Avaya Aura® Web Gateway service, run the following command:

```
svc csa start
```

5. Manually configure the remaining items.

When possible, use the web administration portal to modify configuration settings instead of the configuration utility. For more information about using the web administration portal, see *Administering the Avaya Aura® Web Gateway*.

## Seed node replacement configuration

If a seed node is unavailable, you might experience service loss on an Avaya Aura® Web Gateway cluster. You will also be unavailable to install a new node on the cluster. To prevent this issue from occurring, you can specify a list of backup nodes for the seed node while performing silent installation. If the initial seed node becomes unavailable, Cassandra replaces it with a node from the backup nodes list, so the cluster continues to operate. When you add a new node, Cassandra checks whether the initial seed node is available. If not, Cassandra tries to connect the new node to one of backup nodes.

### Important:

You cannot configure backup nodes using the standard, interactive installation process.

Specify backup nodes in the `SEED_NODE_BACKUP` property of the `installation.properties` file. The value of this parameter is a list of IP addresses separated by commas. For example: `SEED_NODE_BACKUP=192.168.150.3,192.168.150.4`. If the seed node is unavailable, Cassandra tries to replace it with a node listed in `SEED_NODE_BACKUP` in the order specified in the property. On Avaya Aura® Web Gateway, you can review the seed nodes configuration in the `/opt/Avaya/CallSignallingAgent/<version>/cassandra/<version>/conf/cassandra.yaml` file.

## Related links

[Installing additional nodes to create a cluster](#) on page 104

---

## Installing additional nodes to create a cluster

### About this task

You can achieve redundancy and increase capacity by creating a cluster of Avaya Aura® Web Gateway nodes.

The installation procedure for each additional node is similar to the procedure for a single-server or initial node installation, with the addition of some cluster specific configuration. After installing an initial node, use this procedure to create a cluster of Avaya Aura® Web Gateway nodes. You can also use this procedure to add nodes to an existing cluster at a later time.

The virtual IP address and the IP addresses for all nodes of the cluster must be in the same network.

### ! Important:

- When creating or expanding a cluster, for each additional Avaya Aura® Web Gateway node you must use the same resource profile that you used for the initial node. Mixed resource profile clusters are not supported. The resource profiles are set when installing the Avaya Aura® Web Gateway OVA and cannot be modified after the OVA is deployed.
- To avoid performance degradation of the cluster, an external load balancer is recommended for clusters with four or more nodes.

### Before you begin

- Install an initial Avaya Aura® Web Gateway node. For more information, see [Installing the Avaya Aura Web Gateway](#) on page 98.
- Enable the virtual IP configuration on the initial node if you are using the internal load balancer for the cluster.
- Configure the front-end FQDN on the initial node to match the FQDN assigned to the load balancer. If you need to update the front-end FQDN on the initial node, use the configuration utility.
- Deploy a virtual machine on the same network as the initial node for each additional node required. For more information, see the procedures for the appropriate deployment type in [Initial setup](#) on page 50.

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.

The Linux administrator account is created during the deployment process.

2. Do one of the following:

- If you install Avaya Aura® Web Gateway using the OVA, run the following command:

```
app install
```

When you run the `app install` command without specifying a build, then the system automatically picks up the current build in `opt/Avaya`. If you do specify a build by running `app install csa-<version>.bin`, then the system looks for that build first in your current working directory and then in `opt/Avaya`.

- If you install Avaya Aura® Web Gateway as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, <PATH> is the full path to the directory where you extracted the application binary when installing the system layer, and <INSTALLER> is the Avaya Aura® Web Gateway application binary. For example:

```
app install /root/csa-swonly-10.1.0.0/csa-10.1.0.0.bin
```

The system displays the installation screen.

 **Important:**

During the installation, do not resize the screen or the SSH console.

3. Select **Cluster Configuration** and do the following:
  - a. Set the **Initial cluster node** option to `n` (no).
  - b. Ensure that **Local Node IP address** is set to the IP address of the current node.
  - c. Set **Cluster seed node** to the IP address of the initial node.
  - d. Set **User ID (UID) of product user on seed node** to the user ID of the Linux administrator that was used to install the initial Avaya Aura® Web Gateway node.  
The default value is 4000.  
To determine the required UID, open the Linux shell on the initial node using your administrator credentials and then run the following command:
 

```
id -u <adminuser>
```
  - e. To save the changes on the system, select **Apply** and then select **Continue**.
  - f. Select **Return to Main Menu** and press `Enter`.
4. In the **Cassandra Encryption** menu, enable SSL encryption to secure Cassandra database communications between nodes in a cluster.

 **Important:**

- If you want to enable Cassandra internode encryption, you must do so during the initial installation. This setting cannot be changed after the initial installation.
  - If you enabled FIPS mode, ensure that Cassandra internode encryption remains enabled. If you disable Cassandra internode encryption, installation will fail.
5. Select **Front-end host, System Manager and Certificate Configuration** and do the following:
    - a. Select **System Manager FQDN** and enter the FQDN of the Avaya Aura® System Manager that signs the certificates for Avaya Aura® Web Gateway services.
    - b. **(Optional)** Select **System Manager web admin username (o)** and **System Manager web admin password** and provide the credentials.

- c. Select **System Manager HTTPS Port** and type the port for contacting Avaya Aura® System Manager.

The default port is 443.

- d. Select **System Manager Enrollment Password** and type the Avaya Aura® System Manager enrollment password.

- e. Select **Keystore password** and type a password for using the local keystore.

The keystore password on additional nodes should match the keystore password for the initial node.

 **Important:**

You must remember the keystore password for future reference. You need this password for other certificate management tasks.

- f. Configure additional settings that are required for your system as described in [Front-end host, System Manager, and certificate configuration](#) on page 109.

To return to the previous menu, select **Return to Main Menu** and press `Enter`.

6. Select **Deployment settings** and then press the `Spacebar` to select the deployment option that corresponds to the solution that you are installing.

You must configure the same deployment type that you configured on the initial node.

If you have conferencing in your solution, then select **Team Engagement + Conferencing**. Otherwise, you must select **Team Engagement**. Do not select **Conferencing only**.

7. To review the settings, select **Continue** and then select **Accept and continue**.

The system runs pre-install configuration checks.

8. To install the software, select **Continue** and then accept the license agreement.

Wait for several minutes while the installation proceeds.

9. Select **Continue** to start the configuration utility.

 **Important:**

Do not change the settings in **Front-end host, System Manager and Certificate Configuration** without reentering the System Manager enrollment and keystore passwords before applying the changes.

 **Warning:**

Do not configure the LDAP settings on nodes that you add to a cluster. The LDAP configuration is automatically configured for additional nodes when they connect to the initial node.

10. If this is the second node of a cluster and the virtual IP for internal load balancing is enabled on the initial node, then do the following:

**! Important:**

The virtual IP must be enabled only for the initial node and the second node. Do not enable the virtual IP on any other nodes.

- a. Select **Clustering Configuration > Virtual IP Configuration**.
- b. Select **Enable virtual IP** and set the value to `y` (yes).

The system displays additional Virtual IP configuration.

- c. Configure all of the Virtual IP settings as described in [Virtual IP configuration options](#) on page 128.

**! Important:**

You must use the same Virtual IP authentication password that you set on the initial node of the cluster.

- d. To save the changes on the system, select **Apply** and then select **Continue**.
- e. Select **Return to Main Menu** and press `Enter`.
11. To apply the changes, from the main menu, select **Continue** and then select **Yes** to start the services.

The system starts the services.

12. To exit the configuration tool, select **Continue**.

**Next steps**

- Set up the required certificates as described in [Certificate configuration using the configuration utility](#) on page 192.
- Repeat this procedure to add the required number of nodes to the cluster.
- After all of the required cluster nodes are installed, change the default Cassandra database password as described in [Changing the Cassandra user name and password](#) on page 130.
- After all of the required cluster nodes are installed or if new nodes are added to an existing cluster, you must configure the RSA public and private keys on the initial node.

**Related links**

[Seed node replacement configuration](#) on page 103

## 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 apply the changes.

---

## Avaya Aura® Web Gateway initial configuration settings

The following sections describe the initial configuration settings for Avaya Aura® Web Gateway. They also list the equivalent `installation.properties` file parameters for each setting for silent installations. If you do not configure a setting during installation, you can configure it later. You can update many of these settings anytime using the Avaya Aura® Web Gateway administration portal as described in the “Avaya Aura® Web Gateway management with the administration portal” chapter in *Administering the Avaya Aura® Web Gateway*.

**Related links**

[Front-end host, System Manager, and certificate configuration](#) on page 109

[LDAP configuration](#) on page 112

[Cluster configuration](#) on page 127

[Virtual IP configuration options](#) on page 128

[Advanced configuration](#) on page 129

**Front-end host, System Manager, and certificate configuration**

If you do not select the **Front-end host, System Manager and Certificate Configuration** option during the installation, then the self-signed certificates are automatically generated. Self-signed certificates are also generated when:

- The **System Manager FQDN** option is not set.
- The **Use System Manager for certificates** option is set to `n` and certificates were not provided for one of the interfaces: REST, OAMP, or NODE.

You can modify certificate configuration settings from the administration portal anytime. This is useful if you do not complete the certificate configuration as part of the initial setup process or if you generate certificates at a later time.

For information about managing certificates through the Avaya Aura® Web Gateway administration portal, see the managing certificates section in *Administering the Avaya Aura® Web Gateway*.

**⚠ Caution:**

If the system is using System Manager for certificates, then changing the System Manager FQDN after installation will result in the regeneration of certificates. This might impact the client and backend server communication with the Avaya Aura® Web Gateway.

**Table 3: Front-end host, System Manager and Certificate Configuration settings**

| Item name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                           | Equivalent <code>installation.properties</code> file parameter |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Front-end FQDN</b> | <p>The front-end FQDN is the address that end-user clients use to access the services provided by Avaya Aura® Web Gateway .</p> <p>For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an external load balancer is used, set this value to the FQDN of the load balancer.</p> <p>The default value depends on the configuration present in the <code>/etc/hosts</code> file of the server.</p> | <code>REST_FRONTEND_HOST</code>                                |

*Table continues...*

| Item name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Equivalent <code>installation.properties</code> file parameter                                                                         |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Manager FQDN</b>                   | The FQDN of the System Manager that signs the certificates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | SYSTEM_MGR_IP                                                                                                                          |
| <b>System Manager web admin username (o)</b> | The System Manager web administration portal user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | SMGR_USER_NAME                                                                                                                         |
| <b>System Manager web admin password</b>     | The System Manager web administration portal password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | SMGR_USER_PASSWORD                                                                                                                     |
| <b>System Manager HTTPS Port</b>             | The HTTPS port used for the Alarm Agent for the current Avaya Aura® Web Gateway server.<br><br>The default value for this setting is 443.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SYSTEM_MGR_HTTPS_PORT                                                                                                                  |
| <b>System Manager Enrollment Password</b>    | The System Manager enrollment password.<br><br> <b>Note:</b><br><br>To get the password, log in to System Manager and navigate to <b>Service &gt; Security &gt; Certificates &gt; Enrollment Password</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | SYSTEM_MGR_PW                                                                                                                          |
| <b>Override port for remote access</b>       | Specifies the port on the Avaya Aura® Web Gateway server. This port is used by a reverse proxy, such as Avaya SBC, that fronts HTTP-based clients which are external to the enterprise.<br><br>The reverse proxy continues to receive requests from the external clients on port 443, and then forwards them to the Avaya Aura® Web Gateway on the reverse proxy port. Clients within the enterprise continue to access Avaya Aura® Web Gateway directly using port 443.<br><br>Select <b>y</b> (yes) to configure the port for the reverse proxy server or <b>n</b> (no) to keep the default configuration that remains disabled.<br><br> <b>Important:</b><br><br>If this setting is enabled, you cannot set the port to 443, but you can | OVERRIDE_FRONTEND_PORT<br><br>For the <b>Front-end port for reverse proxy</b> setting, the equivalent parameter is REST_FRONTEND_PORT. |

Table continues...

| Item name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Equivalent <code>installation.properties</code> file parameter                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | <p>set it to 8444, which is the default setting, or to any other port.</p> <p>If you select <code>y</code> (yes), the menu displays a new setting for the reverse proxy port:<br/><b>Front-end port for reverse proxy.</b></p> <p>If you override the port for remote access, you must configure this port on the Avaya SBC external interface for Avaya Aura® Web Gateway. For more information, see <i>Administering Avaya Session Border Controller</i>.</p> <p> <b>Note:</b></p> <p>You can also set this port on the Avaya Aura® Web Gateway administration portal under <b>External Access &gt; HTTP Reverse Proxy</b>. After selecting the <b>Front-end port for remote access</b> check box, you can modify the port value.</p> |                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Use System Manager for certificates</b> | <p>Specifies if the certificates are retrieved from System Manager or from imported files.</p> <p>Select <code>y</code> (yes) to retrieve certificates from System Manager or <code>n</code> (no) to retrieve certificates from imported files.</p> <p>If you select <code>n</code> (no), the menu displays new settings for configuring the certificate files. To configure the certificate settings, you must provide the complete file path name to the:</p>                                                                                                                                                                                                                                                                                                                                                          | <p>USE_SMGR</p> <p>If the USE_SMGR option is set to <code>n</code> (no), you must configure the following parameters for importing the certificate files:</p> <ul style="list-style-type: none"> <li>• REST_KEY_FILE</li> <li>• REST_CERT_FILE</li> <li>• OAM_KEY_FILE</li> <li>• OAM_CERT_FILE</li> <li>• NODE_KEY_FILE</li> <li>• NODE_CERT_FILE</li> <li>• CA_CERT_FILE</li> </ul> |
| <b>Local frontend host</b>                 | <p>The local FQDN of the node.</p> <p>The configuration utility uses this value to generate certificates for the node.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | LOCAL_FRONTEND_HOST                                                                                                                                                                                                                                                                                                                                                                   |

Table continues...

| Item name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                        | Equivalent <code>installation.properties</code> file parameter |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
|                          |  <b>Important:</b><br>In a clustered configuration, the local front-end host is different from one node to the other and is also different from the front-end FQDN. In a non-clustered environment, the local front-end host is usually different from the front-end FQDN to create a clustered configuration from a non-clustered configuration. |                                                                |
| <b>Keystore password</b> | The keystore password for the MSS and Tomcat certificates.<br><br>The minimum length for this password is 6 characters. The characters supported for the keystore password are:                                                                                                                                                                                                                                                    | KEYSTORE_PW                                                    |

## LDAP configuration

If you do not complete LDAP configuration during the initial Avaya Aura® Web Gateway setup, then you can complete it later using the Avaya Aura® Web Gateway administration portal. Some administration options, such as configuring multiple LDAP directories, are only available on the administration portal. For more information, see *Administering the Avaya Aura® Web Gateway*.

### Warning:

Changing the LDAP configuration parameters, other than Bind DN and Bind Credential, when they are configured, might invalidate the existing user data. For example, changing how user roles are found can remove one or more roles from the existing user, which will block the user from accessing the Avaya Aura® Web Gateway system. In addition, do not change the server URL unless you need to switch the configuration to another replicated instance of the current LDAP directory. In all the other cases, you must reinstall the Avaya Aura® Web Gateway system.

| Item name                             | Description                                                                                                                                                                                                                                                                                                                                       | Equivalent properties file parameter |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>Load LDAP properties from file</b> | The <b>Load LDAP properties from file</b> menu contains an item called <b>Path to properties file</b> .<br><br>You can create a Java properties file that contains the LDAP properties instead of entering the LDAP configuration settings manually. The <b>Path to properties file</b> option is for configuring the absolute path to this file. | pathToLdapPropertiesFile             |

*Table continues...*

| Item name                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Equivalent properties file parameter                            |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
|                                               | <p>The LDAP properties file must contain the <i>equivalent properties file parameters</i> specified in this table.</p> <p>The default value for this setting is <code>&lt;install_dir&gt;/config/ldap.properties</code>, where <code>&lt;install_dir&gt;</code> is the installation directory.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                 |
| <b>Import Secure LDAP trusted certificate</b> | <p>The <b>Import Secure LDAP trusted certificate</b> menu contains the following items:</p> <ul style="list-style-type: none"> <li>• <b>Certificate file:</b> The path and filename for the LDAP trusted certificate. The certificate file must be in the .PEM format.</li> </ul> <p>If you want to configure secure LDAP for onboard Open LDAP, use the nginx certificate located at <code>/etc/openldap/certs/nginx.crt</code>.</p> <p>You cannot import a certificate if:</p> <ul style="list-style-type: none"> <li>• The certificate contains an unsupported critical extension.</li> <li>• The certificate expired.</li> <li>• The start date of the certificate is in the future.</li> </ul> <p> <b>Important:</b></p> <p>Only configure these settings if you need a Secure LDAP connection.</p> | <p>LDAP_TRUSTSTORE_CERTFILE</p> <p>LDAP_TRUSTSTORE_PASSWORD</p> |
| <b>Directory Type</b>                         | <p>The LDAP directory type of the enterprise.</p> <p>The supported directory types are the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory 2012, 2016, and 2019</li> <li>• Microsoft Active Directory Lightweight Directory Services (AD-LDS)</li> <li>• IBM Domino Server 7.0</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ldapType                                                        |

Table continues...

| Item name                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Equivalent properties file parameter |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                            | <p> <b>Note:</b></p> <p>The Domino server must be patched to support TLS, so Avaya Aura® Web Gateway can connect to the Domino server through secure LDAP (LDAPS). For a list of supported patch fixes, see <a href="https://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0">https://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0</a>.</p> <ul style="list-style-type: none"> <li>• Novell e-Directory 8.8</li> <li>• OpenLDAP 2.4</li> <li>• Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0)</li> </ul> <p>For detailed information about supported product releases, see the <a href="#">Avaya Compatibility Matrix</a>.</p>                                                                                                                   |                                      |
| <b>URL for LDAP server</b> | <p>The URL for gaining access to the LDAP server. This is the mandatory setting.</p> <p>The URL must have one of the following formats:</p> <pre>ldap://&lt;LDAP server FQDN or IP address&gt;:&lt;port&gt; ldaps://&lt;LDAP server FQDN&gt;:&lt;port&gt;</pre> <p><b>For example:</b></p> <pre>ldap://myserver.mycompany.com:3268 ldaps://myserver.mycompany.com:3269</pre> <p>The protocol can be LDAP or LDAPS, depending on the LDAP server type. If you are using LDAPS, you cannot use IP addresses in the URL.</p> <p> <b>Important:</b></p> <p>If FIPS is enabled, use the LDAPS protocol to access the LDAP server.</p> <p>For Microsoft Active Directory, use the catalog LDAP ports.</p> <p>The default global catalog LDAP port values are 3268 for LDAP and 3269 for LDAPS.</p> | ldapUrl                              |

Table continues...

| Item name      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Equivalent properties file parameter |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                | <p>The default domain LDAP ports values are 389 for LDAP and 636 for LDAPS.</p> <p> <b>Note:</b></p> <p>If an FQDN is used to specify the LDAP server, the enterprise might map the FQDN to multiple, replicated LDAP servers using the DNS round-robin mechanism as an attempt for load-balance and for redundancy purpose. Sporadic authentication failures can occur if one of the LDAP servers is offline and the DNS round-robin mechanism resolves the FQDN to the IP of the LDAP server that is offline.</p> <p>If this outcome cannot be tolerated, a more reliable load-balancing mechanism, such as a dedicated load-balancer in front of the LDAP servers, will be needed.</p> <p>For Active Directory, use the Global Catalog service port instead of the default LDAP/LDAPS ports.</p> <p> <b>Important:</b></p> <p>If you are using the global catalog ports, you must configure attribute replication to the global catalog. For more information, see <a href="#">LDAP attributes replication to the global catalog</a> on page 127.</p> |                                      |
| <b>Bind DN</b> | <p>The Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is the mandatory setting.</p> <p>The format of the Bind DN depends on the configuration of the LDAP server.</p> <p> <b>Note:</b></p> <p>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</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | bindDN                               |

*Table continues...*

| Item name                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Equivalent properties file parameter                                                                                                                                                            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | <p>LDAP server can support for LDAP bind.</p> <p>For example: for Active Directory, you can use <code>domain\user</code>, <code>user@domain</code>, as well as the actual DN of the user object.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                 |
| <b>Bind Credential</b>    | <p>Specifies the password of the administrative user.</p> <p>The maximum password length depends on the LDAP server type that you use in your deployment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <p><b>! Important:</b></p> <p>If you configure the LDAP settings using the properties file, you must enter the Bind Credential manually by running the <code>configureCSA.sh</code> script.</p> |
| <b>UID Attribute ID</b>   | <p>The User ID attribute name, as determined by the LDAP server configuration. This is the mandatory setting.</p> <p>This parameter is used for searching users in the LDAP server.</p> <p>For example: <code>sAMAccountName</code></p>                                                                                                                                                                                                                                                                                                                                                                                                   | <code>uidAttrID</code>                                                                                                                                                                          |
| <b>Base Context DN</b>    | <p>The DN of the context used for LDAP authentication.</p> <p>For example:<br/><code>ou=csasusers,dc=example,dc=com</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>baseCtxDN</code>                                                                                                                                                                          |
| <b>Administrator Role</b> | <p>The list of LDAP roles that match the Avaya Aura® Web Gateway Administrator role.</p> <p>For example:</p> <p>If the role is configured as <code>CSAAdmin</code>, <code>CSAxyz</code>, any user whose list of roles contains <code>CSAAdmin</code> or <code>CSAxyz</code> is mapped to the Avaya Aura® Web Gateway Administrator role.</p> <p><b>* Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p> | <code>adminRole</code>                                                                                                                                                                          |

Table continues...

| Item name           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Equivalent properties file parameter |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                     | <p> <b>Important:</b></p> <p>To avoid situations when potential loss of credentials could impact the administration tasks, Avaya recommends creating more than one user account with administrator privileges.</p>                                                                                                                                                                                                                                                                                                                                                                                                                  |                                      |
| <b>Auditor Role</b> | <p>The list of LDAP roles that match the Avaya Aura® Web Gateway Auditor role.</p> <p>For example:</p> <p>If the Auditor role is configured as <code>CSAAuditor,CSAxyz</code>, any user whose list of roles contains the <code>CSAAuditor</code> or <code>CSAxyz</code> role is mapped to the Avaya Aura® Web Gateway AUDITOR role.</p> <p> <b>Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p> | auditorRole                          |
| <b>User Role</b>    | <p>The list of LDAP roles that match the Avaya Aura® Web Gateway User role.</p> <p>For example:</p> <p>If the User role is configured as <code>CSAUser,CSAxyz</code>, any user whose list of roles contains the <code>CSAUser</code> or <code>CSAxyz</code> role is mapped to the Avaya Aura® Web Gateway USER role.</p> <p> <b>Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p>                       | usersRole                            |

Table continues...

| Item name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Equivalent properties file parameter |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>Services Administrator Role</b>           | <p>The list of LDAP roles that match the Services Administrator role.</p> <p>For example:</p> <p>If the User role is configured as <code>CSAUser</code>, <code>CSAxyz</code>, any user whose list of roles contains the <code>CSAUser</code> or <code>CSAxyz</code> role is mapped to the Avaya Aura® Web Gateway Services Administrator role.</p> <p> <b>Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p>     | <code>serviceAdminRole</code>        |
| <b>Services Maintenance and Support Role</b> | <p>The list of LDAP roles that match the Maintenance and Support role.</p> <p>For example:</p> <p>If the User role is configured as <code>CSAUser</code>, <code>CSAxyz</code>, any user whose list of roles contains the <code>CSAUser</code> or <code>CSAxyz</code> role is mapped to the Avaya Aura® Web Gateway Maintenance and Support role.</p> <p> <b>Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p> | <code>serviceMaintenanceRole</code>  |
| <b>Security Administrator Role</b>           | <p>The list of LDAP roles that match the Avaya Aura® Web Gateway Security Administrator role.</p> <p>For example:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <code>securityAdminRole</code>       |

