Installing and Updating Avaya Aura® Media Server Application on customer-supplied hardware and OS

Release 10.2.x
Issue 5
March 2026

Notices

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 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.

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.

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

Use this document when you are working with the Avaya Aura® Media Server (MS) application that is installed on servers you provide.

Important:

Avaya also provides appliance versions of Avaya Aura® MS. Do not use this document when you are working with Avaya Aura® MS as a physical or virtual appliance. For appliance installation, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

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
5	March 2026	Added the section: Changes to platform support on page 7
4	September 2025	Added required repository list.
3	March 2025	Updated the following section • Media Server documentation on page 58 • Add secure boot support
2	February 2025	Update with guidelines for deploying in a Nutanix environment.
1	December 2024	Release 10.2 Initial document.

Chapter 2: Overview

About the Avaya Aura® MS application

The Avaya Aura® MS application is a software-only version of Avaya Aura® Media Server which is installed on servers that you provide.

An Avaya Aura® MS application is installed as follows:

- You must provide a physical server with the Red Hat Enterprise Linux® operating system. Alternatively, you provide a physical server with a supported hypervisor or public cloud, on which you install the Red Hat Enterprise Linux® operating system.
- You must run an Avaya provided installer to install Avaya Aura® MS on your server.
- You must maintain software updates for the operating system.

Important:

Avaya also provides appliance versions of Avaya Aura® Media Server. Do not use this document when you are working with the Avaya Aura® Media Server as an appliance in the VMware® virtualized environment or as an appliance on Avaya Common Server. For appliance installations, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

New in this release

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

Related links

New in Avaya Aura Media Server 10.2 on page 9

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 9

Chapter 3: System requirements and preparation

System requirements

You can install Avaya Aura® Media Server (MS) on the commercially available off-the-shelf (COTS) hardware by using standard server operating systems. The hardware and operating system configuration must meet the minimum system requirements to support the functionality of Avaya Aura® MS. Avaya provides Platform Vendor Independent (PVI) Check software to verify the server you have installed meets the system requirements.

Review the system requirements in this chapter and perform the procedures to configure your system. You must run the PVI Check to verify that the system meets the minimum requirements after configuration.

Hardware requirements and setup

Hardware requirements

Important:

- Intel® processors are strongly recommended, or performance cannot be guaranteed.
- Intel® and AMD processors require minimum SSE 4.1 support.

For installation directly on the physical hardware, the server must meet the following hardware requirements to support Avaya Aura® MS functionality:

Hardware requirements			
Hardware Component	**Minimum**	**Typical**	**High Capacity**
Number of Processor cores	2	4	8 or greater
Processor Speed	1.9 GHz	2.2 GHz or greater	2.5 GHz or greater
Memory	2 GB	4 GB	8 GB or greater
Network Interfaces	1 at 100 Mbps or greater	2 at 1000 Mbps teamed	2 at 1000 Mbps teamed

Table continues…

Hardware requirements			
Hardware Component	**Minimum**	**Typical**	**High Capacity**
Recommended partition size for Avaya Aura® MS software (default partition is `/opt`).	At least 10 GB (3 GB free minimum to install)	50 GB or greater	250 GB or greater
Disk Drive Speed	5,000 RPM	10,000 RPM	10,000 RPM
Input/Output Operations per Second (IOPS)	100	100	100

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 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.
- When deployed in a virtualized environment, the VMs must be deployed using the same virtual hardware configuration (CPUs, memory, disk size, etc) on separate, equally capable hosts.
- 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.

Installing the server

Procedure

1. Install the hardware by following the instructions of the manufacturer.
2. Connect applicable peripheral devices. For example, a monitor, a keyboard, and a mouse.
3. Connect the power cables to the server and to a properly grounded power source.

   Important:

   If your server has redundant power supplies, connect the power cables to both power supplies.
4. Turn the server on.

Configuring server firmware for maximum performance

For maximum system performance, ensure that the energy savings features are disabled or that the maximum performance settings are enabled in firmware configuration.

For more information about the configuration settings and the procedure to enter and alter the firmware settings, see the documentation for your server.

Both BIOS and UEFI boot modes are supported. When UEFI is used, secure boot can be enabled for Avaya Aura® MS versions 10.2.0 SP1 and later. Do not enable secure boot for earlier versions.

Connecting Avaya Aura® MS to the network

Procedure

1. Connect the network cables between the network ports on the back of the server and the required Ethernet switch.

   Important:

   When using multiple network connections, install and connect each network cable to the correct Ethernet switch for network redundancy.

2. At each end of the Ethernet connection, ensure that the Ethernet activity lights are ON.

Hypervisor requirements

Additional requirements and guidelines when using a hypervisor are found in the following section.

Nutanix Acropolis Hypervisor

For deployment into a Nutanix AHV environment, the following is supported:

Nutanix Feature	Avaya Aura® Media Server Support
AHV Versions	Version 6, starting with 6.5
Clone Virtual Machine	Not supported
Resize Virtual Machine	Not supported when the VM is powered on.
Acropolis Dynamic Scheduling (ADS)	Not supported. If ADS is enabled for the cluster, the AAMS VM should only be pinned to a single AHV host.
Hot Migration	Not supported. To migrate to a different physical host, you must first shut down the VM to do a cold migration. For 1+1 HA Clusters, both VMs must be shut down.
Cold Migration	Supported

Table continues…

Nutanix Feature	Avaya Aura® Media Server Support
Snapshots	Not supported on production servers outside of maintenance windows. Supported for temporary use when applying feature packs, service packs, or patches during maintenance windows. 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. Snapshots must be removed before returning the server to production.
Nutanix High Availability (HA)	Not supported.
Overcommitting of Resources	Not supported. Care must be taken to ensure that the total number of vCPUs allocated to VMs on a single host do not exceed the number of vCPUs available on the physical host.
Boot Configuration	Only UEFI is supported
Secure Boot	Supported starting with Avaya Aura® MS 10.2.0 SP1
Networking	Standard Nutanix networking is supported. The media server must have the equivalent bandwidth available as a pair of 1Gbps NICs.

The following requirements are also mandatory:

- For KVM-based hypervisors like Nutanix AHV, 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 VM 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 VM host is not oversubscribed. For maximum system performance, ensure that:
  - Energy savings features are disabled.
  - Maximum performance settings are enabled in the server BIOS.

Nutanix AVH Virtual Machine requirements

When creating the Media Server VM, refer to the *Avaya Aura® Media Server Overview and Specification* document for details on how to calculate the virtual hardware characteristics for the target deployment.

