Upgrading Avaya Aura® Application Enablement Services

Release 10.2.x
Issue 10
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.

Licenses

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

Copyright

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

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.

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.

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

This document describes the procedures for upgrading Avaya Aura® Application Enablement Services from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x on:

- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640
- VMware in customer-provided Virtualized Environment
- Avaya Solutions Platform 130 Release 6.0 (Avaya supplied Kernel-Based Virtual Machine on Red Hat Enterprise Linux R8.10) environment.
- Amazon Web Services (AWS), Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS) in Software-only environment
- Customer provided Software-only environment

Note:

7.1.3.x version is only supported in the transient period when upgrading the Avaya Aura® solution.

This document:

- Includes upgrade checklists and maintenance procedures.
- Does not include optional or customized aspects of a configuration.

The primary audience for this guide is anyone who is involved with upgrading and verifying Application Enablement Services.

Prerequisites

Before upgrading the Avaya Aura® application, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Avaya Solutions Platform
- **For VMware:** VMware® vSphere™ virtualized environment.
- **For KVM:** On RHEL 8.10 virtualized environment.

- **For Amazon Web Services(AWS):** AWS environment.
- **For Google Cloud:** Google Cloud environment.
- **For Azure:** Microsoft Azure environment.
- **For IBM Cloud:** IBM Cloud for VMware Solutions environment
- Linux® Operating System.
- System Manager.
- WebLM

Skills

To administer:

- Solution Deployment Manager.
- VMware® vSphere™ virtualized environment.
- AWS Management Console.
- Google Cloud.
- Microsoft Azure.
- IBM Cloud for VMware Solutions.

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

Changes to platform support

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

Discontinued Platforms:

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

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

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

Change history

Issue	Date	Summary of changes
10	March 2026	Added the section: Changes to platform support on page 8
9	February 2026	Updated the following sections: • Supported servers on page 18 • Supported servers for Avaya Aura applications on page 18 • Software requirements on page 21 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 23 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 148 • Calculating space for the clone on page 151 • Validating a Virtual Machine Backup (clone) on page 153
8	October 2025	Updated the following sections: • Upgrade sequence for Avaya components on page 24 • Optional Upgrade Sequence for Avaya components on page 31
7	August 2025	Updated the following sections: • Upgrade sequence for Avaya components on page 24 • Optional Upgrade Sequence for Avaya components on page 31
6	April 2025	Updated the following section for Release 10.2.1.1: Supported ESXi version on page 21

Table continues…

Issue	Date	Summary of changes
5	December 2024	Added the following sections for Release 10.2.1: • Optional Upgrade Sequence on page 26 • Verify the software version of the Survivable Remote Servers on page 30 • Optional Upgrade Sequence for Avaya components on page 31 • Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based Virtual Machines on page 158 • AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10) on page 37 • Migrating Application Enablement Services from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 70 • Obtaining existing VMware details on page 71 • Obtaining encryption status on page 72 • Obtaining existing network details on page 72 • Checking FIPS status on page 73 • Enabling secure boot on page 73 • Backing up Application Enablement Services on page 74 • Shutting down WebLM virtual machine on VMware on page 74 • Restoring Application Enablement Services using the web console on page 74 • Restoring Application Enablement Services using the command line interface on page 75 • Checking the connection between Communication Manager and Application Enablement Services on page 76 • Verifying that services are online on page 76 • Making test calls using TSAPI and JTAPI on page 77 • Testing DMCC configuration on page 77 • Sending test messages on page 78 • Virtual Machine Backups (clone) as an alternative to snapshots on page 148 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 148 • Validating a Virtual Machine Backup (clone) on page 153 • Rolling back using the Virtual Machine Backup (clone) on page 155

Table continues…

Issue	Date	Summary of changes
		Updated the following sections for Release 10.2.1: • Purpose on page 7 • Prerequisites on page 7 • Supported servers on page 18 • Supported servers for Avaya Aura applications on page 18 • Adding a software-only platform on page 50. • Upgrade checklist for Software-Only environment on page 108 • Prerequisites for an upgrade or update to AE Services on page 109 • Installing the Red Hat Enterprise Linux software for AE Services on page 110 • Upgrading the Red Hat Enterprise Linux software on page 113
4	April 2024	Updated the AE Services resource requirements and the supported footprints on VMware on page 35 section.
3	March 2024	Added the Avaya Aura Security Service Packs overview on page 146 section.
2	February 2024	Updated the Upgrade sequence for Avaya components on page 24 section.
1	December 2023	Release 10.2.x.

Chapter 2: Upgrade overview and considerations

Application Enablement Services upgrade overview

You can use System Manager Solution Deployment Manager, the centralized upgrade solution, to upgrade Application Enablement Services.

With Solution Deployment Manager, you can upgrade Application Enablement Services from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x OVA.

Note:

7.1.3.x version is only supported in the transient period when upgrading the Avaya Aura® solution.

Before upgrading Application Enablement Services to Release 10.2, Avaya recommends that the older Application Enablement Services Release version must be on the latest version of its releases. The latest version for Release 7.1.x, 8.0.x, 8.1.x, and 10.1.x are Release 7.1.3.8, 8.0.1.2, 8.1.3.8, and 10.1.3.1 respectively.

If you are upgrading to Release 10.1 or later, the certificate hostname validation is enabled automatically for an external WebLM server and for all Communication Manager connections.

After the **Enable Certificate Hostname Validation** field is enabled, AE Services verifies the certificate identity in the **Subject Common Name (CN)** or **Subject Alternate Name (SAN)** field of the certificate for the external WebLM server and Communication Manager connections.

If the certificate identity matches with the FQDN/IP address of the WebLM server or with the Communication Manager , then the connection with the external WebLM server and Communication Manager is established, otherwise the connection is dropped.

The server identity certificate must have the following values to establish a secure connection with the WebLM server:

- **Key Usage**: Digital Signature, Key encipherment
- **Extended Key Usage**: id-kp-clientAuth, id-kp-serverAuth

Note:

Extended Key Usage is an optional field, it must have the mentioned values only if it is present in the certificate configuration.

The connection will be dropped if the certificate does not meet the above criteria.