*Table continues...*

| Item name                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Equivalent properties file parameter |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                                 | <p>If the role is configured as <code>CSASecurityAdmin</code>, <code>CSAxyz</code>, any user whose list of roles contains <code>CSASecurityAdmin</code> or <code>CSAxyz</code> is mapped to the Avaya Aura® Web Gateway Security Administrator role.</p> <p> <b>Note:</b></p> <p>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the role name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed.</p>                                                                                                                                                                      |                                      |
| <b>Advanced LDAP parameters</b> | The menu that contains advanced LDAP parameters to configure depending on the structure of the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                      |
| <b>Test User</b>                | <p>If you select <code>testUser</code> and select <b>Apply</b>, this option is used to validate the following LDAP settings:</p> <ul style="list-style-type: none"> <li>• Verifies that the user is searchable with a given base DN and search filter.</li> <li>• Lists the group to which the user belongs — user, administrator, or auditor.</li> <li>• Validates the values for Role Attribute ID and Role Name Attribute.</li> <li>• Verifies the Last Updated Time attribute, role filter syntax, and active users search filter syntax.</li> </ul> <p>The configuration is not saved if any of these validations fail.</p> <p>The <code>testUser</code> parameter is optional. If you do not specify a value, the system skips validation and directly saves the configuration in the database.</p> | <code>testUser</code>                |

## LDAP advanced parameters

The following table describes the settings in the Advanced LDAP parameters menu:

| Item name                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Equivalent properties file parameter |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>Role Filter</b>         | <p>The string to use for role filtering. This is the mandatory setting.</p> <p>The format of the string depends on the LDAP server configuration.</p> <p>For example:<br/> <code>(&amp;(objectClass=group)(member={1}))</code></p>                                                                                                                                                                                                                                                                                                  | <code>roleFilter</code>              |
| <b>Role Attribute ID</b>   | <p>The Role Attribute ID parameter has a different meaning, depending on the value of <b>Role Attribute Is DN</b>:</p> <ul style="list-style-type: none"> <li>• If <b>Role Attribute Is DN</b> is set to true, this is the attribute that contains the DN used to find the object that contains the role name.</li> <li>• If <b>Role Attribute Is DN</b> is set to false, this is the name of the attribute that contains the role name.</li> </ul> <p>For example: <code>memberOf</code></p> <p>This is the mandatory setting.</p> | <code>roleAttrID</code>              |
| <b>Roles Context DN</b>    | <p>The Roles Context DN to use for searching roles.</p> <p>The roles search in LDAP is performed by using the Roles Context DN in combination with the Role Filter.</p> <p>For example:<br/> <code>ou=csasusers,dc=example,dc=com</code></p>                                                                                                                                                                                                                                                                                        | <code>rolesCtxDN</code>              |
| <b>Role Name Attribute</b> | <p>This parameter has a different meaning, depending on the value of <b>Role Attribute Is DN</b>:</p> <ul style="list-style-type: none"> <li>• If <b>Role Attribute Is DN</b> is set to true, the value of the attribute set in <b>Role Attribute ID</b> is used to find the object that contains the role and this parameter stores the name of the attribute that contains the role name.</li> </ul>                                                                                                                              | <code>roleNameAttrID</code>          |

*Table continues...*

| Item name                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Equivalent properties file parameter |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                                           | <ul style="list-style-type: none"> <li>If <b>Role Attribute Is DN</b> is set to false, this parameter is ignored.</li> </ul> <p>For example: <code>cn</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |
| <b>Role Attribute is DN (true/false)</b>  | <p>The setting to determine if the role attribute is stored in the DN or in another object.</p> <p>If you set this parameter to <code>true</code>, the role is stored in the attribute defined by the <b>Role Name Attribute</b> parameter.</p> <p>If you set this parameter to <code>false</code>, the role attribute of the user contains the name of the role.</p>                                                                                                                                                                                                                                           | <code>roleAttrIsDN</code>            |
| <b>Role Recursion</b>                     | <p>The setting to enable or disable role recursion.</p> <p>For example: the user jsmith can be in the Sales group, which can be in the users group. In this case, Role Recursion must be set to true to permit role recursion.</p>                                                                                                                                                                                                                                                                                                                                                                              | <code>roleRecursion</code>           |
| <b>Allow Empty Passwords (true/false)</b> | The setting to determine if empty passwords are allowed in the LDAP directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <code>allowEmptyPasswords</code>     |
| <b>Search Scope (0 - 2)</b>               | <p>The setting to determine the scope of the role search.</p> <p>The role search starts from the <i>Role Context DN</i> and uses the <i>Role Filter</i>. The search scope determines the depth of the search as follows:</p> <ul style="list-style-type: none"> <li>Level 0, also named <code>OBJECT_SCOPE</code>, indicates that the search is performed only on the named role context.</li> <li>Level 1, also named <code>ONELEVEL_SCOPE</code>, indicates that the search is performed directly under the named role context.</li> <li>Level 2, also named <code>SUBTREE_SCOPE</code>, indicates</li> </ul> | <code>searchScope</code>             |

Table continues...

| Item name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Equivalent properties file parameter |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                                    | that the search is performed at the named role context and in the sub-tree rooted at the named role context.                                                                                                                                                                                                                                                                                                                                                                         |                                      |
| <b>Language used in Directory</b>  | <p>The language used in the LDAP directory.</p> <p>The following languages are supported:</p> <ul style="list-style-type: none"> <li>• Russian</li> <li>• German</li> <li>• Spanish</li> <li>• English</li> <li>• Korean</li> <li>• French</li> <li>• Portuguese</li> <li>• Simplified Chinese</li> <li>• Japanese</li> <li>• Italian</li> </ul>                                                                                                                                     | language                             |
| <b>Active users search filter</b>  | <p>The search filter string used to identify active users.</p> <p>If the LDAP server supports a method of determining whether a user is active, this setting must contain the attribute that determines if a user is active.</p> <p>If this setting is not configured, the User Management component handles all the users as active users.</p> <p>For example:</p> <pre>(&amp;(objectClass=user) (objectCategory=Person) (! (userAccountControl:1.2.8 40.113556.1.4.803:=2)))</pre> | activeUsersFilter                    |
| <b>Last updated time attribute</b> | The attribute indicating the last time an LDAP object was modified, in the ASN.1 Generalized Time Notation.                                                                                                                                                                                                                                                                                                                                                                          | lastUpdatedTimeAttr                  |

Table continues...

| Item name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Equivalent properties file parameter |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
|                                | <p>The Avaya Aura® Web Gateway User Management component uses this attribute to identify updated users when synchronizing the user data with the LDAP server.</p> <p>Avaya recommends that you use the following values:</p> <ul style="list-style-type: none"> <li>• For Active Directory: <code>whenChanged</code>.</li> <li>• For OpenLDAP: <code>modifyTimestamp</code>.</li> </ul> <p>If this parameter is not configured, the User Management component compares the data of every user to the data that exists in the LDAP server.</p> <p> <b>Note:</b></p> <p>Configuring this parameter improves the efficiency of the user synchronization process and reduces the traffic between the Avaya Aura® Web Gateway server and the LDAP server during user synchronization.</p> |                                      |
| <b>Load parameter defaults</b> | The script to load the default values for the parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | —                                    |

## Multiple authentication and authorization domains

Before Release 3.4, you could configure multiple LDAPs and have multiple base contexts on each LDAP, but you could only use one of them for authorization and authentication. With the single authentication and authorization domain restriction in place, users had to be provisioned multiple times so they existed in the authentication and authorization domain and in the other LDAPs used for search.

As of Release 3.4, the multiple authentication and authorization feature removes the requirement for a single domain for authentication and authorization and facilitates the following deployments:

- A single LDAP infrastructure belonging to a single organization with multiple configured domains.
- Two distinct LDAP infrastructures belonging to two separate organizations.

The Avaya Aura® Web Gateway supports up to ten LDAP authentication and authorization domains.

When multiple directories are enabled for authentication, you must provide your FQDN to log in. For example: `username@avaya.com`. A short user name is not supported. If you do not have proper data in user name attributes, such as mail and userPrincipalName, you can assign a custom attribute that is used for the UID mapping of user names. All values in the custom attribute must be a fully qualified user name of the form `username@domain`, where `domain` must match one of the base context DN's defined for the LDAP.

During the initial Avaya Aura® Web Gateway installation procedure, you can configure only one LDAP server. If you want to add more LDAP servers, use the web administration portal. For more information, see "Adding a new enterprise LDAP server" in *Administering the Avaya Aura® Web Gateway*.

## Configuring the role search parameters

### About this task

This procedure describes how to configure the LDAP role search parameters when Microsoft Active Directory (AD) is used.

Role search for Avaya Aura® Web Gateway users are really about finding the associated "role" strings for a user in LDAP. For AD, this is about the user group names that a user belongs to.

In Microsoft Active Directory, the DN's of the groups that a user belongs to are stored in the "memberOf" attribute of a user. The "memberOf" attribute also stores the Exchange mailing lists that a user belongs to. Conversely, the group objects that the user belongs to contain a "member" attribute that stores the DN's of all of the users and sub-groups that are members of this group.

### Procedure

1. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
2. Select **LDAP Configuration > Advanced LDAP parameters**.
3. Configure the parameter settings as described in [Parameter settings](#) on page 124.
4. Configure the attributes as described in [Role configuration](#) on page 126.

## LDAP parameter descriptions

### Parameter settings

The following table describes the parameter settings according to the search mechanism that you choose:

| Parameter            | Search mechanism #1:<br>Find the user, extract the group DNs from the “memberOf” attribute, and get the role strings from each of the group objects |                                                                                                                                                           | Search mechanism #2:<br>Find the groups that the user belongs to and extract the role string from one of the attributes |                                                                                                                                                                                                                                                    |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Example                                                                                                                                             | Description                                                                                                                                               | Example                                                                                                                 | Description                                                                                                                                                                                                                                        |
| Role Filter          | (&(objectClass=user)(objectCategory=Person)(<UID attribute ID>={0}))                                                                                | <UID Attribute ID> is the value of the “UID Attribute ID” parameter.<br><br>“{0}” is the placeholder that will be replaced by the authenticating user ID. | (&(objectClass=group)(member={1}))                                                                                      | “{1}” is the placeholder to be replaced by the DN of the user object. The DN is identified during the authentication process.<br><br>This filter looks for a group object whose “member” attribute contains a value of the authenticating user DN. |
| Role Context DN      | ou=Users,dc=global,dc=example,dc=com                                                                                                                | The purpose of the search is to find the user and then extract the role objects from the “memberOf” user attribute.                                       | ou=Groups,dc=global,dc=example,dc=com                                                                                   | The purpose of the search is to find the roles whose “member” attribute contains the user.                                                                                                                                                         |
| Role Attribute ID    | memberOf                                                                                                                                            | This attribute contains the list of DNs of the groups to which the user belongs to.                                                                       | CN                                                                                                                      | This contains the group’s name (for example, “AAWGAdmin”, and so on.)                                                                                                                                                                              |
| Role Attribute is DN | true                                                                                                                                                | The “memberOf” values are the DNs of the group/mailling list objects.                                                                                     | false                                                                                                                   | The “Role Attribute ID” already contains the “role” string name.                                                                                                                                                                                   |
| Role Name Attribute  | CN                                                                                                                                                  | The attribute defined by Role Name Attribute contains the group name.<br><br>For example: AAWGAdmin                                                       |                                                                                                                         | Leave this parameter empty because “Role Attribute is DN” is false.                                                                                                                                                                                |

Table continues...

| Parameter      | Search mechanism #1:<br>Find the user, extract the group DNs from the “memberOf” attribute, and get the role strings from each of the group objects |                                                                                                                                                                                                                                                                                                                                                            | Search mechanism #2:<br>Find the groups that the user belongs to and extract the role string from one of the attributes |                                                                                                                                                                                                                                                                                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | Example                                                                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                | Example                                                                                                                 | Description                                                                                                                                                                                                                                                                              |
| Role Recursion | 0                                                                                                                                                   | <p>This configuration does not allow recursive search.</p> <p> <b>Note:</b></p> <p>Using this configuration, the users under the “AAWGDelegates” group will not be able to use Avaya Aura® Web Gateway so this is not the recommended configuration for this example.</p> | 1 or higher                                                                                                             | <p>You must set this value to 0 if there are no subgroups or a value from 1 to 10 to support searches of users that are in subgroups.</p> <p>In this example, the recursive search is needed to find the user in the “AAWGDelegates” group, so this value must be set to at least 1.</p> |

## Role configuration

To search the role base context and under it, set **Search Scope** to 2 or `SUBTREE_SCOPE`. The configuration of the following roles is the same, regardless of the configured search mechanism:

| Role                                  | Description                                                                                                                                                | Example           |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Administrator Role                    | This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server ADMIN application role.   | AAWGAdmin         |
| User Role                             | This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server USERS application role.   | AAWGUsers         |
| Auditor Role                          | This role specifies the list of the “role” string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server AUDITOR application role. | AAWGAuditor       |
| Service Administrator Role            | Avaya Aura® Web Gateway does not currently use this role. Leave this setting blank.                                                                        |                   |
| Services Maintenance and Support Role | Avaya Aura® Web Gateway does not currently use this role. Leave this setting blank.                                                                        |                   |
| Security Administrator Role           | This role is for updating web certificates from the web administration portal.                                                                             | AAWGSecurityAdmin |

## LDAP attributes replication to the global catalog

If you are using global catalog ports 3268 or 3269 to connect to LDAP, then LDAP queries can only return attributes marked for replication to the global catalog. For example, a user's department cannot be returned because this attribute is not replicated to the global catalog. You must manually add all required attributes in the global catalog attributes list.

## Cluster configuration

Using the Cluster configuration, you can configure the Avaya Aura® Web Gateway nodes in a clustered environment.

| Item name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Equivalent <code>installation.properties</code> file parameter                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Initial cluster node</b>  | <p>The setting to specify if the server where you are performing the installation is the initial node in a cluster.</p> <p>Select <code>y</code> (yes) to set the current node as the initial node in the cluster or <code>n</code> (no) to set the current node as an additional node.</p> <p>The default value for this setting is <code>y</code> (yes).</p> <p>In a standalone installation, set this value to <code>y</code> (yes).</p> <p>If you configure this setting to <code>n</code> (no), the following settings become visible and must be configured:</p> <ul style="list-style-type: none"> <li>• The IP address of the initial cluster node.</li> <li>• The ID of the Linux user performing the installation on the initial node.</li> <li>• The Cassandra database user name for the initial node.</li> <li>• The Cassandra database password for the initial node.</li> </ul> | <p><code>INITIAL_NODE</code></p> <p>If you configure this setting to <code>n</code> (no), you must also configure the following parameters:</p> <ul style="list-style-type: none"> <li>• <code>SEED_NODE</code></li> <li>• <code>REMOTE_UID</code></li> <li>• <code>CURRENT_CASSANDRA_USER</code></li> <li>• <code>CURRENT_CASSANDRA_PASSWORD</code></li> </ul> |
| <b>Local node IP address</b> | The IP address of the local node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <code>CLUSTER_IP_ADDR</code>                                                                                                                                                                                                                                                                                                                                    |

## Virtual IP configuration options

| Option                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Equivalent <code>installation.properties</code> file parameter |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Enable virtual IP</b>                  | <p>The setting to enable the usage of a virtual IP address.</p> <p>If you select <code>n</code> (no), the configuration script does not configure the virtual IP address.</p> <p>If you select <code>y</code> (yes), new configuration settings for the virtual IP address are displayed in the configuration menu. These settings are listed below in this table. If you are performing a silent installation you must also configure these parameters in the <code>installation.properties</code> file.</p> | <code>KA_ENABLED</code>                                        |
| <b>Virtual IP address</b>                 | The virtual IP address shared by all the cluster nodes.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <code>KA_VIRTUAL_IP</code>                                     |
| <b>Virtual IP interface</b>               | The network interface used for the virtual IP address. Unless you are using a configuration that has multiple Ethernet interfaces, you must set this value to <code>eth0</code> (Ethernet-zero).                                                                                                                                                                                                                                                                                                              | <code>KA_INTERFACE</code>                                      |
| <b>Virtual IP master node</b>             | Determines if the current node is the virtual IP master node. As the initial node of the cluster is usually designated the virtual IP master, set this value to <code>y</code> (yes), on the initial node. In addition, as the second node in a cluster is usually designated the virtual IP backup, set this value to <code>n</code> (no) on the second node.                                                                                                                                                | <code>KA_MASTER_YN</code>                                      |
| <b>Virtual IP router ID</b>               | <p>An integer with a value from 1 to 255. The value must be the same for both virtual IP master and backup. The default value is 71.</p> <p>This value must be unique across Virtual Router Redundancy Protocol (VRRP) installations.</p>                                                                                                                                                                                                                                                                     | <code>KA_ROUTER_ID</code>                                      |
| <b>Virtual IP authentication password</b> | The password that the backup node uses for authentication. This password must be the same as the virtual IP authentication password configured for the initial node.                                                                                                                                                                                                                                                                                                                                          | <code>KA_AUTHENTICATION_PASSWORD</code>                        |

### Related links

[Avaya Aura Web Gateway initial configuration settings](#) on page 108

## Advanced configuration

Table 4: Advanced configuration settings

| Item name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Equivalent <code>installation.properties</code> file parameter                                                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Certificate Warning Period</b>            | The number of days before the expiry date of a certificate causes the system to raise an alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>CERT_WARNING_PERIOD</code>                                                                                                                                           |
| <b>OS Security Utility</b>                   | <p>The menu for configuring the firewall automatically on the current node.</p> <p>Select <b>Run the firewall configuration script</b> and press Enter to run the firewall configuration script.</p> <p>Avaya recommends that you run this script to configure the firewall automatically and not perform a manual configuration.</p> <p> <b>Warning:</b></p> <p>The firewall configuration script replaces the current configuration of the firewall on the server where you are performing the installation, so you must open any other ports required for your server manually after you run this script.</p> | <p><code>RUN_FIREWALL_CONFIG</code></p> <p>If you set this parameter to <code>y</code> (yes), the firewall configuration script is run during the silent installation.</p> |
| <b>Long Poll Timeout</b>                     | <p>The menu that contains the <b>Recommended Long Poll Timeout</b> configuration option. Use this option for setting the value to use in the Avaya-Request-Timeout HTTP header for long-poll requests.</p> <p> <b>Important:</b></p> <p>The long poll timeout value can be from 30 to 120. Lowering this value results in increased traffic on the server, but network configuration may require that you set a lower value.</p> <p>If you do not configure this parameter, the default database initialization setting is used.</p>                                                                           | <code>AVAYA_REQUEST_TIMEOUT</code>                                                                                                                                         |
| <b>Configure Host IP for SNMP management</b> | The menu that contains the <b>IP address for managing this server</b> setting for configuring the IP address of the Network Interface to use for SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>SNMP_IP_ADDR</code>                                                                                                                                                  |

Table continues...

| Item name                   | Description                                                                                                                                                                                                                                                                                                                                         | Equivalent installation.properties file parameter |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| <b>Security Banner File</b> | <p>The menu for configuring security banner settings.</p> <p>The <b>Security Banner File</b> setting must contain the path to the security banner file.</p> <p>The security banner file is a text file that contains the security warnings displayed when a user or administrator logs in to the administration portal or using an SSH console.</p> | SECURITY_BANNER_PATH                              |

## Changing the Cassandra user name and password

### About this task

After installing the Avaya Aura® Web Gateway application, you must change the default Cassandra database password to comply with the security requirements.

This procedure describes how to change the Cassandra database user name and password after installing of an Avaya Aura® Web Gateway cluster.

### Before you begin

Install the Avaya Aura® Web Gateway application. If you install an Avaya Aura® Web Gateway cluster, install all cluster nodes before changing the Cassandra database password.

### Procedure

- On the seed node, do the following:
  - Log in to the Avaya Aura® Web Gateway CLI as an administrator.
  - Run the Avaya Aura® Web Gateway configuration utility using the following command:
 

```
app configure
```
  - Select **Cassandra DB User and Password**.
  - Select **New Cassandra Database User Name** and enter the new user name.
  - Select **New Cassandra Database User Password** and enter the new password.
  - Select **Apply**.
- In a cluster deployment, on every non-seed node, do the following:
  - Log in to the Avaya Aura® Web Gateway CLI as an administrator.
  - Run the **cassandraSetPassword** command and specify the new password and user name as parameters.

```
sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/cassandra/cassandraSetPassword.sh <new user name> <new password>
```

- c. Restart Avaya Aura® Web Gateway.

```
svc csa restart
```

---

## Changing the default password for automatic backups

### About this task

Change the default password that Avaya Aura® Web Gateway uses for automatic backups.

### Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal at `https://<AADS FQDN or IP>:8445/admin/`.

For more information about the login procedure, see “Logging in to the Avaya Aura® Web Gateway web administration portal” in *Administering the Avaya Aura® Web Gateway*.

2. Go to **Automatic Backup Configuration**.
3. Select the **Change Password** check box.
4. In **Backup File Password**, type a new password.

The password must comply with the password complexity rules. To view the rules, point the cursor to the **Backup File Password** field.

5. In **Re-Enter Password**, type the password again.
6. Click **Save**.

---

## Starting services using a command line

### About this task

Use this procedure to start application services after you complete installation.

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.  
The Linux administrator account is created during the deployment process.
2. To start the Avaya Aura® Web Gateway services, run the following command:

```
svc csa start
```

---

## Configuring OAMP to use Linux account credentials on the Avaya Aura® Web Gateway administration portal

### About this task

This is an optional procedure that you need to perform if you want to log on to the Avaya Aura® Web Gateway administration portal using Linux account credentials.

### Procedure

1. Log in to the Avaya Aura® Web Gateway CLI as the root user.
2. Run the following command:

```
cdto active
vi tomcat/<tomcatVersion>/conf/catalina.properties
```

3. Locate the `com.avaya.cas.access.groups` properties and update the list of groups allowed to access the web administration portal as required.

Ensure that entries in the group list are separated by a comma. The following is an example:

```
# OAMP access linux groups
com.avaya.cas.access.groups.admin=admingrp
com.avaya.cas.access.groups.securityadmin=admingrp
```

Users that are part of the “admingrp” group have access to the web administration portal by default.

4. Run the following command to apply the changes:

```
svc tomcat restart
```

---

## Uninstalling the Avaya Aura® Web Gateway

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. To remove the Avaya Aura® Web Gateway from the system, run the following command:

```
app uninstall
```

3. When prompted, type the following:
  - a. **uninstall** and press `Enter`.
  - b. **yes** and press `Enter`.

## Removing a non-initial node from the cluster if the node is unavailable

### About this task

Use this procedure to remove an unavailable non-initial cluster node, which cannot be removed using the standard node uninstallation procedure. For example, use this procedure if you cannot log in to the node using an SSH connection or if the Cassandra service is not running on the node.

Do not use this procedure to remove the initial cluster node.

### ! Important:

After performing this procedure, do *not* start the removed node. If you start the node, it will re-appear in the list of cluster nodes.

### Before you begin

Enable EASG functionality. EASG is required to obtain the sroot privileges, which you must use to perform commands in this procedure.

### Procedure

1. If the virtual machine with the node that you want to remove is still running, stop the virtual machine.
2. Log in to the initial node as an administrator using an SSH connection.
3. Run the following command to obtain the sroot privileges:

```
su - sroot
```

4. Run the following commands:

```
cdto cassandra
cd bin
```

5. Run the following command to obtain the UUID of the unavailable node in the Cassandra cluster:

```
./nodetool status
```

The unavailable node has the “DN” status. The node UUID is displayed in the Host ID column. The following is an example of the command output:

```
[root@aaawg bin]$ ./nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load      Tokens     Owns (effective)  Host
ID
UN  233.252.0.2   5.07 MiB   256        100.0%            d1e8b3dc-
f116-4bbc-851d-122c9e400bc3 rack1
DN  233.252.0.3   5.07 MiB   256        100.0%            e2e779ae-
d34d-2a10-23de-5ac14c4af783 rack1
UN  233.252.0.4   5.07 MiB   256        100.0%            12cc1379-5164-8e74-81c0-bc8da8d09341 rack1
```

In this example, the unavailable node has UUID e2e779ae-d34d-2a10-23de-5ac14c4af783.

6. Run the following command:

```
./nodetool removemode <UUID>
```

In this command, UUID is the UUID of the unavailable Cassandra database node. For example:

```
./nodetool removemode e2e779ae-d34d-2a10-23de-5ac14c4af783
```

7. Run the `./nodetool status` command again and ensure that the Cassandra cluster does not contain the unavailable node.

