



# **Deploying and Updating Avaya Aura<sup>®</sup> Media Server Appliance**

Release 10.2.x  
Issue 10  
May 2026

# Notices

© 2026 Avaya LLC. All Rights Reserved.

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

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

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

## Notice

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

## Documentation disclaimer

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

## Link disclaimer

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

## Warranty

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

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

## Hosted Service

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

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

## Copyright

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

## Virtualization

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

## Third Party Components

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

## Service Provider

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

## Compliance with Laws

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

## Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

### **Avaya Toll Fraud intervention**

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

### **Security Vulnerabilities**

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

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

### **Downloading Documentation**

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

### **Contact Avaya Support**

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

### **Trademarks**

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

Avaya is a registered trademark of Avaya LLC.

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

## Contents

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| <b>Chapter 1: Introduction</b>                                                                               | 8  |
| Purpose                                                                                                      | 8  |
| Changes to platform support                                                                                  | 8  |
| Change history                                                                                               | 9  |
| <b>Chapter 2: Overview</b>                                                                                   | 10 |
| About the Avaya Aura® MS appliance                                                                           | 10 |
| New in this release                                                                                          | 10 |
| New in Avaya Aura® Media Server 10.2                                                                         | 11 |
| <b>Chapter 3: Deploying in the VMware® virtualized environment</b>                                           | 12 |
| System requirements                                                                                          | 12 |
| 1+1 High Availability cluster requirements                                                                   | 14 |
| Best practice recommendations                                                                                | 15 |
| Obtaining Avaya Aura® MS OVA                                                                                 | 16 |
| Deploying the OVA file by using vSphere Web Client for vCenter                                               | 16 |
| Deploying the OVA file by using VMware Host Client                                                           | 19 |
| Adding the OVA file to Solution Deployment Manager software library                                          | 22 |
| Deploying the OVA file using Solution Deployment Manager                                                     | 23 |
| <b>Chapter 4: Deploying in the KVM on Red Hat® virtualized environment for ASP 130 Release 6.0 or higher</b> | 26 |
| System requirements                                                                                          | 26 |
| 1+1 High Availability cluster requirements                                                                   | 28 |
| Best practice recommendations                                                                                | 28 |
| Obtaining Avaya Aura® MS KVM Installer                                                                       | 29 |
| Deploying the Avaya Aura® MS KVM installer                                                                   | 29 |
| Upgrading ASP 130 R6.0 or higher without upgrading the AAMS software                                         | 32 |
| Upgrading to ASP 130 R6.0 or higher migration and upgrading the AAMS software                                | 33 |
| <b>Chapter 5: Deploying Avaya Solutions Platform physical appliances</b>                                     | 35 |
| System requirements                                                                                          | 35 |
| ASP 110 (Dell R660XS) active network ports                                                                   | 35 |
| ASP 110 (Dell R640XL) active network ports                                                                   | 36 |
| 1+1 High Availability cluster requirements                                                                   | 36 |
| Deploying the Avaya Aura® MS physical appliance                                                              | 37 |
| Obtaining physical appliance recovery software                                                               | 39 |
| Updating the Avaya Aura® MS physical appliance Boot Mode to UEFI                                             | 39 |
| Reinstalling the Avaya Aura® MS physical appliance running on Dell R660XS hardware (no DVD drive)            | 40 |
| Reinstalling the Avaya Aura® MS physical appliance running on Dell R640 XL hardware                          | 43 |
| <b>Chapter 6: Signing in to the Avaya Aura® MS appliance</b>                                                 | 45 |
| Element Manager                                                                                              | 45 |

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| Accessing Avaya Aura® MS EM.....                                                | 45        |
| Accessing Linux® shells.....                                                    | 45        |
| Changing users in the Linux® shell.....                                         | 46        |
| Avaya support access.....                                                       | 46        |
| Determining the status of EASG.....                                             | 47        |
| Enabling or disabling EASG.....                                                 | 47        |
| Displaying product EASG certificate information.....                            | 48        |
| Loading and managing site certificate.....                                      | 49        |
| <b>Chapter 7: Configuration.....</b>                                            | <b>51</b> |
| Configuring Avaya Aura® MS.....                                                 | 51        |
| Updating the network configuration.....                                         | 51        |
| Resizing an Avaya Virtual Appliance for use as a Video Compositor.....          | 53        |
| Setting the GRUB2 boot password.....                                            | 54        |
| Setting the password complexity configuration.....                              | 54        |
| Customizing the password complexity configuration.....                          | 55        |
| Enabling SELinux.....                                                           | 55        |
| Displaying Linux® SELinux configuration status.....                             | 56        |
| <b>Configuring Avaya Aura® Media Server (MS) physical appliance iDRAC9.....</b> | <b>56</b> |
| <b>Chapter 8: FIPS Mode.....</b>                                                | <b>57</b> |
| Overview.....                                                                   | 57        |
| Enabling FIPS 140-2 Mode.....                                                   | 57        |
| Disabling FIPS 140-2 Mode.....                                                  | 58        |
| Displaying FIPS 140-2 configuration status.....                                 | 58        |
| <b>Chapter 9: File System Integrity Tool (FSIT).....</b>                        | <b>59</b> |
| Overview.....                                                                   | 59        |
| Initializing the AIDE database.....                                             | 59        |
| Enabling daily FSIT scans.....                                                  | 59        |
| Disabling daily FSIT scans.....                                                 | 60        |
| Displaying FSIT scan results.....                                               | 60        |
| Running file system integrity scans on demand.....                              | 61        |
| <b>Chapter 10: Antivirus Software.....</b>                                      | <b>62</b> |
| Overview.....                                                                   | 62        |
| Enabling daily scans and updates.....                                           | 62        |
| Disabling daily scans and updates.....                                          | 63        |
| Displaying update and scan results.....                                         | 63        |
| Running updates and scans on demand.....                                        | 64        |
| <b>Chapter 11: Backup and restore.....</b>                                      | <b>65</b> |
| Performing a backup.....                                                        | 65        |
| Uploading and restoring backup files.....                                       | 66        |
| Alternate procedure for uploading and restoring large backup files.....         | 67        |
| <b>Chapter 12: Updates.....</b>                                                 | <b>68</b> |
| Viewing the installed version and updates.....                                  | 68        |

|                                                                                                       |           |
|-------------------------------------------------------------------------------------------------------|-----------|
| Uploading media server updates.....                                                                   | 68        |
| Uploading and installing media server updates using a Linux® shell.....                               | 69        |
| Deleting an uploaded update.....                                                                      | 70        |
| Installing an update.....                                                                             | 70        |
| Removing an installed update.....                                                                     | 72        |
| Managing media server changes for N+1 load sharing clusters.....                                      | 72        |
| Managing media server changes for 1+1 High Availability clusters.....                                 | 73        |
| Updating the Avaya Aura® MS physical appliance to enable secure boot.....                             | 74        |
| Updating the Avaya Aura® MS VMware virtual appliance to enable secure boot.....                       | 75        |
| Updating the Avaya Aura® MS KVM virtual appliance to enable secure boot.....                          | 76        |
| <b>Chapter 13: Upgrade from a previous release.....</b>                                               | <b>77</b> |
| Upgrade overview.....                                                                                 | 77        |
| Upgrading to Avaya Aura® MS 10.y.....                                                                 | 77        |
| Rolling back to a previous release.....                                                               | 78        |
| Upgrading data manually from Release 8.0.x to a newly deployed Avaya Aura® MS appliance instance..... | 78        |
| <b>Chapter 14: Migrating from ASP 120 to ASP 130.....</b>                                             | <b>81</b> |
| Migration overview.....                                                                               | 81        |
| Migrating ASP 120 (AMS 8.x) to ASP 130 (AMS 10.x).....                                                | 81        |
| Migrating ASP 120 (AMS 10.x) to ASP 130 (AMS 10.x).....                                               | 82        |
| <b>Chapter 15: Patches.....</b>                                                                       | <b>83</b> |
| Quick Fix Engineering overview.....                                                                   | 83        |
| Obtaining QFE.....                                                                                    | 83        |
| Description of the patch tool.....                                                                    | 83        |
| Installing a QFE patch.....                                                                           | 84        |
| Removing a QFE patch.....                                                                             | 86        |
| Managing QFEs for 1+1 High Availability clusters.....                                                 | 88        |
| Managing QFEs for N+1 load sharing clusters.....                                                      | 89        |
| <b>Chapter 16: Troubleshooting the Avaya Aura® MS appliance.....</b>                                  | <b>91</b> |
| Overview.....                                                                                         | 91        |
| Unable to upload files larger than 2 GB.....                                                          | 91        |
| Unable to upload updates.....                                                                         | 91        |
| Backup or restore tasks fail.....                                                                     | 92        |
| Resetting locked login accounts.....                                                                  | 93        |
| Restarting or shutting down from Linux® shell .....                                                   | 93        |
| <b>Chapter 17: Related resources.....</b>                                                             | <b>94</b> |
| Media Server documentation.....                                                                       | 94        |
| Finding documents on the Avaya Support website.....                                                   | 95        |
| Accessing the port matrix document.....                                                               | 95        |
| Avaya Documentation Center navigation.....                                                            | 96        |
| Training.....                                                                                         | 97        |
| Viewing Avaya Mentor videos.....                                                                      | 97        |
| Support.....                                                                                          | 98        |

Using the Avaya InSite Knowledge Base..... 98

# Chapter 1: Introduction

---

## Purpose

Use this document when you are working with the Avaya Aura® Media Server (MS) appliance. This document contains the procedures for:

- Deploying, upgrading, and updating Avaya Aura® Media Server appliances in the VMware® Virtualized Environment.
- Upgrading, updating, and reinstalling Avaya Aura® Media Server appliances on Avaya Common Servers.

### Important:

Avaya also provides a non-appliance, software-only, application version of Avaya Aura® Media Server which is installed on servers that you provide. For non-appliance installation, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

This document is intended for people who install, upgrade, and troubleshoot Avaya Aura® Media Server 10.2 appliances

Administrators of the appliance version of Avaya Aura® Media Server must use this document before referring to any other Avaya Aura® Media Server documents.

Administrators of non-appliance versions of Avaya Aura® Media Server must not use this document.

---

## Changes to platform support

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

### Discontinued Platforms:

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

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

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

## Change history

| Issue | Date          | Summary of changes                                                                                                                                                                                                          |
|-------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10    | May 2026      | Updated the following section: <ul style="list-style-type: none"> <li>• <a href="#">System requirements</a> on page 35</li> </ul>                                                                                           |
| 9     | March 2026    | Added the section: <ul style="list-style-type: none"> <li>• <a href="#">Changes to platform support</a> on page 8</li> </ul>                                                                                                |
| 8     | March 2026    | Updated the following sections: <ul style="list-style-type: none"> <li>• System requirements for Virtualized Environment</li> <li>• System requirements for Common Server</li> </ul>                                        |
| 7     | December 2025 | Updated the following procedure: <ul style="list-style-type: none"> <li>• Restoring the configuration when migrating from VMWare based ASP 130 to KVM based ASP 130.</li> <li>• Backup and restore restrictions.</li> </ul> |
| 6     | December 2025 | Clarified procedure for upgrading appliance from older release (8.0.x or 10.x) to the latest (10.y).                                                                                                                        |
| 5     | July 2025     | Updated KVM requirements.                                                                                                                                                                                                   |
| 4     | March 2025    | Added secure boot support.                                                                                                                                                                                                  |
| 3     | March 2025    | <ul style="list-style-type: none"> <li>• Added Dell R660 info.</li> <li>• Updated the topic <a href="#">Media Server documentation</a> on page 94</li> </ul>                                                                |
| 2     | February 2025 | Updated to include alternate way to run the KVM installer.                                                                                                                                                                  |
| 1     | December 2024 | Initial issue for Release 10.2                                                                                                                                                                                              |

# Chapter 2: Overview

---

## About the Avaya Aura® MS appliance

The Avaya Aura® MS appliance is a software appliance that combines the Avaya Aura® MS software and an optimized Linux® operating system in a single and integrated package.

Avaya appliances are closed systems maintained by Avaya. Avaya manages all software and software updates on appliances. Avaya does not support appliances that have non-Avaya software or software updates installed.

A deployed Avaya Aura® MS appliance includes the following:

- Avaya Aura® MS software
- Avaya Aura® MS Element Manager (EM)
- Security-hardened Linux® operating system
- Customer administrative account
- Pre-configured AVAYA support accounts

There are two types of Avaya Aura® MS appliances:

- Virtual appliances: Avaya Aura® MS appliances in VMware® or KVM on RedHat® virtualized environments.
- Physical appliances: Avaya Aura® MS appliances on Avaya Common Servers.

 **Note:**

This document contains the procedures for all types of Avaya Aura® MS appliances. Ensure that you use the procedures that are appropriate for your appliance type.

 **Important:**

Avaya also provides a non-appliance, software-only, application version of Avaya Aura® Media Server which is installed on servers that you provide. For non-appliance installations, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

---

## New in this release

This section contains features new to Avaya Aura® Media Server 10.2.

## Related links

[New in Avaya Aura Media Server 10.2](#) on page 11

## New in Avaya Aura® Media Server 10.2

- Deployment in the KVM on Red Hat® virtualized environment for ASP 130 (appliance only).
- TLSv1.3 support is added (except for ICE).
- Support for TLSv1.0 is removed. TLSv1.2 is disabled by default (except for ICE).
- Update of dual unicast monitoring.
- Removal of Element Manager tasks that are no longer needed.
- Deployment in a Nutanix environment running the Acropolis Hypervisor (AHV).
- Support for the new Dell R660xs ASP 110 server for physical appliances.
- Secure boot support.

## Related links

[New in this release](#) on page 10

# Chapter 3: Deploying in the VMware® virtualized environment

## System requirements

The Avaya Aura® MS appliance is deployed using a vSphere Web Client or a VMware Host Client. The ESXi host must meet the following system requirements:

| ESXi host resource | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU                | <p>The core processor speed must be at least 2190 MHz and Intel® processors are strongly recommended, or performance cannot be guaranteed. Intel® and AMD processors require minimum SSE 4.1 support.</p> <p>For all VM deployed on a host with an Avaya Aura® MS the total number of vCPU must not exceed the number of physical CPUs.</p> <p>Configuration profile 1 and 2 require 4 vCPUs.</p> <p>Configuration profile 3 and 4 require 8 vCPUs.</p> <p>Configuration profile 5 and 6 require 16 vCPUs.</p> |
| Memory             | <p>Configuration profile 1 and 2 require 4608 MB of memory.</p> <p>Configuration profile 3 and 4 require 8192 MB of memory.</p> <p>Configuration profile 5 and 6 require 16384 MB of memory.</p>                                                                                                                                                                                                                                                                                                               |
| Disk space         | <p>Configuration profile 1, 3, and 5 require 50 GB of ESXi datastore.</p> <p>Configuration profile 2, 4, and 6 require 250 GB of ESXi datastore.</p>                                                                                                                                                                                                                                                                                                                                                           |
| Network bandwidth  | <p>A dedicated pair of 1 Gbps network interfaces must be available in a teamed, failover configuration. Alternatively, 1 Gbps of dedicated bandwidth on a pair of 10 Gbps network interfaces must be available in a teamed, failover configuration.</p>                                                                                                                                                                                                                                                        |
| IOPS               | <p>The system must support 100 Input/Output Operations per Second (IOPS).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |

The following requirements are also mandatory:

- Physical CPUs on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with the media server. A physical CPU refers to a physical CPU core and not to a hyper-thread. For example, the total number of vCPUs across all VMs on an ESXi host that has 12 physical cores with 24 hyper-threads, must not exceed 12.

 **Note:**

This recommendation prevents CPU oversubscription. Therefore, the CPU reservation of the media server VM effectively enforces the minimum CPU core speed of the underlying hardware. The VM fails to start if the underlying hardware does not meet the core speed requirements.

- Do not modify the CPU or memory reservations that are set for Avaya Aura® MS OVA.

 **Note:**

Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. It is mandatory to ensure the ESXi host is not oversubscribed (pCPU <= vCPU for all VMs deployed to that host).

- For maximum system performance, ensure that:
  1. Energy savings features are disabled.
  2. Maximum performance settings are enabled in the server BIOS.
- When deploying the OVA file, select **Thick Provision Lazy Zeroed** option for the VM virtual disks.
- ESXi feature support is detailed in the following table:

| ESXi Feature                | Avaya Aura® Media Server Support                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESXi Versions               | Supported Versions: 7.0 or 8.0                                                                                                                                                                                                                                                                                                                                 |
| Clone Virtual Machine       | Supported. VMs must be shut down before copying.<br><br> <b>Caution:</b><br><br>Cloning should not be used to create additional Avaya Aura® MS server instances. This will result in software failures since multiple Avaya Aura® MS servers are assigned to the same UUID. |
| Large Receive Offload (LRO) | Supported.                                                                                                                                                                                                                                                                                                                                                     |
| Resize Virtual Machine      | Not supported when the VM is powered ON.<br><br>Supported when the VMs are shut down and resized to match one of the supported Avaya profiles, unless otherwise instructed by Avaya.                                                                                                                                                                           |
| VMware Storage vMotion      | Not supported.<br><br>To migrate to a different storage system, you must first shut down the VM. For 1+1 HA Clusters, both VMs must be shut down.                                                                                                                                                                                                              |
| VMware vMotion              | Not supported.<br><br>To migrate to a different physical host, you must first shut down the VM. For 1+1 HA Clusters, both VMs must be shut down.                                                                                                                                                                                                               |

*Table continues...*

| ESXi Feature                                | Avaya Aura® Media Server Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware Snapshots                            | <p>Not supported on production servers outside of maintenance windows.</p> <p>Supported for temporary use when applying feature packs, service packs, or patches during maintenance windows.</p> <p>The VM must be shut down before creating, deleting, or reverting a snapshot. For 1+1 HA clusters, both VMs must be shut down for any snapshot operation on either server.</p> <p>Snapshots adversely impact the VM disk and CPU performance and must be removed before returning the server to production.</p> |
| VMware High Availability (HA)               | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| VMware Distributed Resource Scheduler (DRS) | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Distributed Power Management (DPM)          | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| VMware Fault Tolerance (FT)                 | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| vSphere Standard Switch                     | Supported when the media server has a dedicated pair of 1 Gbps NICs or 1 Gbps of dedicated bandwidth on a pair of 10 Gbps NICs.                                                                                                                                                                                                                                                                                                                                                                                    |
| vSphere Distributed Switch                  | Supported if the vSphere Distributed Switch is engineered to provide same bandwidth as the vSphere Standard Switch. The media server requires a dedicated pair of 1 Gbps NICs or 1 Gbps of dedicated bandwidth on a pair of 10 Gbps NICs.                                                                                                                                                                                                                                                                          |
| CPU and Memory Reservations                 | Supported. Reservations are mandatory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| VSAN support                                | Supported if the VSAN meets media server Input/Output Operations Per Second (IOPS) requirements.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Thin Provisioning                           | Supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## 1+1 High Availability cluster requirements

The 1+1 High Availability cluster configuration ensures uninterrupted availability of media processing in cases where a media server fails. Use the High Availability configuration option when you require the capacity of only a single Avaya Aura® MS.