If the connection is dropped after the upgrade, do one of the following to re-establish the connection:

- Disable **Enable Certificate Hostname Validation** field. For more information, see *Administering Avaya Aura® Application Enablement Services*.
- Add IP address in **Subject Alternate Name** field of the identity certificate of Communication Manager or external WebLM server. For more information, see Communication Manager or System Manager and WebLM documentation.
- Use a resolvable FQDN present in the **Subject Alternate Name** field of the WebLM server or Communication Manager identity certificate. If DNS is not available, add the FQDN to IP address mapping for the host files on AE Services server.

For more information, see PSN020518u on Avaya support site at https://support.avaya.com.

Note:

To upgrade Application Enablement Services by using Solution Deployment Manager, you must have System Manager.

Supported upgrade paths for Application Enablement Services

The following table displays all the upgrade paths from earlier releases to Release 10.2.x.

Note:

- Before starting the application upgrade, upgrade the platform and hypervisor.
- To upgrade AE Services using Solution Deployment Manager, upgrade System Manager. To upgrade System Manager, use Solution Deployment Manager Client. To upgrade AE Services, use System Manager Solution Deployment Manager.
- Upgrade or migration using Solution Deployment Manager is only supported with the same IP address of the application in a Software-only environment.

  A Software-only upgrade is supported for VMware, KVM, RHVH, OpenStack, Hyper-V, Amazon Web Services, Google Cloud, and Microsoft Azure.

Note:

- 7.1.3.x version is only supported in the transient period when upgrading the Avaya Aura® solution.
- For information about terms used in this table, see “Glossary”.

From offer	From Release	To Software-only (VMware, KVM, RHVH, OpenStack, Hyper-V, AWS, Google Cloud, or Azure) 10.2 (ISO)	To ASP 130 (OVA)/VMware 10.2 (OVA)
AVP	7.1.x	Migration using AES web console	Migration using AES web console
	8.0.x	Migration using AES web console	Migration using AES web console
	8.1.x	Migration using AES web console	Fully automated upgrade using SDM
VMware	7.1.x	Migration using AES web console	Fully automated upgrade using SDM
	8.0.x	Migration using AES web console	Migration using AES web console
	8.1.x	Migration using AES web console	Fully automated upgrade using SDM
	10.1.x	Migration using AES web console	Fully automated upgrade using SDM
Software-only	7.1.x	Migration using AES web console	Migration using AES web console
	8.0.x or 8.1.x	Migration using AES web console	Migration using AES web console
	10.1.x	Migration using AES web console	Migration using AES web console
KVM/OpenStack/RHVH (OVA)	7.1.x	Migration using AES web console	Migration using AES web console
	8.0.x or 8.1.x	Migration using AES web console	Migration using AES web console
AWS/GCP/AZURE (ISO)	7.1.x	Migration using AES web console	NA
	8.0.x or 8.1.x	Migration using AES web console	NA
	10.1.x	Migration using AES web console	NA

Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- Avaya WebLM
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Session Border Controller Release 8.0 and later
- Avaya Breeze® platform Release 3.3 and later
- Avaya Aura® Media Server

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Note:

When an application is deployed on a KVM host, Solution Deployment Manager does not support that application.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Hardware-based Session Manager
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- Session Manager Release 7.1.3.x and later
- Communication Manager Release 7.x and later
- Branch Session Manager Release 7.x and later

- Application Enablement Services Release 7.x and later
- Avaya Breeze® platform Release 3.3 and later
- System Manager Release 7.1.3.x and later (using SDM client only)
- WebLM Release 7.x and later

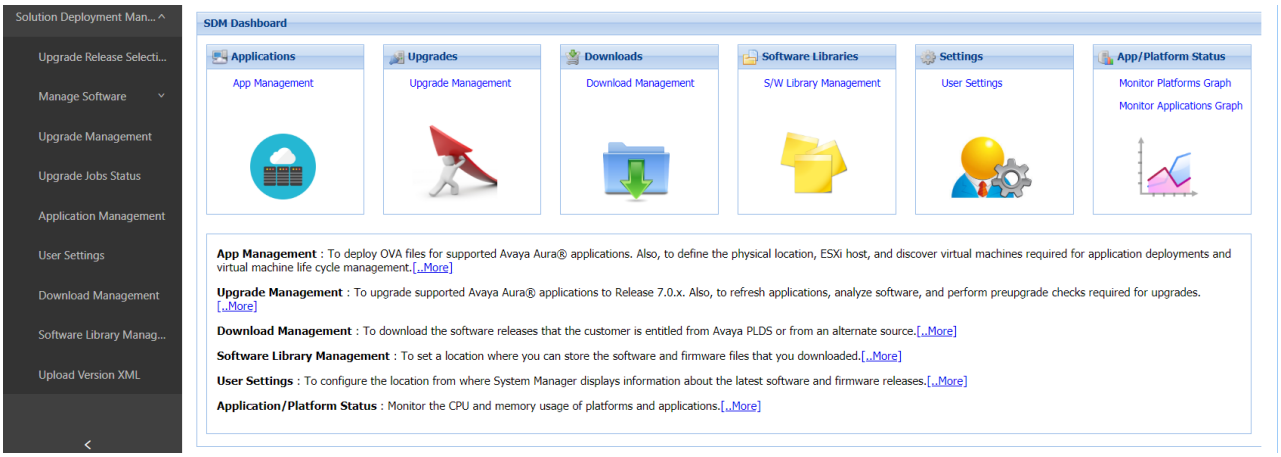
Note:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 10.2.x. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can access the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.x Onwards** or **6.3.8** as the target upgrade. **Release 7.x Onwards** is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
  - Generate the platform Kickstart file for the following Appliance Virtualization Platform or Avaya Solutions Platform platforms:
    - Appliance Virtualization Platform 8.0.x
    - Appliance Virtualization Platform 8.1.x

    - Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1
- **Upgrade Management**: To upgrade Avaya Aura® applications to Release 10.2.x.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the application-specific `version.xml` file to perform upgrades.

Chapter 3: Planning and preconfiguration

Communication Manager and media server requirements

To use AE Services 10.2.x, you must have the Communication Manager Release 7.1.3.x, 8.0.x, 8.1.x, 10.1.x, or 10.2 software.