8. Run the following command:

```
cdto misc
```

9. Run the following command to obtain the UUID of the unavailable Avaya Aura® Web Gateway node:

```
app listnodes
```

The unavailable node has the “down” status. The node UUID is displayed in the Server identifier column. The following is an example of the command output:

```
[root@aawg misc]$ app listnodes
Node IP address  Status  Server identifier  Singleton  Version
233.252.0.2     live    2523a75a-11a2-45ff-ba39-e23af17c316d  master
3.11.0.0
233.252.0.3     down    3edfc879-b374-1c12-a045-a1456cfc277a
3.11.0.0
233.252.0.4     live    6e430dff-7411-f2c4-9a5a-beec23916707
3.11.0.0
```

In this example, the unavailable node has UUID 3edfc879-b374-1c12-a045-a1456cfc277a.

10. Run the following command:

```
./clitool-csa.sh removeClusterNode <UUID>
```

In this command, UUID is the UUID of the unavailable Avaya Aura® Web Gateway node. For example:

```
./clitool-csa.sh removeClusterNode 3edfc879-b374-1c12-a045-a1456cfc277a
```

11. Run the `app listnodes` command again and ensure that the Avaya Aura® Web Gateway cluster does not contain the node.

## Related links

[A node removed from the Cassandra cluster has the “live” status in the app listnodes output](#) on page 186

# Chapter 7: Deploying AAWG on ASP 130 R6.0.x (KVM on RHEL 8.10)

---

## UPDATE December, 2025

This Chapter is temporarily removed as additional certification of Avaya Aura® Web Gateway on Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10) is underway. The ASP R6.0.x Release Notes will be updated when Avaya Aura® Web Gateway is fully certified on ASP R6.0.x and this Chapter will be updated and reposted.

# Chapter 8: Global FQDN configuration

You can use a single FQDN for all services or multiple FQDNs for each service. If you are using multiple FQDNs, you require an external interface on the reverse proxy for each FQDN and separate certificates for each FQDN.

In a single FQDN environment, remote clients and endpoints that participate in conferences interact with multiple components through HTTPS. To eliminate the need for multiple external public IPs, FQDNs, and certificates, the URL rewriting method is used. Using this method, clients and endpoints can access conferences using a single FQDN and a single IP address through port 443.

---

## DNS configuration

- For a single FQDN deployment, configure DNS as follows:
  - For external DNS configuration, have a single FQDN record, for example, `webservices.company.com`, that points to the reverse proxy or load balancer interface for external traffic.
  - For internal DNS configuration, have a single FQDN record, for example, `webservices.company.com`, that points to the reverse proxy or load balancer interface for internal traffic.
- For a multiple FQDNs deployment, configure DNS as follows:
  - For external DNS configuration, each FQDN points to the external load balancer interface.
  - For internal DNS configuration, each FQDN points to the individual server components.

### Related links

[Required FQDNs and certificates](#) on page 27

---

## Configuring the front-end FQDN

### Procedure

1. Log in to the Avaya Aura® Web Gateway administration portal.
2. Navigate to **External Access > HTTP Reverse Proxy**.
3. Configure the following settings:

4. In **Host**, provide the service FQDN.

For example: You can use `webservices.company.com` in a single FQDN deployment.  
In a multiple FQDN deployment, use `webgateway.company.com`.

5. In **Port**, enter 443.
6. 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.

7. If you are configuring a geographically distributed system, select the **Enable use of an external load balancer** check box.
8. Click **Save**.

#### Related links

[Geographical distribution overview](#) on page 13

---

## Avaya Meetings Server configuration for single FQDN deployments

### Configuring Avaya Workplace Client conference control

#### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Settings > Advanced Parameters**.
3. In **Property Name**, enter `com.visionnex.vcms.core.uccp.customizedUCCPURL`.
4. In **Property Value**, enter `https://<Service FQDN>:443/uwd/ws?ticket=`.  
For example: `https://webservices.company.com:443/uwd/ws?ticket=`.
5. Click **Apply**.

### Configuring Web Collaboration

#### Procedure

1. Log in to the Avaya Meetings Management web administration portal.

2. Navigate to **Devices > Devices by Type > <Web Collaboration server name> > Configuration**.
  3. Configure the following settings:
    - a. In **Service FQDN** and **Local FQDN**, enter the service FQDN that resolves to the IP address of the selected Web Collaboration node.  
For example: `webconferencel.company.com`
    - b. In **IP Address**, enter the IP address that is resolved from the service and local FQDNs.
    - c. In **Public URL Branch**, enter `<Service FQDN>/<Web Collaboration Services node prefix>`.  
For example: `webservices.company.com/webconferencel`.
-  **Note:**
- The public branch URL is used to support multiple Web Collaboration Services nodes with a single public FQDN.
4. Repeat the previous steps for each Web Collaboration Services server that is part of the deployment.

# Chapter 9: System Manager, Avaya Aura<sup>®</sup> Device Services, Media Server, and Avaya Meetings Server configurations

---

## Adding the Avaya Aura<sup>®</sup> Web Gateway to System Manager

### About this task

Use this procedure to enable SSO login and add the Avaya Aura<sup>®</sup> Web Gateway FQDN to the System Manager web console.

#### **Note:**

To set up an Avaya Aura<sup>®</sup> 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<sup>®</sup> Web Gateway cluster.

### Before you begin

Ensure that you have administrative privileges to access System Manager.

For information about accessing System Manager, see *Administering Avaya Aura<sup>®</sup> System Manager*.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.

The system displays the New Elements page.

4. In the General section, from **Type**, select **Avaya Aura Web Gateway**.
5. On the New Avaya Aura Web Gateway page, in the General section, provide the following information:
  - **Name:** Type a name for the element.
  - **Type:** Retain the default setting of **Avaya Aura Web Gateway**.

- **Description:** Type a description for the element.
  - **Node:** Type the FQDN address of the Avaya Aura® Web Gateway server.
6. To enable SSO login, in the Access Profile section, perform the following:
    - a. Click **New**.
    - b. In the Application System Supported Protocol section, in the **Protocol** field, click **URI**.
    - c. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
    - d. In the **Access Profile Type** field, click **EMURL**.
    - e. In the **Protocol** field, click **https**.
    - f. In the **Host** field, type the Avaya Aura® Web Gateway server FQDN.
    - g. In the **Port** field, type 8445.
    - h. In the **Path** field, type /admin.
    - i. In the **Order** field, retain the default value.
    - j. In the **Description** field, type a description of the access profile.
    - k. Click **Save**.
  7. Click **Commit**.
  8. On the System Manager console, click **Elements > Web Gateway** to verify that the Avaya Aura® Web Gateway element has been added.

## Configuring SIP Trunks for the Avaya Aura® Web Gateway on System Manager

### About this task

The Avaya Aura® Web Gateway sends SIP messages to Session Manager port 5061 using TLS. Use this procedure to ensure that Session Manager is configured to accept these messages.

### Important:

For an Avaya Aura® Web Gateway cluster, repeat this procedure for each node in the cluster using the respective node IP or local FQDN when required.

### Before you begin

Set up your Avaya Aura® infrastructure, including System Manager.

### Procedure

1. On the System Manager web console, click **Elements > Routing > SIP Entities**.
2. In the SIP Entities area, click **New** to create a new SIP entity for your server.

You can also edit an existing SIP entity using the **Edit** button.

3. On the SIP Entity Details page, configure the following required field settings:
  - **Name:** Type a name for the SIP entity.
  - **FQDN or IP Address:** Type the FQDN or IP address of the Avaya Aura® Web Gateway.
  - **Type:** Select **SIP Trunk**.
  - **SIP Timer B/F (in seconds):** Retain the default value of 4.
  - **SIP Link Monitoring:** Select **Link Monitoring Disabled**.

For information about other fields, see the SIP entity field descriptions in *Administering Avaya Aura® Session Manager*.

4. In the Entity Links area, click **Add** to add entity links between the newly created SIP entity and the entities representing Session Manager.

While mapping the newly created SIP entity with the Session Manager entities, ensure that the following is set:

- **Protocol:** **TLS**.
- **Port:** **5061**.
- **Connection Policy:** **trusted**.

5. Click **Commit** to save the changes.

## Serviceability agents

You must set up serviceability agents to receive Avaya Aura® Web Gateway alarms in System Manager. To configure serviceability agents, set up an SNMPv3 user profile and an SNMP target profile. Then assign the SNMPv3 user profile to the SNMP target profile.

For more information about managing serviceability agents, see *Administering Avaya Aura® System Manager*.

## Setting up an SNMPv3 user profile

### About this task

An SNMPv3 user profile enables you to define privileges so serviceability agents can read and write data in SNMP Management Information Bases (MIBs).

### Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles**.
2. In the User Details section, click **Edit**.
3. In the **User Name** field, type `initial`.
4. In the **Authentication Protocol** field, select **SHA**.  
The **MD5** setting is not supported.
5. In the **Authentication Password** field, type the authentication password.

The default authentication password is `avaya123`.

6. In the **Confirm Authentication Password** field, confirm the password.
7. In the **Privacy Protocol** field, select **AES**.
8. In the **Privacy Password** field, type the privacy password.

The default privacy password is `avaya123`.

9. In the **Confirm Privacy Password** field, confirm the password.
10. In the **Privileges** field, select **Read/Write**.
11. Click **Commit**.

## Setting up an SNMP target profile

### About this task

An SNMP target profile contains settings for sending alarms from Avaya Aura® Web Gateway to System Manager.

### Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles**.
2. On the Target Details tab, click **Edit**.
3. In the **Name** field, type the name of the profile.
4. In the **Description** field, type a description for the profile.
5. In the **IP Address** field, type the System Manager IP address.
6. In the **Port** field, type `10162`.
7. In the **Notification Type** field, select **Trap**.
8. In the **Protocol** field, select **V3**.
9. Click **Commit**.

## Assigning the SNMPv3 user profile

### About this task

You must assign the SNMPv3 user profile to the target profile so System Manager can receive alarms from Avaya Aura® Web Gateway.

### Before you begin

Set up an SNMPv3 user profile and an SNMP target profile.

### Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. Select the Avaya Aura® Web Gateway host name, and click **Manage Profiles**.

3. Click the **SNMP Target Profiles** tab.
4. In the Assignable Profiles section, click the SNMP target profile you created, and click **Assign**.
5. Click the **SNMPv3 User Profiles** tab.
6. In the Assignable Profiles section, select the SNMPv3 profile you created, and click **Assign**.
7. Click **Commit**.

## Configuring a registration expiration timer

### About this task

The Registration Expiration Timer setting in Session Manager defines a time interval for a SIP server to keep SIP clients registered. Avaya Aura® Web Gateway receives this value from Session Manager and uses it as a refresh interval for SIP registration. The minimal refresh interval supported by Avaya Aura® Web Gateway is 600 seconds or 10 minutes. You must ensure that the Registration Expiration timer in Session Manager is set to at least 600 seconds.

### Procedure

1. In System Manager, navigate to **Elements > Session Manager > Device and Location Configuration > Device Settings Groups**.
2. Select the appropriate Device Settings Group.  
If no additional groups were created, select **Default Group**.
3. In the Server Timer section, ensure that the **Registration Expiration Timer Minimum** value is set to at least 600 seconds.

## Configuring Avaya Aura® Media Server in System Manager

### About this task

This procedure outlines the key System Manager configuration required for the Media Server. Use this procedure to administer locations for all Media Server clusters and assign the Endpoint Services Gateway to each Media Server cluster.

#### **Note:**

Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC.

### Procedure

1. Enroll all Media Server clusters in System Manager.

The enrollment must be done using a System Manager account with administrative privileges for adding, changing, deleting, and viewing all Media Server element types. By doing this, the configuration of the Media Server and the nodes within the cluster will be available on the System Manager server. The Media Server must be enrolled with

System Manager release 7.0.1.1 or higher. For more information about System Manager enrollment, see *Implementing and Administering Avaya Aura® Media Server*.

2. Administer locations for all Media Server clusters.
  - a. In System Manager, navigate to **Elements > Media Server > Server Administration**.
  - b. In each required Media Server, set the location.

For more information about Media Server clusters location setting, see *Managing Avaya Aura® Media Server from System Manager*.

3. Assign “Endpoint Services Gateway” to each cluster of Media Server that will be used by the Avaya Aura® Web Gateway.
  - a. In System Manager, navigate to **Elements > Media Server > Application Assignment**.
  - b. Edit the “Endpoint Services Gateway” application.
  - c. Select the required Media Server clusters.

For more information about Media Server cluster location settings, see *Managing Avaya Aura® Media Server from System Manager*.

---

## Configuring Avaya Aura® Media Server settings

### About this task

This procedure describes how to configure Avaya Aura® Media Server to enable Interactive Connectivity Establishment (ICE) and video processing.

#### **Note:**

For performance reasons, Avaya recommends that you use the client-side TURN service. Use server-side TURN only if you cannot use client-side TURN due to your deployment limitations.

For more information about setting up Avaya Aura® Media Server, see *Implementing and Administering Avaya Aura® Media Server*.

### Before you begin

Ensure that WebLM server licensing is configured and enabled in Avaya Aura® Media Server.

### Procedure

1. Log on to the Avaya Aura® Media Server Element Manager using the URL `https://<AMS_EM_FQDN>:8443/emlogin/`.
2. Navigate to **System Configuration > Server Profile > General Settings**.
3. Select **Firewall NAT Tunneling Media Processor** and **Video Media Processor** and then click **Save**.
4. Navigate to **System Configuration > Signaling Protocols > REST > General Settings**.

5. Select **Enable TLS Mutual Authentication** and click **Save**.
6. Do the following to enable the TURN service on the client side:
  - a. Log in to the Avaya Aura® Web Gateway administration portal.
  - b. Navigate to **External Access > Session Border Controller**.
  - c. Select the **Enable TURN in WebRTC client** check box.
  - d. On the Avaya Aura® Media Server Element Manager, navigate to **System Configuration > Media Processing > ICE > STUN/TURN Servers**.
  - e. Ensure that all STUN and TURN servers are disabled.

For more information about enabling client side TURN for the WebRTC clients, see the sections in [WebRTC client side TURN configuration](#) on page 166.

7. **(Optional)** If you cannot use client-side TURN in your deployment, do the following to enable server-side TURN:
  - a. On the Avaya Aura® Media Server Element Manager, navigate to **System Configuration > Media Processing > ICE > STUN/TURN Servers**.
  - b. Select the required STUN and TURN servers.

**+ Tip:**

You can verify the network configuration when you are using Avaya Session Border Controller (Avaya SBC) to provide the STUN/TURN service. The STUN/TURN address and port configured on the media server must match the STUN/TURN Listen IP & Listen port that are configured for the A1 interface of the Avaya SBC. You must also use the default values for the following settings:

- Protocol: UDP.
- Priority: 0.
- Weight: 10.
- Account: disabled.

8. Navigate to **Licensing > General Settings** and ensure that WebLM server licensing is enabled.
9. Navigate to **Licensing > Monitoring** and ensure that Avaya Aura® Media Server has acquired licenses.
10. For the changes to take effect, navigate to **System Status > Element Status** and click **Restart**.

---

# Configuring the Avaya Aura® Web Gateway on Avaya Aura® Device Services

## About this task

Use this procedure to add the Avaya Aura® Web Gateway FQDN to the Avaya Aura® Device Services trusted hosts and to verify HTTP client settings.

For more information about Avaya Aura® Device Services, see the following documents:

- *Deploying Avaya Aura® Device Services*
- *Administering Avaya Aura® Device Services*

## Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > Trusted Hosts** and click **Add**.
2. In **Host**, type the Avaya Aura® Web Gateway FQDN.

### Important:

Avaya Aura® Device Services requires the FQDN or IP address for each Avaya Aura® Web Gateway cluster node added to the Avaya Aura® Device Services trusted hosts list. Avaya Aura® Device Services also requires the FQDN or IP address of the Avaya Aura® Web Gateway cluster.

3. On the **HTTP Clients** tab, ensure that the **REST** and **OAMP** options are not set to **NONE**.

If these options are set to **NONE**, then the trusted host relationship between the Avaya Aura® Web Gateway and Avaya Aura® Device Services will not work. The Avaya Aura® Web Gateway will also not be able to communicate with Avaya Aura® Device Services.

## Uploading clients to the web deployment service

### About this task

Use this procedure to upload Windows and MacOS clients to the web deployment service.

For Avaya Workplace Client for Windows, you can upload **.exe** or **.msi** installation files. For Avaya Workplace Client for Mac, you can upload **.dmg** installation files, which are packaged in a **.zip** archive.

### Note:

This procedure applies to Team Engagement and Conferencing deployments. This document does not describe the Conferencing-only deployment model.

For more information about web deployment client installers, see *Administering Avaya Aura® Device Services*.

## Procedure

1. Download Avaya Workplace Client for Mac or Avaya Workplace Client for Windows installation files from the Avaya Support website.

 **Note:**

You must have PLDS access to download these files.

2. If you are uploading Avaya Workplace Client for Mac, pack the `Avaya Workplace-<version>.dmg` and `Avaya Workplace Sparkle Update-<version>.dmg` files into a `.zip` archive with no intermediate directories.

If the `.zip` archive contains intermediate directories, re-pack the archive so that it only contains the `.dmg` files in the root directory.

3. Log on to the Avaya Aura® Device Services web administration portal and navigate to **Web Deployment > Deployment**.
4. In **Title**, type a name of the updates or appcast for the client installer.
5. In **Description**, type the description of the client installer updates.
6. In **Version**, type the version details for the Avaya Workplace Client release.
7. In **OS**, select the appropriate Avaya Workplace Client platform:
  - Windows
  - Macintosh
8. In **File**, click **Choose File** and select one of the following files to upload:
  - For Avaya Workplace Client for Windows, select the `.exe` or `.msi` installation file.
  - For Avaya Workplace Client for Mac, select the `.zip` archive containing the `.dmg` installation files.

---

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

### About this task

If your deployment includes Conferencing, use this procedure to perform the required configuration on the Avaya Meetings Server Management portal. For more information about Conferencing configuration, see *Deploying Avaya Meetings Server*.

 **Important:**

- For the Avaya Aura® Web Gateway and Avaya Meetings Server to establish a secure connection, each must trust the Root CA that signed the other's certificates. If the System Manager signed certificates are applied in Avaya Meetings Server, no further action is required on the Avaya Aura® Web Gateway.

If the certificates applied in Avaya Meetings Server are signed by a third-party CA other than System Manager, you must follow the steps outlined in [Adding third-party root CA certificates to the Avaya Aura Web Gateway](#) on page 195. For more information about certificates in Avaya Meetings Server, see *Administering Avaya Meetings Management*.

- A separate User Portal device must be added for each node on the Avaya Aura® Web Gateway cluster using its respective IP address and location.

## Procedure

1. Log on to the Avaya Meetings Server Management portal.
2. Do the following to add the Avaya Aura® Web Gateway server as a managed server device on Avaya Meetings Server:
  - a. Navigate to **Devices > User Portals**.
  - b. To add the Avaya Aura® Web Gateway server to the list, click **Add**.  
The system displays the Add Management Server dialog box.
  - c. Enter a unique display name and IP address of the server.
  - d. From the **Location** drop-down menu, select location to match the Avaya Aura® Web Gateway location assignment on the Avaya Aura® Web Gateway administration portal.
  - e. Click **OK**.
3. Wait for a few minutes until the newly added User Portal Device indicator changes from gray to green.

## Route configuration for an external load balancer

Reverse proxy and load balancer need to accept external and internal connections to the <Service FQDN>:443 address. For example: conferencing.avaya.com:443.

Usually, the Avaya Aura® Web Gateway uses its own internal load balancer that distributes requests between cluster nodes. The Avaya Aura® Web Gateway internal load balancer handles internal and external requests differently:

- Internal requests use port 443.
- External requests use port 8444.

When you use an external load balancer, it redirects internal requests to Avaya Aura® Web Gateway port 443 and external requests to Avaya Aura® Web Gateway port 8444.

The following table shows URL replacement methods that you must configure on the external load balancer to update requests to different servers and services.

| Request URL | Destination Address                             | URL Replace | Component                                        |
|-------------|-------------------------------------------------|-------------|--------------------------------------------------|
| /uwd/rest   | <Avaya Meetings Management Virtual IP FQDN>:443 | /uwd/rest   | Avaya Workplace Client Conference Control (UCCS) |
| /uwd/ws     |                                                 | /uwd/wc     |                                                  |
| /wcs1/      | <WCS1 FQDN>:443                                 | /           | Avaya Aura® Media Server                         |
| /wcs2/      | <WCS2 FQDN>:443                                 | /           |                                                  |

*Table continues...*

| Request URL   | Destination Address                                                                                                                                                                                                                                                           | URL Replace   | Component                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------|
| /wcsX/        | <WCSX FQDN>:443                                                                                                                                                                                                                                                               | /             |                             |
| /ups          | <ul style="list-style-type: none"> <li>• &lt;AAWG Node 1 FQDN&gt;:&lt;port&gt;</li> <li>• &lt;AAWG Node 2 FQDN&gt;:&lt;port&gt;</li> <li>• &lt;AAWG Node X FQDN&gt;:&lt;port&gt;</li> </ul> <p>For internal requests, use port 443. For external requests, use port 8444.</p> | /ups          | Avaya Aura® Web Gateway     |
| /csa          |                                                                                                                                                                                                                                                                               | /csa          |                             |
| /uwd/dist     |                                                                                                                                                                                                                                                                               | /uwd/dist     |                             |
| /notification |                                                                                                                                                                                                                                                                               | /notification |                             |
| /portal       |                                                                                                                                                                                                                                                                               | /portal       |                             |
| /acs          | <ul style="list-style-type: none"> <li>• &lt;AADS Node 1 FQDN&gt;:8448</li> <li>• &lt;AADS Node 2 FQDN&gt;:8448</li> <li>• &lt;AADS Node X FQDN&gt;: 8448</li> </ul>                                                                                                          | /acs          | Avaya Aura® Device Services |

# Chapter 10: Avaya Session Border Controller configuration

Use the following sections to configure Avaya Session Border Controller (Avaya SBC) for the Avaya Aura® Web Gateway. You require Avaya SBC when you have clients located outside the enterprise firewall. For example, Avaya SBC is required if you need remote worker functionality. Avaya SBC is not required if all client users are on the private network within the enterprise firewall.

The Avaya Aura® Web Gateway can use the following services:

- Reverse proxy service, which handles HTTP or HTTPS traffic from outside the firewall into the internal network. Reverse proxy is placed on the DMZ and routes HTTP(S) traffic to the Avaya Aura® Web Gateway for external clients.
- TURN service, which is required when the Avaya Aura® Web Gateway interacts with browser-based audio and video clients outside the enterprise.
- Session border controller service, which is required for audio and video clients to make calls outside the enterprise.

Avaya Session Border Controller provides this functionality as an Edge device. You do not need a dedicated Avaya SBC for Avaya Aura® Web Gateway. You can use any Avaya SBC within the enterprise.

For more information about Avaya SBC configuration, see *Administering Avaya Session Border Controller*.