The High Availability configuration deploys as a Primary server and a Backup server. Only one server is active at a time. The other server is waiting in synchronized hot standby to take over instantly.

Both servers must have identical configuration so that either server can take over the full media processing load if the other server fails. Ensure that the deployed servers meet the following requirements:

- Each media server in a 1+1 High Availability cluster deployed as a virtual machine (VM) must be deployed on separate but equally capable host servers with the same hardware and

processor model. The VMs must be deployed using the same configuration profile so that they have the same number of vCPUs.

- There is no inter-cluster communication between different 1+1 High Availability clusters. Different 1+1 High Availability clusters can use different hardware or profiles, but the specifications within a cluster must match.

## Best practice recommendations

Use the following best practices to deploy the Avaya Aura® MS appliance in the VMware® virtualized environment:

- Media server VMs deployed as a High Availability (HA) cluster should be deployed on separate, equally capable host servers.
- All physical servers that can host a VM must have the same CPU, memory, and networking specifications.
- Physical CPUs on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with Avaya Aura® MS. A physical CPU refers to a physical CPU core and not to a hyper-thread. For example, the total number of vCPUs across all VMs on an ESXi host that has 12 physical cores with 24 hyper-threads, must not exceed 12.

### **Note:**

This recommendation prevents CPU oversubscription. Therefore, the CPU reservation of the media server VM effectively enforces the minimum CPU core speed of the underlying hardware. The VM fails to start if the underlying hardware does not meet the core speed requirements.

- Do not modify the CPU or memory reservations that are set for Avaya Aura® MS OVA.

### **Note:**

Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. It is mandatory to ensure the ESXi host is not oversubscribed (pCPU <= vCPU for all VMs deployed to that host).

- For maximum system performance, ensure that the energy savings features are disabled or that the maximum performance settings are enabled in the server BIOS.
- When deploying the OVA file, select **Thick Provision Lazy Zeroed** option for the VM virtual disks.
- If the physical network interfaces on the ESXi host are 10 Gbps interfaces, then NetIOC and traffic shaping must be performed. NetIOC and traffic shaping must allocate 1 Gbps of network bandwidth for the Avaya Aura® MS VM.
- Old media server backup files must be removed to maintain free space on the system.

- You must not modify any operating system files. Avaya manages the operating system on appliances. Modifying system files can cause future system layer updates from Avaya to fail or result in loss of your changes

---

## Obtaining Avaya Aura® MS OVA

### About this task

You can download Avaya Aura® MS OVA from the Avaya Product Licensing and Delivery System (Avaya PLDS) website at <https://plds.avaya.com>.

### Next steps

Deploy the OVA file using vSphere Client.

---

## Deploying the OVA file by using vSphere Web Client for vCenter

### About this task

The steps in this procedure use the vSphere Web Client, which runs in a web browser.

### Before you begin

- Obtain the Avaya Aura® MS OVA file. Save the file on the workstation where you will run vSphere Web Client to configure the new VM.

#### ! Important:

As noted in <https://kb.vmware.com/s/article/84240>, prior to vCenter 7.0 U2, there was minimal certificate verification done on OVA/OVF packages. Starting 7.0 U2, the OVF signing certificates are verified for their expiry, validity and checked if the signing certificate is trusted. This means that the entire chain of the signing certificate must be trusted against the VECS store. For more information on how to update the VECS store, see the [PSN101084832u](#) at the Avaya support website.

- Obtain the following networking configuration settings for the new VM. These settings can be from an existing system if you are redeploying Avaya Aura® MS OVA.

#### ! Important:

If you plan to enroll media servers with Avaya Aura® System Manager, then the media servers and System Manager must use the same NTP server for time synchronization.

- Hostname
- IPv4 address
- IPv4 Netmask

- Gateway IPv4 address
  - Customer account login name
  - Customer account password
  - Time zone
  - **(Optional)** Network domain
  - **(Optional)** IPv4 address of the DNS servers
  - IPv4 address or hostname of the NTP servers
  - **(Optional)** IPv6 address
  - **(Optional)** IPv6 prefix length
  - **(Optional)** IPv6 gateway address
  - **(Optional)** Out of band management IPv4 address
  - **(Optional)** Out of band management IPv4 netmask
  - **(Optional)** Out of band management IPv4 gateway address
  - **(Optional)** Root account password
- Ensure that you turn off the current Avaya Aura® MS VM appliance.

## Procedure

1. Log in to the VMware® host by using the vSphere Web Client.
2. In the vSphere Web Client navigator area on the left, click **vCenter**.
3. In **Inventory Trees**, click **Hosts and Clusters**.
4. Expand the inventory tree of hosts and clusters to locate and select the target deployment host.
5. From the menu, right-click the host and select **Deploy OVF Template**.
6. **(Optional)** If the **Client Integration Access Control** window pops up, click **Allow**.
7. For **1a Select source**, select **Local file**, and click **Browse**.
8. From the file filter drop-down menu in the lower right of the window, click **OVA Packages (\*.ova)**.
9. Select the required Avaya Aura® MS OVA file and click **Next**.
10. Confirm the properties of the OVA file that you selected on the **Review details** page and click **Next**.
11. To accept the End User License Agreement, click **Accept** and **Next**.
12. Enter a name for the new Avaya Aura® MS VM and click **Next**.
13. Select the required deployment configuration profile in the **Configuration** field and click **Next**.

See application documentation for the recommended system profile.

 **Important:**

The VM disk size is always 50 GB when using VMware® deployment tools. To manually extend the disk size above 50 GB, use standard VMware® procedures to edit the virtual hardware settings of a deployed VM.

14. Expand the tree under the vCenter server and select the required datacenter folder and click **Next**.
15. Select **Thick Provision Lazy Zeroed** for the virtual disk format.
16. Select the required destination datastore, and click **Next**.
17. Select the required destination network(s) and click **Next**.
18. Expand **Network Settings** and configure the network details for the new VM on the Customize template page.
19. Expand **System Time Settings** and configure the time settings.
20. If required, expand **IPv6 Address Settings** and configure the IPv6 network details.
21. If required, expand **Out of Band Management Settings** and configure the out of band network details.
22. Expand **Customer Login Settings** and configure the account settings.

 **Note:**

The customer account password is temporary. You must change the password at first login.

23. **(Optional)** To enable customer access to the root account, expand the **Advanced Settings** and enable the **Interactive Initial Boot** option. Click **Next**.

 **Note:**

Setting this option requires you to access the VM console to complete the initial configuration. You will be prompted for the root password in the console session.

24. On the Ready to complete page, verify the options. If the values are incorrect, click **Back** to make changes. Do not select the **Power on after deployment** option. If the values are correct, click **Finish**.
25. Wait for the system to complete deployment. The time that the system requires to complete the deployment depends on the speed of the network connection and server. The system displays the progress in **Recent Tasks > All**.

 **Tip:**

To alter the configuration settings later, run the `netSetup` command in a Linux® shell.

26. Click the refresh arrow () located to the left of your login ID at the top of the vSphere web client page.

The system updates the inventory list and displays the new VM.

27. Select the new VM in the inventory list of the vSphere web client window and click the **Summary** tab.

28. Select **Power On** from the **Actions** menu.

29. To open a console page on your VM, click **Launch Console** on the **Summary** tab.

A console window displays the progress of the VM system initializing. If the system prompts you to confirm or update the configuration due to input error, or after you selected **Interactive Initial Boot**, follow the prompts to complete the configuration.

30. When the VM initialization is complete, the system displays a login prompt. Log in using the customer account that you set up earlier. You must change the password after login.

### Next steps

Configure Avaya Aura® MS.

If this media server virtual appliance will be used as a Video Compositor, you must increase the system capacity. See [Resizing an Avaya Virtual Appliance for use as a Video Compositor](#) on page 53

---

## Deploying the OVA file by using VMware Host Client

### About this task

The steps in this procedure use the VMware Host Client, which runs in a web browser.

### Before you begin

- Obtain the Avaya Aura® MS OVA file. Save the file on the workstation where you will run VMware Host Client to configure the new VM.
- Obtain the following network configuration settings for the new VM. These settings can be from an existing system if you are redeploying Avaya Aura® MS OVA.

#### Important:

If you plan to enroll media servers with Avaya Aura® System Manager, then the media servers and System Manager must use the same NTP server for time synchronization.

- Hostname
- IPv4 address
- IPv4 Netmask
- Gateway IPv4 address
- Customer account login name
- Customer account password
- Time zone
- **(Optional)** Network domain
- **(Optional)** IPv4 address of the DNS servers

- IPv4 address or hostname of the NTP servers
  - **(Optional)** IPv6 address
  - **(Optional)** IPv6 prefix length
  - **(Optional)** IPv6 gateway address
  - **(Optional)** Out of band management IPv4 address
  - **(Optional)** Out of band management IPv4 netmask
  - **(Optional)** Out of band management IPv4 gateway address
  - **(Optional)** Root account password
- Ensure that you turn off the current Avaya Aura® MS VM appliance.

## Procedure

1. Log in to the VMware® host by using the following URL in the VMware Host Client: <https://esxiAddress/ui/#/login>.
2. In the VMware Host Client navigator area on the left, click **Virtual Machines**.
3. Above the list of virtual machines, select **Create / Register VM**.
4. For **1 Select creation type**, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
5. Enter a name for the new Avaya Aura® MS.
6. Click on **Click to select files for drag/drop**.
7. Select the required Avaya Aura® MS OVA file and click **Next**.
8. Select the required destination datastore and click **Next**.
9. To accept the End User License Agreement, click **I Agree** and **Next**.
10. Configure the network details for the new VM.
11. Select the required deployment configuration profile in the **Configuration** field. See application documentation for the recommended system profile.

### Important:

The VM disk size is always 50 GB when using VMware® deployment tools. To manually extend the disk size above 50 GB, use standard VMware® procedures to edit the virtual hardware settings of a deployed VM.

12. Select **Thick** for **Disk Provisioning**.
13. Ensure that **Power on automatically** is cleared and click **Next**.
14. Verify the options. If the values are incorrect, click **Back** to make changes. If the values are correct, click **Finish**.
15. Wait for the system to complete the deployment. The time that the system requires to complete the deployment depends on the speed of the network connection and the speed of the server.

The system displays the progress in **Recent Tasks**.

 **Tip:**

You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.

16. Click the refresh arrow located above the Virtual Machine list.

The system updates the inventory list and displays the new VM.

17. Select the new VM in the Virtual Machine list.

18. Select **Power on** at the top of the pane.

19. To open a console for your VM, click on the console image.

The console displays the progress of the VM initialization.

20. Read the End User License Agreement. Use the spacebar to scroll through the text. Type `yes` to accept the agreement and proceed.

21. After the VM system initialization is complete, you are prompted to configure the VM. Type `y` to proceed.

22. Enter the network settings, date, time, and customer account information for the server.

 **Tip:**

You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.

23. Choose whether to enable root access for the system. If enabled, accept the Root Access Acceptance Statement and enter the root password.

 **Important:**

You must not modify any operating system files. Avaya manages the operating system on appliances. Modifying system files can cause future system layer updates from Avaya to fail or result in loss of your changes.

24. When the VM initialization is complete, the system displays a login prompt. Log in using the customer account that you set up earlier. You must change the password after login.

## Next steps

Configure Avaya Aura® MS.

If this media server virtual appliance will be used as a Video Compositor, you must increase the system capacity. See [Resizing an Avaya Virtual Appliance for use as a Video Compositor](#) on page 53

---

## Adding the OVA file to Solution Deployment Manager software library

### About this task

Use this task to upload an Avaya Aura® Media Server (MS) OVA file when you are using Solution Deployment Manager (SDM) in System Manager to deploy the VM. Alternatively, you can use the SDM Client application, which you download and install on your Windows® computer.

You must transfer an Avaya Aura® Media Server (MS) OVA file to System Manager before you can deploy it using SDM. The OVA file must be added to a software library on the system. OVA files are staged on System Manager and then a library that you specify pulls the staged file in from the staging area. The OVA file is available for deployment after it is in a software library.

### \* Note:

You can deploy and delete an Avaya Aura® Media Server (MS) VM using SDM, but you cannot use SDM to update, patch, or manage Avaya Aura® Media Server (MS). Instead, manage Avaya Aura® Media Server (MS) using the update, backup, and restore procedures in this document.

### Procedure

1. Transfer the OVA file to System Manager by using the **sftp** file transfer tool, or another similar tool. The file must be stored in the `/swlibrary/staging/sync`.
2. Log in to the Avaya Aura® System Manager web console.
3. Navigate to **Services > Solution Deployment Manager > Software Library Management**.
4. Select the required software library.
5. Click **Manage Files**.
6. In the **Sync Files from directory** section, select the checkbox next to the name of the required OVA file.
7. Enter the checksum of the OVA file in the **MD5 Checksum** field.
8. In the **Software Library** field, select a local System Manager library.
9. In the **Product Family** field, select **Avaya Aura Media Server**.
10. In the **Device Type** field, select **OVA**.
11. In the **Software Type** field, select **OVA**.
12. Click **Sync**.  
Wait for the upload to complete.
13. (Optional) Perform the following steps to view the uploaded file in the software library:
  - a. Navigate to **Services > Software Library Management**.
  - b. Select the checkbox next to the name of the library containing the OVA.

- c. Click **Manage Files**.

The uploaded OVA file is listed in the **Software Library Files** section.

### Next steps

Deploy the OVA file using Solution Deployment Manager.

---

## Deploying the OVA file using Solution Deployment Manager

### About this task

Use this task to deploy Avaya Aura® Media Server (MS) virtual appliances on Avaya Solutions Platform (ASP) 130 systems using Solution Deployment Manager (SDM).

#### Important:

If you plan to enroll media servers with Avaya Aura® System Manager, then the media servers and System Manager must use the same NTP server for time synchronization.

### Before you begin

- If you are not able to use SDM in System Manager, then install Avaya SDM Client on your Windows® workstation.
- Upload the Avaya Aura® Media Server (MS) OVA file to an SDM software library or to your Windows® workstation if you are using Avaya SDM Client.
- Obtain the following network configuration settings for the new VM. These settings can be from an existing system if you are redeploying the Avaya Aura® Media Server (MS) OVA file.
  - Hostname
  - IPv4 address
  - IPv4 Netmask
  - Gateway IPv4 address
  - Customer account login name
  - Customer account password
  - Time zone
  - **(Optional)** Network domain
  - **(Optional)** IPv4 address of the DNS servers
  - **(Optional)** IPv4 address or hostname of the NTP servers
  - **(Optional)** IPv6 address
  - **(Optional)** IPv6 prefix length
  - **(Optional)** IPv6 gateway address

- **(Optional)** Out of band management IPv4 address
- **(Optional)** Out of band management IPv4 netmask
- **(Optional)** Out of band management IPv4 gateway address
- **(Optional)** Root account password
- Ensure that the required network interfaces are connected before deploying the OVA. The Avaya Solutions Platform (ASP) 130 and Utility Services IP addresses are available on NIC 1. Media server network interfaces are selected at the time of deployment and use a free network interface controller starting with NIC 4.

## Procedure

1. To gain access to the SDM Dashboard, log in to System Manager and navigate to **Services > Solution Deployment Manager** or launch the Avaya SDM Client on your Windows® computer.
2. Click **VM Management**.
3. Navigate the **Application Management Tree** and click on the name of the target host.
4. On the **Applications** tab, click **New**.  
The system displays the Application Deployment window.
5. In the **Select Location and Platform** section, select the target data store from the **Data Store** drop-down menu.
6. Click **Next**.
7. In the **OVA** section
  - a. Select one of the following:
    - **URL**, in OVA File, type the absolute path to the application OVA file, and click **Submit**.
    - **S/W Library**, in File Name, select the application OVA file.
    - **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.
  - b. Select the required deployment configuration profile in the **Flexi Footprint** field.
  - c. Click **Next**.
8. On the **Configuration Parameters** tab, type a name for the new VM in the **VM Name** field.
9. In the **Network Settings** section on the **Configuration Parameters** tab, enter the required network settings, as follows:
  - a. Enter an IP address for the media server in the **Media Server IP address** field.
  - b. Enter a hostname for the VM in the **Short Hostname** field.
  - c. **(Optional)** Enter the **Network Domain**.
  - d. Enter the **Media Server Netmask** and **Default Gateway**.