Note:

Communication Manager 6.3.x or later provides link bounce resiliency for the Application Enablement Protocol (AEP) transport links that AE Services uses.

- AE Services supports all media servers and gateways that support Communication Manager Release 7.1.3.x, 8.0.x, 8.1.x, 10.1.x, or 10.2.
- AE Services 7.1.3 and later supports both, Control Local Area Network (CLAN) interfaces and Processor Ethernet connections when implementing Survivable Core Server (Enterprise Survivable Server) and Survivable Remote Server (Local Survivable Processor) configurations.

Supported servers

The following servers are supported for deployments and upgrades to Release 10.2.x and later:

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

For fresh installations, use Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

Supported servers for Avaya Aura® applications

The following table lists the Avaya sourced supported servers for the Avaya Aura® applications:

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y

Table continues…

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660xs [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.1/6.x
Avaya Solutions Platform S8300 [4]	N	N	N	Y Release 5.1	Y Release 5.1/6.x

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 6.x. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 6.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

Avaya Solutions Platform 130 Appliance 5.1.x uses VMware vSphere ESXi software to support virtualization. Avaya Solutions Platform 130 Appliance 6.x uses KVM on RHEL software to support virtualization.

[4] Avaya Solutions Platform S8300 5.1.x supports virtualization using VMware vSphere ESXi foundation license for Communication Manager and Branch Session Manager. Avaya Solutions Platform S8300 6.x supports virtualization using KVM on RHEL 8.10 software.

Avaya Solutions Platform 130 Appliance R4/5 uses VMware vSphere ESXi Standard License to support virtualization

Note:

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 6.0.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

With the introduction of Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), you no longer need a specific license key as was the case with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Supported hardware for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see the Broadcom website (formerly VMware).

Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x and Avaya Solutions Platform S8300 Release 6.0.x.

Software requirements

Avaya Aura® supports the following software versions:

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

  Note:

  Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 7.0 or 8.0
  - VMware® vCenter Server 7.0 or 8.0

  To view compatibility with other solution releases, see Broadcom website (formerly VMware) and search for VMware Product Interoperability Matrix.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.

Note:

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

  For more information about upgrading from RHEL 8.4 to RHEL 8.10, see *Upgrading Avaya Aura® Application Enablement Services*

Supported ESXi version

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

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N

Table continues…

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

Note:

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

  Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).
- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

Supported ASP R6.0.x (KVM on RHEL 8.10) version

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

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Y	Y

Note:

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell R660xs or Dell R640. The Dell R660xs only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.
- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660xs server only supports KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660xs, S8300E) is a single host server with preinstalled KVM on RHEL R8.10 software.
- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support website at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you must download and install any updates or patches.

Upgrade sequence for Avaya components

Upgrade Avaya components and solution in the following sequence. If any of the Avaya components are not part of your solution, you can skip that particular component and move to the next component.

Disclaimer on Upgrade Sequence Flexibility

While Avaya recommends following the documented upgrade sequence to maintain solution stability and validated integration, the sequence allows flexibility in specific scenarios. Avaya supports component versions that may be ahead or behind others in the upgrade path, provided they are documented in the Product Compatibility Matrix published on the Avaya Support site. Customers may upgrade individual components out of sequence where such configurations are certified to be interoperable.

Refer to the Product Compatibility Matrix before performing any upgrades out of sequence.

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

If you are using ASP130/S8300 5.0 or earlier, you *must* first upgrade to ASP130/S8300 5.1 or 6.0 before upgrading to Avaya Aura® Release 10.2.x.

To upgrade the Avaya Aura® applications to Release 10.2.x, upgrade the hypervisor to a supported version.

For information about the supported ESXi version, see Supported ESXi version on page 21.

For information about the supported KVM version, see Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 23.

With Aura® R10.2.x, Avaya Messaging R11.0 is compatible. Upgrade Avaya Messaging to R11.0 or later before upgrading Aura® components to R10.2.x.

1. Hard Endpoints- H.323 and SIP
2. Standalone Avaya WebLM.

   Note:

   With Avaya Aura® Release 10.2, WebLM is not available. To upgrade WebLM, use the latest WebLM Release 10.1.3.x. If you upgrade Communication Manager or Application Enablement Services to 10.2 and have a standalone WebLM in the setup, upgrade the standalone WebLM to Release 10.1.3.1 or later. Otherwise, the licensing for Communication Manager and Application Enablement Services will not work.

3. SAL Gateway
4. Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager.

   Starting with 10.2.x, if AAM is managed by System Manager then before upgrading System Manager, clean the AAM data from System Manager.

   In the:

   - Non-Geography Redundancy setup, update standalone System Manager.
   - Geography Redundancy setup, update the primary System Manager.
5. Avaya Aura® Session Manager, Core Session Managers only
6. Avaya Breeze® platform and other Snap-ins
7. Avaya Call Management System
8. Avaya Experience Portal
9. Avaya Oceana®
10. Avaya Aura® Device Services
11. Avaya Aura® Media Server
12. G4XX Media Gateways

    Note:

    To successfully upgrade to Release 43.x, use Gateway 38.21.2 or later. If the gateway runs older loads, the download fails and displays the following message: `Incompatible software image`. To resolve, upgrade to 38.21.2 (G430) / 38.21.3 (G450).
13. Avaya Aura® Branch Session Manager
14. Avaya Aura® Communication Manager Survivable Remote Servers, formerly known as Local Survivable Processors
15. Avaya Aura® Application Enablement Services (AES)
16. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
17. Avaya Aura® Communication Manager Survivable Core Servers, formerly known as Enterprise Survivable Servers
18. Avaya Aura® Communication Manager feature servers and evolution servers

    In a duplex configuration, update the following:

    - Standby Communication Manager server
    - Active Communication Manager server
19. Avaya IP Office™ platform
20. Avaya Messaging, formerly known as Avaya IX™ Messaging and Officelinx

Important:

Avaya Messaging must be upgraded to R11.0 or later before upgrading Aura® components to R10.2.x.

21. Avaya Aura® Web Gateway
22. Workplace Clients

    Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
23. Avaya Session Border Controller (ASBCE)

Note:

- System Manager is an integral part of the Avaya Aura® solution.
- System Manager must be on the same or higher release than the application you are upgrading. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.