For deployment into a Nutanix AHV environment, the following is supported:

VM Characteristic	Avaya Aura® Media Server Requirement
Name	No specific requirements.
Description	No specific requirements.
Timezone	Nutanix requires Linux VMs to use UTC.
vCPU(s)	At least 2. The actual number required depends on the sizing calculations for the deployment. See the *Avaya Aura® Media Server Overview and Specification* document for details.
Number of cores per vCPU	Leave this at the default of 1.
Memory	At least 4GB as seen by the VM. The actual amount required depends on the sizing calculations for the deployment. See the *Avaya Aura® Media Server Overview and Specification* document for details. **Note:** The amount of memory seen by the OS of the VM may differ from the amount configured at the hypervisor. The Linux “free” command can be used to check the amount of memory seen by the OS under the “total” column for the “Mem:” line.
Boot Configuration	Set to UEFI. For Avaya Aura® MS versions prior to 10.2.0 SP1 ensure that “Secure Boot” is not checked. For 10.2.0 SP1 and later, “Secure Boot” can be enabled by checking the box.
Disk	At least 20 GB, with 50GB recommended for most instances.
NIC(s)	At least one NIC. An additional NIC can be configured if network separation is required.
VM Affinity	Only pin to a single host to prevent automatic VM migration.

Software requirements

Supported operating systems

Install Avaya Aura® MS only on the following operating system:

- Red Hat Enterprise Linux® Server 8.x and must be 8.6 or higher.

Important:

Avaya Aura® MS does not support operating systems other than those listed.

MariaDB server

Avaya Aura® MS installations include a MariaDB server. Only one MariaDB server instance must run on the system even if the other MariaDB server instance opens different server ports.

Net-SNMP

Net-SNMP is a suite of management and monitoring applications that you can optionally install. If you require Net-SNMP on your system, install it before you install Avaya Aura® MS.

Required network ports

Avaya Aura® MS requires network ports for communicating with clients and other servers in the network and for media transmission.

Use the document *Avaya Port Matrix: Avaya Aura® Media Server 10.x* to properly configure firewall policies on the local server.

The following table lists default media port ranges. The port ranges are configurable.

External UDP port ranges required for media to clients	
Linux® port range	**Direction required**
6000-32599	Inbound and Outbound

After Avaya Aura® MS is installed, you can use Avaya Aura® MS Element Manager to reassign many of the ports Avaya Aura® MS uses.

Related links

Changing the default software ports on page 27

Third-party software

You can install additional third-party software on the same system, when Avaya Aura® MS is installed on servers that you provide.

Avaya may request that you remove third-party software during troubleshooting support, if the third-party software is suspected of contributing to a problem.

Third-party antivirus scans must be configured to exclude directories that include Avaya Aura® MS software.

Third-party software that scans the system in real-time or that performs full system scans can reduce capacity or impact the functionality of the media server. Scanning should be limited to once a day during periods of low system use.

Obtaining Avaya Aura® MS Software

Linux® software

About this task

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

Red Hat Enterprise Linux installation

Installing RHEL

About this task

Perform the following procedure to install the latest RHEL 8.x operating system and configure the operating system to meet Avaya Aura® MS system requirements. Refer to Red Hat documentation for procedures on how to perform these tasks.

For virtualized systems, refer to the hypervisor documentation for how to install from the RedHat ISO image.

Procedure

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

   Note:

   Ensure that you choose the minimal installation option. You do not need to customize the software installation or include optional packages during initial installation. Use default server installation options.

2. Configure YUM package manager and ensure it is configured to access the following repositories:
   - BaseOS – core set of underlying OS functionality
   - AppStream – user space applications
   - EPEL – additional packages managed by the Fedora Project[PM1]
3. Install the latest package updates and critical security updates using YUM.
4. Add the required user and administrator accounts by using defined procedures for your site.
5. Configure NTP so the server is syncing to one or more NTP sources.
6. Configure Red Hat firewall polices accordingly. Refer to the document *Avaya Port Matrix: Avaya Aura® Media Server 10.2* for details of ports that need to be enabled in the firewall.

7. Restart the server.

Configure core file generation for 1+1 High Availability systems

The system creates a core file when a software process unexpectedly exits. Support engineers use the information in the core file to diagnose problems. The system copies the memory and other system information that is related to the process to a file on a disk. A busy system has large processes. The time taken by the system to create the core file depends on the size of the process in system memory. The larger the process, the longer the duration of the core file creation. Avaya Aura® MS cannot resume service until the core file creation is complete. Therefore, core file generation must be disabled at the system level so that the media server can immediately recover. If core file creation is not disabled, end-users experience temporary voice loss or loss of service when processes unexpectedly quit.

Core file generation must be disabled on the servers that are being configured to use the High Availability feature. Core file generation can be enabled temporarily on High Availability systems when you are working with the Avaya technical support engineers.

Enabling core file generation

About this task

Perform the following procedure to restore typical system defaults for core file generation or when instructed by Avaya support to enable core file generation:

Procedure

In a Linux® shell, enable core file generation using the following command:

```
echo |/usr/libexec/abrt-hook-ccpp %s %c %p %u %g %t e >/proc/sys/kernel/
core_pattern
```

Disabling the core file generation

About this task

Perform the following procedure for the servers that are being configured to use the 1+1 High Availability feature to alter the system configuration for core file generation.

Procedure

In a Linux® shell, disable core file generation using the following command:

```
echo /nowhere/null > /proc/sys/kernel/core_pattern
```

Logical Volume Management support

Avaya Aura® MS is compatible with Logical Volume Management (LVM) on RHEL. You can resize logical volumes on the system provided that the Avaya Aura® MS is not in service and the directory structure is not changed.

Network and security configuration

Securing Avaya Aura® MS installations

About this task

Perform the following procedure to apply the following optional security measures to the operating system you installed:

Procedure

1. **(Optional)** Configure the operating system by using the defined site security procedures.
2. **(Optional)** Install antivirus software and ensure that you exclude the following directories and their subdirectories from the scans:
   - Linux®:

     installpath/ma/MAS/common/log

     installpath/ma/MAS/platdata

     Important:

     Scanning software can degrade the performance and decrease the reliability of the system. Install virus scanning software only if you connect the system to a network exposed to the Internet.

     To maintain the performance of the server, you must schedule virus scans only during maintenance periods or low usage hours.

Virtual Teaming Adapter configuration

Teaming, also called bonding, of the network interfaces on your server into a single logical network interface provides increased throughput and redundancy in case one of the network interfaces fails. Teaming configuration is hardware specific. Follow the procedures provided by your server hardware manufacturer.

Avaya recommends using the active-backup bonding mode to provide fault tolerance for the system.

NIC and switch configuration

Auto-negotiation of transmission speed and duplex mode is mandatory for 1000 BASE-T gigabit Ethernet over copper. To avoid duplex mode mismatches and other interoperability problems, ensure that auto-negotiation is configured on the Network Interface Cards (NICs) and the switch. Configure the NICs and the switch with matching modes. If you disable auto-negotiation and configure the NICs to full-duplex mode or half-duplex mode then the switch must also have auto-negotiation disabled and be set to the matching full-duplex mode or half-duplex mode. For more information, see the configuration procedures your server and switch manufacturer provides.

Chapter 4: Element Manager

Element Manager overview

Element Manager (EM) is an optional, web-based administration tool that facilitates the operation, administration, and maintenance (OAM) of Avaya Aura® MS.