- e. **(Optional)** Enter the **DNS Servers** as required for your network.
10. In the **System Time Settings** section on the **Configuration Parameters** tab, enter the optional time settings.
11. In the **Customer Login Settings** section on the **Configuration Parameters** tab, enter a **Login Name** and initial **Login Password** for your customer account.
12. **(Optional)** In the **IPv6 Address Settings** section on the **Configuration Parameters** tab, select **Autoconfigure IPv6** or enter the **Media Server IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Gateway Address** as required for your network.
13. **(Optional)** In the **Out of Band Management Settings** section on the **Configuration Parameters** tab, enter the **Out of Band Management IPv4 Address**, **Out of Band Interface Netmask**, and the **Out of Band Interface Default Gateway** as required for your network.  
  
After the server completes first boot, access Element Manager to update the IP interface assignment to ensure OAM is set to the IP address assigned to the out-of-band management interface.
14. For 8.0.2 and later, in the **Advanced Settings** section on the **Configuration Parameters** tab, leave the Interactive Initial Boot option disabled.
15. **(Optional)** For 8.0.2 and higher, in the **Customer Root Account** section on the **Configuration Parameters** tab, **Enable Customer Root Account** for this application if required. Accept the Root Access Acceptance Statement and enter the **Customer Root Password**.
16. Click **Deploy**.  
  
The system displays the end user license agreement.
17. Read the license agreement and click **Accept**.
18. To monitor the status of the deployment, click on the **Virtual Machines** tab.
19. **(Optional)** To monitor individual steps of the deployment process, click on **Status Details** in the **Current Action Status** column for the VM you are deploying.
20. Open the VM console and confirm that the login prompt is presented to confirm that the deployment completed successfully.
21. Log in to a Linux® shell by using the customer account to change the initial, temporary password.

## Next steps

Configure Avaya Aura® Media Server (MS).

If this media server virtual appliance will be used as a Video Compositor, you must increase the system capacity. See [Resizing an Avaya Virtual Appliance for use as a Video Compositor](#) on page 53.

# Chapter 4: Deploying in the KVM on Red Hat® virtualized environment for ASP 130 Release 6.0 or higher

## System requirements

The Avaya Aura® MS appliance is deployed using a Linux command line shell.

The KVM on Red Hat® hypervisor host (ASP 130 R6 or higher) must meet the following system requirements:

| KVM on Red Hat® host resource | Requirement                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat® version              | 8.10                                                                                                                                                                                                                                                       |
| CPU                           | The core processor speed must be at least 2.2 GHz.<br>For all VM deployed on a host with an Avaya Aura® MS, the total number of vCPUs must not exceed the number of logical CPUs.<br>Only 4,8, and 16 vCPU instances are supported.                        |
| Memory                        | Memory is allocated based on the number of vCPUs. <ul style="list-style-type: none"><li>• 4 vCPUs require 4608 MB of memory.</li><li>• 8 vCPUs require 8192 MB of memory.</li><li>• 16 vCPUs require 16384 MB of memory.</li></ul>                         |
| Disk space                    | Instances require 50 GB of KVM datastore. A one-time increase of 200 GB is allowed either at VM creation or post VM creation.                                                                                                                              |
| Network bandwidth             | A dedicated pair of 1 Gbps network interfaces must be available in a bonded, active-backup configuration. Alternatively, 1 Gbps of dedicated bandwidth on a pair of 10 Gbps network interfaces must be available in a bonded, active-backup configuration. |
| IOPS                          | The system must support 100 Input/Output Operations per Second (IOPS).                                                                                                                                                                                     |

The following requirements are also mandatory:

- It is mandatory to ensure the KVM on Red Hat® host is not oversubscribed. Logical cores on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with the media server. For example, the total number of vCPUs across all VMs on a

KVM host that has 24 logical cores (12 physical cores with hyper-threading enabled), must not exceed 24.

**\* Note:**

This recommendation prevents CPU oversubscription.

- For maximum system performance, ensure that:
  1. Energy saving features are disabled.
  2. Maximum performance settings are enabled in the server BIOS.
- KVM on Red Hat® feature support is detailed in the following table:

| KVM on Red Hat® Feature     | Avaya Aura® Media Server Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHEL Versions               | Supported Versions: 8.10                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Clone Virtual Machine       | Supported.<br>VMs must be shut down before copying.<br>Note that cloning shouldn't be used to create additional AAMS server instances. This will result in software failures since multiple AAMS servers are assigned to the same UUID.                                                                                                                                                                                                                                                         |
| Large Receive Offload (LRO) | Supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Resize Virtual Machine      | Not supported when the VM is powered on.<br>Supported when the VMs are shut down. A one time resizing to add 200 GB is allowed (max 250GB)                                                                                                                                                                                                                                                                                                                                                      |
| Live Storage Migration      | Not supported.<br>To migrate to a different storage system, you must first shut down the VM. For 1+1 HA Clusters, both VMs must be shut down.                                                                                                                                                                                                                                                                                                                                                   |
| Live Migration              | Not supported.<br>To migrate to a different physical host, you must first shut down the VM. For 1+1 HA Clusters, both VMs must be shut down.                                                                                                                                                                                                                                                                                                                                                    |
| KVM Snapshots (CLI only)    | Not supported on production servers outside of maintenance windows.<br>Supported for temporary use when applying feature packs, service packs, or patches during maintenance windows.<br>The VM must be shut down before creating, deleting, or reverting a snapshot. For 1+1 HA clusters, both VMs must be shut down for any snapshot operation on either server.<br>Snapshots adversely impact the VM disk and CPU performance and must be removed before returning the server to production. |
| KVM High Availability (HA)  | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Fault Tolerance (FT)        | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

*Table continues...*

| KVM on Red Hat® Feature         | Avaya Aura® Media Server Support                                                                                                                                                                                                                |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KVM Overcommitting of Resources | The KVM hypervisor automatically overcommits CPUs and memory. This means that more virtualized CPUs and memory can be allocated to virtual machines than there are logical resources on the system (see Best Practices Recommendation section). |
| Power Management                | Not supported.                                                                                                                                                                                                                                  |
| KVM Secure Boot                 | Not supported prior to 10.2.0 SP1.                                                                                                                                                                                                              |

## 1+1 High Availability cluster requirements

The 1+1 High Availability cluster configuration ensures uninterrupted availability of media processing in cases where a media server fails. Use the High Availability configuration option when you require the capacity of only a single Avaya Aura® MS.

The High Availability configuration deploys as a Primary server and a Backup server. Only one server is active at a time. The other server is waiting in synchronized hot standby to take over instantly.

Both servers must have identical configuration so that either server can take over the full media processing load if the other server fails. Ensure that the deployed servers meet the following requirements:

- Each media server in a 1+1 High Availability cluster deployed as a virtual machine must be deployed on separate but equally capable host servers with the same hardware and processor model. The VMs must be deployed using the same configuration profile so that they have the same number of vCPUs.
- There is no inter-cluster communication between different 1+1 High Availability clusters. Different 1+1 High Availability clusters can use different hardware or profiles, but the specifications within a cluster must match.

## Best practice recommendations

Use the following best practices to deploy the Avaya Aura® MS appliance in the KVM on Red Hat® virtualized environment:

- High Availability (HA) Media Server VMs should be deployed on separate equally capable server hosts.
- All physical servers that can host a VM must have the same CPU, memory, and networking specifications.
- Logical cores on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with the media server. For example, the total number of vCPUs across all VMs on a KVM host that has 24 logical cores (12 physical cores with hyper-threading enabled), must not exceed 24.

**\* Note:**

This recommendation prevents CPU oversubscription.

It is mandatory to ensure the KVM on Red Hat® host is not oversubscribed (Logical Cores <= vCPU for all VM's deployed to that host).

- For maximum system performance, ensure that the energy savings features are disabled or that the maximum performance settings are enabled in the server BIOS.
- Old media server backup files must be removed to maintain free space on the system.

---

## Obtaining Avaya Aura® MS KVM Installer

### About this task

You can download Avaya Aura® MS KVM on Red Hat® installer from the Avaya Product Licensing and Delivery System (Avaya PLDS) at <https://plds.avaya.com>.

### Next steps

Deploy the Avaya Aura® MS appliance using a Linux® command line shell.

---

## Deploying the Avaya Aura® MS KVM installer

### About this task

The steps in this procedure use a Linux® command line shell to create an Avaya Aura® MS appliance. The Avaya Aura® MS KVM appliance installer combines the QCOW2 image plus an installer script that automates the installation.

### Before you begin

- Obtain the Avaya Aura® MS KVM Installer. Save the installer on the KVM on Red Hat® hypervisor.
- Obtain the following network configuration settings for the new VM. These settings can be from an existing system if you are redeploying Avaya Aura® MS KVM image.

### ! Important:

If you plan to enroll media servers with Avaya Aura® System Manager, then the media servers and System Manager must use the same NTP server for time synchronization.

- Hostname
- IPv4 address
- IPv4 Netmask
- Gateway IPv4 address

- Customer account login name
- Customer account password
- Time zone
- Network domain (optional)
- IPv4 address of the DNS servers (optional)
- IPv4 address or hostname of the NTP servers
- IPv6 address (optional)
- IPv6 prefix length (optional)
- IPv6 gateway address (optional)
- Out of band management IPv4 address (optional)
- Out of band management IPv4 netmask (optional)
- Out of band management IPv4 gateway address (optional)
- Root account password (optional)

## Procedure

1. Log in to the KVM on Red Hat® hypervisor host in a Linux® shell as the root user.
2. Navigate to the directory of the Avaya Aura® MS KVM Installer.
3. Type the following command to change the installer file mode:

```
[root@host ~]$ chmod u+x [Avaya-Aura-KVM-Installer]
```

4. Deploy the Avaya Aura® MS VM appliance by running the KVM installer and follow the queries. Note that if the partition holding the Avaya Aura® MS KVM installer is mounted with the **noexec** option (like the `/var/lib/libvirt` directory), directly running the installer will display an **Permission denied** error. In this case, run the installer using the **bash** command like this:

```
[root@host]# bash ./MediaServer_10.2.0.61_A3_2025.01.14_KVM.bin --name AAMS_VM --size 8
```

For example, to deploy an 8 vCPU VM would be as follows:

```
[root@host]# chmod u+x ./ MediaServer_10.2.0.61_A3_2025.01.14_KVM.bin

[root@host]# bash ./MediaServer_10.2.0.61_A3_2025.01.14_KVM.bin --name AAMS_VM --size 8

Destination is not specified. Do you want to use the defaults?
/var/lib/libvirt/images/AAMS_VM.qcow2

Answer y or n [n]: y
Copying disk image to: /var/lib/libvirt/images/AAMS_VM.qcow2
Continue?
Answer y or n [n]: y
Copy successful
Changing ownership of /var/lib/libvirt/images/AAMS_VM.qcow2 to qemu:qemu...
Change of ownership successful.

Deploying VM AAMS_VM with 8 vCPUs and 8192 KB memory using disk /var/lib/libvirt/images/AAMS_VM.qcow2.
Continue?
```

```

Answer y or n [n]: y
Starting install...
Domain creation completed.
You can restart your domain by running:
virsh --connect qemu:///system start AAMS_VM

```

 **Tip:**

For help on using the command, use the command:

```
[root@host ~]$ ./[Avaya-Aura-KVM-Installer] --help.
```

5. To configure the VM settings, log in to the KVM on Red Hat® host by using the following URL:  
<https://<KVM-on-RedHat-host-address>:9090/system>
6. Select **Virtual Machines** in the left menu.
7. Identify the newly created VM and select the **Run** button for that VM.
8. Select the VM by clicking on the name of the VM.
9. In the new window will be the console for the VM. You must click on **Expand** to view the console properly.
10. Read the End User License Agreement. Use the spacebar to scroll through the text. Type 'a' to accept the agreement and proceed.
11. You are now prompted to configure the VM. Type **y** to proceed.
12. Enter the network settings, date, time, and customer account information for the server.

 **Tip:**

You can alter the configuration settings later by running the **netSetup** command in a Linux® shell.

13. Choose whether to enable root access for the system. If enabled, accept the Root Access Acceptance Statement and enter the root password.

 **Important:**

Do not modify any operating system files. Avaya manages the operating system on appliances. Modifying system files can cause future system layer updates from Avaya to fail or result in loss of your changes.

14. When the VM initialization is complete, the system displays a login prompt. Log in using the customer account that you set up earlier. You must change the password after login.

## Next steps

Configure Avaya Aura® MS appliance.

---

## Upgrading ASP 130 R6.0 or higher without upgrading the AAMS software

### About this task

Use this task to upgrade ASP 130 R5 or earlier (VMWare® hypervisor) to ASP 130 R6.0 or higher (KVM on Red Hat® hypervisor) without upgrading the AAMS 10.x software. For more information, refer to *ASP 130 KVM on Red Hat® document* and *Installing Avaya Solutions Platform 130 Series R6.0*.

#### ! Important:

If you are also upgrading AAMS software (8.0.x/10.x to 10.y) then refer to the section ASP 130 R6.0 or higher migration and upgrading the AAMS software.

#### \* Note:

You can deploy the new server with the same or different IP.

### Procedure

1. Log in to the **Element Manager** console of the Avaya Aura® MS appliance running on the VMware host.
2. Perform the backup and copy the backup files from server. For more information on how to perform a backup of the Avaya Aura® MS appliance, see the “Backup and Restore” chapter in this document.
3. Power off the Avaya Aura® MS appliance.
4. Deploy the new Avaya Aura® MS appliance on the KVM for Red Hat® host and configure the first-boot settings as per the settings of the backed-up Avaya Aura® MS appliance.
5. Log in to the **Element Manager** console of the Avaya Aura® MS appliance running on the KVM for Red Hat® host.
6. Restore the back-up files on to the Avaya Aura® MS appliance. For more information on how to perform a restore the backup files of the Avaya Aura® MS appliance, see the “Backup and Restore” chapter in this document.

#### \* Note:

If a different IP is used on the newly deployed KVM server, log in to the **Element Manager** console and navigate to **System Configuration > Network Settings > IP Interface Assignment** to configure the IP Interfaces.

7. Reboot the Avaya Aura® MS appliance.

### Next steps

Configure Avaya Aura® MS appliance.

# Upgrading to ASP 130 R6.0 or higher migration and upgrading the AAMS software

## About this task

Use this task to migrate a Virtual Machine running on a VMWare® hypervisor to a KVM on Red Hat® hypervisor. For more information on migrating, see *Installing Avaya Solutions Platform 130 Series R6.0*.

### \* Note:

You can deploy the new server with the same or different IP.

## Procedure

1. Log in to the Element Manager console of the Avaya Aura® MS appliance running on the VMWare host.
2. Copy the backed-up files off the server.  
For more information on how to perform a backup of the Avaya Aura® MS appliance, see the “Backup and Restore” chapter in this document.
3. Power off the Avaya Aura® MS appliance.
4. Deploy the new Avaya Aura® MS appliance on the KVM for Red Hat® host and configure the first-boot settings as per the settings of the backed-up Avaya Aura® MS appliance.
5. Log in to the Element Manager console of the Avaya Aura® MS appliance running on the KVM for Red Hat® host.
6. Use the upgrade tool to upgrade the system configuration data by entering the following on the command-line:

```
amsupgrade SystemConfigBackupFilename.zip
```

### ! Important:

Restore the system configuration data before restoring the application data to ensure that the application data is restored to the configured location.

### ! Important:

Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same installation path, IP address, and hostname so that the data is compatible with the server configuration.

7. Press **Y** to stop all Avaya Aura® MS services when prompted. The tool upgrades the data.
8. Use the upgrade tool to upgrade the application content data by entering the following on the command-line:

```
amsupgrade AppContentBackupFilename.zip
```

9. Press **Y** to stop all Avaya Aura® MS services when prompted.

The tool upgrades the data.

 **Note:**

The time required to complete the application content upgrade depends on the amount of application data in the backup file.

10. NOTE: If a different IP is used on the newly deployed KVM server, log in to the Element Manager console and navigate to **System Configuration > Network Settings > IP Interface Assignment** to configure the IP Interfaces.
11. Reboot the Avaya Aura® MS appliance.

### Next steps

Configure Avaya Aura® MS appliance.

# Chapter 5: Deploying Avaya Solutions

## Platform physical appliances

---

### System requirements

Avaya Aura® MS physical appliances shipped with the appliance software already installed on Avaya Common Server platforms. The appliances are ready for customer network configuration when deployed. The following appliances are available:

| Material ID | Avaya Common Server Description           |
|-------------|-------------------------------------------|
| 700514272   | ASP 110 DELL SERVER P5 AAMS (Dell R640XL) |
| 700519840   | ASP 110 DELL R660xs SERVER A3 AAMS        |

The required BIOS settings are configured by Avaya prior to delivery.

Two network interfaces are required to support Linux® channel bonding for high availability. Network cables must be plugged in to both active network interface ports.

Optionally, for servers with four or more network interfaces, a second bonded pair can be configured to support out of band management.

Use the diagrams in the following sections to identify the active network interface ports on each server.

For more information about ASP 100 Maintenance and Troubleshooting, refer to [Maintaining and Troubleshooting Avaya Solutions Platform 130 Series](#).

### ASP 110 (Dell R660XS) active network ports

Plug network cables into the SFP28/SFP+ ports (using the appropriate cable and module for your network) labeled as 1 and 2 in the diagram. If out of band management is to be enabled, the first two built-in ports (3 and 4 in the diagram) at the bottom can be connected.