  All applications supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for application versions System Manager supports, see Avaya Aura® Release Notes on the Avaya Support website.
- Uninstall the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.

  Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2. Solution Deployment Manager Client cannot be on Release 10.1 or Release 8.1.

For information about upgrading the application, see the application-specific upgrade guide on the Avaya Support website.

Optional Upgrade Sequence

With the Optional Upgrade Sequence feature, you can upgrade your core Communication Manager before upgrading your Survivable Remote Servers, formerly known as Local Survivable Processors (LSP). This sequence of upgrading has a limitation of configurations not synchronizing between the upgraded core Communication Manager and yet-to-be-upgraded Survivable Remote servers (LSP).

Caution:

Ensure that you read the Limitations of Optional Upgrade Sequence on page 30 before implementing this upgrade sequence.

Note:

The Optional Upgrade Sequence feature does not apply to Survivable Core Server (SCS), formerly known as Enterprise Survivable Server (ESS). Always upgrade Survivable Core Server (ESS) before the core Communication Manager.

If you are using Avaya Solutions Platform (ASP) 130/S8300, ensure that the Optional Upgrade Sequence is feasible for your setup. To verify the feasibility, review the latest ASP documentation for compatibility of Communication Manager release with the underlying Avaya Solutions Platform hypervisor release.

With the Optional Upgrade Sequence feature, you can have your core Communication Manager and Survivable Remote Servers (LSP) in different compatible versions.

- Supported versions of Core Communication Manager: Release 10.1.3.3 and later versions, Release10.2.1 and later versions.
- Supported versions of Survivable Remote Servers (LSP): Release 8.1.3.x, Release 10.1.x.

Traditionally, the existing upgrade sequence requires that all the Survivable Remote Servers (LSP) are upgraded before the core Communication Manager. In environments with a large number of survivable remote sites, the upgrade of the core Communication Manager has to wait until the end of the Communication Manager upgrade to use the latest features and fixes. With the Optional Upgrade Sequence feature, you can upgrade your core Communication Manager to the latest software version and use the latest features and functionalities of the upgraded software before you upgrade your Survivable Remote Servers (LSP). The Optional Upgrade Sequence feature ensures that the Survivable Remote Servers (LSP) running a lower software version continue registering to the core Communication Manager running on a higher version. However, the configurations on the core Communication Manager do not synchronize with Survivable Remote Servers (LSP) because of the difference in the software versions. *Any administrative changes to the upgraded core Communication Manager are unavailable to the Survivable Remote Servers (LSP) running on a lower software version*. The core Communication Manager generates a warning File synchronization (FSY) alarm for the software version mismatch. The core Communication Manager clears the warning alarm after you upgrade the Survivable Remote Servers (LSP) to the same or a higher software version than your core Communication Manager. The administrative changes are also available after the upgrade. Use Optional Upgrade Sequence if you do not expect changes at the branch locations. Select Survivable Remote Servers (LSP) for later upgrades such that they will not be impacted by the limitations of Optional Upgrade Sequence feature.

While you use the latest features from the core Communication Manager, you can continue to upgrade your Survivable Remote Servers (LSP) to the same or a later software version than your core Communication Manager. For example, if you want to upgrade to Avaya Aura® R10.2 which offers Trellix Antivirus support, identify the Survivable Remote Server (LSP) locations where you do not expect administrative changes and upgrade them after you upgrade your core Communication Manager. The upgraded core Communication Manager can utilize the Trellix Antivirus feature at the main location. Note that the configurations from the upgraded core Communication Manager do not synchronize with the yet-to-be-upgraded Survivable Remote Servers (LSP). The yet-to-be-upgraded Survivable Remote Servers (LSP) can register with the core Communication Manager.

Optional Upgrade Sequence comparison

Use the Optional Upgrade Sequence feature if you require your core Communication Manager to utilize the features of the latest release before some of your Survivable Remote Servers (LSP). For example, in a setup with one core Communication Manager, one Survivable Core Server (ESS), and three Survivable Remote Servers (LSP), with the existing Upgrade Sequence feature, you must follow the order of upgrading. With the Optional Upgrade Sequence feature, you can upgrade the core Communication Manager before the Survivable Remote Servers (LSP). The following table provides a few examples of the upgrade paths:

Existing Upgrade Sequence	Optional Upgrade Sequence
• Survivable Core Server (ESS) Release 10.2 • Survivable Remote Server (LSP)1 Release 10.2 • Survivable Remote Server (LSP)2 Release 10.2 • Survivable Remote Server (LSP)3 Release 10.2 • Core Communication Manager Release 10.2 As the software versions of the Survivable Remote Servers (LSP) and the Core Communication Manager are same, the configurations synchronize between these servers and the admin changes are available on all servers.	Example 1: • Survivable Core Server (ESS) Release 10.2.1 • Core Communication Manager Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.1 • Survivable Remote Server (LSP)2 Release 10.1 • Survivable Remote Server (LSP)3 Release 10.1 Example 2: • Survivable Core Server (ESS) Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.2.1 • Main Communication Manager Release 10.2.1 Warning alarm for yet-to-be upgraded LSPs. • Survivable Remote Server (LSP)2 Release 8.x • Survivable Remote Server (LSP)3 Release 10.1 Example 3: • Survivable Core Server (ESS) Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.2.1 • Survivable Remote Server (LSP)2 Release 10.2.1 • Main Communication Manager Release 10.2.1 Warning alarm for yet-to-be upgraded LSPs.

Existing Upgrade Sequence	Optional Upgrade Sequence
	• Survivable Remote Server (LSP)3 Release 10.1

Important:

- Plan carefully before you implement Optional Upgrade Sequence.
- Optional Upgrade Sequence is available for Survivable Remote Servers (LSP). There is no change to the upgrade sequence for other Avaya Aura® components.

Note:

The fixes for any issues with the Optional Upgrade Sequence feature will be available in the latest supported versions. For more information, see Avaya Product Lifecycle Matrix.

Limitations of Optional Upgrade Sequence

The configurations on the core Communication Manager do not synchronize with the Survivable Remote Servers (LSP) because of the difference in the software versions. Any administrative changes to the upgraded core Communication Manager are unavailable to the Survivable Remote Servers (LSP) running on a lower software version. The core Communication Manager generates a warning File synchronization (FSY) alarm for the software version mismatch.