## Related links

[Required FQDNs and certificates](#) on page 27

---

## Avaya Session Border Controller configuration checklist

Perform the tasks in this checklist to configure Avaya SBC.

| No. | Task                                                                 | Notes | ✓ |
|-----|----------------------------------------------------------------------|-------|---|
| 1   | Ensure that you have a pool of IP addresses available for Avaya SBC. | —     |   |

*Table continues...*

| No. | Task                                                                                                           | Notes                                                                                                                                                                                                                                                                                                                                                                                                   | ✓ |
|-----|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 2   | Configure reverse proxy.                                                                                       | <ul style="list-style-type: none"> <li>In a single FQDN for all services deployment, complete the tasks outlined in <a href="#">Reverse proxy configuration checklist for a single FQDN deployment</a> on page 151.</li> <li>In a multiple FQDN deployment, complete the tasks outlined in <a href="#">Reverse proxy configuration checklist for a multiple FQDN deployment</a> on page 152.</li> </ul> |   |
| 3   | If you are planning to use external clients outside the enterprise firewall, configure external client access. | Complete procedures in <a href="#">External client access configuration</a> on page 162.                                                                                                                                                                                                                                                                                                                |   |

## Reverse proxy configuration

### Reverse proxy configuration checklist for a single FQDN deployment

Perform the tasks outlined in this checklist to configure reverse proxy on the Avaya SBC if you are using a single FQDN for all services.

| No. | Task                                           | Notes                                                                                                                                                                 | ✓ |
|-----|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Verify prerequisites.                          | See <a href="#">Prerequisites</a> on page 152.                                                                                                                        |   |
| 2   | Create a TLS server profile for reverse proxy. | See <a href="#">Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment</a> on page 153.                                            |   |
| 3   | Configure a CA.                                | See <a href="#">Certificate Authority configuration checklist</a> on page 155.<br><br>You must have the CA that is used to sign certificates for internal components. |   |
| 4   | Enable web socket support.                     | See <a href="#">Enabling web socket support</a> on page 156.                                                                                                          |   |

*Table continues...*

| No. | Task                                           | Notes                                                                                                                                                                                                                                                                                                                                                                        | ✓ |
|-----|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 5   | Configure external and internal traffic rules. | <ul style="list-style-type: none"> <li>For configuring external traffic rules, see <a href="#">Configuring external traffic rules in a single FQDN for all services deployment</a> on page 156.</li> <li>For configuring internal traffic rules, see <a href="#">Configuring internal traffic rules in a single FQDN for all services deployment</a> on page 158.</li> </ul> |   |

**Related links**

[Avaya Session Border Controller configuration checklist](#) on page 150

## Reverse proxy configuration checklist for a multiple FQDN deployment

Perform the tasks outlined in this checklist to configure reverse proxy on the Avaya SBC if you are using a multiple FQDNs for services.

| No. | Task                                                            | Description                                                                                                                                                       | ✓ |
|-----|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Verify prerequisites.                                           | See <a href="#">Prerequisites</a> on page 152.                                                                                                                    |   |
| 2   | Create TLS server profiles for each service in your deployment. | See <a href="#">Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment</a> on page 154.                                       |   |
| 3   | Configure a CA                                                  | See <a href="#">Certificate Authority configuration checklist</a> on page 155.<br>You must have the CA that is used to sign certificates for internal components. |   |
| 4   | Enable web socket support.                                      | See <a href="#">Enabling web socket support</a> on page 156.                                                                                                      |   |
| 5   | Configure external traffic rules                                | See <a href="#">Configuring external traffic rules in a multiple FQDN deployment</a> on page 160.                                                                 |   |

**Related links**

[Avaya Session Border Controller configuration checklist](#) on page 150

## Prerequisites

Before configuring Avaya SBC as a reverse proxy:

- Ensure that you have a global FQDN.

- If you are using a single FQDN for all services, ensure that you have the following interfaces on Avaya SBC:
  - One B1 interface for external traffic.
  - One A1 interface for outgoing HTTP traffic that runs to Avaya Meetings Server Management, Web Collaboration Services, and Avaya Aura® Web Gateway.
  - One A1 interface for internal enterprise HTTP traffic.
- If you are using multiple FQDNs, ensure that you have the following interfaces on Avaya SBC:
  - One B1 interface per FQDN for each service.
  - One A1 interface for outgoing HTTP traffic that runs to Avaya Meetings Server Management, Web Collaboration Services, and Avaya Aura® Web Gateway components.

## Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                             | ✓ |
|-----|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a certificate signing request.                        | See <a href="#">Certificate setup</a> on page 178.<br>Use the following options specific for this deployment model: <ul style="list-style-type: none"> <li>• For <b>Common Name</b>, use the global FQDN. For example:<br/>webservices.company.com.</li> <li>• For <b>Subject Alternative Name</b>, use the global FQDN. For example:<br/>DNS:webservices.company.com.</li> </ul> |   |
| 2   | Download and save the created .KEY and .CSR files.           |                                                                                                                                                                                                                                                                                                                                                                                   |   |
| 3   | Send the .CSR file to a public CA for signing.               |                                                                                                                                                                                                                                                                                                                                                                                   |   |
| 4   | Install the signed certificate and the key on the Avaya SBC. | See <a href="#">Installing a certificate and a key</a> on page 180.<br>When installing the certificate, use a descriptive name. For example:<br>webservicesCert.                                                                                                                                                                                                                  |   |

*Table continues...*

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                             | ✓ |
|-----|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 5   | Create a TLS server profile using the installed certificate. | <p>See <a href="#">Creating a TLS server profile</a> on page 183.</p> <p>When creating a profile, use the certificate installed on the Avaya SBC in the previous step.</p> <p>Provide a descriptive name for the profile. For example: webservicestlsProfile.</p> |   |

**Related links**

[Reverse proxy configuration checklist for a single FQDN deployment](#) on page 151

## Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ✓ |
|-----|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create certificate signing requests for each service FQDNs.  | <p>See <a href="#">Certificate setup</a> on page 178.</p> <p>Create one certificate for each FQDN used by services deployed in the solution, such as Avaya Meetings Server Management service, Web Collaboration Services, and Avaya Aura® Web Gateway/Portal. If you are using several Web Collaboration Services servers, you need to create a separate CSR for each Web Collaboration Services FQDN. Use the following options specific for this deployment model:</p> <ul style="list-style-type: none"> <li>For <b>Common Name</b>, use the FQDN assigned to that service. For example: <code>conferencing_management.company.com</code> for Avaya Meetings Server Management service.</li> <li>For <b>Subject Alternative Name</b>, use the global FQDN. For example: <code>DNS:conferencing_management.company.com</code> for Avaya Meetings Server Management service.</li> </ul> |   |
| 2   | For each CSR, download and save created .KEY and .CSR files. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |   |
| 3   | Send .CSR files to a public CA for signing.                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |   |

*Table continues...*

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                            | ✓ |
|-----|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 4   | Install the signed certificates and keys on the Avaya SBC.   | <p>See <a href="#">Installing a certificate and a key</a> on page 180.</p> <p>When installing certificates, use descriptive names. For example: <code>conferencingManagementCert</code> for the Avaya Meetings Server Management service certificate.</p> <p><b>* Note:</b></p> <p>When installing a certificate, make sure that you use the corresponding key. Do not install keys of another certificates.</p> |   |
| 5   | Create TLS server profiles using the installed certificates. | <p>See <a href="#">Creating a TLS server profile</a> on page 183.</p> <p>When creating profiles, use certificates installed on the Avaya SBC in the previous step.</p> <p>Provide a descriptive name for each profile. For example: <code>conferenceMgmtTlsProfile</code> for the Avaya Meetings Server Management service profile.</p>                                                                          |   |

**Related links**

[Reverse proxy configuration checklist for a multiple FQDN deployment](#) on page 152

**Certificate Authority configuration checklist**

You must have the CA that is used to sign certificates for internal components.

- In a single FQDN for all services deployment, certificates for internal components are usually signed by the System Manager CA.
- In a multiple FQDN deployment, certificates for internal components are usually signed by a public CA.

To configure a CA, perform the tasks outlined in the following checklist:

| No. | Task                             | Notes                                                                                                                                                                          | ✓ |
|-----|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Install the CA on the Avaya SBC. | <p>See <a href="#">Installing a CA certificate on Avaya SBC</a> on page 182.</p> <p>Provide a descriptive name for the CA. For example: <code>certificateAuthority</code>.</p> |   |

*Table continues...*

| No. | Task                         | Notes                                                                                                                                                                                                                                                                    | ✓ |
|-----|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 2   | Create a TLS client profile. | <p>See <a href="#">Creating a TLS client profile</a> on page 183.</p> <p>When creating the profile, use the CA that you installed in the previous step.</p> <p>Provide a descriptive name for the profile. For example: <code>certificateAuthorityTlsProfile</code>.</p> |   |

**Related links**

[Reverse proxy configuration checklist for a single FQDN deployment](#) on page 151

[Reverse proxy configuration checklist for a multiple FQDN deployment](#) on page 152

## Enabling web socket support

**Procedure**

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Global Profiles > Reverse Proxy Policy**.
3. Click **Add**.
4. In the **Rule Name** field, provide a name for the reverse proxy policy and then click **Next**.
5. In the General area, select the **Allow Web Socket** check box.
6. For the other settings, use the default values.
7. Click **Finish**.

## Configuring external traffic rules in a single FQDN for all services deployment

**Before you begin**

Ensure that you have:

- The TLS server profile for reverse proxy. For more information, see the TLS server profile creation tasks outlined in [Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment](#) on page 153.
- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in [Certificate Authority configuration checklist](#) on page 155.

Use the same TLS server and client profiles when configuring both external and internal traffic rules.

**Procedure**

1. Log in to the Avaya SBC web administration portal.

2. Navigate to **Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.
5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the external B1 interface and the Avaya SBC external leg IP addresses.
7. In **Listen Port**, enter 443.
8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.  
An example of the TLS profile name is `webservicestlsProfile`.
10. **Connect IP**: Select the internal A1 interface and the Avaya SBC internal leg IP address.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.  
An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in [External traffic rules for a single FQDN deployment](#) on page 157.
15. Click **Finish**.

#### Related links

[External traffic rules for a single FQDN deployment](#) on page 157

[Reverse proxy configuration checklist for a single FQDN deployment](#) on page 151

### External traffic rules for a single FQDN deployment

| Server Address                       | White list URL | URL replace   | Description                                                                                                                                                                                           |
|--------------------------------------|----------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Avaya Meetings Management FQDN>:443 | /uwd/<br>rest  | /uwd/<br>rest | Avaya Meetings Control (UCCS) Avaya Meetings Server Management FQDN resolves to the virtual IP of the Avaya Meetings Server Management Server.                                                        |
| <Avaya Meetings Management FQDN>:443 | /uwd/ws        | /uwd/<br>rest | If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: <code>conferencing_management.company.com</code> .                                                   |
| <WCS1 FQDN>: 443                     | /wcs1          | /             | Avaya Aura <sup>®</sup> Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura <sup>®</sup> Media Server, and it resolves to the |
| <WCS2 FQDN>: 443                     | /wcs2          | /             |                                                                                                                                                                                                       |

*Table continues...*

| Server Address                                  | White list URL    | URL replace       | Description                                                                                                                                                        |
|-------------------------------------------------|-------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WCSX FQDN>: 443                                | /wcsX             | /                 | corresponding Avaya Aura® Media Server IP. For example: webconference1.company.com, webconference2.company.com, and so on.                                         |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /acs              | /acs              | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the Avaya Aura® Web Gateway system. For example: webgateway.company.com. |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /ups              | /ups              |                                                                                                                                                                    |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /csa              | /csa              |                                                                                                                                                                    |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /uwd/<br>dist     | /uwd/<br>dist     |                                                                                                                                                                    |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /notifica<br>tion | /notifica<br>tion |                                                                                                                                                                    |
| <Avaya Aura® Web GatewayVirtual IP FQDN>: 8444  | /portal           | /portal           |                                                                                                                                                                    |

## Configuring internal traffic rules in a single FQDN for all services deployment

### Before you begin

Ensure that you have:

- The TLS server profile for reverse proxy. For more information, see the TLS server profile creation tasks outlined in [Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment](#) on page 153.
- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in [Certificate Authority configuration checklist](#) on page 155.

Use the same TLS server and client profiles when configuring both external and internal traffic rules.

### Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.

5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the internal A1 interface and the Avaya SBC external leg IP address.
7. In **Listen Port**, enter 443.
8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.  
An example of the TLS server profile name is `webservicesTlsProfile`.
10. In **Connect IP**, select the internal A1 interface and the Avaya SBC internal leg IP addresses.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.  
An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in [Internal traffic rules for a single FQDN deployment](#) on page 159.
15. Click **Finish**.

#### Related links

[Internal traffic rules for a single FQDN deployment](#) on page 159

[Reverse proxy configuration checklist for a single FQDN deployment](#) on page 151

### Internal traffic rules for a single FQDN deployment

| Server Address                                 | White list URL | URL replace   | Description                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|----------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Avaya Meetings Management FQDN>:443           | /uwd/<br>rest  | /uwd/<br>rest | Avaya Meetings Control (UCCS) Avaya Meetings Management FQDN resolves to the virtual IP of the Avaya Meetings Management.                                                                                                                                                                                                            |
| <Avaya Meetings Management FQDN>:443           | /uwd/ws        | /uwd/<br>rest | If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: <code>conferencing_management.company.com</code> .                                                                                                                                                                                  |
| <WCS1 FQDN>: 443                               | /wcs1          | /             | Avaya Aura® Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura® Media Server, and it resolves to the corresponding Avaya Aura® Media Server IP. For example: <code>webconference1.company.com</code> , <code>webconference2.company.com</code> , and so on. |
| <WCS2 FQDN>: 443                               | /wcs2          | /             |                                                                                                                                                                                                                                                                                                                                      |
| <WCSX FQDN>: 443                               | /wcsX          | /             |                                                                                                                                                                                                                                                                                                                                      |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /acs           | /acs          | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the                                                                                                                                                                                                                                        |

*Table continues...*

| Server Address                                 | White list URL    | URL replace       | Description                                                          |
|------------------------------------------------|-------------------|-------------------|----------------------------------------------------------------------|
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /ups              | /ups              | Avaya Aura® Web Gateway system. For example: webgateway.company.com. |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /csa              | /csa              |                                                                      |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /uwd/<br>dist     | /uwd/<br>dist     |                                                                      |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /notifica<br>tion | /notifica<br>tion |                                                                      |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | /portal           | /portal           |                                                                      |

## Configuring external traffic rules in a multiple FQDN deployment

### About this task

Perform this procedure for each service in your deployment. For example, if you have multiple Web Collaboration Services servers in your deployment, you must perform this procedure for each server.

### Before you begin

Ensure that you have:

- TLS server profiles for each service in your deployment. For more information, see the TLS server profile creation tasks outlined in [Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment](#) on page 154.
- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in [Reverse proxy configuration checklist for a multiple FQDN deployment](#) on page 152.

### Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Device Specific Settings > DMZ Services > Relay Services > Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.
5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the external B1 interface and the Avaya SBC external leg IP address.
7. In **Listen Port**, enter 443.

8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.  
An example of the TLS server profile name for Web Collaboration Services is `webservicesTLSProfile`.
10. In **Connect IP**, select the internal interface A1 and the Avaya SBC internal leg IP address.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.  
An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in [External traffic rules for a single FQDN deployment](#) on page 157.
15. Click **Finish**.

#### Related links

[External traffic rules in a multiple FQDN deployment](#) on page 161

[Reverse proxy configuration checklist for a multiple FQDN deployment](#) on page 152

## External traffic rules in a multiple FQDN deployment

### Traffic rules for Avaya Meetings Server Management

| Server Address                       | White list URL | URL replace   | Description                                                                                                                                         |
|--------------------------------------|----------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <Avaya Meetings Management FQDN>:443 | /uwd/<br>rest  | /uwd/<br>rest | Avaya Meetings Control (UCCS) Avaya Meetings Management FQDN resolves to the virtual IP of the Avaya Meetings Management.                           |
| <Avaya Meetings Management FQDN>:443 | /uwd/ws        | /uwd/<br>rest | If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: <code>conferencing_management.company.com</code> . |

### Traffic rules for Web Collaboration Services

| Server Address   | White list URL | URL replace | Description                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WCSX FQDN>: 443 | /              | /           | Avaya Aura® Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura® Media Server, and it resolves to the corresponding Avaya Aura® Media Server IP. For example: <code>webconference1.company.com</code> , <code>webconference2.company.com</code> , and so on. |

### Traffic rules for Avaya Aura® Web Gateway/Portal

| Server Address                                  | White list URL | URL replace | Description                                                                                                                                                                      |
|-------------------------------------------------|----------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | /              | /           | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the Avaya Aura® Web Gateway system. For example: <code>webgateway.company.com</code> . |

## External client access configuration

The following sections describe how to configure Avaya SBC if you are planning to use any external clients, including WebRTC, mobile, or desktop clients, outside the enterprise firewall.

### External client access configuration checklist

Perform the tasks outlined in this checklist if you are planning to use any external clients, including WebRTC, mobile, or desktop clients, outside the enterprise firewall.

| No. | Task                                                                         | Notes                                                                                                       | ✓ |
|-----|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a server TLS profile for a management interface.                      | See <a href="#">Checklist for creation of a TLS server profile for a management interface</a> on page 162.  |   |
| 2   | Configure Avaya SBC load monitoring.                                         | See <a href="#">Configuring Avaya SBC load monitoring</a> on page 163.                                      |   |
| 3   | Add Avaya SBC to the Avaya Aura® Web Gateway.                                | See <a href="#">Adding Avaya Session Border Controller to the Avaya Aura Web Gateway</a> on page 164.       |   |
| 4   | If you have conferencing, add Avaya SBC to Avaya Meetings Server Management. | See <a href="#">Adding Avaya Session Border Controller to Avaya Meetings Server Management</a> on page 165. |   |
| 5   | Configure WebRTC client side TURN.                                           | See <a href="#">WebRTC client side TURN configuration</a> on page 166.                                      |   |
| 6   | Configure support for external native media clients.                         | See <a href="#">External native clients media configuration</a> on page 171.                                |   |

## Checklist for creation of a TLS server profile for a management interface

Perform the tasks in this checklist to configure certificates and create a TLS server profile for a management interface. This is required for external client access configuration.

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ✓ |
|-----|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a certificate signing request.                        | <p>See <a href="#">Creating a certificate signing request on Avaya Session Border Controller</a> on page 178.</p> <p>When creating a CSR, use the following options:</p> <ul style="list-style-type: none"> <li>• For <b>Common Name</b>, use the management interface FQDN. For example:<br/>asbce_management.company.com.</li> <li>• For <b>Subject Alternative Name</b>, provide both the FQDN and IP address of the management interface. For example:<br/>DNS:asbce_management.company.com<br/>IP:10.10.10.10</li> </ul> |   |
| 2   | Download and save created .KEY and .CSR files.               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |   |
| 3   | Send the .CSR file to the System Manager CA for signing.     | See <a href="#">Signing certificates with the System Manager CA</a> on page 179.                                                                                                                                                                                                                                                                                                                                                                                                                                              |   |
| 4   | Install the signed certificate and the key on the Avaya SBC. | <p>See <a href="#">Installing a certificate and a key</a> on page 180.</p> <p>When installing the certificate, use a descriptive name. For example:<br/>asbceManagementCert.</p>                                                                                                                                                                                                                                                                                                                                              |   |
| 5   | Create a TLS server profile using the installed certificate. | <p>See <a href="#">Creating a TLS server profile</a> on page 183.</p> <p>When creating a profile, use the certificate installed on the Avaya SBC in the previous step.</p> <p>Provide a descriptive name for the profile. For example: asbceManagementTlsProfile.</p>                                                                                                                                                                                                                                                         |   |

**Related links**

[External client access configuration checklist](#) on page 162

## Configuring Avaya SBC load monitoring

**About this task**

Perform this procedure if you are using external clients in your deployment.

## Before you begin

Ensure that you have:

- The internal A1 interface that will be used for load monitoring.

 **Note:**

This A1 interface must also be used for the TURN relay setup.

- An FQDN for the Avaya SBC management interface. For more information, see [Required FQDNs and certificates](#) on page 27.
- A TLS server profile. For more information about creating this profile, see [Checklist for creation of a TLS server profile for a management interface](#) on page 162.

## Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Device Specific Settings > Advanced Options > Load Monitoring**.
3. Click **Add** to create a new monitoring profile.
4. In **Load Balancer Type**, select **INTERNAL**.

This is the load balancer on the A1 side of the network. Avaya Aura® Web Gateway performs load balancing towards the internal side. All HTTP requests sent for dialing out use the internal load balancer logic to identify the appropriate Avaya SBC.

5. In **Transport**, select **TLS**.
6. In **TLS Profile**, select the TLS server profile that you created.

For more information, see the tasks outlined in [Checklist for creation of a TLS server profile for a management interface](#) on page 162.

7. In **Listen IP**, select the internal A1 interface.

To enable external WebRTC clients, the same interface must be configured for the TURN server as the A1 interface.

8. In **Service Type**, select **TURN**.
9. Click **Finish**.

## Next steps

Add Avaya SBC to the Avaya Aura® Web Gateway.

# Adding Avaya Session Border Controller to the Avaya Aura® Web Gateway

## Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal.
2. Click **Add** to add a new Avaya SBC or click **Edit** to update the information for the existing Avaya SBC connection.

3. In **SIP Address**, type the FQDN or IP address of the internal A1 interface of the Avaya SBC that is used for SIP signaling to interact with Avaya Aura® Web Gateway.

For more information, see [External native clients media configuration](#) on page 171.

4. In **IP Port**, enter 5061.
5. In **SIP Protocol**, select **TLS**.
6. In **HTTP Address**, type the internal Avaya SBC FQDN specified for the load monitoring entry.  
For example: `asbce_management.company.com`.
7. In **HTTP Port**, enter 443.
8. In **HTTP Protocol**, select **https**.
9. In **Location**, specify the location of the Avaya SBC server.
10. Click **Save**.

### Next steps

If you have conferencing, add Avaya SBC to Avaya Meetings Server Management.

## Adding Avaya Session Border Controller to Avaya Meetings Server Management

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Devices > Devices by Type > ASBCE**.
3. Click **Add**.
4. On the Add ABSCE page, do the following:
  - a. In **Name**, enter a name for the Avaya SBC server.
  - b. In **IP Address**, enter any of the Avaya SBC IP addresses.
  - c. In **Location**, select the location of the Avaya SBC server.

5. Click **OK**.

6. Select the Avaya SBC name from the list and do the following:

- a. In **Listen/Relay Internal IP**, enter the Avaya SBC IP address of the internal A1 interface configured for the load balancer and for STUN/TURN interface.

For more information, see [Configuring Avaya SBC load monitoring](#) on page 163 and [WebRTC client side TURN configuration](#) on page 166.

- b. In **Port**, enter 3478.

- c. In **Listen/Relay Public IP**, enter one of the following Avaya SBC public IP addresses of the STUN/TURN interface:

- The IP address of the external B1 interface.
- The firewall NAT public IP address of the external B1 interface.

For more information about the B1 interface, see [WebRTC client side TURN configuration](#) on page 166.

- d. In **Port**, enter 3478.

- e. In **Internal SIP IP**, type the FQDN or IP address of the internal A1 interface of the Avaya SBC that is used for SIP signaling.

For more information about interaction with Avaya Aura® Web Gateway, see [External native clients media configuration](#) on page 171.

- f. In **SIP Protocol** select **TLS**.

- g. In **SIP Port**, enter 5061.

- h. In **Local HTTP IP**, enter the internal A1 address configured for the load monitoring entry.

For example, `asbce_management.company.com`.

- i. In **HTTP protocol**, select **https**.

- j. In **HTTP port**, enter 443.

7. Click **OK**.

## WebRTC client side TURN configuration

Avaya recommends using client side TURN instead of sever side TURN whenever possible. If you use server side TURN and WebRTC browsers are behind a firewall that blocks UDP traffic, you might experience issues with WebRTC calls. Clients are loaded from your browser and no installation is required on client users' computers.

Use these sections to enable client side TURN for WebRTC browsers outside your enterprise firewall.

To enable client side TURN, you need to open TCP port 443 on the external firewall.

### Related links

[External client access configuration checklist](#) on page 162

## Checklist for WebRTC client side TURN configuration

Perform the tasks outlined in this checklist to configure external client access.

| No. | Task                  | Notes                                          | ✓ |
|-----|-----------------------|------------------------------------------------|---|
| 1   | Verify prerequisites. | See <a href="#">Prerequisites</a> on page 167. |   |

*Table continues...*

| No. | Task                                                                                                       | Notes                                                                                                                   | ✓ |
|-----|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---|
| 2   | Create a TLS server profile that is used if media tunneling requires better readability through firewalls. | See <a href="#">TLS server profile checklist for client side TURN configuration</a> on page 167.                        |   |
| 3   | Configure firewall rules.                                                                                  | See <a href="#">Firewall configuration</a> on page 168.                                                                 |   |
| 4   | Configure a TURN/STUN profile for WebRTC calls on Avaya SBC.                                               | See <a href="#">Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller</a> on page 169.    |   |
| 5   | Configure the TURN relay service for WebRTC calls on Avaya SBC.                                            | See <a href="#">Configuring the TURN relay service for WebRTC calls on Avaya Session Border Controller</a> on page 170. |   |
| 6   | Configure a STUN server on the Avaya Aura® Web Gateway.                                                    | See <a href="#">TURN/STUN service configuration on the Avaya Aura Web Gateway</a> on page 170.                          |   |
| 7   | Enable TURN usage in a WebRTC client.                                                                      | See <a href="#">Enabling TURN usage in a WebRTC client</a> on page 171.                                                 |   |

## Prerequisites

Before configuring WebRTC client side TURN settings, do the following:

- Add Avaya SBC to the Avaya Aura® Web Gateway. For more information, see [Adding Avaya Session Border Controller to the Avaya Aura Web Gateway](#) on page 164.
- Configure one B1 interface IP address on the Avaya SBC.