Some adopting products provide a different OAM management system for Avaya Aura® MS. Those systems have similar functionality although the navigation and interface are different.

The procedures in the document are based on the optional EM installed by the Avaya Aura® MS installer.

For more information and detailed procedures about using Avaya Aura® MS EM, see *Implementing and Administering Avaya Aura® Media Server*.

EM installation

When performing the Avaya Aura® MS installation procedures, you can choose to install the Avaya Aura® MS EM for management of the system. If you do not have an alternate OAM management system, you can install EM to configure Avaya Aura® MS.

An Avaya Aura® MS installer that runs in silent mode automatically installs EM unless you or the adopting product installer configures the installation properties to exclude the installation of EM.

Accessing Avaya Aura® MS EM

About this task

You need to gain access to EM to perform some of the procedures in this document. Perform the following procedure to gain access to Avaya Aura® MS EM.

For more information on using Avaya Aura® MS EM and configuring your browser to use Avaya Aura® MS EM, see *Implementing and Administering Avaya Aura® Media Server*. If you are using a different element manager refer to the appropriate documentation.

Before you begin

Signing into Element Manager (EM) is required for systems that have the optional Avaya Aura® MS EM installed. You must first install Avaya Aura® MS with EM to perform the following procedure.

Procedure

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

   `https://`*`serverAddress`*`:8443/em`

   serverIP is the address of Avaya Aura® MS. For example,

   `https://135.60.86.209:8443/em`

2. Sign into Avaya Aura® MS EM by using the **username** `admin` and the **password** `Admin123$`. After initial login, you will be prompted to change the admin password

Chapter 5: Installation

Linux® installation

You can install Avaya Aura® MS on servers that run the Linux® operating system using one of the following modes:

- Interactive command-line mode
- Silent install mode

Adopting products can automatically install Avaya Aura® MS as a component of the product solution. Additionally, the adopting products usually use the silent mode of Avaya Aura® MS installation. The following installation procedures are not necessary if the adopting product installs Avaya Aura® MS.

Installing Avaya Aura® MS on Linux® using the interactive command-line mode

Before you begin

- Complete the system requirement and preparation procedures.
- Perform any restarts that the system preparation procedures require before installing the software.
- Ensure YUM is configured and all installed packages are updated prior to installation.
- Ensure NTP is configured to sync with one or more NTP servers.
- Ensure Red Hat firewall is configured according to *Avaya Port Matrix: Avaya Aura® Media Server 10.2*.

Procedure

1. Change to root user by using the following command:

   ```
   su -
   ```

2. Download the installer file to the server or insert the Avaya Aura® MS installation DVD into the DVD drive of the server.
3. Change the current directory to the location of the downloaded installer or the drive where Avaya Aura® MS installation DVD resides.

   The name of the installation file is in the following format:

   `MediaServer_10.2.0.build_yyyy.mm.dd.bin`

For example, `MediaServer_10.2.0.39_2024.09.23.bin`.

4. Apply executable permissions to the installer file:

   `chmod 755 filename`

5. Enter the following command to run the installer:

   `./filename`

   where *filename* is the Avaya Aura® MS installer.

   Note:

   If the system is missing the required packages and if YUM is not enabled, you see the following messages and then the installer exits:

   ```
   This system is not registered to Red Hat Subscription
   Management. You can use subscription-manager to register.

   ERROR: Unable to install packages using yum
   ```

   For more information about how to enable YUM, see the Red Hat YUM manual.

6. If you see a list of packages to download and if the system prompts you to install the required packages, press `Y` and then press `Enter`.
7. Read the installation overview and press `Enter`.
8. Press `Enter` to read through the pages of the license agreement.
9. To accept the terms of the license agreement, enter `Y` and press `Enter`.
10. **(Optional)** The EM option provides a web-based management system for Avaya Aura® MS when you do not use another management system. To install EM on Avaya Aura® MS, perform the following steps:
    a. The system prompts you to install EM. Press `Y` and then press `Enter`.
    b. The system prompts you for a Linux® group name to use for EM login. Press `Enter` to accept the default name or type another defined Linux® group and press `Enter`.

    Important:

    The Linux® group that you specify must contain users who can successfully authenticate against Secure Shell (SSH).
11. Choose the installation destination by specifying a location or accepting the default location by pressing `Enter`.
12. Confirm the installation options shown in the installation summary and press `Enter` to install Avaya Aura® MS.

Installing Avaya Aura® MS on Linux® using the silent mode

About this task

The silent mode of installing Avaya Aura® MS is typically used by adopting product installers that install Avaya Aura® MS as a component of the product solution.

You can control the options for the silent installation by creating the `silent_install.properties` file and then specifying this file in the command for running the installer.

Perform the following procedure to install Avaya Aura® MS in the silent mode with no user interaction:

Before you begin

Complete the system requirement and preparation procedures. Perform any restarts that the system preparation procedures require before installing the software.

Procedure

1. Change to root user by running the following command:

   ```
   su -
   ```

2. Download the installer file to the server or insert the Avaya Aura® MS installation DVD into the DVD drive of the server.

3. Change the directory to the location of the downloaded installer or the drive where the Avaya Aura® MS installation DVD is located.

   The name of the installation file is in the following format:

   `MediaServer_10.2.0.`*`build_yyyy.mm.dd`*`.bin`

   For example, `MediaServer_10.2.0.39_2024.09.23.bin`.

4. Apply executable permissions to the installer file:

   ```
   chmod 755 filename
   ```

5. To modify the default Linux® installation directory and other options, use a text editor to create the file `silent_install.properties` with the following content:

   ```
   #Choose Options
   #--------------
   INSTALL_EMLITE_SILENT=y
   LINUX_GROUP=root

   #Choose Install Folder (no spaces)
   #---------------------
   USER_INSTALL_DIR=/opt/avaya
   ```

6. In the **Choose Options** section, you can install the Avaya Aura® MS EM by setting `INSTALL_EMLITE_SILENT=Y` or bypass installation of EM by setting `INSTALL_EMLITE_SILENT=N`.

   Setting `INSTALL_EMLITE_SILENT` to `Y` provides a Web-based management system for Avaya Aura® MS when another management system is not being used.

Set the `LINUX_GROUP` to use for EM login.

Important:

The Linux® group that you specify must contain users who can successfully authenticate against Secure Shell (SSH).

7. In the **Choose Install Folder** section of the file, type a directory name to specify the location to install Avaya Aura® MS. The installation path must not contain spaces.
8. Save the changes and exit the text editor.
9. Run the silent installation from a Linux® shell by entering the following command:

   `./`*`filename`* `-i silent -f` *`location`*`/silent_install.properties`

   Where *filename* is the Avaya Aura® MS installation file with a name similar to `MediaServer_10.2.0.39_2024.09.23.bin` and location is the directory where the `silent_install.properties` file that you want to use is located.

   Tip:

   The installation is complete when the system CPU is idle. You can monitor the system CPU activity using a command like `top` in a Linux® shell.