The alarm clears automatically, and the administrative changes synchronize from the core server after you upgrade the Survivable Remote Servers (LSP) to the same or a later software version than your core Communication Manager.

For more information about the FSY alarm, see

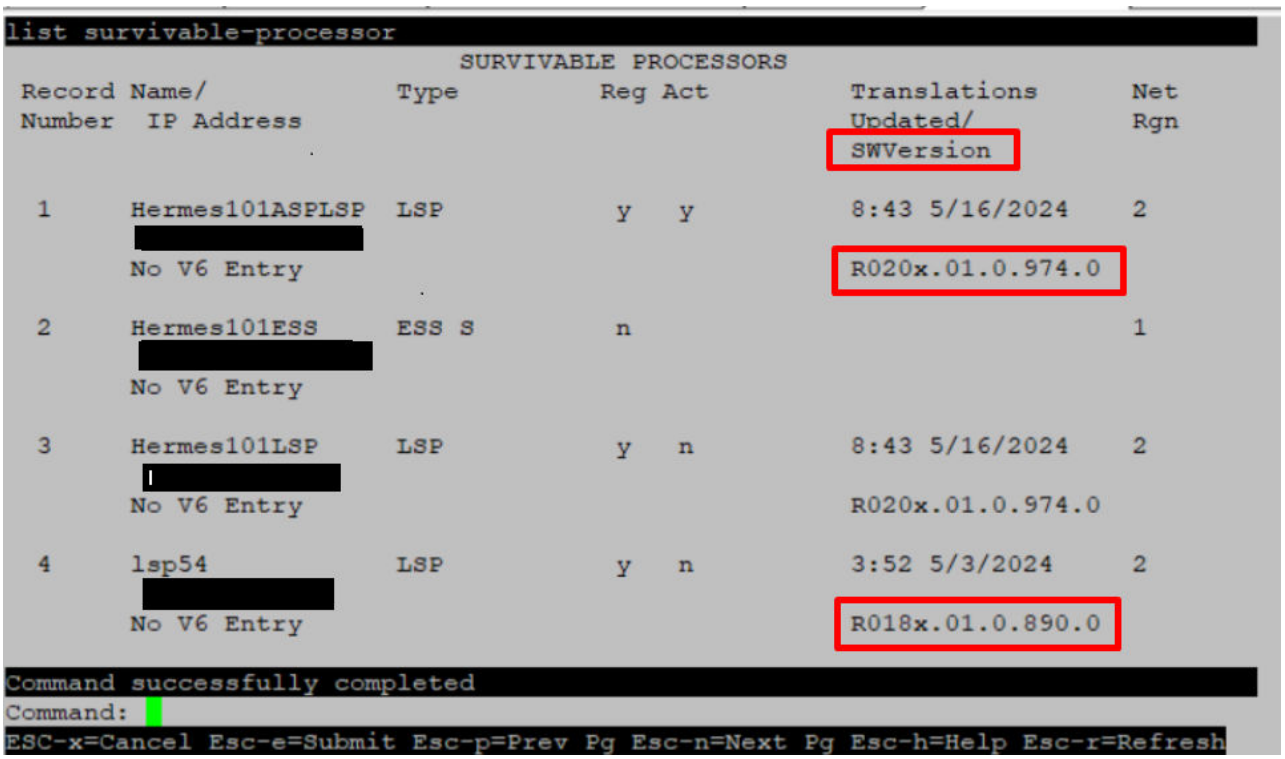
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference

Related links

Verify the software version of the Survivable Remote Servers on page 30
Optional Upgrade Sequence for Avaya components on page 31

Verify the software version of the Survivable Remote Servers

If you use the Optional Upgrade Sequence feature, your core Communication Manager and Survivable Remote Servers (LSP) might not run on the same software version. You can check the software version of each Survivable Remote Server (LSP) in your network and upgrade them to the same or a later software version than your core Communication Manager. To view the software version, log in to the core Communication Manager through SAT and run the `list survivable-processor` command. The list displays all the Survivable Remote Servers (LSP) and their current software version.



To read the software version numbers displayed on the SAT screen, refer to the Software version field description topic in *Administering Avaya Aura® Communication Manager*.

Related links

Optional Upgrade Sequence on page 26

Optional Upgrade Sequence for Avaya components

Upgrade Avaya components and solution in the following sequence. If any of the Avaya components are not part of your solution, you can skip that particular component and move to the next component.

If you choose the Optional Upgrade Sequence feature, you can upgrade the core Communication Manager before you upgrade your Survivable Remote Servers (LSP). In the following Optional Upgrade Sequence, you can skip steps 12 to 14. Note that if you skip the order of sequence, skip all the optional steps. For more information, read Optional Upgrade Sequence on page 26.

Disclaimer on Upgrade Sequence Flexibility

While Avaya recommends following the documented upgrade sequence to maintain solution stability and validated integration, the sequence allows flexibility in specific scenarios. Avaya supports component versions that may be ahead or behind others in the upgrade path, provided they are documented in the Product Compatibility Matrix published on the Avaya Support site. Customers may upgrade individual components out of sequence where such configurations are certified to be interoperable.

Refer to the Product Compatibility Matrix before performing any upgrades out of sequence.

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

If you are using ASP130/S8300 5.0 or earlier, you *must* first upgrade to ASP130/S8300 5.1 or 6.0 before upgrading to Avaya Aura® Release 10.2.x.

To upgrade the Avaya Aura® applications to Release 10.2.x, upgrade the hypervisor to a supported version.

For information about the supported ESXi version, see Supported ESXi version on page 21.

For information about the supported KVM version, see Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 23.

With Aura® R10.2.x, Avaya Messaging R11.0 is compatible. Upgrade Avaya Messaging to R11.0 or later before upgrading Aura® components to R10.2.x.

1. Hard Endpoints- H.323 and SIP
2. Standalone Avaya WebLM.

   Note:

   With Avaya Aura® Release 10.2, standalone WebLM is not available. To upgrade standalone WebLM, use the latest standalone WebLM Release 10.1.3.x. If you upgrade Communication Manager or Application Enablement Services to 10.2 and have a standalone WebLM in the setup, upgrade the standalone WebLM to Release 10.1.3.1 or later. Otherwise, the licensing for Communication Manager and Application Enablement Services will not work.
3. SAL Gateway
4. Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager.