Additional internal A1 interfaces are not required. Use the same A1 interface IP that you used for load monitoring. For more information, see [Configuring Avaya SBC load monitoring](#) on page 163.

## TLS server profile checklist for client side TURN configuration

Perform the tasks outlined in this checklist to create a TLS server profile that is used if media tunneling requires better readability through firewalls.

| No. | Task                                  | Notes                                                                                                                                                                                                                                                                                                                                                                | ✓ |
|-----|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a certificate signing request. | See <a href="#">Certificate setup</a> on page 178.<br>Use the following options: <ul style="list-style-type: none"> <li>• For <b>Common Name</b>, use the TURN media FQDN. For example: <code>turnmedia.company.com</code>.</li> <li>• For <b>Subject Alternative Name</b>, use the TURN media FQDN. For example: <code>DNS:turnmedia.company.com</code>.</li> </ul> |   |

*Table continues...*

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                    | ✓ |
|-----|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 2   | Download and save the created .KEY and .CSR files.           |                                                                                                                                                                                                                                                          |   |
| 3   | Send the .CSR file to a public CA for signing.               |                                                                                                                                                                                                                                                          |   |
| 4   | Install the signed certificate and the key on the Avaya SBC. | See <a href="#">Installing a certificate and a key</a> on page 180.<br><br>When installing the certificate, use a descriptive name. For example: turnmediaCert.                                                                                          |   |
| 5   | Create a TLS server profile using the installed certificate. | See <a href="#">Creating a TLS server profile</a> on page 183.<br><br>When creating a profile, use the certificate installed on the Avaya SBC in the previous step.<br><br>Provide a descriptive name for the profile. For example: turnmediaTlsProfile. |   |

## Firewall configuration

### External firewall rules

| Port | Protocol    | Description                                                                                                                                                                                                |
|------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 443  | TLS         | For TLS TURN. For traffic that runs from the internet to Avaya SBC on the B interface.<br><br>This option is only required if you are using TLS TURN and it provides better readability through firewalls. |
| 3478 | TCP and UDP | For UDP media. For traffic that runs from the internet to Avaya SBC on the B interface.<br><br>This option is only required if you are using direct WebRTC media.                                          |

### Internal firewall rules

| Port           | Protocol | Description                                                                                                                               |
|----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 3478           | UDP      | For UDP media from Avaya SBC. For traffic that runs from the A interface of Avaya SBC to the MCU 7K servers and Avaya Aura® Media Server. |
| 50000 to 55000 | UDP      | For UDP media from Avaya SBC. For traffic that runs from the A interface of Avaya SBC to the MCU 7K servers and Avaya Aura® Media Server. |

*Table continues...*

| Port           | Protocol | Description                                                                                                            |
|----------------|----------|------------------------------------------------------------------------------------------------------------------------|
| 12000 to 13200 | UDP      | For UPD media from media servers. For traffic that runs from MCU 7K servers to the A interface of Avaya SBC.           |
| 16384 to 16984 | UDP      | For UPD media from media servers. For traffic that runs from MCU 7K servers to the A interface of Avaya SBC.           |
| 6000 to 32588  | UDP      | For UPD media from media servers. For traffic that runs from Avaya Aura® Media Server to the A interface of Avaya SBC. |

## Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller

### Procedure

1. Log in to the Avaya SBC web administration interface.
2. Navigate to **Device Specific Settings > TURN/STUN Service**.
3. From the Application pane, select the Avaya SBC device for which the new TURN/STUN profile will be created.
4. Click **TURN/STUN Profiles**.
5. Click **Add**.

The system displays the Add TURN/STUN Profile window.

6. In **Profile Name**, provide a name for the TURN/STUN profile.

For example: `turnProfileForWebrtcCalls`.

7. In **UDP Listen Port**, enter 3478.
8. In **TCP/TLS Listen Port**, enter 443.
9. If TLS TURN media is required, then in **TLS Server Profile**, specify the TLS server profile for a management interface that you created.

For more information, see the tasks outlined in [TLS server profile checklist for client side TURN configuration](#) on page 167. An example of the TLS server profile name is `turnmediaTlsProfile`.

10. In **Media Relay Port Range**, specify a range that does not overlap with the port range used by Avaya SBC for other protocols, such as SIP.

The default range is 50000 to 55000.

11. Select the **Authentication** check box.
12. Select the **Client Authentication** check box.
13. Select the **UDP Relay** check box.
14. Click **Finish**.

## Configuring the TURN relay service for WebRTC calls on Avaya Session Border Controller

### Procedure

1. Log in to the Avaya SBC web administration interface.
2. Navigate to **Device Specific Settings > TURN/STUN Service**.
3. From the Application pane, select the Avaya SBC device for which you need to create a new TURN relay service.
4. Click **TURN/STUN Relay**.
5. Click **Add**.

The system displays the Add TURN/STUN IP Pairing window.

6. In **Listen IP**, provide the listen IP address of the TURN server from the B1 interface.

#### **Important:**

Do *not* use this IP address for any other interface bound to port 443.

7. In **Media Relay**, provide the media relay IP address of the TURN server from the internal A1 interface that you used for load monitoring.
8. In **Service FQDN**, provide the FQDN that resolves to the address specified in the **Listen IP** field.

For example, `turnmedia.company.com`.

9. In **TURN/STUN Profile**, select the TURN/STUN profile that you created for WebRTC calls.
10. Complete the following fields:

In **TURN/STUN Profile**, select the TURN/STUN profile that you created for WebRTC calls.

For example: `turnProfileForWebrtcCalls`. For more information, see [Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller](#) on page 169.

11. Click **Finish**.

## TURN/STUN service configuration on the Avaya Aura® Web Gateway

You can add a new STUN server and set the STUN server priority from **External Access > STUN Servers** on the Avaya Aura® Web Gateway administration portal. If you use client side TURN, you must add the IP address of Avaya SBC as a STUN server. Avaya recommends using client side TURN whenever possible.

You must use port 3478 when adding a new STUN server.

For more information about configuring STUN server settings on Avaya Aura® Web Gateway, see “Managing STUN server settings” in *Administering the Avaya Aura® Web Gateway*.

## Enabling TURN usage in a WebRTC client

### Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access > Session Border Controller**.
2. Select the **Enable TURN in WebRTC Client** check box.
3. Click **Save**.

## External native clients media configuration

Use the following sections if you are planning to use Avaya Workplace Client mobile and desktop clients outside of your enterprise firewall.

### Related links

[External client access configuration checklist](#) on page 162

## External native clients media configuration checklist

Perform the tasks outlined in this checklist if you are planning to use Avaya Workplace Client mobile and desktop clients outside of your enterprise firewall.

| No. | Task                                                                            | TLS server profile required for SIP communications with Avaya SBC                                                                                                                                                                                                                                                                                                                                                                        | ✓ |
|-----|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Verify prerequisites.                                                           | See <a href="#">Prerequisites</a> on page 172.                                                                                                                                                                                                                                                                                                                                                                                           |   |
| 1   | Create a TLS server profile for required for SIP communications with Avaya SBC. | See <a href="#">TLS server profile checklist for external native clients media configuration</a> on page 172.<br><br>In a multiple FQDN deployment, you can use the TLS server profile for Avaya Meetings Server Management, which you created during the reverse proxy configuration. For more information, see <a href="#">Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment</a> on page 154. |   |
| 2   | Create a TLS server profile for HTTP media tunneling.                           | See <a href="#">TLS server profile checklist for media tunneling interfaces</a> on page 173.                                                                                                                                                                                                                                                                                                                                             |   |
| 3   | Configure firewall rules.                                                       | See <a href="#">Firewall configuration</a> on page 174.                                                                                                                                                                                                                                                                                                                                                                                  |   |
| 4   | Configure the Avaya SBC signaling interface.                                    | See <a href="#">Configuring the Avaya Session Border Controller signaling interface</a> on page 174.                                                                                                                                                                                                                                                                                                                                     |   |
| 5   | Configure the Avaya SBC media interface.                                        | See <a href="#">Configuring the Avaya Session Border Controller media interface</a> on page 175.                                                                                                                                                                                                                                                                                                                                         |   |
| 6   | Configure Avaya SBC server flows.                                               | See <a href="#">Configuring Avaya Session Border Controller server flows</a> on page 176.                                                                                                                                                                                                                                                                                                                                                |   |

## Prerequisites

Before configuring support for external native clients media, do the following:

- Add Avaya SBC to the Avaya Aura® Web Gateway. For more information, see [Adding Avaya Session Border Controller to the Avaya Aura Web Gateway](#) on page 164.
- Configure one A interface IP address and one B interface IP address on the Avaya SBC.

## TLS server profile checklist for external native clients media configuration

Perform the following tasks to create a TLS server profile required for SIP communications with Avaya SBC.

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                                                            | ✓ |
|-----|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a certificate signing request.                        | See <a href="#">Certificate setup</a> on page 178.<br>Use the following options:<br><ul style="list-style-type: none"> <li>• For <b>Common Name</b>, use the Avaya Meetings Management FQDN. For example:<br/>conferencing_management.company.com.</li> <li>• For <b>Subject Alternative Name</b>, use the Avaya Meetings Management FQDN. For example:<br/>DNS:conferencing_management.comp any.com.</li> </ul> |   |
| 2   | Download and save the created .KEY and .CSR files.           |                                                                                                                                                                                                                                                                                                                                                                                                                  |   |
| 3   | Send the .CSR file to the System Manager CA for signing.     | See <a href="#">Signing certificates with the System Manager CA</a> on page 179.                                                                                                                                                                                                                                                                                                                                 |   |
| 4   | Install the signed certificate and the key on the Avaya SBC. | See <a href="#">Installing a certificate and a key</a> on page 180.<br>When installing the certificate, use a descriptive name. For example:<br>conferencingManagementSipCert.                                                                                                                                                                                                                                   |   |
| 5   | Create a TLS server profile using the installed certificate. | See <a href="#">Creating a TLS server profile</a> on page 183.<br>When creating a profile, use the certificate installed on Avaya SBC in the previous step.<br>Provide a descriptive name for the profile. For example:<br>conferencingManagementSipTlsProfile.                                                                                                                                                  |   |

**Related links**

[External native clients media configuration checklist](#) on page 171

[TLS server profile checklist for media tunneling interfaces](#) on page 173

**TLS server profile checklist for media tunneling interfaces**

Perform the following tasks to create a TLS server profile required for SIP communications with Avaya SBC.

| No. | Task                                                         | Notes                                                                                                                                                                                                                                                                                                                                                                           | ✓ |
|-----|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Create a certificate signing request.                        | See <a href="#">Certificate setup</a> on page 178.<br>Use the following options:<br><ul style="list-style-type: none"> <li>• For <b>Common Name</b>, use the HTTP media tunneling FQDN. For example: <code>media.company.com</code>.</li> <li>• For <b>Subject Alternative Name</b>, use the HTTPS media tunneling. For example: <code>DNS:media.company.com</code>.</li> </ul> |   |
| 2   | Download and save the created .KEY and .CSR files.           |                                                                                                                                                                                                                                                                                                                                                                                 |   |
| 3   | Send the .CSR file to a public CA for signing.               |                                                                                                                                                                                                                                                                                                                                                                                 |   |
| 4   | Install the signed certificate and the key on the Avaya SBC. | See <a href="#">Installing a certificate and a key</a> on page 180.<br>When installing the certificate, use a descriptive name. For example: <code>mediaCert</code> .                                                                                                                                                                                                           |   |
| 5   | Create a TLS server profile using the installed certificate. | See <a href="#">Creating a TLS server profile</a> on page 183.<br>When creating a profile, use the certificate installed on Avaya SBC in the previous step.<br>Provide a descriptive name for the profile. For example: <code>mediaTlsProfile</code> .                                                                                                                          |   |

**Related links**

[External native clients media configuration checklist](#) on page 171

[TLS server profile checklist for external native clients media configuration](#) on page 172

## Firewall configuration

### External firewall rules

| Port           | Protocol | Description                                                                                                                                                                                              |
|----------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 443            | TCP      | For HTTPS media tunneling. From the internet to Avaya SBC on the B interface.<br><br>This option is only required if you are using media tunneling and it requires better readability through firewalls. |
| 35000 to 40000 | UDP      | For UDP media. From the internet to Avaya SBC on the B interface.<br><br>This option is only required if you are using direct RTP media.                                                                 |
| 3400, 3580     | TCP      | For UDP media. From the internet to Avaya SBC on the B interface.<br><br>This option is only required if you are using direct RTP media.                                                                 |

### Internal firewall rules

| Port           | Protocol | Description                                                                                                                              |
|----------------|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| 35000 to 40000 | UDP      | For UDP media from Avaya SBC. For media traffic that runs from the A interface of Avaya SBC to the MCU 7K and MCU 6K servers.            |
| 12000 to 13200 | UDP      | For UDP media from media services. For media traffic that runs from MCU 7K servers to the A interface of Avaya SBC.                      |
| 16384 to 16984 | UDP      | For UDP media from media services. For media traffic that runs from MCU 7K servers to the A interface of Avaya SBC.                      |
| 6000 to 17999  | UDP      | For UDP media from media services. For media traffic that runs from Avaya Aura® Media Server to the A interface of Avaya SBC.            |
| 5061           | TCP      | For SIP communications. For traffic that runs from the Avaya Aura® Web Gateway to the Avaya SBC SIP communications A interface.          |
| 5061           | TCP      | For SIP communications. For traffic that runs from the Avaya SBC SIP communications A interface to the Avaya Meetings Management server. |

## Configuring the Avaya Session Border Controller signaling interface

### About this task

Use this procedure to configure a signaling interface that will be used for SIP communication between the Avaya Aura® Web Gateway and Avaya SBC.

### Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Device Specific Settings > Signaling Interface**.

3. Click **OK**.
4. In **Name**, provide a name.
5. In **IP Address**, provide the network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBC used by SIP signaling messages traversing the network.
6. Leave the **TCP Port** field blank.
7. Leave the **UDP Port** field blank.
8. In **TLS Port**, enter 5061.
9. In **TLS Profile**, select the TLS server profile created for SIP signaling.

For example: `conferencingManagementSipTlsProfile`. For more information, see [TLS server profile checklist for external native clients media configuration](#) on page 172.

10. Click **Finish**.

## Configuring the Avaya Session Border Controller media interface

### About this task

Media data can be passed through the default UDP port range or tunneled through port 443.

### Procedure

1. Log in to the Avaya SBC web administration portal.

Perform steps 2 and 3 if you want to set up media data tunneling through port 443. Otherwise, continue from step 4.

2. Navigate to **Device Specific Settings > Advanced Options > Feature Control**.
3. Select the **Media Tunneling** check box and then click **Save**.
4. To configure an external media interface, do the following:
  - a. Navigate to **Device Specific Settings > Media Interface** and then click **Add**.
  - b. In **Name**, provide a name for the media interface.  
For example: `externalMediaInterfaceProfile`.
  - c. From **IP Address**, select the B1 IP address.

#### Important:

- Do not use this IP address for any other interface bound to port 443, such as for HTTP tunneling configuration.
  - Do not use VLAN tag for the media tunneled interface.
- d. If you are using media tunneling, from **TLS Profile**, select the required TLS server profile for the media interface that you have created when performing [TLS server profile checklist for media tunneling interfaces](#) on page 173.

For example, `mediaTlsProfile`.

If media tunneling is disabled, set this field to **None**.

- e. In **Buffer Size**, provide the required buffer size for media data.
5. To configure the internal media interface, do the following:
  - a. Navigate to **Device Specific Settings > Media Interface** and then click **Add**.
  - b. In **Name**, provide a name for the media interface.  
For example: `internalMediaInterfaceProfile`.
  - c. From **IP Address**, select the A1 IP address.
6. To enable video media, do the following:
  - a. Navigate to **Domain Policies > Application Rules** and then clone an existing media rule or create a new one.
  - b. For the new application rule, select **In** and **Out** for both the Audio and Video application types.
  - c. Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** as required.
  - d. Click **Finish**.
7. To configure media encryption and enable Binary Floor Control Protocol (BFCP) or Far End Camera Control (FECC), do the following:
  - a. Navigate to **Domain Policies > Media Rules** and clone an existing media rule or create a new one.
  - b. For the new media rule, navigate to **Encryption > Miscellaneous** and select the **Capacity Negotiation** check box.
  - c. On the Audio Encryption screen, in all **Preferred Format** fields, select **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**.
  - d. On the Advanced tab, select the **BFCP Enabled** and **FECC Enabled** check boxes.
8. To configure a policy group using the newly created application and media rules, navigate to **Domain policies > End Point Policy Groups**, create a new group, and add the required application and media rules to that group.

## Configuring Avaya Session Border Controller server flows

### Before you begin

Ensure that you have the TLS client profile created when you configured a certificate authority for reverse proxy. For more information, see [Certificate Authority configuration checklist](#) on page 155. An example of the TLS client profile name is `certificateAuthorityTlsProfile`.

### Procedure

1. Log in to the Avaya SBC web administration portal.
2. To create an interworking profile, do the following:
  - a. Navigate to **Global Profiles > Server Interworking** and then select **Add**.

- b. For the new profile, use the default options for all settings.
  - c. In the Advanced Options section, set **Has Remote SBC** to **No (disabled)**.
- 3. To add a configuration for Avaya Meetings Management, do the following:
  - a. Navigate to **Global Profiles > Server Configuration** and then click **Add**.
  - b. From **Sever Type**, select **Trunk Server**.
  - c. Leave **SIP domain** blank.
  - d. From **TLS Client Profile**, select the TLS client profile that you created when you configured a certificate authority for reverse proxy.
  - e. Add the Avaya Meetings Management FQDN with port 5061 and the TLS protocol specified.
  - f. In the Advanced Options section, select the **Enable Grooming** check box and then select the previously created interworking profile.
- 4. To add a configuration for the Avaya Aura® Web Gateway, do the following:
  - a. Navigate to **Global Profiles > Server Configuration** and then click **Add**.
  - b. From **Sever Type**, select **Trunk Server**.
  - c. Leave **SIP domain** blank.
  - d. From **TLS Client Profile**, select the TLS client profile that you created when you configured a certificate authority for reverse proxy.
  - e. Add the Avaya Aura® Web Gateway FQDN with port 5061 and TLS protocol specified.
  - f. Repeat the previous substep for FQDNs of all Avaya Aura® Web Gateway nodes.
  - g. In the Advanced Options section, select the **Enable Grooming** check box and then select the interworking profile created in the previous step.
- 5. To add a flow for Avaya Meetings Management, do the following:
  - a. Navigate to **Device Specific Settings > End Point Flows > Server Flows** and then select **Add**.
  - b. In **Flow Name**, provide a name for the flow.  
For example: EqMngFlow.
  - c. From **Server Configuration**, select the Avaya Meetings Management configuration that you created in step 3.
  - d. From **Received Interface**, select the internal A1 interface.
  - e. From **Signaling Interface**, select the internal A1 interface.
  - f. From **Media Interface**, select the internal A1 interface.
  - g. From **End Point Policy Group**, select **required**.

6. To add a flow for the Avaya Aura® Web Gateway, do the following:
  - a. Navigate to **Device Specific Settings > End Point Flows > Server Flows** and then select **Add**.
  - b. In **Flow Name**, provide a name for the flow.  
For example: AAWGFlow.
  - c. From **Server Configuration**, select the Avaya Aura® Web Gateway configuration that you created in step 4.
  - d. From **Received Interface**, select the internal A1 interface.
  - e. From **Signaling Interface**, select the internal A1 interface.
  - f. From **Media Interface**, select the external B1 interface.
  - g. From **End Point Policy Group**, select **required**.

---

## Certificate setup

The following sections describe how to configure certificates. Use the web administration interface to configure System Manager certificates. The configuration utility (app configure) only supports third party certificates.

## Creating a certificate signing request on Avaya Session Border Controller

### Procedure

1. Log in to the Avaya SBC web administration interface.
2. Navigate to **TLS Management > Certificates**.
3. Click **Generate CSR**.
4. Complete the following fields:
  - a. **Country Name**: Provide the name of the country within which the certificate is being created in the ISO 3166 format.
  - b. **State/Province Name**: Provide the state or province where the certificate is being created.
  - c. **Locality Name**: Provide the city where the certificate is being created.
  - d. **Organization Name**: Provide the name of the company or organization creating the certificate.
  - e. **Organizational Unit**: Provide the group within the company or organization creating the certificate.
  - f. **Common Name**: Provide a FQDN that resolves to the IP address of the server where this certificate will be installed. You cannot provide wildcard (\*) characters in the field.

- g. **Algorithm:** Select **SHA256**.
  - h. **Key Size (Modulus Length):** Select **2048**.
  - i. **Key Usage Extension(s):** Select the purpose for which the public key might be used: Key Encipherment, Non-Repudiation, or Digital Signature.
  - j. **Extended Key Usage:** Select **Server Authentication** and **Client Authentication**.
  - k. **Subject Alt Name:** Provide information FQDNs or IP addresses that must be included into the certificate.  
 Use the following format: `DNS:<FQDN>, IP:<IP address>`.  
 You can specify multiple FQDNs or IP addresses.
  - l. **Passphrase:** Provide the password used when encrypting the private key.
  - m. **Confirm Passphrase:** Reenter the password that you entered in the **Passphrase** field.
  - n. **Contact Name:** Provide the name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.
  - o. **Contact E-mail:** Provide the email address of the contact.
5. Click **Generate CSR**.
  6. Download and save the CSR request file in the `.CSR` format.
  7. Delete the key file generated and saved on Avaya Session Border Controller.

### Next steps

Provide the `.CSR` file to a CA for signing.

## Signing certificates with the System Manager CA

### Procedure

1. Log in to the System Manager web administration portal.
2. Navigate to **Security > Certificates > Authority**.
3. Ensure that the certificate profile is set as follows:
  - a. **Key Usage Extension** set to Digital Signature and Key Encipherment.
  - b. **Extended Key Usage:** set to Server Authentication and Client Authentication.
4. If you do not have an end entity, do the following:
  - a. Navigate to **Add End Entity**.
  - b. Provide a user name and password for the new entity.  
 The user name and password are required for issuing the certificate.
  - c. Continue performing the procedure from step 6.

5. If you already configured an end entity, do the following:
  - a. Navigate to **Search End Entity**.
  - b. Enter the user name that you provided when creating the entity and then click **Edit End Entity**.
  - c. In **Status**, select **New** and enter the password.
  - d. Continue performing the procedure from the following step.
6. Configure the end entity fields as follows:
  - a. **Subject DN > CN**: FQDN of the server interface that provides TLS support.
  - b. **Subject Alternative Name**: For **DNS name**, enter the FQDN of the server interface that provides TLS support, and for **IP Address**, enter the IP address of the IP requiring TLS support.
  - c. **Certificate Profile**: Enter `ID_CLIENT_SERVER` with relevant key features.
  - d. **CA**: Enter `tmdefaultca`.
  - e. **Token**: Select **User Generated**.
7. Click **Add** if you are configuring a new entity or **Save** if you are configuring the existing entity.
8. Navigate to **Public Web > Enroll**.
9. Click **Create Certificate from CSR**.
10. Enter the user name and password that you used when creating the end entity.
11. Open the CSR request file in the `CSR` format in a text editor and copy its content into a text box on the page.
12. In **Result Type**, select **PEM certificate only**.
13. Click **OK**.

A certificate file in the `.PEM` format is created.
14. Save the certificate file on an external storage device.