   Important:

   If any errors occur during the silent mode installation, the system stops the installation and saves the errors to log files in the `/var/log/mas/install` directory. You cannot install Avaya Aura® MS if the system is missing the required packages and if YUM is not enabled. For more information about how to enable YUM, see the Red Hat YUM manual.

Related links

System requirements on page 11

Linux® uninstallation

You can use the following modes to remove Avaya Aura® MS from servers that run the Linux® operating system:

- The interactive command-line mode
- The silent install mode

When you uninstall the media server software, you can retain the system configuration and application content data on the media server. System configuration data includes all the configuration settings configured by administrators using the management system. Application content data includes data stored in the media server Content Store, such as audio prompts, recordings, or user data files.

If you select the preserve data option during the uninstallation process, the data remains on the system. Any subsequent reinstallation of the media server software automatically uses your preserved settings and application data.

Adopting products can automatically uninstall Avaya Aura® MS. The adopting products usually use the silent mode for uninstalling Avaya Aura® MS. The following uninstallation procedures are not necessary if the adopting product uninstalls Avaya Aura® MS.

Uninstalling Avaya Aura® MS from Linux® using the interactive command-line mode

Before you begin

Uninstall any Avaya Aura® MS packaged applications listed on the **EM** > **Applications** > **Packaged Applications** page before you uninstall Avaya Aura® MS.

See the application documentation for the detailed uninstallation procedures. Ensure that you select the preserve application data option, if applicable to your applications.

Important:

You lose all the application data if you do not accept the default option to preserve application data.

Procedure

1. Locate the uninstaller:

   `cd` *`installpath`*`/UninstallMediaServer`

2. To run the uninstaller, type:

   `./UninstallMediaServer`

3. To proceed with the uninstallation process, press `Enter`.
4. Choose what you want to do with the Avaya Aura® MS data:
   a. If you want to preserve system configuration and application content data, type `1` and press `Enter`.
   b. If you do not want to preserve system configuration and application content, type `2` and press `Enter`.

   Important:

   You lose the data if you do not accept the default action to Preserve System Configuration and Application Content data.

5. Read the uninstallation summary to confirm your selections and then press `Enter` to uninstall the media server.

Uninstalling Avaya Aura® MS from Linux® using the silent mode

Before you begin

You must uninstall any Avaya Aura® MS packaged applications listed under **EM** > **Applications** > **Packaged Applications** before uninstalling Avaya Aura® MS.

See the application documentation for the detailed uninstallation procedures. Ensure that you select the preserve application data option, if applicable to your applications.

Important:

You lose all the application data if you do not select the option to preserve application data.

Procedure

1. Locate the uninstaller:

   `cd installpath/UninstallMediaServer`

2. To run the silent uninstaller, enter one of the following commands.

   Important:

   You lose all the data if you add the option `-DREMOVE_USER_DATA=1` and if you do not use the default action to preserve system configuration and application content data.

   To preserve data, type the following command:

   ```
   ./UninstallMediaServer -i silent
   ```

   To remove data, type the following command:

   ```
   ./UninstallMediaServer -i silent -DREMOVE_USER_DATA=1
   ```

   As the uninstallation process is in the silent mode, you do not see anything on the screen after this point.

   Wait for the uninstallation process to complete.

   Tip:

   The uninstallation is complete when the system CPU is idle. You can monitor the system CPU activity using a command like `top` in a Linux® shell.

Changing the default software ports

About this task

Perform the following procedure to reassign the ports that Avaya Aura® MS uses.

Procedure

1. Perform the following steps to change the default ports for Avaya Aura® MS components:
   a. Navigate to **EM** > **System Configuration** > **Network Settings** > **Advanced Settings** > **Port Assignments**.
   b. Change the required port values.
   c. Click **Save**.
   d. Click **Confirm**.
2. To change the default ports that Avaya Aura® MS EM uses, edit the HTTP and HTTPS connector port values in the following file:
   - Linux®: `installpath/ma/apache-tomcat/conf/server.xml`

   Important:

   The `redirectPort` value for the HTTP connector must match the `Connector port` of the HTTPS connector.
3. Restart the server.

Chapter 6: 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. 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. The **-h** option includes the detailed history of the patch on the current system.
amspatch apply patchname [-v]	Applies the specified patch to the system. Apply patches in numerical order. You can specify all as the patch name to apply all available patches. The **-v** 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. Remove patches in reverse numerical order. The **-v** 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-10.2.0.39-0001` before you install `QFE-platform-10.2.0.39-0002`

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 clustersManaging QFEs for N+1 load sharing clusters on page 35.
- 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 clustersManaging QFEs for 1+1 High Availability clusters on page 34.
- Ensure that the QFE is downloaded to the target server, and that the QFE file is in the QFE directory of the Avaya Aura® MS installation:
  - Linux®:

    `installpath/ma/MAS/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 **Stop**.
5. Click **Confirm**.
6. Open a Linux® shell.
7. On Linux®, change to root user by running the following command:

   ```
   su –
   ```
8. 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.

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

   `amspatch apply patchname`

   To apply all available patches, enter the following command:

   `amspatch apply all`

10. Press `y` to continue.
11. After the patch application is complete, open EM and navigate to **EM** > **Tools** > **Manage Software** > **Inventory**.
12. Verify whether the patch version listed in the **Patch Level** column is correct.
13. **(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**.
14. Unlock Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and select **More Actions** > **Unlock**.
15. Click **Confirm**.
16. 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 N+1 load sharing clusters on page 35
Managing QFEs for 1+1 High Availability clusters on page 34

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-10.2.0.39-0001` and `QFE-platform-10.2.0.39-0002` are both installed on your system, you must remove `QFE-platform-10.2.0.39-0002` before you remove `QFE-platform-10.2.0.39-0001`

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.

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.

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 **Stop**.
5. Click **Confirm**.
6. Open a Linux® shell on Avaya Aura® MS.
7. On Linux®, change to root user by running the following command:

   ```
   su –
   ```

8. 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.
9. Enter the following command:

   ```
   amspatch remove patchname
   ```

10. After the patch removal is complete, open the EM and navigate to **EM** > **Tools** > **Manage Software** > **Inventory**.

11. Verify that the patch version listed in the **Patch Level** column is correct.
12. Start Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and selecting **More Actions** > **Start**.
13. Click **Confirm**.
14. Unlock Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and select **More Actions** > **Unlock**.
15. Click **Confirm**.
16. 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 34
Managing QFEs for N+1 load sharing clusters on page 35

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 30
Removing a QFE patch on page 32

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 30
Removing a QFE patch on page 32

Chapter 7: Service packs

Installing a service pack

About this task

To update Avaya Aura® MS to the latest software, you must install service packs on the system.

Service pack updates are fully automated and preserve all the system configuration and application content data.

Perform service pack installations during scheduled maintenance times.

Use the following procedure to update your existing 10.2 system to the latest 10.2 software release.