   In the:

   - Non-Geography Redundancy setup, update standalone System Manager.
   - Geography Redundancy setup, update the primary System Manager.
5. Avaya Aura® Session Manager, Core Session Managers only
6. Avaya Breeze® platform and other Snap-ins
7. Avaya Call Management System
8. Avaya Experience Portal
9. Avaya Oceana®
10. Avaya Aura® Device Services
11. Avaya Aura® Media Server
12. ***Optional****:* G4XX Media Gateways

Note:

To successfully upgrade to Release 43.x, use Gateway 38.21.2 or later. If the gateway runs older loads, the download fails and displays the following message: `Incompatible software image`. To resolve, upgrade to 38.21.2 (G430) / 38.21.3 (G450).

If you skip the order of sequence, skip all the optional steps.

Important:

Ensure to read the Limitations of Optional Upgrade Sequence on page 30 before you skip this step.

13. ***Optional****:* Avaya Aura® Branch Session Manager

    Note:

    If you skip the order of sequence, skip all the optional steps.

    Important:

    Ensure to read the Limitations of Optional Upgrade Sequence on page 30 before you skip this step.

14. ***Optional****:* Avaya Aura® Communication Manager Survivable Remote Servers formerly known as Local Survivable Processors.

    Note:

    If you skip the order of sequence, skip all the optional steps.

    Important:

    Ensure to read the Limitations of Optional Upgrade Sequence on page 30 before you skip this step.

15. Avaya Aura® Application Enablement Services
16. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
17. Avaya Aura® Communication Manager Survivable Core Servers, formerly known as Enterprise Survivable Servers
18. Avaya Aura® Communication Manager feature servers and evolution servers

    In a duplex configuration, update the following:

    - Standby Communication Manager server
    - Active Communication Manager server

19. Avaya IP Office™ platform
20. Avaya Messaging, formerly known as Avaya IX™ Messaging and Officelinx

    Important:

    Avaya Messaging must be upgraded to R11.0 or later before upgrading Aura® components to R10.2.x.

21. Avaya Aura® Web Gateway
22. Workplace Clients

    Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
23. Avaya Session Border Controller (ASBCE)

Note:

- System Manager is an integral part of the Avaya Aura® solution.
- System Manager must be on the same or higher release than the application you are upgrading. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.

  All applications supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for application versions System Manager supports, see Avaya Aura® Release Notes on the Avaya Support website.
- Uninstall the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.

  Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2. Solution Deployment Manager Client cannot be on Release 10.1 or Release 8.1.

For information about upgrading the application, see the application-specific upgrade guide on the Avaya Support website.

Related links

Optional Upgrade Sequence on page 26

Software details of Application Enablement Services

For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at https://support.avaya.com/.

Customer configuration data

The following table identifies the key customer configuration information required during the deployment and configuration process for Application Enablement Services:

Required data for Application Enablement Services	Example value
Hostname or fully qualified domain name for the Application Enablement Services virtual machine.	aesserver1

Table continues…

Required data for Application Enablement Services	Example value
DNS search path. **Note:** If you leave this value blank, you must modify or add `search` *<dns search path>* in the file `etc/resolv.conf` after you deploy the Application Enablement Services virtual machine successfully.	example.com
Default gateway address of the Application Enablement Services virtual machine.	123.45.67.254
Domain name servers for the Application Enablement Services virtual machine.	123.45.1.2
IP address of the Application Enablement Services virtual machine interface for eth0, the public interface.	123.45.67.89
Netmask or prefix for the Application Enablement Services virtual machine interface for eth0 (Public interface).	255.255.255.0
IP address of the Application Enablement Services virtual machine interface for eth1 (Private interface).	123.45.67.90
Enter the Netmask or prefix for the Application Enablement Services virtual machine interface for eth1 (Private interface).	255.255.255.0
IP address of the Application Enablement Services virtual machine interface for eth2 (Out of Band Management interface).	
Netmask or prefix for the Application Enablement Services virtual machine interface for eth2 (Out of Band Management interface).	
Network Time Protocol (NTP) hostname or IP address.	

Note:

- DHCP is activated only after you configure it from the command line after initial deployment.
- DHCP does not start when you start Application Enablement Services for the first time.
- Avaya recommends that you should not use DHCP with Application Enablement Services.

AE Services resource requirements and the supported footprints on VMware

The following tables show the resource requirements and the supported footprints for deploying AE Services using the following platforms:

Note:

Avaya Aura® Application Enablement Services supports VMware hosts with Hyperthreading enabled at the BIOS level.

To improve the performance of the GRHA, use profiles 2 and 3.

Footprints	Profile 1	Profile 2	Profile 3
vCPUs	1	2	4
CPU MHz Reservation **Note:** Reservations are applicable to VMware only.	2190 MHz	4380 MHz	8760 MHz
RAM	4 GiB	4 GiB	6 GiB
HDD	55 GiB	55 GiB	55 GiB
NICs	1 to 3*	1 to 3*	1 to 3*

Note:

* Depending on the network topology, you can configure the following types of networks:

1. Public network (Mandatory)
2. Private network (Optional)
3. Out of Band Management (Optional)

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

		DMCC, WTI — Third party call control: Avaya Aura® Contact Center		DMCC — First Party call control		TSAPI, DLG, CVLAN
Profile	**Footprint**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Profile 1	**1 CPU and 4 GiB RAM**	1K 10K	20K BHCC 6K BHCC	1K	9K BHCC	1K MPS
Profile 2	**2 CPU and 4 GiB RAM**	2.5K 12K	50K BHCC 12K BHCC	2.4K	18K BHCC	1K MPS
Profile 3	**4 CPU and 6 GiB RAM**	5K 20K	100K BHCC 24K BHCC	8K	36K BHCC	2K MPS

AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10)

The following tables show the resource requirements and the supported footprints for deploying AE Services using the following platforms:

Note:

Avaya Aura® Application Enablement Services supports KVM hosts with Hyperthreading enabled at the BIOS level.

To improve the performance of the GRHA, use profiles 2 and 3.