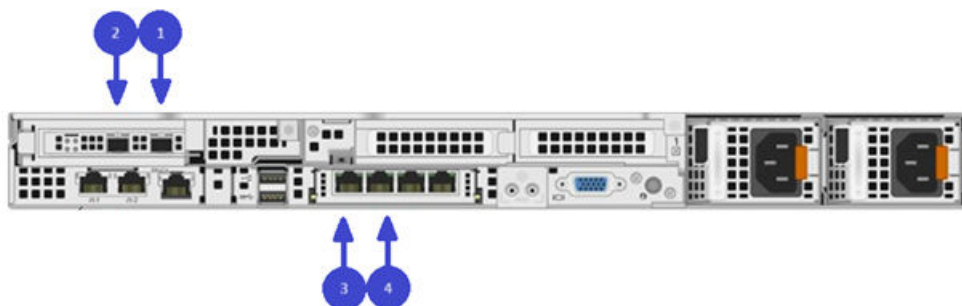
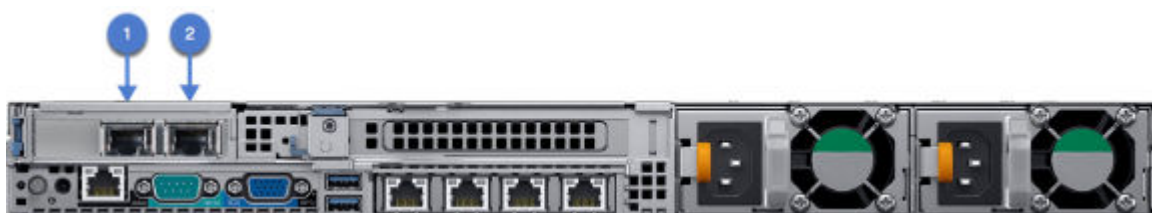


**Figure 1: Active Network Ports for ASP 110 (Dell R660XS)**

## ASP 110 (Dell R640XL) active network ports

Plug Ethernet cables into the Ethernet ports labeled as 1 and 2 in the diagram. The corresponding ports on the R640XL chassis are labeled as 0 and 1 in the top row of Ethernet ports. If out of band management is to be enabled, the first two built-in ports (1 and 2) at the bottom can be connected. The top row of ports is read from left to right, and is labeled 0 through 1. The bottom row of ports is read from left to right, and is labeled 1 through 4.



## 1+1 High Availability cluster requirements

The 1+1 High Availability cluster configuration ensures uninterrupted availability of media processing in cases where a media server fails. Use the High Availability configuration option when you require the capacity of only a single Avaya Aura® MS.

The High Availability configuration deploys as a Primary server and a Backup server. Only one server is active at a time. The other server is waiting in synchronized hot standby to take over instantly.

Both servers must have identical configuration so that either server can take over the full media processing load if the other server fails. Ensure that the deployed servers meet the following requirements:

- Each media server in a 1+1 High Availability cluster deployed as an Avaya physical appliance must be deployed on similar hardware with the same processor model. The servers can be from a different manufacturer, but the two systems must have the same clock rate, number of cores, bus speed, and other performance-critical specifications.

- There is no inter-cluster communication between different 1+1 High Availability clusters. Different 1+1 High Availability clusters can use different hardware or profiles, but the specifications within a cluster must match.

---

## Deploying the Avaya Aura® MS physical appliance

### About this task

New Avaya Aura® MS appliances are shipped with the appliance software already installed and are ready to be deployed in the customer network.

The system automatically enters the customer configuration procedure when it starts for the first time after deployment.

Perform the following procedure to configure the Avaya Aura® MS appliance at the customer site.

### Important:

If you plan to enroll media servers with Avaya Aura® System Manager, then the media servers and System Manager must use the same NTP server for time synchronization.

### Before you begin

Obtain the following network and server information:

- Hostname
- IPv4 address
- IPv4 Netmask
- Gateway IPv4 address
- Customer account login name
- Customer account password
- Time zone
- Network domain (optional)
- IPv4/FQDN of the DNS servers (optional)
- IPv4 address or hostname of the NTP servers
- IPv6 address (optional)
- IPv6 prefix length (optional)
- IPv6 gateway address (optional)
- Out of band management IPv4 address (optional)
- Out of band management IPv4 netmask (optional)
- Out of band management IPv4 gateway address (optional)
- Root account password (optional)

## Procedure

1. Install one of the supported Avaya Common Server hardware platforms and plug in the network and power cables.
2. Turn on the Avaya Aura® MS appliance server.
3. Press `Y`, and then press `Enter` to start the configuration procedure.

The system displays the instructions to configure the system time.

### **Note:**

If `N` is provided as the response, then the server is automatically turned off. Configuration takes place the next time that the server is turned on.

4. Press `Enter` to continue.
5. When prompted, enter the network parameters, date, time, and customer account information for the server.

### **Tip:**

You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.

6. Verify the network configuration values in the response summary.

If required, press `U` to update a value before proceeding.

7. Press `C` and then press `Enter` to continue.

The system applies the network configuration and displays a prompt to configure the customer login ID.

8. Enter a login ID to use for the customer account and press `Enter`.

9. Press `C` and then press `Enter` to continue.

The system displays the set password prompt.

10. Enter a password for the login ID to use for the customer account and press `Enter`.

11. Type the password again to confirm and press `Enter`.

12. Choose whether to enable root access for the system. If enabled, accept the Root Access Acceptance Statement and enter the root password.

The server configuration is complete. After several seconds, system initialization is complete and the system displays the login prompt.

### **Important:**

You must not modify any operating system files. Avaya manages the operating system on appliances. Modifying system files can cause future system layer updates from Avaya to fail or result in loss of your changes.

13. Log in using the customer account that you set up earlier. You must change the password after login.

---

## Obtaining physical appliance recovery software

New Avaya Aura® MS appliances are shipped with the appliance software already installed. Avaya Aura® MS appliance software is only required to support the field replacement procedure, for example, disk replacement.

You can download an ISO image of the Avaya Aura® MS recovery software from the Avaya Product Licensing and Delivery System (Avaya PLDS) website at <https://plds.avaya.com>.

### Next Steps:

Reinstall the Avaya Aura® MS physical appliance.

---

## Updating the Avaya Aura® MS physical appliance Boot Mode to UEFI

### About this task

New Avaya Aura® MS appliances are shipped with the appliance software installed and the Boot Mode set appropriately. When reinstalling an Avaya Aura® MS appliance software version newer than 10.1.0 SP2 onto a server that previously used an earlier version, the **Boot Mode** must be set **UEFI**.

### ! Important:

Changing the **Boot Mode** to **UEFI** will prevent the previously installed system from booting. A reinstall must be done after this procedure to use the appliance.

Perform the following procedure to configure the **Boot Mode** in preparation for reinstallation of the Avaya Aura® MS appliance.

### Before you begin

The power to the server must be On to boot the system.

### Procedure

1. Restart the server using one of the following methods:
  - Press **Control+Alt+Delete** and select **Restart**.
  - Type `reboot` in a Linux® shell.
  - Press the power button to switch Off the server and press the power button again to switch it On.

- Press the reset button until the server restarts.
2. To enter **System Setup** menu, press **F2** during boot.
  3. Navigate to **System Bios > Boot Settings**.

 **Note:**

If the **Boot Mode** is already set to **UEFI**, no further changes are required.

4. Set **Boot Mode** to **UEFI**.
5. Select **Back**, **Finish**, and **Yes** to save the changes. Select **OK** to confirm the changes.
6. Select **Finish** and **Yes** to confirm the changes.  
The system will reboot.
7. press **F2** during boot to enter **System Setup** menu.
8. Navigate to **System Bios > Boot Settings > UEFI Boot Settings**.
9. Under **Boot Option Enable/Disable**, ensure that **PXE Device 1: Integrated NIC 1 Port 1 Partition 1** is not selected.
10. Select **Back**.
11. Select **Back**.
12. Select **Finish** and **Yes** to save the changes. Select **OK** to confirm the changes.

 **Tip:**

Insert the new installation DVD before completing the final confirmation.

 **Tip:**

If updating to version 10.2.0 SP1 or newer, enable secure boot before exiting.

13. Select **Finish** and **Yes** to complete all the changes.

The system will reboot.

### Next steps

Reinstall the Avaya Aura® MS physical appliance.

---

## Reinstalling the Avaya Aura® MS physical appliance running on Dell R660XS hardware (no DVD drive)

### About this task

New Avaya Aura® MS appliances are shipped with the appliance software already installed. The Avaya Aura® MS appliance software is reinstalled only to support field replacement procedures, For example, disk replacement.

**! Important:**

All data is lost when you reinstall Avaya Aura® MS appliance.

Perform the following procedure to format the system disk and reinstall Avaya Aura® MS appliance.

**Before you begin**

- Obtain the Avaya Aura® MS physical appliance software installation ISO. The install ISO must be version 10.2.0.52\_A2 or later.
- Write the ISO to a USB drive of at least 8GB in size. A tool such as Rufus or the Linux command `dd` can be used.
- Ensure the server is powered off.

**Procedure**

1. Connect the bootable USB drive into one of the USB ports on the server.

**\* Note:**

If a USB 3.0 device is used, it must be plugged into the lower USB port on the back of the server (port 2 in the diagram), as that is the only USB 3.0 compliant port.

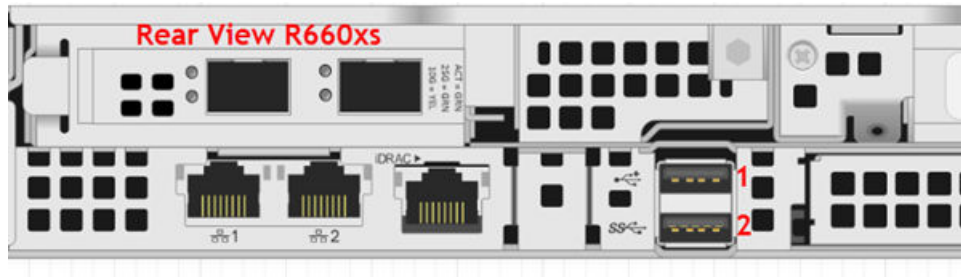


**Figure 2: Rear view of R660XS**

2. Power on the server.
3. While the server is booting, press the **F11** key when prompted to enter the **Boot Manager**.

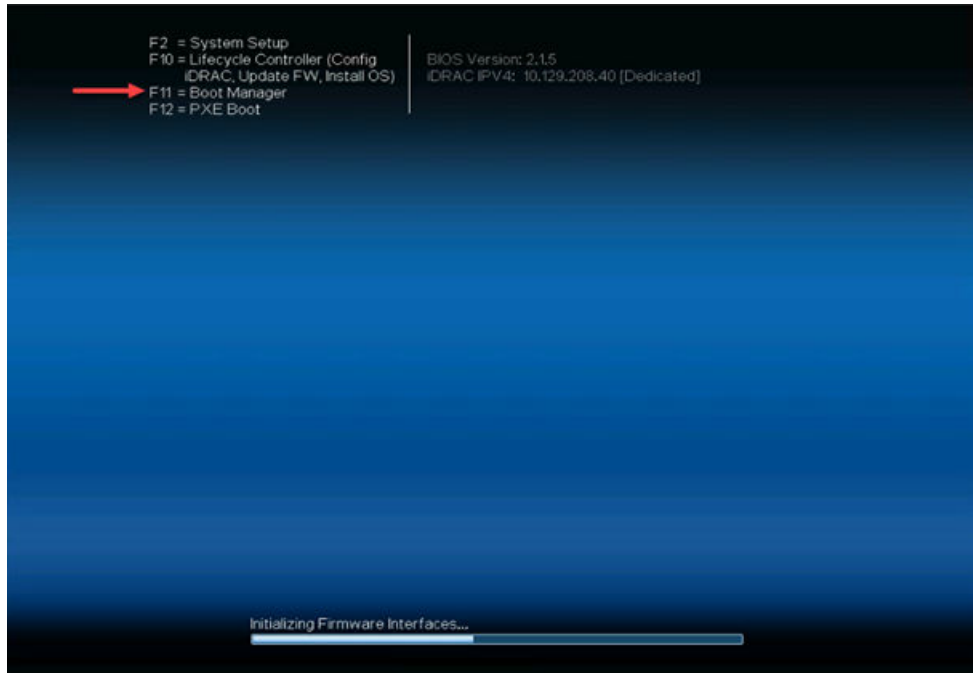


**Figure 3: Boot Manager**

4. Use the arrow keys on the keyboard to navigate the **Boot Manger** menu. Select the **One-shot UEFI Boot Menu** and press **Enter**. Then select the USB device containing the install image and press **Enter**. The name of the menu item will depend on which port is used, and the type of the USB device. For example, it may say **Disk connected to back USB 2: <Name of USB device>**.

The system will now boot from the installation device. After several minutes, the system displays the Avaya Aura® Media Server Welcome screen.

**+ Tip:**

The Welcome screen displays the appliance build number, a list of detected network interfaces, and a list of attached storage devices with their sizes. Review this information for accuracy to verify whether these characteristics are as expected.

5. Press **Y** to proceed with the installation.

The system installs the operating system, and automatically reboots. The system proceeds with the installation of the Avaya Aura® Media Server after the reboot. After several minutes, the system displays the installation result.

**\* Note:**

When you type **N** in response to the confirmation prompt, then the installation is cancelled, and the server is automatically turned off. The installation can be restarted later.

6. Press **Enter** to turn off the server.

The system turns off and is ready to be configured the next time that the server is turned on. The USB installation device can now be removed.

 **Note:**

The next time the server is turned on, the system confirms that a configuration must be performed. If **n** is provided as the response, then the server is immediately turned off. This procedure is useful for verifying that the system successfully starts after it is reinstalled. Use the **y** response only when the system is ready to be configured.

### Next steps

Deploy the Avaya Aura® Media Server physical appliance.

---

## Reinstalling the Avaya Aura® MS physical appliance running on Dell R640 XL hardware

### About this task

New Avaya Aura® MS appliances are shipped with the appliance software installed. The Avaya Aura® MS appliance software is reinstalled only to support field replacement procedures, for example, disk replacement.

 **Important:**

All data is lost when you reinstall Avaya Aura® MS appliance.

Perform the following procedure to format the system disk and reinstall Avaya Aura® MS appliance.

### Before you begin

- Obtain the Avaya Aura® MS physical appliance software installation DVD.
- The power to the server must be On to open the disc tray.
- To reinstall using 10.1.0 SP2 or later, ensure that the system BIOS Boot Mode is set to UEFI.

### Procedure

1. Open the system disc tray, insert the Avaya Aura® MS appliance installation disc, and close the disc tray.
2. Restart the server by using one of the following methods:
  - Press `Control+Alt+Delete` on your keyboard, and select **Restart**.
  - Type `reboot` in a Linux® shell.
  - Press the power button to turn the server off and then press the power button again to turn it back on.
  - Press the reset button until the server restarts.

The system restarts from the installation disc. After several minutes, the system displays the Avaya Aura® Media Server welcome screen.

**+ Tip:**

The welcome screen displays the appliance build number, a list of detected network interfaces, and a list of attached storage devices with their sizes. Review this information for accuracy to verify whether these characteristics are as expected.

3. Press `Y` to proceed with the installation.

The system installs the operating system, ejects the disc tray, and automatically reboots. The system automatically installs Avaya Aura® MS after the reboot. After several minutes, the system displays the installation result.

**\* Note:**

When you type `N` in response to the confirmation prompt, then the installation is cancelled and the server is automatically turned off. The installation can be restarted later.

4. Press `Enter` to turn off the server.

The system turns off and is ready to be configured the next time that the server is turned on.

**\* Note:**

The next time the server is turned on, the system confirms that a configuration must be performed. If `N` is provided as the response, then the server is immediately turned off. This procedure is useful for verifying that the system successfully starts. Use the `Y` response only when the system is ready to be configured.

## Next steps

Deploy the Avaya Aura® MS physical appliance.

# Chapter 6: Signing in to the Avaya Aura<sup>®</sup> MS appliance

---

## Element Manager

Element Manager (EM) is a web-based administration tool that facilitates the operation, administration, and maintenance (OAM) of Avaya Aura<sup>®</sup> MS.

For more information and detailed procedures about using Avaya Aura<sup>®</sup> MS EM and configuring your browser to use Avaya Aura<sup>®</sup> MS EM, see *Implementing and Administering Avaya Aura<sup>®</sup> Media Server*.

---

## Accessing Avaya Aura<sup>®</sup> MS EM

### About this task

Use this procedure to gain access to EM on the Avaya Aura<sup>®</sup> MS appliance. You need EM to perform some procedures mentioned in this document.

### Procedure

1. In a web browser, type the following URL:

`https://serverIP:8443/em`

where, *serverIP* is the address of Avaya Aura<sup>®</sup> MS. For example,

`https://10.60.86.209:8443/em`

2. Sign in to Avaya Aura<sup>®</sup> MS EM by using the username `admin` and specify the password `Admin123$`. After initial login you will be prompted to change the admin password.

---

## Accessing Linux<sup>®</sup> shells

You must gain access to Linux<sup>®</sup> shells to perform some of the procedures in this document. Use Secure Shell (SSH) to access the Linux<sup>®</sup> command-line on the Avaya Aura<sup>®</sup> MS appliance. Use

the customer account or support account credentials for SSH log in. The customer account is created during customer server configuration of the Avaya Aura® MS appliance.

The Linux® shell is also accessible through the console. For VMware ESXi hosted virtual appliances, the console is accessed using the VMware management tools: vSphere client, vCenter Web client, or ESXi host web client. See VMware documentation for console access details. For physical appliances, the console is accessed by connecting a monitor and keyboard directly to the physical server.

The system supports a maximum of five simultaneous logins for each user account. The system rejects additional SSH and Putty sessions when five sessions are already logged in.

 **Note:**

To protect the system, the customer account does not have root privileges by default. Avaya has added some root privileges to the customer account using Linux® sudoer aliases. Root privileges are available if you enabled them at the time of deployment.