Note:

Some steps in the following procedure are specific to Avaya Aura® MS EM. If you are using a different management system, your actions will be different for those steps.

Before you begin

Ensure that you:

- Download the service pack installer for the Avaya Aura® Media Server application from Avaya Product Licensing and Delivery System (Avaya PLDS).
- Back up the system.

  In case of unforeseen problems during the update installation, you can use the backup to restore the system to the previous configuration.
- Apply the service pack 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 service packs for N+1 load sharing clusters.
- Apply the service pack to 1+1 High Availability clusters by applying the service pack to the standby server first and then applying the service pack to the other server. See, Managing QFEs for 1+1 High Availability clusters.

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 click **Stop**.
5. Click **Confirm**.
6. Transfer the service pack installer to the server.
7. As a Linux® root user, navigate the file system to locate the service pack installer and run the installer as follows:

   - Linux®:

     ```
     ./MediaServer_10.2.0.39_2024.09.23.bin
     ```

   Tip:

   You can use GUI, command-line, or the silent installer mode for the upgrade. For more information about the procedures for the different modes, see the installation section.

8. When the system displays the update summary, select the option to install the update.
9. Follow the prompts to complete the installation.
10. **(Optional)** Update each application by running the installation for each application.

    For application update procedures, see application documentation.

11. After the update completes, verify that the required software is installed. To verify, navigate to **EM** > **Tools** > **Manage Software** > **Inventory**.
12. Start Avaya Aura® MSby navigating to **EM** > **System Status** > **Element Status** and click **Start**.
13. Click **Confirm**.
14. Select **EM** > **System Status** > **Element Status** > **More Actions** > **Unlock**.
15. Click **Confirm**.
16. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

Related links

Linux installation on page 22
Managing service packs for N+1 load sharing clusters on page 42
Managing QFEs for 1+1 High Availability clusters on page 34

Removing a service pack

About this task

The service pack removal procedure downgrades your software to the previous software version.

If you follow this procedure, do not have to reconfigure or reprovision the system. All system configuration and application data is preserved.

Remove service packs during scheduled maintenance times.

Perform the following procedure to remove an installed service pack from your system:

Note:

Some of the steps in this procedure are specific to the Avaya Aura® MS EM. If you are using a different management system, your actions will be different for those steps.

Before you begin

Before proceeding with the software removal, ensure that you:

- Obtain the installer for the earlier software release. When uninstalling and preserving data to remove a service pack, you can only go back to the previously installed software version. You cannot install a version older than the software previously installed because the data is not compatible.
- Back up your system.

  In case of unforeseen problems during the downgrade, you can use the backup to restore your system to the previous configuration.
- Remove service packs one node at a time in a cluster configuration. The other nodes in the cluster maintain service.
- Remove the service pack from the standby server first and then remove the service pack from the active server when upgrading High Availability server pairs.

Procedure

1. Prevent new sessions from starting on the system by navigating to **EM** > **System Status** > **Element Status** > **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 the sessions, stop Avaya Aura® MS by navigating to**EM** > **System Status** > **Element Status**and clicking **Stop**.

5. Click **Confirm**.
6. Before uninstalling Avaya Aura® MS, you must uninstall Avaya Aura® MS packaged applications that are listed under**EM** > **Applications** > **Packaged Applications**.

   See the application documentation for the detailed uninstallation procedures.

   Ensure that you select the preserve data option, if applicable to your applications.

   Important:

   You lose all the data if you do not accept the default action to preserve application data.
7. Uninstall the current Avaya Aura® MS installation but ensure that you select the option to preserve system configuration and application content data.

   Important:

   You lose all the data if you do not accept the default action to preserve system configuration and application content data.
8. Uninstall the media server software by using the following command:
   - Linux®:

     In a Linux® shell type:

     ```
     installpath/UninstallMediaServer/UninstallMediaServer
     ```
9. If the system prompts for restart, then restart the system after the uninstallation process is complete. .
10. As a Linux® root user, navigate the file system to locate the installer and run the installer as follows:
    - Linux®: `./MediaServer_10.2.0.39_2024.09.23.bin`

    The installer automatically detects the preserved configuration and application content data. Therefore, the system does not prompt you to choose an installation location or to reselect any other options. The installer uses the original location and selections.
11. Follow the prompts to exit the installer.
12. Install each application by running the installation for each application.

    For application installation procedures, see application documentation.
13. Open EM and navigate to **EM** > **Tools** > **Manage Software** > **Inventory**.
14. Verify whether the software versions listed are correct.
15. If at any time the system prompted you for a restart but you deferred the restart, restart your system now.
16. After the system restarts, open **EM**.
17. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

Related links

Linux installation on page 22

Managing service packs for 1+1 High Availability clusters

About this task

When working with service packs on High Availability clusters, perform the service pack installation or removal procedures in the following order to maintain service: Apply or remove the service pack for the standby server first. Then after activating the updated standby server, apply or remove the service pack for the active server.

Perform the following procedure to apply or remove service packs for 1+1 High Availability clusters:

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 service pack for the standby server, start from Step 6 of the Installing a service pack procedure or the Removing a service pack procedure.

   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 service pack for the standby server, start from Step 6 of the Installing a service pack procedure or the Removing a service pack procedure.

    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 service pack on page 37
Removing a service pack on page 39

Managing service packs for N+1 load sharing clusters

About this task

For N+1 load sharing clusters, apply or remove service packs on 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.

Perform the following procedure to apply or remove service packs for servers in a cluster:

Procedure

1. For the Primary server, follow the procedure to install or remove a service pack.

   Wait for any alarms to clear as the server returns to service after installing or removing the service pack.

2. For the Secondary server, follow the procedure to install or remove a service pack.

   Wait for any alarms to clear as the server returns to service after installing or removing the service pack.

3. For each Standard server, follow the procedure to install or remove a service pack.

   Wait for any alarms to clear as the server returns to service after installing or removing the service pack.

Related links

Installing a service pack on page 37
Removing a service pack on page 39

Chapter 8: Upgrade from a previous release

Upgrade overview

You can upgrade a system from Avaya Aura® MS 8.0.x or 10.1.0 to the latest Avaya Aura® MS 10.2 and preserve the configuration and application data.

Upgrade to Avaya Aura® MS 10.2 by running the installer on the system. The installer automatically preserves system configuration data and application data. It removes the old media server and installs the new software release

If you are replacing the operating system, additional steps are necessary to preserve the media server configuration and application data. These steps should be performed while you are re-imaging the disk to replace the operating system.

Perform upgrades only during the maintenance window or during non-peak usage time.

The upgrade procedures set the operational state to Pending Lock. The purpose of placing Avaya Aura® MS 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, then 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.

Note:

Note that Avaya Aura® MS 10.2 only supports Red Hat 8.x and requires 8.6 or higher. If your server is currently on Red Hat 7.x, then you must update the Red Hat release prior to upgrading to Avaya Aura® MS 10.2. It is recommended that you deploy a new Red Hat 8 server with the same network configuration and follow the Upgrading manually on page 48 procedure.