Footprints	Profile 1	Profile 2	Profile 3
vCPUs	1	2	4
CPU MHz Reservation **Note:** Reservations are applicable to VMware only.	2190 MHz	4380 MHz	8760 MHz
RAM	4 GiB	4 GiB	6 GiB
HDD	55 GiB	55 GiB	55 GiB
NICs	1 to 3*	1 to 3*	1 to 3*

Note:

* Depending on the network topology, you can configure the following types of networks:

1. Public network (Mandatory)
2. Private network (Optional)
3. Out of Band Management (Optional)

A gibibyte = 1024^3 and gigabyte = 1000^3

		DMCC, WTI — Third party call control: Avaya Aura® Contact Center		DMCC — First Party call control		TSAPI, DLG, CVLAN
Profile	**Footprint**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Profile 1	**1 CPU and 4 GiB RAM**	1K 10K	20K BHCC 6K BHCC	1K	9K BHCC	1K MPS
Profile 2	**2 CPU and 4 GiB RAM**	2.5K 12K	50K BHCC 12K BHCC	2.4K	18K BHCC	1K MPS

Table continues…

		DMCC, WTI — Third party call control: Avaya Aura® Contact Center		DMCC — First Party call control		TSAPI, DLG, CVLAN
Profile	**Footprint**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Profile 3	**4 CPU and 6 GiB RAM**	5K 20K	100K BHCC 24K BHCC	8K	36K BHCC	2K MPS

Chapter 4: Preupgrade tasks

Verifying the software version

About this task

You can see the software version in the upper-right corner of the AE Services Management Console window. If not, you can run the **swversion** command.

Procedure

1. Log in to the AE Services command line interface.
2. At the prompt, type the **swversion** command.
3. Verify the version number and build number.

Verifying the license

Procedure

1. Log in to AE Services Management Console.
2. On the main menu, click **Licensing** > **WebLM Server Access**.
3. On the Web License Manager main menu, click **Licensed Products** > **Application_Enablement**.
4. On the Application Enablement (Standard License file) page, verify the Licensed Features settings.

Verifying the AE Service IP (Local IP) settings

Procedure

1. Log in to AE Services Management Console.
2. From the main menu, select **Networking > AE Service IP (Local IP)**.

The settings on the AE Services IP (Local IP) page should match the settings you specified during initial deployment.

- If you set up a single NIC configuration, the IP settings in the Client Connectivity, Switch Connectivity, and Media Connectivity fields should be the same.
- If you set up a dual NIC configuration, the IP settings should match the settings you specified during initial deployment.

Note:

The private network segment should contain one subnet; this is the only supported configuration. You can configure any default gateway for public and private network segments. However, Avaya recommends using a public gateway as the default gateway to enable access to AE Services through both public and private network segments. After deployment, you must add static routes through CLI to make AE Services accessible from the private network segment.

Verifying the Network Configuration settings

Procedure

1. Log in to AE Services Management Console.
2. On the main menu, click **Networking** > **Network Configure**.
3. On the Network Configure page, verify the settings that you configured on the AE Services server.

Verifying the time zone and NTP server settings

Procedure

1. From your browser, log in to AE Services Management Console.
2. From the main menu, select **Maintenance** > **Date Time/NTP Server**.

   The settings for the time zone and NTP server should match the settings you typed on the Date/Time Initialization screen when you installed the software.

Backing up the AE Services server data

Procedure

1. Log in to the AE Services Management Console with the appropriate user account and password.

2. From the AE Services Console main menu, select **Maintenance > Server Data > Backup**.
3. If you do not want to encrypt the backup file, click **Continue**.
4. If you want to encrypt the backup file, perform the following steps:
   a. Click the **Encrypt Backup File** check box, and then click **Continue**.
   b. In the **Password** box, type the password you want to use for the encrypted backup file.

      The password must consist of 15 to 256 characters. This password cannot contain the following characters: ` (single quotation), " (double quotation), ' (apostrophe), \ (back slash), and % (percent).

   c. Click **Continue**.
5. Click the **Here** link to download the file.

   The File Download dialog box appears. You can specify the location where you want to save the backup file. For example, save the file to your local computer or another computer used for storing backups.

   The backup file is named *ServerName_AESReleaseVersion*_aesvcsdb*DDMMYYYY*.tar.gz.enc where *DDMMYYYY* is a date stamp, and *enc* indicates that the file is encrypted. If the file is not encrypted, *enc* will not appear in the file name.

   Example of:

   - Encrypted backup file: *acme_r6 -2-0-11-0_aesvcsdb18062012.tar.gz.enc*
   - Unencrypted backup file: *acme_r6 -2-0-11-0_aesvcsdb18062012.tar.gz*
6. Click **Save**.

   Note:

   The tar file MD5 checksum is displayed on the web page. Use this checksum to verify the file was downloaded correctly.

Uploading a file to the software library

About this task

Use the procedure to upload software files, such as OVA, images, and firmware that are required during the deployment, migration, upgrade, and update of Avaya Aura® applications.

Before you begin

- On the Download Management page, click **Refresh Families**.
- When you add or update details in the application-specific `versions.xml` file, click **Refresh Families** again to get the updated information.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the System Manager command line interface, copy the required OVA file to the `/swlibrary/staging/sync/` location that you had created in System Manager.

   Note:

   You require admin privileges to access the `/swlibrary/staging/sync/` location.

   The system displays the file that you copied in the Sync Files from directory section.
5. Provide the following information:
   - **SHA256 Checksum**: The value mentioned in the source or original location of the file.
   - **Software Library**: The local or remote software library.
   - **Product Family**

     Note:

     For SAL, in **Product Family**, **Device Type**, and **Software Type** fields, select **Others**.
   - **Device Type**
   - **Software Type**

   If the file is already in `versions.xml`, the system populates the information.

   If the file does not exist in `versions.xml`, the system does not display the file details. Therefore, you cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from Application Management.
6. Select the file.
7. Click **Sync**.

   In File Sync Started Message, the system displays the status of the schedule of the job.
8. Click **OK**.

   When the job completes, the system displays the file in the Software Library Files section.
9. To check the status of the job, click **Services** > **Scheduler** > **Pending Jobs**.

   When the job is complete, the system displays the file in the Software Library Files area and removes from Sync Files from directory.