### Next steps

Install the signed certificate.

## Installing a certificate and a key

### Procedure

1. Rename the certificate key in the `.PEM` format and the key file in the `.KEY` format so that these files use the same file name.

For example: `certificate1.pem` and `certificate1.key`.

**! Important:**

Do not use the dot (.) symbol in the file name.

2. Log in to the Avaya SBC web administration portal.
3. Navigate to **TLS Management > Certificates**.
4. Click **Install**.
5. Configure the following fields:

- a. **Type:** Select a type of the certificate that you want to install.
- b. **Name:** Provide a name for the certificate that you want to install.

This field is optional. If you do not provide a name, then the file name of the uploaded certificate file will be used as the certificate name.

**\* Note:**

If you provide a name that matches the name of one of installed certificates, the system replaces that certificate with the certificate that you are installing.

- c. **Override Existing:** Select if you can install a certificate with the name that matches the name of one of already installed certificates.

If the check box is cleared, the system displays an error message when you try to install a certificate with the same name. If the check box is selected, the system replaces the existing certificate with the certificate you are installing.

- d. **Allow Weak Certificate Key:** Select if you can install a certificate signed using a weak key.

If the option is selected, the system bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.

- e. **Certificate File:** Specify a location of the certificate file on your computer.

**! Important:**

If the third-party CA provides separate Root CA and intermediate certificates, you must combine these certificates into a single file before installing to Avaya SBC. To combine the files, append the content of each certificate file one after another. Add the content of the root CA certificate to the end of this single file.

- f. **Key:** Specify the private key that you want to use.

You can opt to use the existing key from the file system or select a file containing another key.

- g. **Key File:** Specify the key file.

This button is displayed when you select **Upload Key File** in the **Key** field.

6. Click **Upload**.

7. Log in to Avaya SBC as root using an SSH connection.

The port is 222. Use the `ipcs` user name and password.

8. Navigate to the `/usr/local/ipcs/cert/key` directory.

9. Run the `enc_key <filename> <passphrase>` command.

In this command, `<filename>` is the name of the encryption key file and `<passphrase>` is the passphrase you used while generating the CSR.

10. Restart Avaya SBC.

## Installing the Avaya Meetings Management CA certificate to Avaya SBC

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Settings > Security > Certificates**.
3. Click on the Avaya Meetings Management certificate and download the `caroot.crt` file.
4. Log in to the Avaya SBC web administration portal.
5. Navigate to **TLS Management > Certificates**.
6. Click **Install**.
7. Configure the following fields:
  - a. **Type**: Select **CA Certificate**.
  - b. **Name**: Enter a name for the certificate.
  - c. **Overwrite Existing**: Select if you want to overwrite an existing certificate with the name that matches the name of the certificate you are installing.
  - d. **Allow weak Certificate key**: Select this check box if the CA certificate is signed with a weak key.
  - e. **Certificate File**: Select the `caroot.crt` certificate downloaded from the Avaya Meetings Management web administration portal.
8. Click **Upload**.

## Installing a CA certificate on Avaya SBC

### Procedure

1. Log in to the System Manager web administration portal.
2. Navigate to **Security > Certificates > Authority > CA Structure & CRLs**.
3. Download the required CA certificate file in the `.PEM` format.
4. Log in to the Avaya SBC web administration portal.

5. Navigate to **TLS Management > Certificates**.

6. Select **Install**.

7. Complete the following fields:

a. **Type**: Select **CA Certificate**.

b. **Name**: Enter a name for the certificate.

If you have not downloaded the Private Key, you must type the name you provided in the **Common Name** field while generating CSR. If you have downloaded the Private Key, you can type any name for the certificate.

c. **Overwrite Existing**: Select if you need to replace the existing certificate that has the same name.

d. **Allow Weak Certificate Key**: Select if the certificate is signed with a weak key.

e. **Certificate File**: select the CA certificate file downloaded from Avaya Meetings Management.

8. Press **Upload**.

---

## TLS client and server profiles setup

### Creating a TLS server profile

#### Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **TLS Management > Server Profiles**.
3. Click **Add**.
4. In **Profile Name**, enter a name for the profile.
5. In **Certificate**, select the installed CA certificate that you want to associate with the profile.
6. If you are creating a profile for media tunneling interfaces, in the **Peer Verification** field, select **Optional**.
7. Complete the remaining fields as required and then click **Next**.
8. Select the required TLS versions and then click **Finish**.

The system displays the new profile on the Server Profile page.

### Creating a TLS client profile

#### Procedure

1. Log in to the Avaya SBC web administration portal.

2. Navigate to **TLS Management > Client Profiles**.
3. Click **Add**.
4. In **Profile Name**, enter a name for the profile.
5. In **Certificate**, select the installed CA certificate that you want to associate with the profile.
6. Complete the remaining fields as required and then click **Next**.
7. Select the required TLS versions and then click **Finish**.

The system displays the new profile on the Client Profile page.

---

## Configuring Avaya SBC network interfaces

### Procedure

1. Log in to the Avaya SBC web administration portal.
2. Navigate to **Device Specific Settings > Network Management > Networks**.
3. Configure the following interfaces:
  - Internal interface A1 with at least one IP address associated with it.
  - External interface B1 with at least one IP address associated with it.

# Chapter 11: Troubleshooting

---

## Unexpected characters in the /etc/hosts file on a localhost line

### Condition

When you deploy Avaya Aura® Web Gateway on AWS, Avaya Aura® Web Gateway displays the following error:

```
Hostname Check .....  
Found unexpected characters in /etc/hosts on a localhost line  
(127.0.0.1 or localhost )  
Hostname Check ..... [FAILED]
```

### Cause

The /etc/hosts file is incorrectly configured when the virtual machine is created.

The following is an example of incorrectly configured localhost entries in the /etc/hosts file:

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4  
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
```

### Solution

1. Log in to the Avaya Aura® Web Gateway CLI as the root user.
2. Open the /etc/hosts file in the vi text editor:  

```
vi /etc/hosts
```
3. Reconfigure the lines that contain localhost entries as shown in the following example:

```
127.0.0.1 localhost.localdomain localhost  
::1 localhost6.localdomain6 localhost6
```

Ensure that the lines does not contain any redundant space and tab characters.

4. Save the /etc/hosts file.
5. Repeat the Avaya Aura® Web Gateway installation procedure.

---

## A node removed from the Cassandra cluster has the “live” status in the app listnodes output

### Condition

When you remove a node from the cluster, the `app listnodes` command output indicates that the status of the node removed from the Cassandra cluster is “live”. You cannot remove this node from the Avaya Aura® Web Gateway cluster using the `./clitool-csa.sh removeClusterNode <node_uuid>` command.

### Cause

The local Avaya Aura® Web Gateway clock might not be synchronized with the NTP server.

### Solution

1. Ensure that the Avaya Aura® Web Gateway clock is synchronized with the NTP server as described in [Checking the Chrony service status](#) on page 79.
2. Run the following command to view the node status:  

```
app listnodes
```
3. Depending on the node status, do one of the following to remove the node:
  - If the node status is “down”, run the following command:  

```
./clitool-csa.sh removeClusterNode <node_uuid>
```
  - If the node status is “live”, run the following command:  

```
./clitool-csa.sh removeClusterNode <node_uuid> force
```
4. Run the `app listnodes` command and ensure that the Avaya Aura® Web Gateway cluster does not contain the node.
5. If the cluster still contains the node, contact Avaya support.

# Chapter 12: Resources

## Documentation

The following table lists other related documentation. All Avaya documentation is available at <http://support.avaya.com/>. Many documents are also available at <http://documentation.avaya.com/>.

| Title                                                                           | Use this document to:                                                                                    | Audience                                                                                                                                                                                          |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Overview and planning                                                           |                                                                                                          |                                                                                                                                                                                                   |
| <i>Avaya Aura® Core Solution Description</i>                                    | Understand the strategic, enterprise, and functional views of the Avaya Aura® architecture.              | <ul style="list-style-type: none"><li>• Customers</li><li>• Sales, services, and support personnel</li></ul>                                                                                      |
| <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> | Understand the features of Avaya Aura® Communication Manager.                                            |                                                                                                                                                                                                   |
| <i>What's New in Avaya Aura® Release 10.2</i>                                   | Understand the new and enhanced features of Avaya Aura® components.                                      | <ul style="list-style-type: none"><li>• Contractors</li><li>• Employees</li><li>• Channel associates</li><li>• Sales, services, and support personnel</li><li>• Avaya Business Partners</li></ul> |
| Using                                                                           |                                                                                                          |                                                                                                                                                                                                   |
| <i>Avaya Scopia® Desktop Client User Guide</i>                                  | Use the Avaya Scopia® desktop client. This document also provides usage information for the user portal. | End users                                                                                                                                                                                         |
| Deploying                                                                       |                                                                                                          |                                                                                                                                                                                                   |
| <i>Deploying Avaya Aura® Device Services</i>                                    | Install, administer, configure, and maintain Avaya Aura® Device Services.                                | Implementation personnel                                                                                                                                                                          |
| <i>Deploying Avaya Multimedia Messaging</i>                                     | Install, configure, and administer Avaya Multimedia Messaging.                                           |                                                                                                                                                                                                   |

*Table continues...*

| Title                                                                          | Use this document to:                                                                                                                                                          | Audience                                                                                                                                                |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Deploying Avaya Meetings Server</i>                                         | Install, configure, and maintain the Avaya Meetings Server.                                                                                                                    |                                                                                                                                                         |
| Administering                                                                  |                                                                                                                                                                                |                                                                                                                                                         |
| <i>Administering Avaya Aura® Device Services</i>                               | Use management tools, manage data and security, and perform periodic maintenance tasks in Avaya Aura® Device Services.                                                         | <ul style="list-style-type: none"> <li>• System administrators</li> <li>• Implementation personnel</li> <li>• Services and support personnel</li> </ul> |
| <i>Administering Avaya Aura® Communication Manager</i>                         | Administer Avaya Aura® Communication Manager on the following servers: <ul style="list-style-type: none"> <li>• Avaya media gateways</li> <li>• Avaya S8XXX Servers</li> </ul> |                                                                                                                                                         |
| <i>Administering Network Connectivity on Avaya Aura® Communication Manager</i> | Understand the network components of Avaya Aura® Communication Manager.                                                                                                        |                                                                                                                                                         |
| <i>Administering Avaya Aura® Session Manager</i>                               | Administer Avaya Aura® Session Manager.                                                                                                                                        |                                                                                                                                                         |
| <i>Administering Avaya Aura® System Manager</i>                                | Perform configuration and management tasks in Avaya Aura® System Manager.                                                                                                      |                                                                                                                                                         |
| <i>Administering Avaya Session Border Controller</i>                           | Perform configuration, system administration, and troubleshooting tasks in Avaya Aura® Session Border Controller.                                                              |                                                                                                                                                         |
| <i>Implementing and Administering Avaya Aura® Media Server</i>                 | Perform configuration, system administration, and troubleshooting tasks in Avaya Aura® Media Server.                                                                           |                                                                                                                                                         |

## Finding documents on the Avaya Support website

### Procedure

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

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click  to display the search results.

## Avaya Documentation Center navigation

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

### Important:

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

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

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

You can do the following:

- Create, rename, and delete a collection.

- Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
  - Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
  - View and manage your watchlist by clicking **Watchlist** from the top menu with your name.
- You can do the following:
- Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
  - Send feedback for a topic.

---

## Training

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 **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

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

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

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

 **Note:**

Videos are not available for all products.

---

## Support

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

## Using the Avaya InSite Knowledge Base

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

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

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

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

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

# Appendix A: Certificate configuration using the configuration utility

The following sections describe how to configure certificates using the configuration utility process. You can only use the configuration utility for the configuration of third party certificates. If you are using System Manager certificates, you must use the web administration portal.

You can also manage and update certificates using the Avaya Aura® Web Gateway web administration portal. For more information about working with the web administration portal, see *Administering the Avaya Aura® Web Gateway*.

## Important:

The web administration portal is the preferred method for managing certificates. Use the configuration utility process to configure certificates for troubleshooting purposes, but after this is done, perform certificate management from the web administration portal when possible.

---

## Generating Certificate Signing Requests

### About this task

Use this procedure to generate a Certificate Signing Request (CSR).

## Important:

You must use this procedure if you are not using System Manager as the only Certificate Authority (CA) to sign certificates for all solution components.

### Before you begin

Ensure that Avaya Aura® Web Gateway is successfully installed with System Manager signed certificates. This is the default setting for installation.

### Procedure

1. Run the following command:

```
mkdir /tmp/AAWGportalCerts
chmod 770 /tmp/AAWGportalCerts
```

The system creates an `AAWGportalCerts` directory in `/tmp/` for the output of the script that will generate the CSRs.

2. Run the following command to navigate to the directory containing the script:

```
cdto misc
```

3. To generate a CSR, run the following command:

```
sudo ./createCSR.sh /tmp/AAWGportalCerts frontEndFQDN localFQDN  
organizationNameorganizationUnit locality stateOrProvince countryCode emailAddress
```

### Important:

This command is a single Linux command and must be entered as a single line even if it appears as several lines in the document.

The parameters for this script are:

- `frontEndFQDN`: For a cluster installation, this is the FQDN of the Virtual IP or external load balancer. For simple, non-clustered installations, this is the FQDN of the server where Avaya Aura® Web Gateway is installed.
  - `localFQDN`: The FQDN of the server.
  - `organizationName`: The name of the organization.
  - `organizationUnit`: The name of the unit or sub-organization. For example, "Design".
  - `locality`: The name of the city or town.
  - `state`: The two-digit state or province code.
  - `countryCode`: The two-digit country code.
  - `emailAddress`: The administrator email address.
4. Verify that `/tmp/AAWGportalCerts` contains the `.key` and `.csr` files for front-end.

Use the `frontEnd.csr` and `frontEnd.key` files to generate certificates. You can ignore `.csr` and `.key` files for node, OAMP, and SIP.

---

## Getting certificates signed by the third-party CA

### About this task

Avaya Aura® Web Gateway accepts certificates in either the PEM or PKCS12 formats.

### Note:

- PEM is a Base64 encoded ASCII format. The certificate data is prefixed with the `-----BEGIN CERTIFICATE-----` line and followed by the `-----END CERTIFICATE-----` line. The most common file name extensions are `.pem`, `.crt`, and `.cer`.

- PKCS12 is a binary format that contains the server certificate, intermediate certificates and the private key in a single encryptable file. The file name extensions for this format are .pfx and .p12.

### Before you begin

- Ensure that the CA is configured to include extendedKeyUsage for both the client and the server in the generated certificates.
- Open the Linux shell using the Linux administrator account credentials.

### Procedure

1. Transfer the `frontEnd.csr` file from Avaya Aura® Web Gateway so that it can be used during signed certificate generation process on your third-party CA.
2. Transfer certificates to Avaya Aura® Web Gateway.
  - a. Transfer the signed `.crt` file to `/opt/Avaya/AAWGportalCerts`, and name it `frontEnd.crt`.
  - b. Transfer the third-party root CA certificate to `/opt/Avaya/AAWGportalCerts`, and name it `rootCA.crt`.
  - c. Transfer any third-party intermediary CA certificates to `/opt/Avaya/AAWGportalCerts`, and name them `intermediary1.crt`, `intermediary2.crt`, and so on in ascending order of the certificate chain until the root CA.
3. To create a certificate chain containing the front end certificate, arrange all intermediary CA certificates (if any) and the root CA certificate in the correct order, and then run the following command:

```
cat frontEnd.crt intermediary1.crt intermediary2.crt ... rootCA.crt >
frontEndCerts.crt
```

---

## Applying third-party signed certificates to the Avaya Aura® Web Gateway

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.

The Linux administrator account is created during the deployment process.
2. To open the Avaya Aura® Web Gateway configuration utility, run the following command:

```
app configure
```

3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **Use System Manager for Certificates**, and then select **No**.

5. Select the following options, type the file path shown, and then select **OK** for each option:
  - a. For **REST interface key file**, type `/opt/Avaya/AAWGportalCerts/frontEnd.key`.
  - b. For **REST interface certificate file**, type value `/opt/Avaya/AAWGportalCerts/frontEndCerts.crt`.
  - c. For **OAM interface key file**, type value `/opt/Avaya/AAWGportalCerts/frontEnd.key`.
  - d. For **OAM interface certificate file**, type value `/opt/Avaya/AAWGportalCerts/frontEndCerts.crt`.
  - e. For **Keystore password**, type the same keystore password that you used at the time of installation.
6. Select **Apply** and **Continue** for the specified certificates to be processed.
7. Select **Exit Configure** to exit this menu.

---

## Adding third-party root CA certificates to the Avaya Aura® Web Gateway

### About this task

Use this procedure to trust additional root CAs. For example, you can add the:

- LDAP root CA certificate if you are using a secure LDAP connection.
- SIP CA certificate if Session Manager has certificates signed by the SIP CA.

You can manage truststore certificates by using the Avaya Aura® Web Gateway administration portal as described in *Administering the Avaya Aura® Web Gateway*.

Do not use this procedure to add the System Manager root CA certificate because that was already added during the initial installation.

### Procedure

1. Run the following command to open the configuration utility:
 

```
app configure
```
2. Select **Add a Certificate to the TrustStore**.
3. To add a certificate, select **Certificate file** and specify the path to the file.
4. Select **Apply**.

If the provided file contains certificate chain, then all certificates will be added to the truststore.

# Creating a Certificate Signing Request (CSR) using OpenSSL

## About this task

Use this procedure to generate a CSR using OpenSSL.

You can also generate a CSR using the Avaya Aura® Web Gateway web administration portal.

## Before you begin

Ensure that you have the OpenSSL utility.

## Procedure

1. Create an OpenSSL configuration file.

For example:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name

[req_distinguished_name]

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = dnsserver10927.company.com
DNS.2 = dnsserver10938.company.com
DNS.3 = dnsserver10955.company.com
```

The `alt_names` section defines the Subject Alternative Names list and must contain FQDNs of all nodes in the cluster. For Open LDAP, the `alt_names` section must also contain the `localhost.localdomain` and, for IPv6, `localhost6.localdomain` records.

2. Run the following command:

```
openssl req -out <CSR_request_file>.csr -newkey rsa:2048 -nodes -keyout
<CSR_key_file>.key -config <configuration_file>
```

In this command:

- `<CSR_request_file>.csr` specifies a CSR file name.
- `<CSR_key_file>.key` specifies a file containing a private key that is used to add the signed certificate to the system.
- `<configuration_file>` specifies the OpenSSL configuration file that was created in the previous step.

For example:

```
openssl req -out createCSR.csr -newkey rsa:2048 -nodes -keyout keyCSR.key -config
configCSR.config
```

---

# Signing identity certificates for Avaya Aura® Web Gateway using third-party CA certificates

## About this task

You can use the following procedure to sign identity certificates for Avaya Aura® Web Gateway using third-party CA certificates.

### \* Note:

In the following procedure, the third-party CA certificate can be a public CA or an internal private CA.

## Before you begin

- Create a CSR with the following X509 extensions:
  - keyUsage = nonRepudiation, digitalSignature, keyEncipherment
  - extendedKeyUsage = serverAuth, clientAuth
- Ensure that the CSR contains the following:
  - If the certificate is only used on the Avaya SBC, the request contains the subjectAltName extension that lists the cluster FQDN in the SAN.
  - If the certificate is used on both Avaya SBC and the Avaya Aura® Web Gateway server, the request contains the subjectAltName extension that lists the cluster FQDN as well as the FQDN of each cluster member in the SAN.

### \* Note:

From the security perspective, Avaya recommends that you generate separate certificates for each node, including the cluster FQDN and the individual cluster node FQDN in subjectAltName.

- Do *not* provide the password for a key because password protected keys are not supported.
- Ensure that the key generated along with the CSR is stored safely.
- Ensure that once the certificate is generated, you have received the identity certificate, root CA certificate, and all intermediate CA certificates in the .PEM format from the certification authority. If these certificates are not in the .PEM format, you can convert these certificates using the OpenSSL tool.
- Generate the identity certificate chain as described in [Generating an identity certificate chain](#) on page 198.
- Obtain the System Manager root CA certificate.
- Generate the trust certificate chain by concatenating the following certificates into a `trustchain.PEM` file:
  - All intermediate CA certificates.
  - The root CA certificate.
  - The System Manager root CA certificate.

## Procedure

1. Log on to Avaya Aura® Web Gateway using your SSH credentials.
2. If you are using reverse proxy on the Avaya SBC to Avaya Aura® Web Gateway, import the intermediate CA certificate and the root CA certificate to the Avaya SBC trust store.
3. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
4. Do the following to import intermediate CA certificates to Avaya Aura® Web Gateway:
  - a. Select **Add a Certificate to the TrustStore**.
  - b. Click **Select**.
  - c. Enter the path to the certificate file and then click **OK**.
  - d. Click **Apply** to import the certificate.
  - e. Repeat these steps for all intermediate CA certificates.

Avaya Aura® Web Gateway does not import a certificate into the truststore if the certificate has unsupported critical extensions, expired, or if the certificate start date is in the future.

5. Click **Front-end host, System Manager and Certificate Configuration**.
6. Click **Use System Manager for Certificates** and type `n` to not use System Manager for certificates.
7. Click **REST Interface certificate configuration**. If the certificate is not in the PKCS12 format, type `n` on the REST Interface certificate configuration screen.
8. Add the key file to the REST interface PEM key file and the certificate chain to the REST interface PEM certificate file.
9. Click **Signing authority certificate configuration** on the Front-end host, System Manager and Certificate Configuration screen.
10. If the CA root certificate is not in the PKCS12 format, type `n`.
11. Click **Signing Authority PEM certificate file** and add the `trustchain.PEM` trust certificate chain that you have created.
12. Click **Return to previous menu**.
13. Click **Apply**.

## Generating an identity certificate chain

### 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.

### Before you begin

Upload the third-party CA-signed identity certificate, root CA certificate, and all intermediate CA certificates in the PEM format to Avaya Aura® Web Gateway using a file transfer program, such as SFTP or SCP.

### 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_certificate_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
```

---

## Configuring System Manager to trust third-party root CA certificates

### About this task

This procedure is not applicable for deployments without Avaya Aura®.

### Procedure

1. Log on to the System Manager web console.
2. Click **Home** > **Services** > **Inventory** > **Manage Elements**.
3. Select System Manager from the **Elements**.
4. Click **Configure Trusted Certificates** in the **More Actions** list.
5. Click **Add** and select **Import from file**.
6. Click **Choose File** and browse to the third-party root CA certificate.

7. Click **Commit**.
8. Restart the System Manager JBOSS™ process.

From the SSH session on the System Manager, run the following command as a root user:

```
service jboss restart
```

 **Note:**

The `service jboss restart` command affects the service for the System Manager.

---

## 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. To generate a CSR, run the following command:

```
sudo ./createCSR.sh /tmp/AAWGportalCerts frontEndFQDN localFQDN  
organizationNameorganizationUnit locality stateOrProvince countryCode emailAddress
```

 **Important:**

This command is a single Linux command and must be entered as a single line even if it appears as several lines in the document.

The parameters for this script are:

- `frontEndFQDN`: For a cluster installation, this is the FQDN of the Virtual IP or external load balancer. For simple, non-clustered installations, this is the FQDN of the server where Avaya Aura® Web Gateway is installed.
- `localFQDN`: The FQDN of the server.
- `organizationName`: The name of the organization.
- `organizationUnit`: The name of the unit or sub-organization. For example, "Design".
- `locality`: The name of the city or town.
- `state`: The two-digit state or province code.
- `countryCode`: The two-digit country code.
- `emailAddress`: The administrator email address.

Avaya Aura® Web Gateway create the `oamp.csr` and `oamp.key` files in the `/tmp/AAWGportalCerts` directory.

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 200.
- 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` or `.p12` file.

The following is an example of the command to convert the `.pem` file to a `.p12` file:

```
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 202.