---

## Changing users in the Linux® shell

Once logged in to the command-line, it is sometimes required to change to a different account. The standard Linux utility 'su' is used to transition from one account to another. For example, to change to the root account:

```
su - root
```

When SELinux is disabled, you will be prompted for the target account's credentials.

When SELinux is enabled, you will first be prompted for the current account's credentials, followed by the target account credentials. The credentials prompted for could be either the account's password, or the EASG credentials for EASG-enabled accounts.

---

## Avaya support access

### About this task

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® MS remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Procedures are provided to manage EASG:

1. Determine the status of EASG
2. Enable or disable EASG

3. Display product EASG certificate information
4. Loading and managing site certificates

**Related links**

[Determining the status of EASG](#) on page 47

[Enabling or disabling EASG](#) on page 47

[Displaying product EASG certificate information](#) on page 48

[Loading and managing site certificate](#) on page 49

## Determining the status of EASG

**About this task**

Use this procedure to determine if the of EASG is enabled or disabled.

**Before you begin**

Register the Media Server with Avaya Global Registration tool (GRT) to provide remote connectivity.

**Procedure**

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

The customer account is created during the deployment procedure.

2. Type the following command to Enable EASG:

```
[cust@host ~]$ EASGStatus  
EASG is enabled
```

**Related links**

[Avaya support access](#) on page 46

## Enabling or disabling EASG

**About this task**

You can use `EASGManage` to enable EASG which grants Avaya support access to the `craft` and `sroot` system accounts. EASG remains enabled until you disable it. You can use `EASGManage` to disable EASG and remove Avaya support access to the `craft` and `sroot` system accounts. EASG remains disabled until you enable it.

**Before you begin**

Register the Media Server with Avaya Global Registration Tool (GRT) to provide remote connectivity.

**Procedure**

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

The customer account is created during the deployment procedure.

2. Type the following command to enable EASG:

```
[cust@host ~]$ 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: 'cust', on Oct 18 2016 - 14:02

3. To disable EASG type the following command:

```
[cust@host ~]$ EASGManage --disableEASG
```

By disabling Avaya Services Logins you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.

Do you want to continue [yes/no]? yes

EASG Access is disabled. Performed by user ID: 'cust', on Oct 18 2016 - 14:01

## Related links

[Avaya support access](#) on page 46

## Displaying product EASG certificate information

### About this task

You can use the `EASGProductCert` tool to display information about the product certificate, which includes information about when the certificate expires.

### Before you begin

Register the Media Server with Avaya Global Registration Tool (GRT) to provide remote connectivity.

### Procedure

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

The customer account is created during the deployment procedure.

2. Type the following command to enable EASG:

```
[cust@host ~]$ EASGProductCert --certInfo
```

Subject: CN=Avaya Aura Media Server 10.2, OU=EASG, O=Avaya LLC

Serial Number: 30066

Expiration: Sep 17 04:00:00 2036 GMT

Trust Chain:

1. O=Avaya, OU=IT, CN=AvayaITrootCA2

2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2

3. O=Avaya LLC, OU=EASG, CN=EASG Intermediate CA

4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya LLC

5. CN=Avaya Aura Media Server 10.2, OU=EASG, O=Avaya LLC

**Related links**

[Avaya support access](#) on page 46

**Loading and managing site certificate****About this task**

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

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

**Before you begin**

Obtain the site certificate from the Avaya support technician.

**Procedure**

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

The customer account is created during the deployment procedure.

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

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

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

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

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

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

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

#### Related links

[Avaya support access](#) on page 46

# Chapter 7: Configuration

---

## Configuring Avaya Aura® MS

To configure Avaya Aura® MS, enable additional capabilities, and create clusters, see *Implementing and Administering Avaya Aura® Media Server*.

---

## Updating the network configuration

### About this task

Server networking information can be updated by using the `netSetup` command in a Linux® shell. The `netSetup` command guides you through the process of updating the following settings:

- Time zone and UTC
- Date and time
- Hostname
- IPv4 address
- IPv4 Netmask
- Gateway IPv4 address
- IPv6 autoconfigure
- IPv6 address
- IPv6 prefix length
- IPv6 gateway address
- Domain name
- Static route(s) (virtual appliance and systems with out of band management enabled only only)
- Up to three DNS server IPv4 addresses
- Up to three NTP server IPv4 addresses or hostnames
- Out of band management IPv4 address
- Out of band management IPv4 netmask
- Out of band management IPv4 gateway address

## Before you begin

Stop Avaya Aura® MS before changing the network configuration. See *Implementing and Administering Avaya Aura® Media Server*.

## Procedure

1. If you are making changes to the IP address or FQDN you must disenroll AAMS cluster from System Manager first.
2. Log in to a Linux® shell using the customer account.
3. Type the following command:

```
netSetup
```

Follow the on-screen prompts to update the network settings.

For Avaya Appliance Virtualization Platform systems, accept the system-determined default value for the **Enable static route** prompt. **Enable static route** has a default value of `Y` for Avaya Aura® Appliance Virtualization Platform systems. When you press `Enter` with a value of `Y`, the system displays prompts that allow you to reconfigure the Utility Services static route.

For all appliances, if the secondary network interface is enabled, and specific static routing is required, change the value to `Y` and proceed to configure the additional static routes.

All other virtual appliance installations must use the default value of `N` for **Enable static route**.

4. Perform the following steps if you changed the IP addresses or hostname.
  - a. Navigate to **EM > System Configuration > Network Settings > IP Interface Assignment**.
  - b. **IP Interface Assignment** fields show errors, due to the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
  - c. If you are using security certificates with information dependent on FQDN or other server specific information, create new certificates. To update the certificates, navigate to **EM > Security Certificate Management**.
  - d. If this server is a member of a load sharing cluster or High Availability cluster, then navigate to **EM > Cluster Configuration > Server Designation**.  
On each server, ensure that the IP address you just changed is updated.
  - e. If this server is a primary server of a master cluster, then replication clusters that point to the master cluster must be updated with the new address of this server.

On the primary node in each replication cluster, navigate to **EM > Cluster Configuration > Replication Settings > Master Cluster Primary Node Address**.

For more information on configuring each item, see *Implementing and Administering Avaya Aura® Media Server*.

5. You must restart the server. Use one of the following methods to restart the server:
  - Type `reboot` in a Linux® shell.
  - Press the power button to turn the server off and then press the power button again to turn it back on.
  - Press the reset button until the server restarts.
6. Enroll the cluster with SMGR.

### Next steps

If required for your solution, enroll the cluster with Avaya Aura® System Manager.

---

## Resizing an Avaya Virtual Appliance for use as a Video Compositor

### About this task

Use this task to increase the capacity of a deployed Avaya Aura® MS VM for use as a Video Compositor Media Processor (VCMP).

### Before you begin

- Ensure that the host has at least 28 available physical CPUs.
- Ensure that the host has at least 28672 MB of available memory.

### Procedure

1. Log in to the VMware® host by using the vSphere Client Windows application, the vSphere Web Client for vCenter, or the VMware Host Client and locate the VM that you want to update.
2. To shut down the VM, right-click on your VM and select **Power > Shut Down Guest OS**.
3. To update the VM configuration, right-click on the VM and select **Edit Settings...**
4. To configure the CPU properties, open the **CPU** details section and perform the following steps:
  - a. Set **CPU** to 28 .
  - b. Set **Cores per Socket** to 14 .
  - c. Set **Reservation** to 61320 MHz .
5. To configure the memory properties, open the **Memory** details section and perform the follow steps:
  - a. Set **Memory** to 28 .
  - b. Set **Reservation** to 61320 MHz .

6. To apply the changes, click **OK**.
7. To start the appliance, right-click on the VM and select **Power > Power on**.

---

## Setting the GRUB2 boot password

### About this task

Some environments require that the GRUB2 boot password is set, however, there is no capability to interact with the GRUB2 boot.

Perform the following procedure to configure the GRUB2 boot password.

### Procedure

1. Log in to a Linux® shell using the root or sroot account.
2. To configure the GRUB2 boot password, type the following command:

```
grub2-setpassword
```

3. Follow the prompts to configure the password.

---

## Setting the password complexity configuration

### About this task

The Avaya Aura® MS appliance provides the capability to configure the Linux password complexity as well as other key system security parameters. There are two pre-configured profiles provided. One profile contains the default configuration, and the other profile is a hardened configuration appropriate for deployments with more stringent requirements. If required, you can create a custom profile for the system.

Perform this procedure to set the system password profile.

### Procedure

1. Log in to a Linux® shell using the root or sroot account.
2. To set the system configuration, type the following command:

```
/opt/avaya/bin/setSysConfig.sh <path to the desired system config profile>  
Where <path to the desired system config profile>is one of:  
/opt/avaya/etc/hardened-sys-config.conf  
/opt/avaya/etc/default-sys-config.conf  
/opt/avaya/app/pub/custom-sys-config.conf (or any custom profile name of your  
choice)
```

---

## Customizing the password complexity configuration

### About this task

Perform this procedure to customize the system configuration profile.

### Procedure

1. Log in to a Linux® shell using the root or sroot account.
2. To set the current directory to the public directory, type the following command:  

```
cdpub
```
3. Copy the existing profile to the current directory by typing the following command:  

```
cp /opt/avaya/etc/default-sys-config.conf ./custom-sys-config.conf
```
4. Edit the custom configuration file, setting the properties to the values required by your application.

#### Important:

Only edit the property values in the configuration files and ensure that the new values are valid for the file and property that you are updating. Unsupported values can cause unexpected system behavior.

---

## Enabling SELinux

### About this task

The Avaya Aura® MS appliance supports enabling SELinux on Linux®. SELinux is disabled by default and can be enabled if required.

#### Important:

Enabling SELinux requires multiple reboots which can result in disruption to service.

Perform the following procedure to enable SELinux on the Linux® operating system.

### Procedure

1. Log in to a Linux® shell using the root or sroot account.
2. To enable SELinux in permissive mode, type the following command: 

```
/opt/avaya/bin/selinuxManage.sh -enableStep1
```

#### Note:

SELinux in permissive mode is required before enabling enforced mode.

3. To restart the system and apply the SELinux permissive mode change, type the following command: 

```
reboot
```
4. After the reboot, log in to a Linux® shell using the root or sroot account.

5. To enable SELinux in enforced mode, type the following command: `/opt/avaya/bin/selinuxManage.sh -enableStep2`
6. To restart the system and apply the SELinux enforced mode change, type the following command: `reboot`

---

## Displaying Linux<sup>®</sup> SELinux configuration status

### About this task

Perform the following procedure to display the SELinux configuration status on the Linux<sup>®</sup> operating system.

### Procedure

1. Log in to a Linux<sup>®</sup> shell using the customer account.
2. To display the SELinux configuration status, type the following command: `sestatus`

---

## Configuring Avaya Aura<sup>®</sup> Media Server (MS) physical appliance iDRAC9

For basic configuration for the iDRAC9 on the Avaya Aura<sup>®</sup> MS physical appliance, see [Avaya Solutions Platform 130 Series iDRAC9 Best Practices](#).

To configure SNMP traps, refer to [Installing the Avaya Solutions Platform 130 Series](#) section *Dell R640 SNMP trap configuration using iDRAC9*.

# Chapter 8: FIPS Mode

---

## Overview

The Avaya Aura<sup>®</sup> MS appliance supports running in FIPS140-2 mode. The FIPS 140-2 mode is disabled by default and can be enabled or disabled as required.

 **Important:**

Enabling and disabling FIPS 140-2 mode requires a reboot which can result in a service disruption.

---

## Enabling FIPS 140-2 Mode

### About this task

Perform the following procedure to enable FIPS 140-2 mode on the Linux<sup>®</sup> operating system and the Avaya Aura<sup>®</sup> MS application software.

### Before you begin

- Department of Defense (DoD) approved FIPS 140-2 compliant certificates must be installed prior to configuring FIPS 140-2 mode.
- FIPS 140-2 compliant ciphers must be configured.

### Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings**.
2. Click **Connection Security**.
3. To enable FIPS 140-2 mode, check the **Enable FIPS** check box.
4. Click **Save**.
5. Log in to a Linux<sup>®</sup> shell using the customer account.
6. To restart the system and apply the change, type the following command:

```
reboot
```

---

## Disabling FIPS 140-2 Mode

### About this task

Perform the following procedure to disable FIPS 140-2 mode on the Linux® operating system.

### Procedure

1. Navigate to **EM > System Configuration > Network Settings > General Settings**.
2. Click **Connection Security** in the shortcut bar.
3. To disable FIPS 140-2 mode, clear the **Enable FIPS** checkbox.
4. Click **Save**.
5. Log in to a Linux® shell using the customer account.
6. To restart the system and apply the change, type the following command:

```
reboot
```

---

## Displaying FIPS 140-2 configuration status

### About this task

Perform the following procedure to display the FIPS 140-2 mode on the Linux® operating system.

### Procedure

1. Log in to a Linux® shell using the customer account
2. To display the FIPS 140-2 mode, type the following command:

```
fipsManage --isEnabled
```

# Chapter 9: File System Integrity Tool (FSIT)

---

## Overview

The Avaya Aura® MS appliance contains a File System Integrity Tool (FSIT) based on Linux® Advanced Intrusion Detection Environment (AIDE) software. Direct access to AIDE software and configuration is not supported. An SSH interface is provided to initialize and update the AIDE database, enable and disable daily scans, run on demand scans, and to display the results of the last scan.

 **Important:**

Antivirus scans, antivirus updates and File System Integrity Tool (FSIT) scans should not be scheduled to run at the same time. These tools should only run during the least busy period to ensure that there is no impact to system services.

---

## Initializing the AIDE database

### About this task

Before running a file system integrity check, the database must be initialized. The initialization step provides a baseline to determine if there are changes applied to the file system. This is required after installing updates, to either the media server or the system layer, or making configuration changes, because the database needs to be updated to create a new baseline.

### Procedure

1. Log in to a Linux® shell using the customer account.
2. To initialize or update the AIDE database, type the following command:

```
fsit -updateDB
```

---

## Enabling daily FSIT scans

### About this task

Perform the following procedure to enable daily file system integrity scans to start at a designated hour and minute.

**Procedure**

1. Log in to a Linux® shell using the customer account.
2. Use the following command to enable daily file system integrity scans. The time that the scan runs is designated by the hour (0-23) and minute (0-59) parameters. An existing scan schedule is replaced when a new scan schedule is added

```
fsit -enableScan <hour> <minute>
```

**Next steps**

Review update and scan results daily.

---

## Disabling daily FSIT scans

**About this task**

Perform the following procedure to disable daily file system integrity scans.

**Procedure**

1. Log in to a Linux® shell using the customer account.
2. To disable the daily file system integrity scans, type the following command:

```
fsit -disableScan
```

---

## Displaying FSIT scan results

**About this task**

Perform the following procedure to review FSIT configuration and output of the last scan.

**Procedure**

1. Log in to a Linux® shell using the customer account.
2. To display the results of last antivirus update and scan, type the following command:

```
fsit -status
```

The system displays results similar to the following example.

The output indicates the initialization state of the database, the last time the database was updated and the start time of daily system scans. Last Scan indicates the last time a scheduled or manual scan ran and whether the scan completed successfully. The summary section displays a count of the files that were added, removed, or changed on the system, after the last database initialization.

```
Database      : Initialized
Last DB Update: Completed (Fri Dec 22 13:49:54 CST 2017)
Daily Scan    : 07:05
```

```

Last Scan      : Completed (Fri Dec 22 14:47:25 CST 2017)

AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2017-12-22 14:46:26

Summary:
  Total number of files:      43477
  Added files:                0
  Removed files:              0
  Changed files:              1

-----
Changed files:
-----

changed: /etc/cron.d/aide-daily.cron

-----
Detailed information about changes:
-----

File: /etc/cron.d/aide-daily.cron
SHA512   : zGIU8pfzE5PMGktpGz8PouT5UPdidkoU , FSOC7zRosOejotRZ3AUAWJC3Wu5+QIPG

```

---

## Running file system integrity scans on demand

### About this task

Perform the following procedure to initiate a file system integrity check now.

### Procedure

1. Log in to a Linux<sup>®</sup> shell using the customer account.
2. To run a system file system integrity check, type the following command:

```
fsit -scanNow
```

### Next steps

Review update and scan results.

# Chapter 10: Antivirus Software

---

## Overview

The Avaya Aura® MS appliance contains embedded antivirus engine ClamAV® that is disabled by default. When ClamAV® is enabled, it can detect Trojans, viruses, malware and other malicious threats. An SSH interface is provided to enable and disable daily updates, daily scans, run on demand scans and updates, and to display the results of the last scan.

Avaya appliances are closed systems maintained by Avaya. Avaya manages all software and software updates on appliances. Avaya does not support appliances that have non-Avaya software or software updates installed.

### Important:

Antivirus scans, antivirus updates and File System Integrity Tool (FSIT) scans should not be scheduled to run at the same time. These tools should only run during the least busy period to ensure that there is no impact to system services.

---

## Enabling daily scans and updates

### About this task

Perform the following procedure to enable daily antivirus scans and updates to start at a designated time.

### Procedure

1. Log in to a Linux® shell using the customer account.
2. Use the following command to enable daily virus database updates. The time that the update runs is designated by the hour (0-23) and minute (0-59) parameters. An existing update schedule is replaced when a new update schedule is added.  
`avScan -enableUpdate <hour> <minute>`
3. Use the following command to enable daily virus scans. The time that the scan runs is designated by the hour (0-23) and minute (0-59) parameters. An existing scan schedule is replaced when a new scan schedule is added.  
`avScan -enableScan <hour> <minute>`

**Next steps**

Review update and scan results daily.

---

## Disabling daily scans and updates

**About this task**

Perform the following procedure to disable daily Antivirus scans and updates.

**Procedure**

1. Log in to a Linux® shell using the customer account.
2. To disable daily virus database updates, type the following command:  
`avScan -disableUpdate`
3. To disable daily virus scans, type the following command :  
`avScan -disableScan`

---

## Displaying update and scan results

**About this task**

Perform the following procedure frequently to review the results of the last antivirus update and scan.

**Procedure**

1. Log in to a Linux® shell using the customer account.
2. To display the results of last antivirus update and scan, type the following command:  
`avScan -status`

The system displays results similar to the following example. At the end of the report, the SCAN SUMMARY section displays the scan results and the number of infected files detected, if any. If there are infected files, then each infected file is displayed before the SCAN SUMMARY section. In this example there is one infected file, /root/testfile.txt.

Daily Update indicates the start time of daily virus definition updates. Last Update indicates the last time a scheduled or manual update ran and whether the update completed successfully.

Daily Scan indicates the start time of daily system virus scans. Last Scan indicates the last time a scheduled or manual scan ran and whether the scan completed successfully.