Simplex media server upgrade overview

A standalone media server that is not part of a cluster is referred to as a simplex media server.

A simplex media server is upgraded as follows:

- Back up the server data.

- End active sessions by setting the server through a progression of Pending Lock, Lock, and Stopped states.
- Uninstall media server applications.
- Perform either the automatic or manual upgrade procedure.
- Verify the system is functional and that there are no unexpected alarms.
- Back up the new system.

1+1 High Availability cluster upgrade overview

1+1 High Availability clusters can provide continuous access to services during upgrades, when you upgrade one server at a time.

High Availability servers are upgraded as follows:

- Enable **Local High Availability State Lock** on the Active server.
- Upgrade the Standby server by performing the procedure to upgrade a simplex media server.
- Disable the **Local High Availability State Lock** on the Active server and failover to the newly upgraded Standby server.
- Enable **Local High Availability State Lock** on the newly Active server.
- Upgrade the Standby server by performing the procedure to upgrade a simplex media server.
- Disable the **Local High Availability State Lock** on the Active server.

N+1 load sharing cluster upgrade overview

In load sharing media server installations, you can maintain continuous access to the media server services during upgrades, by upgrading one cluster server at a time. Either the Primary or Secondary server must remain in service for the cluster to remain operational. Cluster service is lost if the Primary and Secondary servers are out of service at the same time.

N+1 load sharing clusters of Avaya Aura® MS nodes are upgraded as follows:

- For the Primary server, perform the procedure to upgrade a simplex Avaya Aura® MS.

  Wait for any alarms to clear as the server returns to service after the upgrade.
- For each Standard server, perform the procedure to upgrade a simplex Avaya Aura® MS.

  Wait for any alarms to clear as the server returns to service after the upgrade.
- For the Secondary server, perform the procedure to upgrade a simplex Avaya Aura® MS.

Prerequisites for upgrade

Prior to upgrading to Avaya Aura® MS 10.2:

- Ensure that the current media servers are on 8.0.x or an earlier 10.1.0 release. You can check the installed software version on the EM Home page or by navigating to **EM** > **System Status** > **Element Status** > **Installed Software Packages**
- Ensure that the system meets the minimum hardware requirements. For more information, see the system requirements.
- Ensure that the system meets the minimum software requirements. For more information, see the system requirements.

Related links

System requirements on page 11

Performing a backup

About this task

Before upgrading your system, create a backup of the system configuration and application data for each media server. Following is a basic backup procedure that you can use during the upgrade procedures. For more information about backup and restore, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Tasks**.
2. Create or select an existing backup task which includes System Configuration and Application Content backup types.
3. Click **Run Now**.
4. Monitor the Backup and Restore History Log at **EM** > **Tools** > **Backup and Restore** > **History Log**.

   After the backup is complete, the log shows a completed backup task entry.
5. Ensure that the backup files are saved to their required FTP location or local default destination.

   There is one file for each backup type for a total of two backup files.
6. If you are using a local backup destination and want to install a new operating system, you must move the backup files to a safe location. You can find the local backups in:

   - *installpath*/ma/MAS/platdata/EAM/Backups

Important:

If you are re-imaging the disk or replacing the operating system as part of the upgrade, ensure that you transfer the backup files off the server for safe keeping.

Choose an upgrade procedure

There are two upgrade procedures that are available in order to offer the flexibility required for the upgrade requirements. Use the following information to choose the upgrade procedure that is appropriate for the installation:

- Manual procedure: Is identical to the procedure used for upgrades in previous releases.

  The manual procedure is useful when you need to customize the upgrade procedure or alter the procedure to include additional steps like operating system or hardware upgrade.

  Use the manual upgrade procedure when you need to also upgrade any of the following during the upgrade:

  - Entire server
  - System disk
  - Operating system
- Automated procedure: Automatically runs the same steps as the manual procedure for you with no user interaction.

Upgrading automatically

About this task

Perform the following procedure to upgrade when you run the Avaya Aura® MS 10.2 installer on an existing Avaya Aura® MS an earlier 10.1.0 system. The procedure includes steps to prepare the system for upgrade and to bring the system back in to service as follows:

- Set the server through a progression of Pending Lock, Lock, and Stopped states to take the server out of service for the upgrade.
- Uninstall packaged applications.
- Upgrade to the new software.
- Verify that the system is functional and that there are no unexpected alarms.

Before you begin

- Ensure that the system meets the prerequisites for upgrade. See the upgrade prerequisites earlier in this chapter.
- Create media server backups. Backups are necessary if a rollback to Avaya Aura® MS is required.

- If you are upgrading a server that is member of a cluster, ensure that you are performing the task as part of one of the cluster upgrade procedures before continuing. Ensure that you start at the correct step in the following procedure, if specified by the cluster upgrade procedure.
- If you are not updating the operating system, disk drive, or server hardware, you can use the automated procedure to upgrade the media server without first uninstalling the previous release.

Procedure

1. Prevent new sessions from starting on the system by navigating to **EM** > **System Status** > **Element Status** and selecting **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 the sessions, stop Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and clicking **Stop**.
5. Click **Confirm**.
6. Transfer the Avaya Aura® MS 10.x installer to the server.
7. As a Linux® root user, navigate the file system to locate the installer and run the installer as follows: `./MediaServer_10.2.0.39_2024.09.23.bin`
8. When the system displays the upgrade introduction, select the option to install the upgrade.
9. Read and accept the license agreement.
10. Review the installation summary and select **Install** to start the upgrade.
11. After the upgrade, press **Enter** to exit the installer
12. **(Optional)** Install the latest versions of each required application by running the installer for each application.

    For application installation procedures, see application documentation.
13. Ensure that the required software is installed by navigating to **EM** > **Tools** > **Manage Software** > **Inventory**.
14. Check for any service-impacting alarms and perform an appropriate test for the system. For example, place a call to the application.

Important:

The upgrade process ensures that the system configuration parameters and all application data are 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.

Related links

System requirements on page 11
Linux installation on page 22
System requirements on page 11

Upgrading manually

About this task

Perform the following procedure to upgrade Avaya Aura® MS and update the operating system, disk drive, or server hardware. The procedure includes steps to prepare the system for upgrade and to bring the system back in to service as follows:

- Set the server through a progression of Pending Lock, Lock, and Stopped states to take the server out of service for the upgrade.
- Uninstall packaged applications.
- Uninstall the Avaya Aura® MS software.
- Optionally upgrade the server operating system or hardware.
- Perform a clean installation of the new software.
- Use the Avaya Aura® MS 10.x upgrade tool to restore and upgrade preserved configuration and application data from the previous release.
- Verify that the system is functional and that there are no unexpected alarms.

Before you begin

- Ensure that the system meets the perquisites for upgrade. See the upgrade perquisites earlier in this chapter.
- 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.
- If you are upgrading a server that is member of a cluster, ensure that you are performing the 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 selecting **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 the media server, 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 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 the data will be lost if you do not have backups of your current Avaya Aura® MS 10.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 11.
8. Uninstall the current Avaya Aura® MS installation but do not preserve data. Select the option to remove all data during uninstallation. The backups are used to restore and upgrade the data.