## 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 Mozilla 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"
```

## Available certificate validation options

| Name                  | Description                                                                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OPTIONAL</b>       | 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.                                                                           |
| <b>NONE</b>           | 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. |
| <b>OPTIONAL_NO_CA</b> | 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).          |
| <b>REQUIRED</b>       | 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.                                                                   |

# Appendix B: Best Practices for VMware performance and features

For information on the hardware requirements for Avaya Aura® Web Gateway, see *Installing the Avaya Solutions Platform 130 Series*, which is available at <https://support.avaya.com>.

## Related links

[Timekeeping](#) on page 203

[VMware Tools](#) on page 204

[VMware networking best practices](#) on page 205

[Storage](#) on page 208

---

## Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine. If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service

cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the **chronyc sources -v** command from a command window. The results from this command:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **chronyd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

#### Related links

[Best Practices for VMware performance and features](#) on page 203

---

## VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at <http://kb.vmware.com/kb/340>.

#### Important:

*Do not* upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

#### Related links

[Best Practices for VMware performance and features](#) on page 203

---

## VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

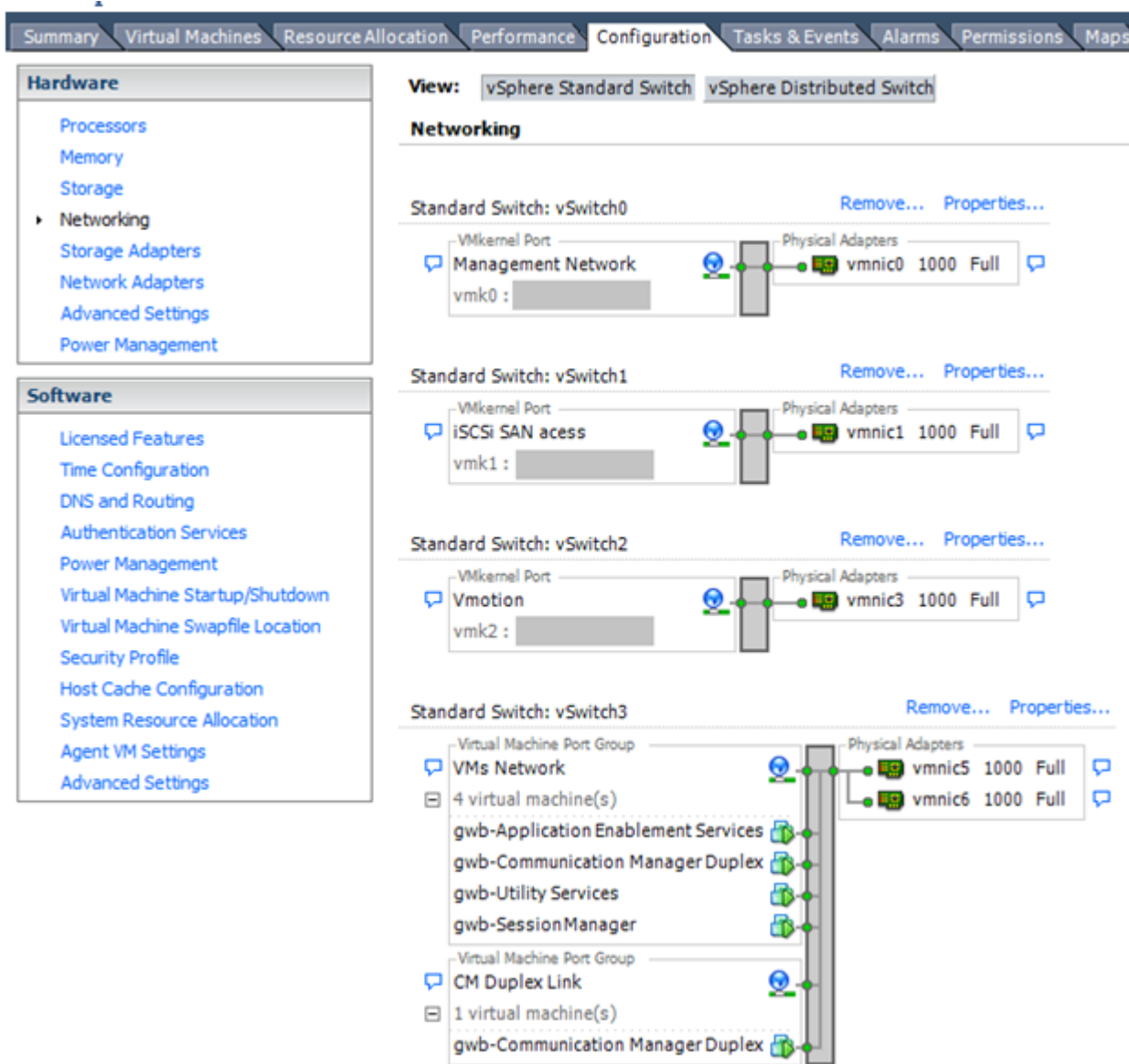
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

**Disclaimer:** The images in this section represent older ESXi versions and may vary for the latest ESXi versions.

## Networking Avaya applications on VMware ESXi – Example 1

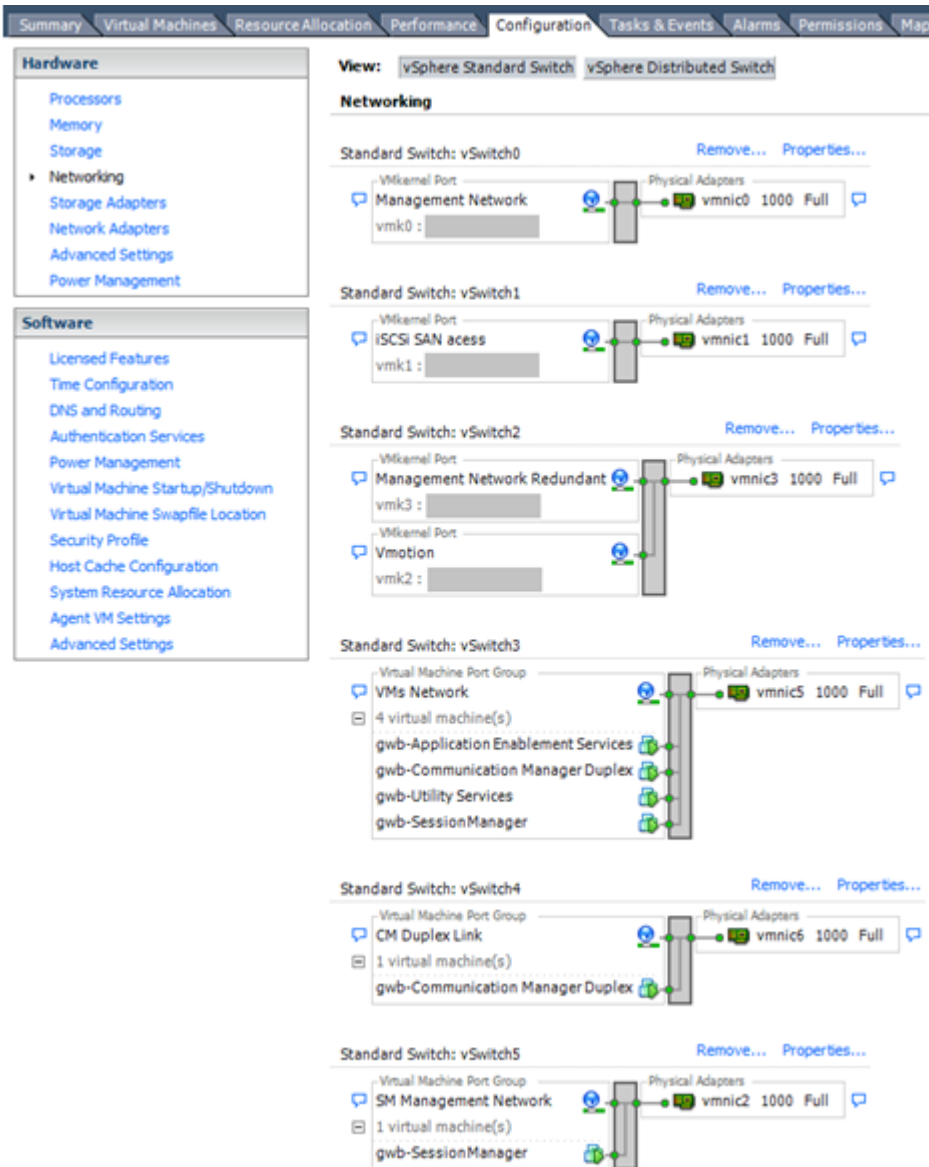


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3

can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

## Networking Avaya applications on VMware ESXi – Example 2



This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

## References

| Title                             | Link                                                                                                       |
|-----------------------------------|------------------------------------------------------------------------------------------------------------|
| Product Support Notice PSN003556u | Go to <a href="https://support.avaya.com">https://support.avaya.com</a> and search for PSN003556u.         |
| VMware vSphere 8.0 Documentation  | Go to Broadcom website (formerly known as VMware) and search for <i>VMware vSphere 8.0 Documentation</i> . |
| VMware vSphere 7.0 Documentation  | Go to Broadcom website (formerly known as VMware) and search for <i>VMware vSphere 7.0 Documentation</i> . |

### Related links

[Best Practices for VMware performance and features](#) on page 203

---

## Storage

There is no stipulation on the underlying storage vendor type and storage technology used. Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

### Related links

[Best Practices for VMware performance and features](#) on page 203

---

## Best Practices for VMware features

### VMware High Availability

VMware High Availability (HA) provides automatic detection of hardware failures, server failures, and operating system failures. In the event of a physical server failure, VMware HA automatically restarts the affected virtual machine on other production servers that have spare capacity. In the event of an operating system failure, VMware HA restarts the affected virtual machine on the same server.

VMware HA ensures that capacity is available to restart all virtual machines that are affected by a service failure. HA continuously monitors capacity utilization and reserves spare capacity to restart virtual machines.

VMware HA helps users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions along with suggested remediation steps.

For more information, see the VMware website at [https://www.vmware.com/pdf/ha\\_datasheet.pdf](https://www.vmware.com/pdf/ha_datasheet.pdf).

**\* Note:**

- All virtual machines and their configuration files must be on shared storage, e.g. Fibre Channel SAN, iSCSI SAN, or SAN iSCSI NAS.
- The console network must have redundant network paths to have reliable failure detection for HA clusters. VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses virtual machine priority to decide order of restart.
- VMware HA only works across a LAN. VMware HA does not work across a WAN.

**Related links**

[Best Practices for VMware performance and features](#) on page 203

## VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

**Related links**

[Best Practices for VMware performance and features](#) on page 203

## VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

 **Caution:**

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.

- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the Take Snapshot window, clear the **Include virtual machine's memory** check box.

- Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

 **Note:**

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

### Related resources

| Title                                                                                             | Link                                                                                   |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Best practices for virtual machine snapshots in the VMware environment                            | <a href="#">Best Practices for virtual machine snapshots in the VMware environment</a> |
| Understanding virtual machine snapshots in VMware ESXi and ESX                                    | <a href="#">Understanding virtual machine snapshots in VMware ESXi and ESX</a>         |
| Working with snapshots                                                                            | <a href="#">Working with snapshots</a>                                                 |
| Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots | <a href="#">Send alarms when virtual machines are running from snapshots</a>           |

### Related links

[Best Practices for VMware performance and features](#) on page 203

# Appendix C: Creating RHEL virtual machine on Nutanix

---

## Uploading the RHEL ISO to Nutanix server

### About this task

You can install RHEL on Nutanix 6.5 and later, after uploading the standard RHEL ISO image on the Nutanix server.

#### **Note:**

The RHEL ISO must be customer-provided. Avaya is not responsible for the RHEL ISO image.

### Procedure

1. Log in to Nutanix server using Nutanix Prism web console.
2. Navigate to **Home > Settings > Image Configuration**.
3. In the **Image Configuration** screen, click **Upload Image**.  
Nutanix Prism web console displays the **Create Image** window.
4. In the **Name** field, enter a name for the image.
5. In the **Image Type** field, select the ISO image to upload.
6. In the **Storage Container** field, select the required option.
7. Under **Image Source** field, either browse for the ISO image through URL or upload the image file if stored in your local machine.
8. Click **Save**.

You can view the image upload status from the drop-down list on top of the **Home** page.

### Next steps

Installing RHEL on Nutanix 6.5 and later.

---

# Installing RHEL on the Nutanix server

## Before you begin

- Upload the RHEL image on Nutanix 6.5 and later.
- Log in to Nutanix 6.5 server using the Nutanix Prism web console.

## Procedure

1. Navigate to **Home > VM**.
2. In the **VM** page, click **Create VM**.
3. In the **Create VM** window under **General Configurations**, enter appropriate values in the **Name**, **Description**, and **Timezone** fields.
4. In the **vCPUs** field under **Compute Details**, enter the number of CPUs required for the application.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.
7. Under **Boot Configuration**, select **UEFI**.
8. Under **Disks**, click the Edit icon for the CD-ROM disk type, and do the following:
  - a. In the **Type** field, ensure **CD-ROM** is displayed.
  - b. In the **Operation** field, select **Clone from Image Service**.
  - c. In the **Bus Type** field, Avaya recommends selecting **IDE**.
  - d. In the **Image** field, select the RHEL ISO Image.
  - e. Click **Update**.

The CD-ROM and the disk size are displayed.

9. Click **Add New Disk** next to **Disks**, and do the following:
  - a. In the **Type** field, select **Disk**.
  - b. In the **Operations** field, select **Allocate on Storage Container**.
  - c. In the **Bus Type** field, select the same bus type which you selected while updating the disk.
  - d. In the **Storage Container** field, select the appropriate storage container.
  - e. In the **Size** field, enter the required GiB size.
  - f. Click **Add**.
10. Under **Network Adapters (NIC)**, do the following:
  - a. Click **Add New NIC** to add a Network Interface Card (NIC).
  - b. In the **Create NIC** window, select the **Subnet Name**.

- c. In the **Network Connection State** field, select **Connected**.
  - d. Click **Add**.
  - e. To add multiple NICs, repeat 10.a to 10.d.
11. Under **VM Host Affinity**, click **Set Affinity** and do the following:
  - a. In the **Set VM Host Affinity** window, select the hosts.

Select multiple hosts to ensure one node (virtual machine) runs in case another node fails.
  - b. Click **Save**.

After the successful creation of virtual machine, virtual machine appears in the VM page.
12. Select the newly created VM and click **Power On**.
13. Click **Launch Console**.

 **Note:**

The **Launch Console** button is enabled only when the virtual machine is Powered On.  
After the RHEL boots, Red Hat Enterprise Linux 8.10 welcome screen appears.

14. Click **Continue**.
15. In the **Installation Summary** screen, under **LOCALIZATION**, click **Language Support** to select the supported language.
16. Click **Time & Date** to set the required timezone.
17. Under **SOFTWARE**, click **Software Selection**.
18. Select **Minimal Install** and then click **Done**.
19. Under **SYSTEM**, click **Installation Destination** and do the following:
  - a. Under **Storage Configuration**, select the **Custom** radio button and click **Done**.
  - b. In the **Manual Partitioning** window, set the partitioning as required.
  - c. Click the **+** icon to create a new mount point.
  - d. Select the available partition from the **Mount Point** drop-down menu. To add custom partitions, type the required partition name. For eg: `/etc/opt/defty`.
  - e. Enter the capacity in GiB in the **Desired Capacity** field and then click **Add Mount Point**.
  - f. In the **Manual Partitioning** window, click **Done**.
  - g. In the **Summary of Changes** window, click **Accept Changes**.
  - h. Click **Done**.

20. Click **Network & Host Name** and do the following:
  - a. Enter a name in the **Host Name** field and click **Apply**.
  - b. To configure the IP, click **Configure**.
  - c. Click **IPV4 Settings** and select the required option from the **Method** drop-down menu.
  - d. Click **Done**.
21. Under **USER SETTINGS**, click **Root Password**.

In the **Root Password** window, set a password for the root user and then click **Done**.
22. Click **User Creation** and in the Create User window, enter the details and click **Done**.
23. Click **Begin Installation**.

The RHEL virtual machine is installed on the Nutanix 6.5 server and later.
24. Click **Reboot System** to reboot the RHEL virtual machine.

# Glossary

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Busy Hour Call Attempts</b>                   | The maximum number of calls supported for one hour in peak traffic conditions.                                                                                                                                                                                                                                                                                                                                                |
| <b>Cassandra</b>                                 | Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see <a href="https://cassandra.apache.org/">https://cassandra.apache.org/</a> .                                                                                                                                                                                          |
| <b>Domain Name System (DNS)</b>                  | A system that maps and converts domain and host names to IP addresses.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Fully Qualified Domain Name (FQDN)</b>        | A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).                                                                                                                                                                                                                                                                                                          |
| <b>Network Time Protocol (NTP)</b>               | A protocol used to synchronize the real-time clock in a computer.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Secure Shell (SSH)</b>                        | 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. |
| <b>Simple Network Management Protocol (SNMP)</b> | A protocol for managing devices on IP networks.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>SSL (Secure Sockets Layer) Protocol</b>       | 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.                                                                                                        |
| <b>TCP</b>                                       | Transmission Control Protocol.                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>TLS</b>                                       | Transport Layer Security                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>UDP</b>                                       | User Datagram Protocol. This is a communication method, similar to TCP.                                                                                                                                                                                                                                                                                                                                                       |

# Index

## A

|                                                       |                                           |
|-------------------------------------------------------|-------------------------------------------|
| ABSCE                                                 |                                           |
| configuring server flows .....                        | <a href="#">176</a>                       |
| adding                                                |                                           |
| Avaya Aura Web Gateway .....                          | <a href="#">139</a>                       |
| adding third-party root certificates                  |                                           |
| Avaya Aura Web Gateway server .....                   | <a href="#">195</a>                       |
| administration portal                                 |                                           |
| Linux account .....                                   | <a href="#">132</a>                       |
| administrative user                                   |                                           |
| creating .....                                        | <a href="#">72</a>                        |
| advanced configuration .....                          | <a href="#">129</a>                       |
| Amazon Web Services                                   |                                           |
| creating security groups .....                        | <a href="#">86</a>                        |
| managing load balancers .....                         | <a href="#">92</a>                        |
| application layer                                     |                                           |
| installation checklist .....                          | <a href="#">98</a>                        |
| applying third-party certificates                     |                                           |
| Avaya Aura Web Gateway server .....                   | <a href="#">194</a>                       |
| architecture                                          |                                           |
| diagram .....                                         | <a href="#">11</a>                        |
| ASBCE                                                 |                                           |
| configuring .....                                     | <a href="#">150</a>                       |
| configuring external client access .....              | <a href="#">162</a>                       |
| configuring external traffic rules                    |                                           |
| multiple FQDNs deployment .....                       | <a href="#">160</a>                       |
| single FQDN deployment .....                          | <a href="#">156</a>                       |
| configuring internal traffic rules .....              | <a href="#">158</a>                       |
| configuring on AAWG .....                             | <a href="#">164</a>                       |
| configuring reverse proxy .....                       | <a href="#">151</a> , <a href="#">152</a> |
| configuring TURN relay for WebRTC .....               | <a href="#">170</a>                       |
| creating CRS .....                                    | <a href="#">178</a>                       |
| CSR                                                   |                                           |
| creating request on ASBCE .....                       | <a href="#">178</a>                       |
| installing CA certificates .....                      | <a href="#">182</a>                       |
| overview .....                                        | <a href="#">150</a>                       |
| attributes replication .....                          | <a href="#">127</a>                       |
| automatic backups                                     |                                           |
| changing default password .....                       | <a href="#">131</a>                       |
| available certificate validation options .....        | <a href="#">202</a>                       |
| Avaya Aura Device Services                            |                                           |
| uploading Avaya IX Workplace clients .....            | <a href="#">146</a>                       |
| Avaya Aura® application                               |                                           |
| ESXi version .....                                    | <a href="#">31</a>                        |
| Avaya InSite Knowledge Base .....                     | <a href="#">191</a>                       |
| Avaya IX Workplace                                    |                                           |
| uploading installation files on Device Services ..... | <a href="#">146</a>                       |
| Avaya Meetings Server                                 |                                           |
| configuration .....                                   | <a href="#">147</a>                       |
| Avaya support website .....                           | <a href="#">191</a>                       |
| Avaya Workplace Client                                |                                           |
| configuring conference control .....                  | <a href="#">137</a>                       |

|                                          |                     |
|------------------------------------------|---------------------|
| AWS                                      |                     |
| manage load balancer certificates .....  | <a href="#">84</a>  |
| AWS installation                         |                     |
| incorrect characters in hosts file ..... | <a href="#">185</a> |
| AWS resource profiles                    |                     |
| specifications .....                     | <a href="#">30</a>  |

## B

|                                |                     |
|--------------------------------|---------------------|
| best practices                 |                     |
| performance and features ..... | <a href="#">203</a> |
| VMware networking .....        | <a href="#">205</a> |

## C

|                                                           |                                           |
|-----------------------------------------------------------|-------------------------------------------|
| CA signed certificates .....                              | <a href="#">197</a>                       |
| Cassandra                                                 |                                           |
| changing default password .....                           | <a href="#">130</a>                       |
| certificate                                               |                                           |
| for reverse proxy .....                                   | <a href="#">153</a> , <a href="#">154</a> |
| installing .....                                          | <a href="#">180</a>                       |
| setup .....                                               | <a href="#">192</a>                       |
| signing identity certificates using CA certificates ..... | <a href="#">197</a>                       |
| signing with System Manager CA .....                      | <a href="#">179</a>                       |
| certificate authority                                     |                                           |
| configuring for reverse proxy .....                       | <a href="#">155</a>                       |
| certificate signing requests .....                        | <a href="#">196</a>                       |
| generating .....                                          | <a href="#">192</a>                       |
| certificates                                              |                                           |
| creating client certificate .....                         | <a href="#">200</a>                       |
| generating identity certificate chain .....               | <a href="#">198</a>                       |
| importing to web browsers .....                           | <a href="#">201</a>                       |
| load balancer certificates for AWS deployment .....       | <a href="#">84</a>                        |
| changing                                                  |                                           |
| Cassandra password .....                                  | <a href="#">130</a>                       |
| characters in passwords .....                             | <a href="#">49</a>                        |
| checking                                                  |                                           |
| Chrony status .....                                       | <a href="#">79</a>                        |
| checking connection                                       |                                           |
| System Manager .....                                      | <a href="#">80</a>                        |
| checklist                                                 |                                           |
| Avaya Aura Web Gateway application installation .....     | <a href="#">98</a>                        |
| configuring                                               |                                           |
| reverse proxy .....                                       | <a href="#">152</a>                       |
| external client access configuration .....                | <a href="#">162</a>                       |
| external native clients media configuration .....         | <a href="#">171</a>                       |
| OVA-based deployment .....                                | <a href="#">51</a>                        |
| planning .....                                            | <a href="#">24</a>                        |
| reverse proxy configuration .....                         |                                           |
| multiple FQDNs deployment .....                           | <a href="#">152</a>                       |
| single FQDN deployment .....                              | <a href="#">151</a>                       |
| WebRTC client side TURN configuration .....               | <a href="#">166</a>                       |
| Chrony service                                            |                                           |

|                                                          |                                           |
|----------------------------------------------------------|-------------------------------------------|
| Chrony service ( <i>continued</i> )                      |                                           |
| checking status .....                                    | <a href="#">79</a>                        |
| client side TURN configuration .....                     | <a href="#">166</a>                       |
| clients                                                  |                                           |
| uploading Avaya IX Workplace to Device Services ....     | <a href="#">146</a>                       |
| cluster configuration .....                              | <a href="#">127</a>                       |
| collection                                               |                                           |
| delete .....                                             | <a href="#">189</a>                       |
| edit .....                                               | <a href="#">189</a>                       |
| generating PDF .....                                     | <a href="#">189</a>                       |
| sharing content .....                                    | <a href="#">189</a>                       |
| commands .....                                           | <a href="#">35</a>                        |
| system layer .....                                       | <a href="#">37</a>                        |
| components .....                                         | <a href="#">19</a>                        |
| configuration                                            |                                           |
| advanced configuration .....                             | <a href="#">129</a>                       |
| conferencing .....                                       | <a href="#">147</a>                       |
| LDAP advanced parameters in Configuration Utility ...    | <a href="#">119</a>                       |
| LDAP parameters in Configuration Utility .....           | <a href="#">112</a>                       |
| configuration worksheet .....                            | <a href="#">21</a>                        |
| configure                                                |                                           |
| ABSCE signaling interface .....                          | <a href="#">174</a>                       |
| ASBCE load monitoring .....                              | <a href="#">163</a>                       |
| ASBCE network interfaces .....                           | <a href="#">184</a>                       |
| ASBCE on AAWG .....                                      | <a href="#">164</a>                       |
| ASBCE server flow .....                                  | <a href="#">176</a>                       |
| DNS .....                                                | <a href="#">136</a>                       |
| external native clients media .....                      | <a href="#">171</a>                       |
| front-end FQDN .....                                     | <a href="#">136</a>                       |
| media interface for ASBCE .....                          | <a href="#">175</a>                       |
| Web Collaboration .....                                  | <a href="#">137</a>                       |
| Workplace Client conference control .....                | <a href="#">137</a>                       |
| configuring                                              |                                           |
| ASBCE .....                                              | <a href="#">150</a>                       |
| ASBCE on Avaya Meetings Server .....                     | <a href="#">165</a>                       |
| Avaya Aura Device Services .....                         | <a href="#">146</a>                       |
| Avaya Aura Media Server .....                            | <a href="#">144</a>                       |
| Avaya Aura Web Gateway .....                             | <a href="#">146</a>                       |
| certificates .....                                       | <a href="#">192</a>                       |
| external client access .....                             | <a href="#">162</a>                       |
| external native clients media .....                      | <a href="#">171</a>                       |
| Media Server .....                                       | <a href="#">143</a>                       |
| password rules .....                                     | <a href="#">46</a>                        |
| registration expiration timer .....                      | <a href="#">143</a>                       |
| reverse proxy .....                                      | <a href="#">151</a> , <a href="#">152</a> |
| role search parameters .....                             | <a href="#">124</a>                       |
| RSA public and private keys .....                        | <a href="#">107</a>                       |
| secure boot .....                                        | <a href="#">63</a>                        |
| SIP Trunks .....                                         | <a href="#">140</a>                       |
| SSH connections .....                                    | <a href="#">107</a>                       |
| STUN on AAWG .....                                       | <a href="#">170</a>                       |
| System Manager .....                                     | <a href="#">143</a>                       |
| WebRTC client side TURN .....                            | <a href="#">166</a>                       |
| configuring AAWG                                         |                                           |
| settings .....                                           | <a href="#">108</a>                       |
| configuring on AAWG .....                                | <a href="#">170</a>                       |
| connection types .....                                   | <a href="#">31</a>                        |
| content                                                  |                                           |
| publishing PDF output .....                              | <a href="#">189</a>                       |
| searching .....                                          | <a href="#">189</a>                       |
| sharing .....                                            | <a href="#">189</a>                       |
| sort by last updated .....                               | <a href="#">189</a>                       |
| watching for updates .....                               | <a href="#">189</a>                       |
| create                                                   |                                           |
| administrative user .....                                | <a href="#">72</a>                        |
| create a cluster                                         |                                           |
| installing additional nodes .....                        | <a href="#">104</a>                       |
| creating                                                 |                                           |
| client certificate .....                                 | <a href="#">200</a>                       |
| disk partitioning for software-only .....                | <a href="#">70</a>                        |
| Elastic load balancer on AWS .....                       | <a href="#">92</a>                        |
| server profile for management interface .....            | <a href="#">162</a>                       |