```
avScan -status
```

```
Daily Update: 05:00
Last Update  : Completed (Fri Nov 10 05:10:00 EST 2017)
Daily Scan   : 05:30
Last Scan    : Completed (Fri Nov 10 05:45:00 EST 2017)
```

```
-----
/root/testfile.txt: Eicar-Test-Signature FOUND
```

```
----- SCAN SUMMARY -----
Known viruses: 4490129
Engine version: 0.99.2
Scanned directories: 4811
Scanned files: 31037
Infected files: 1
Data scanned: 2977.86 MB
Data read: 2994.16 MB (ratio 0.99:1)
Time: 637.462 sec (10 m 37 s)
```

---

## Running updates and scans on demand

### About this task

Perform the following procedure to initiate on demand updates and/or scans.

### Procedure

1. Log in to a Linux® shell using the customer account.
2. To run an antivirus database update, type the following command:

```
avScan -updateNow
```

3. To run a system scan, type the following command:

```
avScan -scanNow
```

### Next steps

Review update and scan results.

# Chapter 11: Backup and restore

---

## Performing a backup

### About this task

Perform the following procedure to create a backup of the system configuration and application content. For more information about backup and restore, see *Implementing and Administering Avaya Aura® Media Server*.

### Procedure

1. To backup Avaya Aura® MS data, navigate to **EM > Tools > Backup and Restore > Backup Tasks**.
2. Create or select an existing backup task that includes System Configuration and Application Content backup types.
3. To create a backup task, navigate to **EM > Tools > Backup and Restore > Backup Destination**.
4. Click **Add**.
5. Specify the destination name.
6. Enter the following:
  - Hostname
  - FTP user name
  - FTP Password
7. Select one of the following:
  - **SFTP**
  - **FTP**
8. Configure Remote finger print if **SFTP** is used.
9. Click **Save**.
10. Navigate to **EM > Tools > Backup and Restore > Backup Tasks**.
11. Click **Add Backup Task**.
12. Specify a backup task name.
13. Select backup types to include in the backup.

14. Click **Run Now**.
15. To monitor the Backup and Restore History Log, navigate to **EM > Tools > Backup and Restore > History Log**.

After the backup is complete, the log shows a completed backup task entry.

16. If you are using an FTP or SFTP backup destination, ensure that the backup files are saved to their required location.

There is one file for each backup type for a total of two backup files.

17. If you are using a local backup destination and about to perform an upgrade or redeploy of the Avaya Aura® Media Server (MS) appliance, you must move the backup files to a safe location by performing the following steps:

- a. Log in to a Linux® shell using the customer account.
- b. Change to the public directory by using the `cdpub` alias or the following command:

```
cd /opt/avaya/app/pub
```

- c. List the backups available on the local system by using the following command:

```
bkupFile -list
```

- d. Move the recent configuration and application data backups from the local backup storage to the current directory by using the following commands:

```
bkupFile -retrieve SystemConfiguration_backup.zip
```

```
bkupFile -retrieve ApplicationContent_backup.zip
```

- e. Save both backup files in a safe location by using the `sftp` file transfer tool, or another similar tool, to transfer the files off the server.
- f. After you confirm the files are saved in a safe location, you can delete the backup files from the current directory to free disk space.

---

## Uploading and restoring backup files

### About this task

Use this procedure to upload backup files to Avaya Aura® MS appliance.

#### Important:

If you are restoring the backup to a system then the systems major.minor.subminor version must match the major.minor.subminor version of the system the backup came from. If it doesn't, you must use the migration tool `amsupgrade` to migrate the data forward.

### Procedure

1. Perform the EM web browser-based upload task.

See Uploading a backup file for a restore in *Implementing and Administering Avaya Aura® Media Server*.

2. Perform the EM task to restore data using a backup saved in the default local backup destination.

See Restoring from the local destination in *Implementing and Administering Avaya Aura® Media Server*.

#### Related links

[Alternate procedure for uploading and restoring large backup files](#) on page 67

---

## Alternate procedure for uploading and restoring large backup files

### About this task

Use this procedure if you encounter errors when using EM to upload backup files to Avaya Aura® MS appliance. Many browsers have a 2 GB limit on file upload. Perform the following procedure to upload backup files larger than 2 GB to the local backup destination.

### Procedure

1. Log in to a Linux® shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:  

```
cd /opt/avaya/app/pub.
```
3. Transfer the configuration and application data backups to the system by pulling them with the `sftp` file transfer tool, or another similar tool.
4. Move the configuration and application data backups from the current directory into the local backup storage by using the following commands:

```
bkupFile -insert SystemConfiguration_backup.zip
```

```
bkupFile -insert ApplicationContent_backup.zip
```

5. Confirm the backup files are available on the local system by typing the following command:

```
bkupFile -list
```

6. Perform the EM task to restore data using a backup saved in the local backup destination.

For information about restoring from the local destination, see *Implementing and Administering Avaya Aura® Media Server 7.8*.

# Chapter 12: Updates

---

## Viewing the installed version and updates

### About this task

Perform the following procedure to display information about the currently installed software.

### Procedure

1. Log in to Avaya Aura® MS EM by using the customer account username and password.
2. Display the installed software by navigating to **EM > Tools > Manage Software > Inventory**.

EM displays the currently installed software versions for the application and system layers.

3. Display details about the last installed update by navigating to **EM > Tools > Manage Software > History**.

EM displays the last installed updates for the application and system layers. Only official updates are listed.

### Related links

[Accessing Avaya Aura MS EM](#) on page 45

---

## Uploading media server updates

### About this task

The Avaya Aura® MS application and system software updates are versioned and delivered separately. Uploading the software updates makes them available for installation.

Perform the following procedure to upload each required software update to Avaya Aura® MS.

### Procedure

1. Navigate to **EM > Tools > Manage Software > Updates**.
2. To select the software update to upload, click **Browse**.

The selected file must be an official Avaya Aura® MS update package in ISO format.

3. Click **Upload**.

The browser shows a progress spinner while the system uploads the file.

When the upload completes the system displays the license agreement.

4. Read the license agreement and click **Accept**.

The browser shows a progress spinner while the system verifies the integrity and authenticity of the update.

The system displays the details of the update including the filename of the uploaded file.

5. Use the chevron buttons to expand (▼) and collapse (▲) additional details about the update.

### Next steps

Repeat this procedure for each required update.

Install the update.

### Related links

[Uploading and installing media server updates using a Linux® shell](#) on page 69

[Unable to upload updates](#) on page 91

[Installing an update](#) on page 70

[Deleting an uploaded update](#) on page 70

---

## Uploading and installing media server updates using a Linux® shell

### About this task

The Avaya Aura® MS application and system software updates are versioned and delivered separately. Uploading the software updates makes them available for installation.

Perform the following procedure to upload each required software update to Avaya Aura® MS.

### Procedure

1. Log in to a Linux® shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:

```
cd /opt/avaya/app/pub
```

3. Transfer an official update package in ISO format to the system by using the `sftp` file transfer tool, or another similar tool, to pull the files to the pub directory.

#### Tip:

After you upload the update to one server, you can copy the update to other local server is faster than transferring the file multiple times from a workstation that may be on another network.

4. Run the following command to stage the software:

```
stageUpdate -stage -f softwareUpdate.iso
```

5. Run the following command to install the update:

```
installUpdate
```

### Next steps

Repeat this procedure for each required update.

Install the update.

### Related links

[Installing an update](#) on page 70

[Deleting an uploaded update](#) on page 70

---

## Deleting an uploaded update

### About this task

Perform the following procedure to remove an update that has been uploaded to the media server but not yet installed.

### Procedure

1. To view the uploaded updates, navigate to **EM > Tool > Manage Software > Updates**.
2. To delete an update click **Delete** next to the update.

The system immediately deletes the update.

---

## Installing an update

### About this task

Perform the following procedure to update the media server with the latest software release.

### Before you begin

Before applying media server updates, ensure that you:

- Upload an update by using the [Uploading media server updates](#) on page 68 task. You can upload an update prior to the scheduled maintenance time for installing an update, to avoid delays during the maintenance time.
- If both system layer and application layer updates exist, upload both, starting with the system layer update followed by the application layer update, before installing.
- Back up the system. In case of unforeseen problems during the update installation, you can use the backup to restore the system to the current configuration.

- Apply the updates to one node at a time in a cluster configuration, while the other nodes in the cluster maintain service. For High Availability clusters, see [Managing media server changes for 1+1 High Availability clusters](#) on page 73.
- Perform the installation during scheduled maintenance.

## Procedure

1. To prevent new sessions from starting on the system, navigate to **EM > System Status > Element Status** and select **More Actions > Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM > System Status > Monitoring > Active Sessions**.

Wait for the active sessions to end. The media server automatically changes to the Locked state after all the sessions have ended.

Perform the following steps if you want to continue before the active sessions end:

- a. Manually lock Avaya Aura® MS, by navigating to **EM > System Status > Element Status** and clicking **More Actions > Lock**. Locking the media server also ends any remaining sessions.
  - b. Click **Confirm**.
4. To install the uploaded updates, navigate to **EM > Tools > Manage Software > Updates** and click **Install Updates...**
  5. Click **Confirm**.  
The browser shows a progress spinner while the update is installed.  
The update is complete when you can log in to EM.
  6. Navigate to **EM > Tools > Manage Software > History**.
  7. Verify that the expected versions are displayed.
  8. Use the chevron buttons (▼) to expand the details about each update.
  9. Verify that each listed update component indicates **(Installed)**.
  10. Select **EM > System Status > Element Status > More Actions > Unlock**.
  11. Click **Confirm**.
  12. Check for any service-impacting alarms and perform an appropriate test of the system.

For example, place a call to the application.

## Related links

[Uploading media server updates](#) on page 68

[Managing media server changes for 1+1 High Availability clusters](#) on page 73

---

## Removing an installed update

### About this task

The update removal procedure removes service packs, feature packs and update revisions from the system.

If you follow this procedure, you do not have to re-configure or re-provision the system. All system configuration and application content data are preserved.

Remove updates during scheduled maintenance times.

Perform the following procedure to remove an installed update from your system.

### Before you begin

Before proceeding with the software removal, ensure that you:

- Use Element Manager to upload the previously installed software version so that you can reinstall the earlier software. You cannot install a version older than the original factory version installed on the appliance.
- Back up the system.

In case of unforeseen problems during the update removal, you can use the backup to restore the system to the current configuration.

- Remove updates one node at a time in a cluster configuration. The other nodes in the cluster maintain service. For High Availability clusters, see [Managing media server changes for 1+1 High Availability clusters](#) on page 73.

### Procedure

1. To remove the currently installed update and roll back to an earlier update, you must first upload the required earlier update to the media server. See [Uploading media server updates](#) on page 68.
2. To install the earlier update, see [Installing an update](#) on page 70.

### Related links

[Uploading media server updates](#) on page 68

[Installing an update](#) on page 70

---

## Managing media server changes for N+1 load sharing clusters

### About this task

Load sharing media server clusters can provide continuous access to services during updates, when you update one server at a time.

The Primary and Secondary nodes in the cluster require special consideration during the update, since these nodes have master Content Store components on them serving the data needs of the entire cluster. To provide continuous content access, either the Primary or Secondary server must

remain in service during the updates. Standard nodes can only connect to Primary or Secondary servers on the same software release. To ensure that the Standard nodes have a connection to a Primary or Secondary server on the same release during the cluster update, the Primary is updated first and the Secondary server is updated last.

Use this procedure to update N+1 load sharing clusters.

### Procedure

1. To update the Primary server, use the procedure for [Installing an update](#) on page 70.  
Wait for any alarms to clear as the server returns to service after the upgrade.
2. To upgrade each Standard server, use the procedure for [Installing an update](#) on page 70.  
Wait for any alarms to clear as the server returns to service after the upgrade.
3. To upgrade the Secondary server, use the procedure for [Installing an update](#) on page 70.
4. Verify the success of the installation.

Check for any service-impacting alarms and perform a test of the system. For example, place a call to an application, and verify all the nodes in the cluster receive calls.

---

## Managing media server changes for 1+1 High Availability clusters

### About this task

Use this procedure to install or remove a media server update in High Availability clusters. Changes are applied as follows, to prevent loss of service:

1. Apply or remove the update for the standby server.
2. After activating the updated standby server, apply or remove the update for the other server.

### Before you begin

If you are updating both the system layer and the Avaya Aura<sup>®</sup> MS software, then update the system layer software first.

### Procedure

1. Navigate to **EM > Element Status** on each server and determine which server has the **High Availability State** of Standby or Active.
2. To lock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and select **Local High Availability State Lock**.
3. Click **Save**.
4. Click **Confirm**.

5. To install or remove an update for the standby server, go to Step 4 of the procedure for [Installing an update](#) on page 70.  
Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.
6. To unlock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and clear **Local High Availability State Lock**.
7. Click **Save**.
8. Click **Confirm**.
9. To put the active server in the standby state, navigate to **EM > Element Status** and select **Failover** from the **More Actions** drop-down menu.
10. Click **Confirm**.  
The active server is now the standby server.
11. To lock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and select **Local High Availability State Lock**.
12. Click **Save**.
13. Click **Confirm**.
14. To install or remove an update for the standby server, go to Step 4 of the procedure for [Installing an update](#) on page 70.
15. Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.
16. To unlock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and clear **Local High Availability State Lock**.
17. Click **Save**.
18. Click **Confirm**.

---

## Updating the Avaya Aura® MS physical appliance to enable secure boot

### About this task

New Avaya Aura® MS appliances are shipped with the appliance software already installed and the secure boot configuration set appropriately. When updating or reinstalling an Avaya Aura® MS appliance to software version 10.2.0 SP1 or newer, the secure boot setting can be enabled.

Versions prior to 10.2.0 SP1 do not support secure boot and will encounter errors if secure boot is enabled.

Enabling secure boot is not required to run any version of the Avaya Aura® MS appliance but is recommended to increase the security of the system.

**Before you begin**

- The power to the server must be on so that the system can boot.

**Procedure**

1. If not already in the firmware configuration, restart the server by using one of the following methods:
  - a. Press **Control+Alt+Delete** on your keyboard and select **Restart**.
  - b. Type **reboot** in a Linux® shell.
  - c. Press the power button to turn the server off and then press the power button again to turn it back on.
  - d. Press the reset button until the server restarts.
  - e. Enter the System Setup menu by pressing **F2** during boot.
2. Navigate to **System BIOS > System Security**.
3. Under the **SECURE BOOT** section, set **Secure Boot** to **Enabled**.
4. Select **OK** to acknowledge the Setup Password warning, then **Back**.
5. Select **Finish**, and **Yes** to save changes. Then select **OK** to confirm that changes were saved.
6. Select **Finish** and **Yes** to complete all of the changes. The system will reboot.

---

## Updating the Avaya Aura® MS VMware virtual appliance to enable secure boot

**About this task**

New Avaya Aura® MS appliances are deployed with the appliance software already installed and the secure boot configuration set appropriately. When updating an existing VM to an Avaya Aura® MS appliance software version 10.2.0 SP1 or newer, the secure boot setting can be enabled.

Versions prior to 10.2.0 SP1 do not support secure boot and will encounter errors if secure boot is enabled.

Enabling secure boot is not required to run any version of the Avaya Aura® MS appliance but is recommended to increase the security of the system.

Some VMs may be configured to use the BIOS boot option instead of EFI/UEFI. This procedure only applies to VMs using the EFI/UEFI boot option.

**Procedure**

1. Log in to the VMware® host by using the vSphere Client Windows application, the vSphere Web Client for vCenter, or the VMware Host Client and locate the VM that you want to update.

2. To shut down the VM, right-click on your VM and select **Power > Shut Down Guest OS**.
3. To update the VM configuration, right-click on the VM and select **Edit Settings...**
4. Select the **VM Options** tab at the top.
5. Expand the **Boot Options** section. Check the **Enabled** checkbox for the **Secure Boot** item.

 **Note:**

If the Firmware is set to **BIOS**, this procedure is not applicable.

6. To apply the changes, click **OK**.
7. To start the appliance, right-click on the VM and select **Power > Power on**.

---

## Updating the Avaya Aura<sup>®</sup> MS KVM virtual appliance to enable secure boot

### About this task

New Avaya Aura<sup>®</sup> MS appliances are deployed with the appliance software already installed and the secure boot configuration set appropriately. When updating an Avaya Aura<sup>®</sup> MS appliance software version 10.2.0 SP1 or newer, the secure boot setting may be set to enabled. For KVM on Red Hat<sup>®</sup> appliances this setting cannot be changed in-place and requires re-deploying the target VM.

Enabling secure boot is not required to run any version of the Avaya Aura<sup>®</sup> MS appliance but is recommended to increase the security of the system.

### Before you begin

- Note the appliance-specific configuration for the target VM (hostname, IP, netmask, gateway, etc). This information is required when re-deploying the VM and is not backed up by the Avaya Aura<sup>®</sup> MS backup procedure.
- Create Avaya Aura<sup>®</sup> MS backups of the current system. Configuration and application data backups of the current installation are required to preserve the data through the upgrade process and if a rollback is required.
- Ensure that you have saved the Avaya Aura<sup>®</sup> MS backups in a safe location

### Procedure

1. Shut down the VM that will be re-deployed.
2. Deploy a new AMS 10.2.0 SP1 (or later) virtual appliance on ASP 130 using procedures described in [Deploying Avaya Aura<sup>®</sup> MS KVM Installer](#) on page 29.
3. Restore existing configuration using task [Uploading and restoring backup files](#) on page 66.
4. Once the new instance is confirmed to be restored properly, remove the old instance.

# Chapter 13: Upgrade from a previous release

---

## Upgrade overview

You can upgrade a system from Avaya Aura® MS 8.0.x or 10.x to the latest Avaya Aura® MS 10.y release by applying the 10.x upgrade on the existing Avaya Aura® MS appliance with the old software.

It is recommended to perform upgrades only during the maintenance window or at an off peak-usage time.

The upgrade procedures set the operational state of the media server to Pending Lock. The purpose of placing the media server in the Pending Lock state is to ensure that the system does not start any new sessions. After all the sessions on the server have ended, the server can be upgraded without disruption to any users.

When you are ready to upgrade the server, the operational state is set to Locked, which ends any remaining active sessions.

If the media server is set to Pending Lock before the upgrade maintenance window, then the system ends a minimum number of user sessions, if any.

---

## Upgrading to Avaya Aura® MS 10.y

### About this task

To upgrade Avaya Aura® MS 8.0.x or 10.x to the latest Avaya Aura® MS 10.y release, install the 10.y software using the procedures described in the chapter, "Updates".

#### **Note:**

You must stage both updates (system layer first, followed by media server) prior to attempting to install 10.y if the server contains 8.x or 10.x software.

---

## Rolling back to a previous release

### About this task

Rolling back the system restores the system to the pre-upgrade state by reinstalling the previous release of Avaya MS. You might need to roll back the system if:

- Functionality in the new version is not compatible with other components of your solution.
- The upgrade process encountered an error and did not complete successfully.
- An unsupported upgrade path ended the upgrade process.
- The upgrade tool could not read the backup data file.
- You stopped the upgrade during the procedure.

### Procedure

1. Turn off the Avaya Aura<sup>®</sup> MS 8.0.x appliance.
2. Use one of the following methods to restore an older Avaya MS appliance:
  - If you still have the older Avaya MS VM, turn it on to return it to service.
  - If you no longer have the older Avaya MS VM, then redeploy the older Avaya MS. Use your backup files of the older release to restore the system configuration and application data after it is deployed.

---

## Upgrading data manually from Release 8.0.x to a newly deployed Avaya Aura<sup>®</sup> MS appliance instance

### About this task

Use this procedure if you deploy a new appliance and want to migrate your existing data from 8.0.x appliance.

### Before you begin

- Ensure that the system meets the prerequisites for upgrade.
- Create Avaya Aura<sup>®</sup> MS backups of the current system. Configuration and application data backups of the current installation are required to preserve the data through the upgrade process and if a rollback is required.
- If you are upgrading a server that is a member of a cluster, ensure that you are performing this task as part of one of the cluster upgrade procedures before continuing. Ensure that you start at the correct step in the following procedure, as specified by the cluster upgrade procedure.

### Procedure

1. Prevent new sessions from starting on the system by navigating to **EM > System Status > Element Status** and select **More Actions > Pending Lock**.

2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM > System Status > Monitoring > Active Sessions** to

Wait for the active sessions to end. The system automatically changes to the Locked state after all the sessions have ended.

Perform the following steps if you want to continue before the active sessions end:

- a. Manually lock the media server, by navigating to **EM > System Status > Element Status** and **More Actions > Lock**. Locking the media server also ends any remaining sessions.
  - b. Click **Confirm**.
4. After the system ends the sessions, stop the media server by navigating to **EM > System Status > Element Status** and clicking **Stop**.
  5. Click **Confirm**.
  6. Ensure that you have system configuration and application content data backups before proceeding. Backup files are used to upgrade the current data. All data will be lost if you do not have data backups of your current Avaya Aura® MS 8.x data.
  7. If you are replacing the hardware or the operating system, ensure that you have saved the Avaya Aura® MS backups off the server in a safe location and proceed to step 13.
  8. Transfer the system configuration and application content backup files saved earlier to the server.
  9. Open a shell on Avaya Aura® MS.
  10. Obtain root access.
  11. From the command-line, change to the directory where you have saved the backup files.
  12. Use the upgrade tool to upgrade the system configuration data by entering the following on command-line:

```
amsupgrade SystemConfigBackupFilename.zip
```

 **Important:**

- Restore the system configuration data before restoring the application data to ensure that the application data is restored to the configured location.
  - Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same installation path, IP address, and hostname so that the data is compatible with the server configuration.
13. Press **Y** to stop all Avaya Aura® MS services when prompted.

The tool upgrades the data.

14. Use the upgrade tool to upgrade the application content data by entering the following on the command-line:

```
amsupgrade AppContentBackupFilename.zip
```

15. Press **Y** to stop all Avaya Aura® MS services when prompted. The tool upgrades the data.

 **Note:**

The time required to complete the application content upgrade depends on the amount of application data in the backup file.

16. Verify the required software is installed by navigating to **EM > Tools > Manage Software > Inventory**.
17. Start Avaya Aura® MS by navigating to **EM > System Status > Element Status** and clicking **Start**.
18. Click **Confirm**.
19. Check for any service-impacting alarms and perform an appropriate test for the system. For example, place a call to the application.

 **Important:**

Running the upgrade tool, as recommended in this procedure, ensures that the system configuration parameters and all application data is upgraded and ready to use. However, there are new and updated system configuration options in this release that are not automatically configured. To ensure that the new options are configured properly, see *Implementing and Administering Avaya Aura® Media Server*. Many systems might not need any additional configuration.

# Chapter 14: Migrating from ASP 120 to ASP 130

---

## Migration overview

Avaya Solutions Platform (ASP) is a turnkey hardware solution. ASP 120 has gone End of Sale (EoS). You can migrate Avaya Aura® MS 8.0.x or 10.x deployed on ASP 120 to ASP 130. Perform the migration during the maintenance window or non-peak usage time.

The migration procedures set the operational state of the media server to Pending Lock. The purpose of placing the media server in the Pending Lock state is to ensure that the Avaya Aura® MS does not start any new sessions. After all the sessions on the server end, the server can be upgraded without disrupting any user.

When you are ready to migrate the server, the operational state is set to Locked, ending the remaining active sessions.

If the media server is set to Pending Lock before the upgrade maintenance window, the Avaya Aura® MS ends a minimum number of user sessions.

---

## Migrating ASP 120 (AMS 8.x) to ASP 130 (AMS 10.x)

### About this task

Use this procedure to migrate from AMS 8.x deployed on ASP 120 to AMS 10.x deployed on ASP 130.

### Before you begin

- Create Avaya Aura® MS backups of the current system. Configuration and application data backups of the current installation are required to preserve the data through the upgrade process and if a rollback is required.
- Ensure that you have saved the Avaya Aura® MS backups away from the server in a safe location.
- To migrate a server that is a member of a cluster, ensure that you perform this task as part of one of the cluster upgrade procedures before continuing. Ensure that you start at the correct step in the following procedure, as specified by the cluster upgrade procedure.

## Procedure

1. Deploy a new AMS 10.x virtual appliance on ASP 130 using procedures described in the chapter, “Deploying in the VMware® virtualized environment”.
2. Migrate 8.x data using task [Upgrading data manually from Release 8.0.x to a newly deployed Avaya Aura MS appliance instance](#) on page 78.

---

# Migrating ASP 120 (AMS 10.x) to ASP 130 (AMS 10.x)

## About this task

Use this procedure to migrate from AMS 10.x deployed on ASP 120 to AMS 10.x deployed on ASP 130.

## Before you begin

- Create Avaya Aura® MS backups of the current system. Configuration and application data backups of the current installation are required to preserve the data through the upgrade process and if a rollback is required.
- Ensure that you have saved the Avaya Aura® MS backups away from the server in a safe location.
- To migrate a server that is a member of a cluster, ensure that you perform this task as part of one of the cluster upgrade procedures before continuing. Ensure that you start at the correct step in the following procedure, as specified by the cluster upgrade procedure.

## Procedure

1. Deploy a new AMS 10.x virtual appliance on ASP 130 using procedures described in the chapter, “Deploying in the VMware® virtualized environment”.
2. Restore the existing configuration using task [Uploading and restoring backup files](#) on page 66.

# Chapter 15: Patches

---

## Quick Fix Engineering overview

You can use Quick Fix Engineering (QFE), also referred to as a Hot Fix, to apply an urgent patch to Avaya Aura® MS systems that need an immediate fix before the next official service pack or release. QFE patches do not typically go through a formal product verification cycle.

 **Important:**

Apply a QFE patch only if Avaya recommends the patch for your installation.

---

## Obtaining QFE

### About this task

Use the following procedure to download the required QFE patch from Avaya Support to Avaya Aura® MS.

### Procedure

Follow the download instructions that the Avaya technical support engineer provides.

---

## Description of the patch tool

Use the `amspatch` command-line tool to apply the QFE patches to the system.

The tool usage is as follows:

```
amspatch [apply | remove | info | list | fullinfo] [options]
```

The following table lists the typical usage of the tool:

| Command                                                    | Description                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| amspatch list [applied   available   all]                  | Lists the patches on the system.<br><br>The available patches are present in the QFE directory. You can apply these patches to the installed software when required.                                                                                                             |
| amspatch info [patchname   applied   available   all] [-h] | Provides detailed information about a patch or list of patches.<br><br>The <b>-h</b> option includes the detailed history of the patch on the current system.                                                                                                                    |
| amspatch apply patchname [-v]                              | Applies the specified patch to the system.<br><br>Apply patches in numerical order.<br><br>You can specify all as the patch name to apply all available patches.<br><br>The <b>-v</b> option specifies verbose output. The verbose output is always recorded in the history log. |
| amspatch remove patchname [-v]                             | Removes the specified patch from the system.<br><br>Remove patches in reverse numerical order.<br><br>The <b>-v</b> option specifies verbose output. The verbose output is always recorded to the history log.                                                                   |

## Installing a QFE patch

### About this task

Perform the following procedure to install a QFE patch to the system. When possible, apply patches during a maintenance window:

#### Important:

You must apply QFE patches in sequential, numerical order because new patches depend on previously installed QFE patches. For example, you must install `QFE-platform-10.2.0.230-0001` before you install `QFE-platform-10.2.0.230-0002`.

#### Note:

Some steps in the following procedure are specific to the Avaya Aura® MS EM management system. If you are using a different management system, the procedure is different.

### Before you begin

Before proceeding with the QFE installation, ensure that you:

- Back up your system.

In case of unforeseen problems, you can use the backup to restore your system to the previous configuration.

- Apply patches to N+1 load sharing clusters one node at a time so that the other nodes in the cluster can provide service during the procedure. See, [Managing QFEs for N+1 load sharing clusters](#) on page 89.
- Apply patches to 1+1 High Availability clusters by applying the QFE to the standby server first and then applying the QFE to the other server. See, [Managing QFEs for 1+1 High Availability clusters](#) on page 88.
- Ensure that the QFE is downloaded and staged on the target server. Root access is required to stage the QFE file, so contact Avaya support if root access is not available. To stage the QFE as root, copy it to the QFE directory `$MASHOME/qfe`.

## Procedure

1. Prevent new sessions from starting on the system by navigating to **EM > System Status > Element Status** and select **More Actions > Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM > System Status > Monitoring > Active Sessions**.

Wait for the active sessions to end. The system automatically changes to the Locked state after all the sessions have ended.

Perform the following steps if you want to continue before the active sessions end:

- a. Manually lock Avaya Aura® MS, by navigating to **EM > System Status > Element Status** and clicking **More Actions > Lock**.

Locking the media server also ends any remaining sessions.

- b. Click **Confirm**.
4. After the system ends all the sessions, stop Avaya Aura® MS by navigating to **EM > System Status > Element Status** and select **More Actions > Stop**.
  5. Click **Confirm**.
  6. Open a Linux® shell.
  7. Enter the following command to get the actual name of the patch to be applied:

```
amspatch list all
```

Remember the name of the patch listed under the QFE column for use in the next steps. This name can be different from the file name.

If you do not see the QFE patch in the list of available patches, then check the following:

- The patch file is present in the patch QFE directory.
- The patch file you downloaded is not set to read-only.

8. Enter the following command to apply a single patch:

```
amspatch apply patchname
```

To apply all available patches enter the following command:

```
amspatch apply all
```

9. Press **y** to continue.
10. After the patch application is complete, open EM and navigate to **EM > Tools > Manage Software > Inventory**.
11. Verify whether the patch version listed in the **Patch Level** column is correct.
12. **(Optional)** If you stopped the media server in Step 6, then start Avaya Aura® MS with the following steps:
  - a. Navigate to **EM > System Status > Element Status** and select **Start**.
  - b. Click **Confirm**.
13. Unlock Avaya Aura® MS by navigating to **EM > System Status > Element Status** and select **More Actions > Unlock**.
14. Click **Confirm**.
15. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

#### Related links

[Managing QFEs for 1+1 High Availability clusters](#) on page 88

[Managing QFEs for N+1 load sharing clusters](#) on page 89

---

## Removing a QFE patch

### About this task

Remove a QFE patch to revert the system to the state before you installed the patch. Remove patches during a maintenance window when possible.

Perform the following procedures to remove a QFE patch from the system:

#### Important:

You must remove QFE patches in reverse, numerical order. For example, if QFE-platform-10.2.0.230-0001 and QFE-platform-10.2.0.230-0002 are both installed on your system, you must remove QFE-platform-10.2.0.230-0002 before you remove QFE-platform-10.2.0.230-0001

#### Note:

Some steps in the following procedure are specific to the Avaya Aura® MS EM management system. If you are using a different management system, the procedure is different.

## Before you begin

Remove a QFE from N+1 load sharing clusters one node at a time so that other nodes in the cluster can provide service during the procedure. See, [Managing QFEs for N+1 load sharing clusters](#) on page 89.

For 1+1 High Availability clusters, remove the QFE from the standby server first and then remove the QFE from the other server. See, [Managing QFEs for 1+1 High Availability clusters](#) on page 88.

## Procedure

1. Prevent new sessions from starting on the system by navigating to **EM > System Status > Element Status** and select **More Actions > Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM > System Status > Monitoring > Active Sessions**.

Wait for the active sessions to end. The system automatically changes to the Locked state after all the sessions have ended.

Perform the following steps if you want to continue before the active sessions end:

- a. Manually lock Avaya Aura® MS, by navigating to **EM > System Status > Element Status** and clicking **More Actions > Lock**.

Locking the media server also ends any remaining sessions.

- b. Click **Confirm**.
4. After the system ends all the sessions, stop Avaya Aura® MS by navigating to **EM > System Status > Element Status** and selecting **More Actions > Stop**.
5. Click **Confirm**.
6. Open a Linux® shell on Avaya Aura® MS.
7. Enter the following command to get the actual name of the patch to remove:

```
amspatch list all
```

Remember the name of the patch listed under the QFE column for use in the next step. This name can be different from the file name.

8. Enter the following command:
- ```
amspatch remove patchname
```
9. After the patch removal is complete, open the EM and navigate to **EM > Tools > Manage Software > Inventory**.
  10. Verify that the patch version listed in the **Patch Level** column is correct.
  11. Start Avaya Aura® MS by navigating to **EM > System Status > Element Status** and selecting **More Actions > Start**.
  12. Click **Confirm**.

13. Unlock Avaya Aura® MS by navigating to **EM > System Status > Element Status** and select **More Actions > Unlock**.
14. Click **Confirm**.
15. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

#### Related links

[Managing QFEs for 1+1 High Availability clusters](#) on page 88

[Managing QFEs for N+1 load sharing clusters](#) on page 89

---

## Managing QFEs for 1+1 High Availability clusters

### About this task

Use this procedure to install or remove QFEs for High Availability clusters. Changes are applied as follows, to prevent loss of service:

1. Apply or remove the QFE for the standby server.
2. After activating the updated standby server, apply or remove the QFE for the other server.

### Procedure

1. Navigate to **EM > Element Status** on each server and determine which server has the **High Availability State of Standby**.
2. To lock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and select the **Local High Availability State Lock** checkbox.
3. Click **Save**.
4. Click **Confirm**.
5. To install or remove a QFE for the standby server, go to Step 6 of the procedure to install or remove a QFE .

Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.

6. To unlock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and clear the **Local High Availability State Lock** checkbox.
7. Click **Save**.
8. Click **Confirm**.
9. To put the active server in standby, navigate to **EM > Element Status** and select **Failover** from the **More Actions** drop-down menu.
10. Click **Confirm**.

The active server is now the standby server.

11. To lock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and select the **Local High Availability State Lock** checkbox.
12. Click **Save**.
13. Click **Confirm**.
14. To install or remove a QFE for the standby server, go to Step 6 of the procedure to install or remove a QFE .  
  
Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.
15. To unlock the state on the active server, navigate to **EM > Cluster Configuration > High Availability** and clear the **Local High Availability State Lock** checkbox.
16. Click **Save**.
17. Click **Confirm**.

#### Related links

[Installing a QFE patch](#) on page 84

[Removing a QFE patch](#) on page 86

---

## Managing QFEs for N+1 load sharing clusters

### About this task

Perform the following procedure to apply or remove QFEs for N+1 load sharing clusters:

### Before you begin

For N+1 load sharing clusters, apply or remove QFEs one cluster node at a time to avoid service interruption. Either the Primary or Secondary server must remain in service for the cluster to remain fully operational.

### Procedure

1. For the Primary server, follow the procedure to install or remove a QFE.  
  
Wait for any alarms to clear as the server returns to service after installing or removing the QFE.
2. For the Secondary server, follow the procedure to install or remove a QFE.  
  
Wait for any alarms to clear as the server returns to service after installing or removing the QFE.
3. For each Standard server, follow the procedure to install or remove a QFE.  
  
Wait for any alarms to clear as the server returns to service after installing or removing the QFE.

### Related links

[Installing a QFE patch](#) on page 84

[Removing a QFE patch](#) on page 86

# Chapter 16: Troubleshooting the Avaya Aura<sup>®</sup> MS appliance

---

## Overview

This chapter contains troubleshooting information specific to an Avaya Aura<sup>®</sup> MS appliance deployment. For general Avaya Aura<sup>®</sup> MS troubleshooting, see the “Troubleshooting” chapter in *Implementing and Administering Avaya Aura<sup>®</sup> Media Server*.

---

## Unable to upload files larger than 2 GB

You can encounter errors when using EM to upload large backup files to the Avaya Aura<sup>®</sup> MS appliance. Many browsers have a 2 GB limit on file upload.

### Proposed Solutions

- Use the latest versions of the Chrome or Firefox browsers. These browsers support file uploads greater than 2 GB.
- Use an alternate upload procedure listed in the “Related links” section.

### Related links

[Unable to upload updates](#) on page 91

[Alternate procedure for uploading and restoring large backup files](#) on page 67

---

## Unable to upload updates

If there is a situation where you cannot use your browser, EM, Avaya Aura<sup>®</sup> MS is not installed, or there is a software incompatibility preventing you from uploading new software, you can use an alternate upload procedure.

### Proposed Solution

1. Log in to a Linux<sup>®</sup> shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:

```
cd /opt/avaya/app/pub
```

3. Transfer the update package to the pub directory. You can use the `sftp` file transfer tool, or another similar tool, to transfer the file. The file must be an official update from Avaya in ISO format.

4. Run the following command to stage the software:

```
stageUpdate -stage -f softwareUpdate.iso
```

5. Now that the software is staged, you can complete the installation following the appropriate task to apply Avaya Aura® MS or system updates.

## Backup or restore tasks fail

The system requires temporary work space to create and restore backup archives of the application content. The work space required is equal to two times amount of data stored in the media server. For example, a system which will contain 2 GB of data in the Content Store, the `/opt/avaya/app` volume must be provisioned with at least 6 GB of space. This equates to 2 GB of stored data and 4 GB of required free workspace for backup and restore operations.

Old backup files should be removed to maintain free space on the system.

Perform the following procedure to ensure there is enough free disk space on the volume for a backup or restore.

### Proposed Solution

1. Log in to a Linux® shell using the customer account.
2. Display the available disk space on the system by issuing the following command:

```
df -h
```

3. Note the amount of space in the **Avail** column of the output for the line containing `/opt/avaya/app` in the **Mounted on** column.

For example, in the following example output, the available space is 47 GB.

| Filesystem                   | Size | Used | Avail | Use% | Mounted on     |
|------------------------------|------|------|-------|------|----------------|
| /dev/mapper/storage_vg-root1 | 3.9G | 943M | 2.7G  | 26%  | /              |
| tmpfs                        | 2.0G | 1.5M | 2.0G  | 1%   | /dev/shm       |
| /dev/sdal                    | 4.0G | 171M | 3.6G  | 5%   | /boot          |
| /dev/mapper/storage_vg-home  | 2.9G | 4.6M | 2.8G  | 1%   | /home          |
| /dev/mapper/storage_vg-app   | 51G  | 1.3G | 47G   | 3%   | /opt/avaya/app |
| /dev/mapper/storage_vg-var1  | 5.8G | 383M | 5.2G  | 7%   | /var           |

4. Remove old backup files and other unnecessary files to create the required space. Perform the following steps to remove backup files:

- a. Use the following command to list the current backup files:

```
bkupFile -list
```

- b. Remove a backup file with the following commands:

```
bkupFile -retrieve filename
rm filename
```

---

## Resetting locked login accounts

If you are unable to log in to the system, the account might be locked.

The system locks the customer account after four failed login attempts.

The system supports a maximum of five simultaneous logins per user account. The system rejects additional SSH, Rsync, and Putty sessions when five sessions are already logged in.

### Proposed Solution

1. Close unused sessions if the maximum number of sessions has been exceeded.
2. Before you log in again, wait for about 20 minutes for the system to reset the locked account.
3. Contact Avaya support if the problem persists.

Avaya support personnel with root or sroot access can reset accounts that get locked as a result of too many failed log in attempts.

---

## Restarting or shutting down from Linux® shell

Some maintenance tasks and configuration procedures require you to restart or shutdown the server. Use the following commands in a Linux® shell to restart or gracefully power-off the server.

### Proposed Solution

- To restart the server, type the following command in a Linux® shell:

```
reboot
```

- To power-off the server with graceful shutdown, type the following command in a Linux® shell:

```
shutdown
```

# Chapter 17: Related resources

## Media Server documentation

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

| Title                                                                                                                        | Description                                                                                                                                          | Audience                                                               |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Overview                                                                                                                     |                                                                                                                                                      |                                                                        |
| <i>Avaya Aura® Media Server Overview and Specification</i>                                                                   | Describes the key features of Media Server                                                                                                           | Customers and sales, services, and support personnel                   |
| Implementing and administering                                                                                               |                                                                                                                                                      |                                                                        |
| <i>Deploying and Updating Avaya Aura® Media Server Appliance</i>                                                             | Deploy, update, and troubleshoot Avaya Aura® Media Server appliances deployed in the VMware® virtualized environment or on Avaya Solutions Platform. | System administrators, implementation engineers, and support personnel |
| <i>Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS</i>                     | Install, upgrade, and patch software-only version of Avaya Aura® Media Server on customer provided hardware platform.                                | System administrators, implementation engineers, and support personnel |
| <i>Implementing and Administering Avaya Aura® Media Server</i>                                                               | Deploy update, upgrade and patch, non-appliance versions of Avaya Aura® Media Server deployed on Platform Vendor Independent (PVI) servers.          | System administrators, implementation engineers, and support personnel |
| iDRAC configuration                                                                                                          |                                                                                                                                                      |                                                                        |
| <i>Avaya Solutions Platform 130 Series iDRAC9 Best Practices</i>                                                             | Prepare the iDRAC for remote access and SNMP trap reporting.                                                                                         | System administrators, and implementation engineers                    |
| <i>Installing the Avaya Solutions Platform 130 Series 6.0.x- Only Section Dell R640 SNMP trap configuration using iDRAC9</i> | Configure the physical appliance iDRAC9 SNMP traps.                                                                                                  | System administrators, and implementation engineers                    |

### Related links

[Finding documents on the Avaya Support website](#) on page 95

[Accessing the port matrix document](#) on page 95

[Avaya Documentation Center navigation](#) on page 96

## 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.

### Related links

[Media Server documentation](#) on page 94

## Accessing the port matrix document

### Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Select Release**, select the appropriate release number.  
This field is not available if there is only one release for the product.
5. From the **Select Content Type** list, select one or both of the following options:
  - **Application & Technical Notes**
  - **Design, Development & System Mgt**

## Related links

[Media Server documentation](#) on page 94

## 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.

### Related links

[Media Server documentation](#) on page 94

---

## Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click > to search for the course.

| Course code | Course title                            |
|-------------|-----------------------------------------|
| 71201V      | Integrating Avaya Aura® Core Components |
| 72201V      | Supporting Avaya Aura® Core Components  |

---

## 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](https://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.

### Related links

[Using the Avaya InSite Knowledge Base](#) on page 98

## 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.

**Related links**

[Support](#) on page 98

# Index

## Numerics

|                                                          |                                         |
|----------------------------------------------------------|-----------------------------------------|
| 1+1 high availability cluster requirements .....         | <a href="#">14</a> , <a href="#">36</a> |
| 1+1 high availability cluster requirements for KVM ..... | <a href="#">28</a>                      |
| 10.x .....                                               | <a href="#">82</a>                      |
| 8.x to 10.x .....                                        | <a href="#">81</a>                      |

## A

|                                                      |                                         |
|------------------------------------------------------|-----------------------------------------|
| access                                               |                                         |
| EM .....                                             | <a href="#">45</a>                      |
| accessing                                            |                                         |
| Linux shells .....                                   | <a href="#">45</a>                      |
| Accessing Avaya Aura MS EM .....                     | <a href="#">45</a>                      |
| accessing port matrix .....                          | <a href="#">95</a>                      |
| add ova to sdm .....                                 | <a href="#">22</a>                      |
| antivirus software overview .....                    | <a href="#">62</a>                      |
| appliance recover software                           |                                         |
| Obtaining physical appliance recovery software ..... | <a href="#">39</a>                      |
| ASP 110 .....                                        | <a href="#">35</a> , <a href="#">36</a> |
| ASP 110 (Dell R640XL) active network ports .....     | <a href="#">36</a>                      |
| ASP 110 (Dell R660xs) active network ports .....     | <a href="#">35</a>                      |
| Avaya Aura MS appliance                              |                                         |
| package .....                                        | <a href="#">10</a>                      |
| upload and restore backup files .....                | <a href="#">66</a>                      |
| upload and restore large backup files .....          | <a href="#">67</a>                      |
| Avaya Aura MS KVM                                    |                                         |
| deploying .....                                      | <a href="#">29</a>                      |
| Avaya Aura MS physical appliance                     |                                         |
| deploying .....                                      | <a href="#">37</a>                      |
| Avaya InSite Knowledge Base .....                    | <a href="#">98</a>                      |
| Avaya support access .....                           | <a href="#">46</a>                      |
| Avaya support website .....                          | <a href="#">98</a>                      |

## B

|                               |                    |
|-------------------------------|--------------------|
| backup or restore             |                    |
| tasks fail .....              | <a href="#">92</a> |
| best practice                 |                    |
| recommendations .....         | <a href="#">15</a> |
| recommendations for KVM ..... | <a href="#">28</a> |

## C

|                                   |                    |
|-----------------------------------|--------------------|
| changes to platform support ..... | <a href="#">8</a>  |
| changing                          |                    |
| users in Linux shell .....        | <a href="#">46</a> |
| collection                        |                    |
| delete .....                      | <a href="#">96</a> |
| edit .....                        | <a href="#">96</a> |
| generating PDF .....              | <a href="#">96</a> |
| sharing content .....             | <a href="#">96</a> |

|                                                                      |                    |
|----------------------------------------------------------------------|--------------------|
| common server physical appliance                                     |                    |
| system requirements .....                                            | <a href="#">35</a> |
| configure FIPS mode on Linux .....                                   | <a href="#">57</a> |
| configuring                                                          |                    |
| Avaya Aura MS .....                                                  | <a href="#">51</a> |
| Configuring(Avaya Aura Media Server Physical appliance iDRAC9) ..... | <a href="#">56</a> |
| content                                                              |                    |
| publishing PDF output .....                                          | <a href="#">96</a> |
| searching .....                                                      | <a href="#">96</a> |
| sharing .....                                                        | <a href="#">96</a> |
| sort by last updated .....                                           | <a href="#">96</a> |
| watching for updates .....                                           | <a href="#">96</a> |

## D

|                                                    |                    |
|----------------------------------------------------|--------------------|
| Deleting an uploaded update .....                  | <a href="#">70</a> |
| deploy                                             |                    |
| OVA .....                                          | <a href="#">16</a> |
| deploy ova using sdm .....                         | <a href="#">23</a> |
| deploying                                          |                    |
| Avaya Aura MS .....                                | <a href="#">37</a> |
| Avaya Aura MS KVM installer .....                  | <a href="#">29</a> |
| deploying OVA file, VMware host client .....       | <a href="#">19</a> |
| Determining the status of EASG .....               | <a href="#">47</a> |
| Disable Daily FSIT Scans .....                     | <a href="#">60</a> |
| Disable Daily Scans .....                          | <a href="#">63</a> |
| Disable FIPS 140-2 on appliance .....              | <a href="#">58</a> |
| Display product EASG certificate information ..... | <a href="#">48</a> |
| document changes .....                             | <a href="#">9</a>  |
| documentation                                      |                    |
| Media Server .....                                 | <a href="#">94</a> |
| documentation center .....                         | <a href="#">96</a> |
| finding content .....                              | <a href="#">96</a> |
| navigation .....                                   | <a href="#">96</a> |
| documentation portal .....                         | <a href="#">96</a> |

## E

|                                 |                    |
|---------------------------------|--------------------|
| Element Manager .....           | <a href="#">45</a> |
| Enable Daily FSIT Scans .....   | <a href="#">59</a> |
| enable daily scans .....        | <a href="#">62</a> |
| Enable FIPS 140-2 on Mode ..... | <a href="#">57</a> |
| enabling SELinux .....          | <a href="#">55</a> |

## F

|                                                  |                    |
|--------------------------------------------------|--------------------|
| File System Integrity Tool (FSIT) Overview ..... | <a href="#">59</a> |
| finding content on documentation center .....    | <a href="#">96</a> |
| finding port matrix .....                        | <a href="#">95</a> |

## G

GRUB2, boot password ..... [54](#)

## I

Initialize AIDE Database ..... [59](#)

Installing an Update ..... [70](#)

## K

KB  
Support site ..... [98](#)

## L

Linux shells  
accessing ..... [45](#)

Loading and managing site certificate ..... [49](#)

## M

manage  
N+1 load sharing clusters ..... [89](#)

QFEs for 1+1 High Availability clusters ..... [88](#)

Managing media server changes for 1+1 High Availability  
clusters ..... [73](#)

Managing media server changes for N+1 load sharing  
clusters ..... [72](#)

media server updates  
upload ..... [69](#)

migrating ..... [81](#), [82](#)  
from Release 8.0.x to Release 10.1.x ..... [78](#)

migrating to asp 130 ..... [81](#), [82](#)

migration ..... [81](#)

Migration asp 120 to asp 130 ..... [81](#), [82](#)

## N

network configuration  
updating ..... [51](#)

new in media server 10.2 ..... [11](#)

new in release 10.2 ..... [11](#)

new in this release ..... [10](#)

## O

Obtaining Avaya Aura® MS KVM ..... [29](#)

Obtaining Avaya Aura® MS OVA ..... [16](#)

On Demand File System Integrity Scan ..... [61](#)

On Demand Updates and Scans ..... [64](#)

overview ..... [81](#)

## P

password complexity configuration ..... [54](#), [55](#)

port matrix ..... [95](#)

## Q

QFE  
install ..... [84](#)  
obtain QFE ..... [83](#)  
overview ..... [83](#)  
patch tool ..... [83](#)  
remove ..... [86](#)

## R

reinstalling  
Avaya Aura MS ..... [43](#)

Reinstalling Avaya Aura MS physical appliance running  
on Dell R660xs ..... [40](#)

Removing an installed update ..... [72](#)

resetting locked login accounts ..... [93](#)

resizing avaya virtual appliance, video compositor ..... [53](#)

Restarting or shutting down from Linux® shell ..... [93](#)

Review Last FSIT Scan Output ..... [60](#)

Review Last Update and Scan Output ..... [63](#)

roll back to 7.8 ..... [78](#)

## S

searching for content ..... [96](#)

SELinux, configuration status ..... [56](#)

sharing content ..... [96](#)

sort documents ..... [96](#)

support ..... [98](#)

system requirements ..... [12](#), [26](#)

## T

training ..... [97](#)

troubleshooting  
overview ..... [91](#)

## U

unable to upload files  
larger than 2 GB ..... [91](#)

update boot mode to UEFI ..... [39](#)

updating  
network configuration ..... [51](#)

Updating( virtual appliance to enable secure boot) ..... [75](#)

Updating(Avaya Aura MS KVM virtual appliance to  
enable secure boot) ..... [76](#)

Updating(Avaya Aura MS physical appliance to enable  
secure boot) ..... [74](#)

upgrade

|                                                   |                    |
|---------------------------------------------------|--------------------|
| upgrade ( <i>continued</i> )                      |                    |
| backup .....                                      | <a href="#">65</a> |
| upgrade 8.0.x                                     |                    |
| 10.x .....                                        | <a href="#">77</a> |
| upgrade .....                                     | <a href="#">77</a> |
| upgrade overview .....                            | <a href="#">77</a> |
| Upgrading                                         |                    |
| ASP 130 R6.0 or higher migration .....            | <a href="#">33</a> |
| ASP 130 R6.0 without uparding AAMS software ..... | <a href="#">32</a> |
| upload                                            |                    |
| media server updates .....                        | <a href="#">69</a> |
| upload updates .....                              | <a href="#">91</a> |
| uploading                                         |                    |
| media server updates .....                        | <a href="#">68</a> |
| uploading and restoring backup files              |                    |
| Avaya Aura MS appliance .....                     | <a href="#">66</a> |
| uploading and restoring large backup files        |                    |
| Avaya Aura MS appliance .....                     | <a href="#">67</a> |

## V

|                                                     |                    |
|-----------------------------------------------------|--------------------|
| videos .....                                        | <a href="#">97</a> |
| View FIPS 140-2 on Linux configuration status ..... | <a href="#">58</a> |
| viewing                                             |                    |
| installed version and updates .....                 | <a href="#">68</a> |
| vmware system requirements .....                    | <a href="#">12</a> |
| vSphere Web Client .....                            | <a href="#">16</a> |

## W

|                   |                    |
|-------------------|--------------------|
| watchlist .....   | <a href="#">96</a> |
| what is new ..... | <a href="#">11</a> |