   Use an appropriate uninstallation method for the system. For more information on uninstallation methods, see uninstallation.
9. Use an appropriate installation method to install Avaya Aura® MS 10.2 on the system. For more information on installation methods, see the Installation chapter.
10. After the installation is complete, log in to the new Avaya Aura® MS EM.

    If security alert dialog boxes appear in the browser, accept the new security conditions to proceed.
11. Stop Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and clicking **Stop**.
12. Click **Confirm**.
13. Ensure that the system configuration and application content backup files saved earlier are available on the server.
14. Open a Linux® shell on Avaya Aura® MS.
15. Obtain root access.
16. From the command-line, change to the directory where you have saved the backup files.

17. 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.

18. Press `Y` to stop all Avaya Aura® MS services when prompted.

    The tool upgrades the data.

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

    `amsupgrade AppContentBackupFilename.zip`

20. Press `Y` to stop all Avaya Aura® MS services when prompted.

    The tool upgrades the data.

    Tip:

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

21. **(Optional)** Install the latest versions of each required application by running the installer for each application.

    For application installation procedures, see application documentation.

22. Verify the required software is installed by navigating to **EM** > **Tools** > **Manage Software** > **Inventory**.

23. Start Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and clicking **Start**.

24. Click **Confirm**.

25. 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.

Related links

Linux installation on page 22
System requirements on page 11

Upgrading 1+1 High Availability clusters

About this task

1+1 High Availability clusters can provide continuous access to services during upgrades, when you upgrade one server at a time. You can do this by first upgrading the standby server. After activating the upgraded standby server, then you upgrade the other server.

Procedure

1. Navigate to **EM** > **Element Status** on each server and determine which server has **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 upgrade the standby server, go to Step 6 of the automatic or manual upgrade procedure.

   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 upgrade the standby server, go to Step 6 of the automatic or manual upgrade procedure.

    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

Upgrading automatically on page 46
Upgrading manually on page 48

Upgrading N+1 load sharing clusters

About this task

Load sharing media server clusters can provide continuous access to services during upgrades when you upgrade one server at a time.

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

Use the following procedure to upgrade N+1 load sharing clusters:

Procedure

1. For the Primary server, perform the automatic or manual Avaya MS 7.8 upgrade procedure.

   Wait for any alarms to clear as the server returns to service after the upgrade.

2. For each Standard server, perform the automatic or manual Avaya MS 7.8 upgrade procedure.

   Wait for any alarms to clear as the server returns to service after the upgrade.

3. For the Secondary server, perform the automatic or manual Avaya MS 7.8 upgrade procedure.
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.

Related links

Upgrading automatically on page 46
Upgrading manually on page 48

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 Aura® 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.

To roll back to Avaya Aura® MS 8.0.x or earlier 10.1.0 requires a complete uninstall of Avaya Aura® MS 10.2 and reinstall of the previous release. Avaya Aura® MS backups are used to restore the system configuration and application data. Therefore, all configuration settings and application data are rolled back to the state of the previous installation.

To roll back a multi-server cluster, perform the following procedure on each server one at a time. When you roll back the servers one at a time, the other servers in the cluster can provide service. It is recommended that you roll back the Primary node first and then follow with the Secondary node and standard nodes, if any.

Important:

Either the Primary or Secondary server must remain in service for the cluster to remain operational. Cluster service is lost if the Primary and Secondary servers are out of service at the same time.

Perform the following procedure to roll back Avaya Aura® MS 10.2 to a previous version of Avaya Aura® MS.

Procedure

1. Uninstall Avaya Aura® MS 10.2 and ensure that you select the option to remove all data.

   Use an appropriate uninstallation method for the system. For more information on uninstallation methods, see uninstallation.

2. Install the previous Avaya Aura® MS release.

   Use an appropriate installation method for the system. For more information on installation methods for Avaya Aura® MS, see *Installing, Upgrading, and Patching Avaya Aura® MS*.

3. Restore system configuration and application data using Avaya Aura® MS backup files from the previous installation. You cannot restore Avaya Aura® MS 10.2 backup files to an Avaya Aura® MS 8.0.x or 10.1.0 system.

Use an appropriate restore method for the system. For more information on restore methods for Avaya Aura® MS, see *Installing, Upgrading, and Patching Avaya Aura® MS*.

Related links

Linux installation on page 22

Chapter 9: Server replacement

Replacing Avaya Aura® MS hardware

About this task

Avaya Aura® MS data is installation specific. The information saved in backup files contains pathnames, node UUIDs, hostnames, and IP addresses. The Avaya Aura® MS backup files are used in the process of replacing or rebuilding a server, but the new server must be configured to work with the existing data.

Perform the following procedure to replace failed server hardware or move an existing Avaya Aura® MS installation to a new server with the same address.

Before you begin

- Ensure that you have Avaya Aura® MS backups of the server you are replacing. If the server being replaced has failed, obtain the most recent backups available.
- If you are using node-locked licensing, ensure that you have licenses for the new server.

Procedure

1. Determine the following information about the server being replaced:
   - IP address
   - Hostname
2. Decommission the old server so that there are no hostname or IP address network conflicts with the new server.
3. Using the information from Step 1, complete the system requirement and preparation procedures and any restarts that the system preparation procedures require. For more information, see system requirements.
4. Use an appropriate installation method to install Avaya Aura® MS on the new system. For more information on installation methods, see the *Installation* chapter.
5. Restore the backup files to the new system. See restore in *Implementing and Administering Avaya Aura® Media Server*.
6. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

Related links

Linux installation on page 22
System requirements on page 11

Moving Avaya Aura® MS data to a new server

About this task

Avaya Aura® MS data is installation specific. The information saved in backup files contains pathnames, node UUIDs, hostnames, and IP addresses. The Avaya Aura® MS backup files are used in the process of moving data to a new server. However, the new server must be configured to work with the existing data and the new IP address and hostname.

All system configuration and application data on the target server is replaced with the data in the backups.

Perform the following procedure to migrate Avaya Aura® MS configuration settings and application data to a new Avaya Aura® MS installation that has a different address.

Before you begin

- Ensure that you have Avaya Aura® MS backups of the data you want to move to another server.
- Complete the system requirement and preparation procedures for the new server. Complete any restarts that the system preparation procedures require. For more information, see system requirements.
- If you are using node-locked licensing, ensure that you have licenses for the new server.