| TLS client profile .....                                 | <a href="#">183</a>                       |
| TLS server profile .....                                 | <a href="#">183</a>                       |
| TLS server profile for client side TURN .....            | <a href="#">167</a>                       |
| TLS server profile for eternal native clients media .... | <a href="#">172</a>                       |
| TLS server profile for media tunneling interface .....   | <a href="#">173</a>                       |
| creating a key pair .....                                | <a href="#">83</a>                        |
| <b>D</b>                                                 |                                           |
| data encryption                                          |                                           |
| encryptionPassPhrase command .....                       | <a href="#">47</a>                        |
| field descriptions .....                                 | <a href="#">57</a>                        |
| overview .....                                           | <a href="#">18</a>                        |
| data encryption commands .....                           | <a href="#">47</a>                        |
| encryptionRemoteKey .....                                | <a href="#">48</a>                        |
| encryptionStatus .....                                   | <a href="#">48</a>                        |
| deploying                                                |                                           |
| Avaya Aura Web Gateway OVA .....                         | <a href="#">60</a>                        |
| Solution Deployment Manager .....                        | <a href="#">60</a>                        |
| supported vSphere clients .....                          | <a href="#">54</a>                        |
| using Host Client .....                                  | <a href="#">58</a>                        |
| using vSphere Client .....                               | <a href="#">54</a>                        |
| deployment models                                        |                                           |
| configuration requirements .....                         | <a href="#">21</a>                        |
| deployment options                                       |                                           |
| OVA-based .....                                          | <a href="#">50</a>                        |
| deployment process .....                                 | <a href="#">21</a>                        |
| deploymentsoftware-only                                  |                                           |
| AWS .....                                                | <a href="#">50</a>                        |
| VMware .....                                             | <a href="#">50</a>                        |
| descriptions                                             |                                           |
| LDAP parameter .....                                     | <a href="#">124</a>                       |
| diagram                                                  |                                           |
| geographical distribution topology .....                 | <a href="#">13</a>                        |
| solution architecture .....                              | <a href="#">11</a>                        |
| topology .....                                           | <a href="#">11</a>                        |
| disabling                                                |                                           |
| FIPS .....                                               | <a href="#">65</a>                        |
| STIG hardening .....                                     | <a href="#">66</a>                        |
| disk partitioning .....                                  | <a href="#">32</a>                        |
| for software-only deployments .....                      | <a href="#">70</a>                        |
| DNS configuration .....                                  | <a href="#">136</a>                       |

|                                                 |          |                                                       |        |
|-------------------------------------------------|----------|-------------------------------------------------------|--------|
| document changes .....                          | 9        | geo distribution                                      |        |
| documentation center .....                      | 189      | external load balancer .....                          | 33     |
| finding content .....                           | 189      | geographical distribution                             |        |
| navigation .....                                | 189      | overview .....                                        | 13     |
| documentation portal .....                      | 189      | topology diagram .....                                | 13     |
| downloading software                            |          | topology for a call between data centers .....        | 14     |
| using PLDS .....                                | 53       | topology for a call within the same data center ..... | 16     |
| <b>E</b>                                        |          | getting certificates                                  |        |
| EASG                                            |          | third-party CA .....                                  | 193    |
| enabling from CLI .....                         | 62       | global catalog                                        |        |
| field descriptions .....                        | 58       | attributes replication .....                          | 127    |
| enabling                                        |          | <b>H</b>                                              |        |
| additional RPMs for software-only .....         | 76       | haveged                                               |        |
| EASG .....                                      | 62       | enabling .....                                        | 74     |
| FIPS .....                                      | 64       | Host Client .....                                     | 58     |
| FIPS for software-only systems .....            | 74       | hosts file                                            |        |
| root access for AWS VM .....                    | 90       | unexpected characters .....                           | 185    |
| STIG hardening .....                            | 65       | <b>I</b>                                              |        |
| web socket support for reverse proxy .....      | 156      | identity certificates .....                           | 197    |
| encryptionPassphrase .....                      | 47       | identity certificate                                  |        |
| encryptionRemoteKey .....                       | 48       | generating certificate chain .....                    | 198    |
| encryptionStatus .....                          | 48       | importing                                             |        |
| ESXi version                                    |          | client certificates to web browsers .....             | 201    |
| Avaya Aura® application .....                   | 31       | installation                                          |        |
| external access configuration                   |          | checklist .....                                       | 67, 80 |
| creating TLS server profile for management      |          | on customer-provided physical servers or virtual      |        |
| interface .....                                 | 162      | machines .....                                        | 66, 80 |
| external client access configuration .....      | 162      | installation checklist .....                          | 98     |
| external load balancer                          |          | installer utility                                     |        |
| routes configuration .....                      | 148      | cluster configuration .....                           | 127    |
| external traffic                                |          | installing                                            |        |
| configuring rules .....                         | 156, 160 | additional RPMs for software-only .....               | 76     |
| rules for multiple FQDNs model .....            | 161      | Avaya Aura Web Gateway .....                          | 98     |
| rules for single FQDN deployment .....          | 157      | certificates on ASBCE .....                           | 180    |
| <b>F</b>                                        |          | RHEL .....                                            | 69     |
| features best practices .....                   | 203      | system layer for software-only .....                  | 77     |
| finding content on documentation center .....   | 189      | installing additional nodes .....                     | 104    |
| FIPS                                            |          | installing Avaya Aura Web Gateway                     |        |
| disabling .....                                 | 64, 65   | unexpected characters in hosts .....                  | 185    |
| haveged service .....                           | 74       | installing RPMs for software-only .....               | 73     |
| firewall configuration                          |          | internal traffic                                      |        |
| for external native clients media support ..... | 174      | configuring rules .....                               | 158    |
| for WebRTC client side TURN support .....       | 168      | rules for single FQDN deployment .....                | 159    |
| footprint hardware matrix                       |          | iOS                                                   |        |
| AAWG on VMware and ASP 130 .....                | 30       | push notifications .....                              | 17     |
| FQDN configuration .....                        | 136      | <b>K</b>                                              |        |
| <b>G</b>                                        |          | KB                                                    |        |
| generating                                      |          | Support site .....                                    | 191    |
| certificate signing requests .....              | 192      | key pair                                              |        |
| generating identity certificate chain .....     | 198      | creating .....                                        | 83     |

## L

|                                                         |                     |
|---------------------------------------------------------|---------------------|
| LDAP                                                    |                     |
| advanced Configuration Utility settings .....           | <a href="#">119</a> |
| Configuration Utility settings .....                    | <a href="#">112</a> |
| global catalog .....                                    | <a href="#">127</a> |
| multiple authentication and authorization domains ..... | <a href="#">123</a> |
| LDAP parameter                                          |                     |
| descriptions .....                                      | <a href="#">124</a> |
| Linux alias commands .....                              | <a href="#">35</a>  |
| load balancer                                           |                     |
| for AWS software-only installation .....                | <a href="#">92</a>  |
| requirements .....                                      | <a href="#">33</a>  |
| routes configuration .....                              | <a href="#">148</a> |
| load balancer certificates                              |                     |
| AWS deployment .....                                    | <a href="#">84</a>  |
| load monitoring                                         |                     |
| configuring .....                                       | <a href="#">163</a> |

## M

|                                       |                     |
|---------------------------------------|---------------------|
| multiple authentication domains ..... | <a href="#">123</a> |
|---------------------------------------|---------------------|

## N

|                              |                                           |
|------------------------------|-------------------------------------------|
| networking considerations    |                                           |
| Amazon Web Services .....    | <a href="#">31</a>                        |
| New in this release .....    | <a href="#">10</a>                        |
| node                         |                                           |
| removing from cluster .....  | <a href="#">95</a> , <a href="#">133</a>  |
| non-root administrative user |                                           |
| creating .....               | <a href="#">72</a>                        |
| NTP time source .....        | <a href="#">203</a>                       |
| Nutanix .....                | <a href="#">212</a> , <a href="#">213</a> |

## O

|                                          |                     |
|------------------------------------------|---------------------|
| OAMP configuration                       |                     |
| Linux account .....                      | <a href="#">132</a> |
| obtaining                                |                     |
| Avaya Aura Web Gateway OVA .....         | <a href="#">52</a>  |
| OpenSSL .....                            | <a href="#">196</a> |
| optional RPMs .....                      | <a href="#">76</a>  |
| OVA                                      |                     |
| data encryption field descriptions ..... | <a href="#">57</a>  |
| EASG field descriptions .....            | <a href="#">58</a>  |
| OVA deployment .....                     | <a href="#">54</a>  |
| supported vSphere clients .....          | <a href="#">54</a>  |
| using Host Client .....                  | <a href="#">58</a>  |
| using vSphere Client .....               | <a href="#">54</a>  |
| OVA-based deployment                     |                     |
| checklist .....                          | <a href="#">51</a>  |
| OVA-based deployments .....              | <a href="#">50</a>  |
| overview                                 |                     |
| Avaya Aura Web Gateway .....             | <a href="#">10</a>  |

## P

|                                                       |                     |
|-------------------------------------------------------|---------------------|
| packages                                              |                     |
| RHEL package management .....                         | <a href="#">76</a>  |
| password                                              |                     |
| changing default password for automatic backups ..... | <a href="#">131</a> |
| password rules                                        |                     |
| configuring .....                                     | <a href="#">46</a>  |
| supported characters .....                            | <a href="#">49</a>  |
| performance best practices .....                      | <a href="#">203</a> |
| pinging                                               |                     |
| System Manager .....                                  | <a href="#">80</a>  |
| planning .....                                        | <a href="#">24</a>  |
| PLDS                                                  |                     |
| downloading software .....                            | <a href="#">53</a>  |
| preinstallation .....                                 | <a href="#">24</a>  |
| prerequisites                                         |                     |
| certificates .....                                    | <a href="#">27</a>  |
| FQDN .....                                            | <a href="#">27</a>  |
| IP addresses .....                                    | <a href="#">27</a>  |
| system layer installation on AWS .....                | <a href="#">90</a>  |
| push notifications .....                              | <a href="#">17</a>  |

## R

|                                                        |                                           |
|--------------------------------------------------------|-------------------------------------------|
| Red Hat subscription .....                             | <a href="#">76</a>                        |
| related documentation .....                            | <a href="#">187</a>                       |
| removing                                               |                                           |
| node from cluster .....                                | <a href="#">186</a>                       |
| unavailable non-initial node .....                     | <a href="#">95</a> , <a href="#">133</a>  |
| replacing                                              |                                           |
| seed node .....                                        | <a href="#">103</a>                       |
| required                                               |                                           |
| skills and knowledge .....                             | <a href="#">26</a>                        |
| requirements                                           |                                           |
| configuration requirements for deployment models ..... | <a href="#">21</a>                        |
| external load balancer .....                           | <a href="#">33</a>                        |
| resource profile specifications .....                  | <a href="#">29</a>                        |
| AAWG on VMware and ASP 130 .....                       | <a href="#">30</a>                        |
| reverse proxy                                          |                                           |
| configuring certificate authority .....                | <a href="#">155</a>                       |
| configuring external traffic rules                     |                                           |
| multiple FQDNs deployment .....                        | <a href="#">160</a>                       |
| single FQDN deployment .....                           | <a href="#">156</a>                       |
| configuring internal traffic rules .....               | <a href="#">158</a>                       |
| configuring TLS server profile .....                   | <a href="#">153</a> , <a href="#">154</a> |
| configuring web socket support .....                   | <a href="#">156</a>                       |
| creating security certificate .....                    | <a href="#">153</a> , <a href="#">154</a> |
| installing Avaya Meetings Management certificate ..... | <a href="#">182</a>                       |
| reverse proxy configuration .....                      | <a href="#">151</a>                       |
| prerequisites .....                                    | <a href="#">152</a>                       |
| reviewing                                              |                                           |
| data encryption status .....                           | <a href="#">48</a>                        |
| RHEL .....                                             | <a href="#">212</a>                       |
| additional RPMs .....                                  | <a href="#">73</a>                        |
| installing .....                                       | <a href="#">69</a>                        |
| packages .....                                         | <a href="#">76</a>                        |

|                                   |                     |
|-----------------------------------|---------------------|
| RHEL Installation .....           | <a href="#">213</a> |
| RSA public and private keys ..... | <a href="#">107</a> |

## S

|                                                      |                     |
|------------------------------------------------------|---------------------|
| searching for content .....                          | <a href="#">189</a> |
| secure boot .....                                    | <a href="#">63</a>  |
| checking status .....                                | <a href="#">64</a>  |
| seed node .....                                      |                     |
| configuring backup nodes .....                       | <a href="#">103</a> |
| serviceability agents .....                          | <a href="#">141</a> |
| Session Manager .....                                |                     |
| configuring registration expiration timer .....      | <a href="#">143</a> |
| settings .....                                       |                     |
| initial AAWG configuration .....                     | <a href="#">108</a> |
| sharing content .....                                | <a href="#">189</a> |
| signing certificates with System Manager CA .....    | <a href="#">179</a> |
| silent installation .....                            | <a href="#">102</a> |
| skills and knowledge .....                           | <a href="#">26</a>  |
| snapshots .....                                      | <a href="#">209</a> |
| SNMP target profile .....                            |                     |
| setting up .....                                     | <a href="#">142</a> |
| SNMPv3 user profile .....                            |                     |
| assigning .....                                      | <a href="#">142</a> |
| setting up .....                                     | <a href="#">141</a> |
| software requirements .....                          | <a href="#">28</a>  |
| software-only .....                                  |                     |
| additional packages .....                            | <a href="#">76</a>  |
| additional RPMs .....                                | <a href="#">73</a>  |
| Amazon Web Services .....                            |                     |
| prerequisites for software-only .....                |                     |
| installation .....                                   | <a href="#">83</a>  |
| Amazon Web Services installation prerequisites ..... | <a href="#">83</a>  |
| AWS installation checklist .....                     | <a href="#">80</a>  |
| checklist .....                                      |                     |
| software-only installation on AWS .....              | <a href="#">80</a>  |
| software-only installation on VMware .....           | <a href="#">67</a>  |
| configuring DNS settings .....                       | <a href="#">89</a>  |
| configuring idle timeout .....                       | <a href="#">95</a>  |
| creating disk partitioning .....                     | <a href="#">70</a>  |
| creating security groups for AWS .....               | <a href="#">86</a>  |
| creating target groups .....                         | <a href="#">91</a>  |
| disk partitions .....                                | <a href="#">69</a>  |
| enabling Haveged service .....                       | <a href="#">74</a>  |
| enabling root access for AWS VM .....                | <a href="#">90</a>  |
| installing RHEL on AWS .....                         | <a href="#">88</a>  |
| system layer installation .....                      | <a href="#">77</a>  |
| system layer prerequisites for AWS .....             | <a href="#">90</a>  |
| VMware installation checklist .....                  | <a href="#">67</a>  |
| software-only deployments .....                      |                     |
| Amazon Web Services .....                            | <a href="#">80</a>  |
| VMWare .....                                         | <a href="#">66</a>  |
| software-only installation .....                     |                     |
| creating administrative users .....                  | <a href="#">72</a>  |
| solution architecture .....                          | <a href="#">11</a>  |
| sort documents .....                                 | <a href="#">189</a> |
| special characters .....                             | <a href="#">49</a>  |

|                                                 |                        |
|-------------------------------------------------|------------------------|
| specifications .....                            |                        |
| virtual disk volume .....                       | <a href="#">32</a>     |
| SSH connections .....                           |                        |
| cluster .....                                   | <a href="#">107</a>    |
| start .....                                     |                        |
| services .....                                  | <a href="#">131</a>    |
| STIG hardening .....                            |                        |
| disabling additional hardening options .....    | <a href="#">66</a>     |
| enabling .....                                  | <a href="#">65</a>     |
| storage .....                                   | <a href="#">208</a>    |
| STUN .....                                      | <a href="#">170</a>    |
| subscription .....                              |                        |
| Red Hat subscription .....                      | <a href="#">76</a>     |
| support .....                                   | <a href="#">191</a>    |
| supported vSphere clients .....                 | <a href="#">54</a>     |
| sys .....                                       | <a href="#">37</a>     |
| sys seccomp .....                               | <a href="#">38</a>     |
| sys smcvmgt .....                               | <a href="#">42</a>     |
| examples .....                                  | <a href="#">45</a>     |
| sys versions .....                              | <a href="#">38</a>     |
| sys volmgt .....                                | <a href="#">39</a>     |
| system layer .....                              |                        |
| commands .....                                  | <a href="#">37</a>     |
| for software-only .....                         | <a href="#">77</a>     |
| seccomp .....                                   | <a href="#">38</a>     |
| smcvmgt .....                                   | <a href="#">42, 45</a> |
| versions .....                                  | <a href="#">38</a>     |
| volmgt .....                                    | <a href="#">39</a>     |
| System Manager .....                            |                        |
| configuring registration expiration timer ..... | <a href="#">143</a>    |
| settings .....                                  | <a href="#">140</a>    |
| Solution Deployment Manager .....               | <a href="#">60</a>     |

## T

|                                             |                          |
|---------------------------------------------|--------------------------|
| target groups .....                         | <a href="#">91</a>       |
| third-party CA .....                        |                          |
| generating identity certificate chain ..... | <a href="#">198</a>      |
| getting certificates .....                  | <a href="#">193</a>      |
| third-party root CA .....                   | <a href="#">199</a>      |
| time synchronization .....                  |                          |
| checking status .....                       | <a href="#">79</a>       |
| timekeeping .....                           | <a href="#">203</a>      |
| TLS client profile .....                    |                          |
| creating .....                              | <a href="#">183</a>      |
| TLS server profile .....                    |                          |
| creating .....                              | <a href="#">183</a>      |
| for client side TURN .....                  | <a href="#">167</a>      |
| for external native clients media .....     | <a href="#">172</a>      |
| for media tunneling interface .....         | <a href="#">173</a>      |
| for reverse proxy .....                     | <a href="#">153, 154</a> |
| topology diagram .....                      | <a href="#">11</a>       |
| call between data centers .....             | <a href="#">14</a>       |
| call within the same data center .....      | <a href="#">16</a>       |
| geographical distribution .....             | <a href="#">13</a>       |
| traffic rules for security groups .....     |                          |
| Avaya Aura Web Gateway .....                | <a href="#">86</a>       |

|                                                        |                     |
|--------------------------------------------------------|---------------------|
| traffic rules for security groups ( <i>continued</i> ) |                     |
| Web Services load balancer .....                       | <a href="#">87</a>  |
| training .....                                         | <a href="#">190</a> |
| troubleshooting                                        |                     |
| removing node from cluster .....                       | <a href="#">186</a> |
| unexpected characters in hosts file .....              | <a href="#">185</a> |
| TURN                                                   |                     |
| client side configuration .....                        | <a href="#">166</a> |
| TURN for a WebRTC client                               |                     |
| configuring .....                                      | <a href="#">171</a> |

## U

|                                             |                                          |
|---------------------------------------------|------------------------------------------|
| UEFI .....                                  | <a href="#">63</a>                       |
| UEFI secure boot                            |                                          |
| checking status .....                       | <a href="#">64</a>                       |
| unavailable node                            |                                          |
| removing from cluster .....                 | <a href="#">95</a> , <a href="#">133</a> |
| uninstall                                   |                                          |
| Avaya Aura Web Gateway .....                | <a href="#">95</a> , <a href="#">132</a> |
| Update                                      |                                          |
| December 2025 .....                         | <a href="#">135</a>                      |
| uploading                                   |                                          |
| Avaya IX Workplace to Device Services ..... | <a href="#">146</a>                      |
| using alias .....                           | <a href="#">35</a>                       |
| utility installer                           |                                          |
| certificate configuration .....             | <a href="#">109</a>                      |
| front-end host .....                        | <a href="#">109</a>                      |

## V

|                                    |                     |
|------------------------------------|---------------------|
| videos .....                       | <a href="#">190</a> |
| virtual IP configuration .....     | <a href="#">128</a> |
| Virtual Machine .....              | <a href="#">212</a> |
| vMotion .....                      | <a href="#">209</a> |
| VMware High Availability .....     | <a href="#">208</a> |
| VMware networking                  |                     |
| best practices .....               | <a href="#">205</a> |
| VMware software requirements ..... | <a href="#">28</a>  |
| VMware Tools .....                 | <a href="#">204</a> |
| vSphere .....                      | <a href="#">54</a>  |
| vSphere clients .....              | <a href="#">54</a>  |

## W

|                                                     |                     |
|-----------------------------------------------------|---------------------|
| watchlist .....                                     | <a href="#">189</a> |
| web browser requirements .....                      | <a href="#">19</a>  |
| web deployment service                              |                     |
| uploading Avaya IX Workplace on Device Services ... | <a href="#">146</a> |
| web socket                                          |                     |
| enabling for reverse proxy .....                    | <a href="#">156</a> |
| WebRTC                                              |                     |
| configuring client side TURN .....                  | <a href="#">166</a> |
| configuring TURN/STUN profile on ASBCE .....        | <a href="#">169</a> |