Procedure

1. Determine the following information about the server being replaced:
   - IP address
   - Hostname
2. Determine the following information about the new server:
   - IP address
   - Hostname
3. Complete the system requirement and preparation procedures and any restarts that the system preparation procedures require. For more information, see system requirements.
4. Use an appropriate installation method to install Avaya Aura® MS on the new system. For more information about installation methods, see the *Installation* chapter.
5. Restore the backup files to the new system. See *Implementing and Administering Avaya Aura® Media Server*.
6. On the new system, update the following server specific configuration items. Replace the IP addresses and hostname determined in Step 1 with the IP addresses and hostname from Step 2. For more information on configuring each item see *Implementing and Administering Avaya Aura® Media Server*.
   a. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.
   b. IP Interface Assignment fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.

c. If you are using nodal licensing, navigate to **EM** > **Licensing** > **General Settings** and update the keys field with the new node-locked license.

d. Security certificates with information dependent on FQDN or other server specific information, must be replaced. Update the system with the new certificates by navigating to **EM** > **Security Certificate Management**.

e. 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 and ensure the IP address you just changed is updated on each server.

f. If this 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**.

7. If any of the configuration changes in Step 6 require a system restart or Avaya Aura® MS restart to take effect, perform the restart now.
8. Check for any service-impacting alarms and perform an appropriate test of the system, for example, place a call to the application.

Related links

Linux installation on page 22
System requirements on page 11

Chapter 10: 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		
Avaya Aura® Media Server Overview and Specification	Describes the key features of Media Server	Customers and sales, services, and support personnel
Implementing and administering		
Deploying and Updating Avaya Aura® Media Server Appliance	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
Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS	Install, upgrade, and patch software-only version of Avaya Aura® Media Server on customer provided hardware platform.	System administrators, implementation engineers, and support personnel
Implementing and Administering Avaya Aura® Media Server	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		
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Prepare the iDRAC for remote access and SNMP trap reporting.	System administrators, and implementation engineers
Installing the Avaya Solutions Platform 130 Series 6.0.x- Only Section *Dell R640 SNMP trap configuration using iDRAC9*	Configure the physical appliance iDRAC9 SNMP traps.	System administrators, and implementation engineers

Related links

Finding documents on the Avaya Support website on page 59
Accessing the port matrix document on page 59
Avaya Documentation Center navigation on page 60

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 58

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 58

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 58

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 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 62

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 62

Appendix A: Creating RHEL virtual machine on Nutanix

Uploading the RHEL ISO to Nutanix server

About this task

You can install RHEL on Nutanix 6.5 and later, after uploading the standard RHEL ISO image on the Nutanix server.

Note:

The RHEL ISO must be customer-provided. Avaya is not responsible for the RHEL ISO image.

Procedure

1. Log in to Nutanix server using Nutanix Prism web console.
2. Navigate to **Home** > **Settings** > **Image Configuration**.
3. In the **Image Configuration** screen, click **Upload Image**.

   Nutanix Prism web console displays the **Create Image** window.
4. In the **Name** field, enter a name for the image.
5. In the **Image Type** field, select the ISO image to upload.
6. In the **Storage Container** field, select the required option.
7. Under **Image Source** field, either browse for the ISO image through URL or upload the image file if stored in your local machine.
8. Click **Save**.

   You can view the image upload status from the drop-down list on top of the **Home** page.

Next steps

Installing RHEL on Nutanix 6.5 and later.

Installing RHEL on the Nutanix server

Before you begin

- Upload the RHEL image on Nutanix 6.5 and later.
- Log in to Nutanix 6.5 server using the Nutanix Prism web console.

Procedure

1. Navigate to **Home** > **VM**.
2. In the **VM** page, click **Create VM**.
3. In the **Create VM** window under **General Configurations**, enter appropriate values in the **Name**, **Description**, and **Timezone** fields.
4. In the **vCPUs** field under **Compute Details**, enter the number of CPUs required for the application.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.
7. Under **Boot Configuration**, select **UEFI**.
8. Under **Disks**, click the Edit icon for the CD-ROM disk type, and do the following:
   a. In the **Type** field, ensure **CD-ROM** is displayed.
   b. In the **Operation** field, select **Clone from Image Service**.
   c. In the **Bus Type** field, Avaya recommends selecting **IDE**.
   d. In the **Image** field, select the RHEL ISO Image.
   e. Click **Update**.

   The CD-ROM and the disk size are displayed.
9. Click **Add New Disk** next to **Disks**, and do the following:
   a. In the **Type** field, select Disk.
   b. In the **Operations** field, select **Allocate on Storage Container**.
   c. In the **Bus Type** field, select the same bus type which you selected while updating the disk.
   d. In the **Storage Container** field, select the appropriate storage container.
   e. In the **Size** field, enter the required GiB size.
   f. Click **Add**.
10. Under **Network Adapters (NIC)**, do the following:
    a. Click **Add New NIC** to add a Network Interface Card (NIC).
    b. In the **Create NIC** window, select the **Subnet Name**.

c. In the **Network Connection State** field, select **Connected**.

d. Click **Add**.

e. To add multiple NICs, repeat 10.a to 10.d.

11. Under **VM Host Affinity**, click **Set Affinity** and do the following:

    a. In the **Set VM Host Affinity** window, select the hosts.

       Select multiple hosts to ensure one node (virtual machine) runs in case another node fails.

    b. Click **Save**.

    After the successful creation of virtual machine, virtual machine appears in the VM page.

12. Select the newly created VM and click **Power On**.
13. Click **Launch Console**.

    Note:

    The **Launch Console** button is enabled only when the virtual machine is Powered On.

    After the RHEL boots, Red Hat Enterprise Linux 8.10 welcome screen appears.

14. Click **Continue**.
15. In the **Installation Summary** screen, under **LOCALIZATION**, click **Language Support** to select the supported language.
16. Click **Time & Date** to set the required timezone.
17. Under **SOFTWARE**, click **Software Selection**.
18. Select **Minimal Install** and then click **Done**.
19. Under **SYSTEM**, click **Installation Destination** and do the following:

    a. Under **Storage Configuration**, select the **Custom** radio button and click **Done**.

    b. In the **Manual Partitioning** window, set the partitioning as required.

    c. Click the **+** icon to create a new mount point.

    d. Select the available partition from the **Mount Point** drop-down menu. To add custom partitions, type the required partition name. For eg:`/etc/opt/defty`.

    e. Enter the capacity in GiB in the **Desired Capacity** field and then click **Add Mount Point**.

    f. In the **Manual Partitioning** window, click **Done**.

    g. In the **Summary of Changes** window, click **Accept Changes**.

    h. Click **Done**.

20. Click **Network & Host Name** and do the following:
    a. Enter a name in the **Host Name** field and click **Apply**.
    b. To configure the IP, click **Configure**.
    c. Click **IPV4 Settings** and select the required option from the **Method** drop-down menu.
    d. Click **Done**.
21. Under **USER SETTINGS**, click **Root Password**.

    In the **Root Password** window, set a password for the root user and then click **Done**.
22. Click **User Creation** and in the Create User window, enter the details and click **Done**.
23. Click **Begin Installation**.

    The RHEL virtual machine is installed on the Nutanix 6.5 server and later.
24. Click **Reboot System** to reboot the RHEL virtual machine.

Index

Numerics

A

C

D

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W