Adding an Application Enablement Services instance to System Manager

About this task

Use the following procedure if you are migrating or deploying AE Services using Solution Deployment Manager, or if you are connecting Presence Services snap-in to the AE Services server using the AE Services connector.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Application Enablement Services**.
5. In the General section, do the following:
   a. In the **Name** field, type the name of the application.
   b. In the **Description** field, add a description for this entity.

      This field is optional.
   c. In the **Node** field, type the IP address of the management interface of the AE Services server.
6. In the remaining required fields, enter the appropriate information.

   For more information, see “Adding an Application Enablement Services instance to System Manager field descriptions ”.
7. Click **Commit**.

Related links

Adding an Application Enablement Services instance to System Manager field descriptions on page 43

Adding an Application Enablement Services instance to System Manager field descriptions

General

Name	Description
Name	The name of the Application Enablement Services instance.
Type	The type of the Application Enablement Services instance.
Description	The description of the AE Services server.
Node	The IP address/FQDN of the management interface of the AE Services server.

Port Details

Name	Description
Name	The name of the port to be used for the AE Services server.
Protocol	The protocol type supported by the port and the AE Services server. The options are: • http • https • jnp • rmi • tsapi
Port	The port number to be used for the AE Services server.
Description	The description of the port details.

Attributes

Name	Description
aes.aesMachineName.name	The hostname of the AE Services server.

Assign Elements

Name	Description
Assignment Name	The name to assign the Communication Manager instance to the AE Services server. **Note:** **Assignment Name** must be same as the Switch Connection name in the AE Services management console.
Name	The name of the Communication Manager instance.
Node	The IP address/FQDN of the management interface of the Communication Manager instance.
Type	The type of the Communication Manager instance.
Version	The version number of the Communication Manager instance.

Button	Description
Commit	Adds a AE Services instance in the inventory.
Save	Saves all the entries.
Cancel	Cancels your action and returns to the previous page.

Related links

Adding an Application Enablement Services instance to System Manager on page 43

Virtual machine management

Application management

The Application Management link from Solution Deployment Manager provides the application management capabilities that you can use to do the following.

- Supports password change and patch installation of the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform Release 8.x or earlier and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

  Note:

  For the Avaya Aura® Messaging element, trust re-establishment is not required.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA or ISO file on the platform by using System Manager Solution Deployment Manager or the Solution Deployment Manager client.

Managing the location

Viewing a location

Procedure

Click the Locations tab.

The Locations section lists all locations.

Adding a location

About this task

You can define the physical location of the host and configure the location-specific information. You can update the information later.

Procedure

1. On the **Locations** tab, in the Locations section, click **New**.
2. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
3. Click **Save**.

   System Manager displays the new location in the **Application Management Tree** section.

Related links

New and Edit location field descriptions on page 46

Editing the location

Procedure

1. On the **Locations** tab, in the Locations section, select a location that you want to edit.
2. Click **Edit**.
3. In the Edit Location section, make the required changes.
4. Click **Save**.

Related links

New and Edit location field descriptions on page 46

Deleting a location

Procedure

1. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
2. Click **Delete**.
3. In the Delete confirmation dialog box, click **Yes**.

   The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number. Administrators use the field to check entitlements.
Address	The address where the host is located.

Table continues…

Name	Description
City	The city where the host is located.
State/Province/Region	The state, province, or region where the host is located.
Zip/Postal Code	The zip code of the host location.
Country	The country where the host is located.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnet mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server.

Button	Description
Save	Saves the location information and returns to the Locations section.
Edit	Updates the location information and returns to the Locations section.
Delete	Deletes the location information, and moves the host to the Unknown location section.
Cancel	Cancels the add or edit operations, and returns to the Locations section.

Managing the platform

Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

About this task

Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or Avaya Solutions Platform 130 Release 5.1 host. You can associate an ESXi host with an existing location.

If you add a standalone ESXi host to the System Manager Solution Deployment Manager or the Solution Deployment Manager client, add the standalone ESXi host using its FQDN.

Note:

You can add a VMware ESXi host in Solution Deployment Manager if the Standard or Enterprise VMware license is applied on the VMware ESXi host.

If the VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or the VMware ESXi host is in the evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

Solution Deployment Manager supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add another host, System Manager displays the following error message:

```
Retrieving host certificate info is failed: Unable to communicate with
host. Connection timed out: connect. Solution Deployment Manager only
supports host management of VMware-based hosts and Avaya Appliance
Virtualization Platform (AVP).
```

Solution Deployment Manager 10.2.1 does not support ASP 130/S8300 R6.0.x (KVM on RHEL 8.10). You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to VMware ESXi host.

Note:

- To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA before you add the host to the SDM inventory.
- To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP Address of the ESXi host. Otherwise, Solution Deployment Manager does not support adding the ESXi host in Solution Deployment Manager.
- To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the IP address to add an Avaya Solutions Platform host.

Before you begin

Add a location.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
3. In the New Platform section, do the following:
   a. Provide details such as the platform name, platform FQDN or IP address, username, and password.

      For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root username.

   b. In **Platform Type**, select **AVP/ESXi**.

   c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.
4. Click **Save**.
5. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can accept the certificate. If the certificate is invalid, Solution Deployment Manager displays the error. To generate the certificate, see the VMware documentation.

In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

Next steps

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface".
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.

4. In the New Platform section, do the following:
    a. Provide details of Platform name, Platform FQDN, username, and password.

       For Avaya Solutions Platform 130 deployment, you can also provide the root username.

    b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

Next steps

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that the system populates **Application Name** and **Application Version** for each virtual machine.

Adding a software-only platform

About this task

Use this procedure to add an operating system to Solution Deployment Manager. In Release 10.2.x, System Manager supports the Red Hat Enterprise Linux (RHEL) 8.4, or RHEL 8.10 (64-bit) operating system.

Before you begin

Add a location.

Procedure

1. On the **Platforms** tab, click **Add**.
2. In **Platform Name**, type the name of the platform.
3. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
4. In **User Name**, type the username of the base operating system.

   For a software-only deployment, the username must have the permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.

5. In **Password**, type the password of the base operating system.
6. In **Platform Type**, select **OS**.
7. Click **Save**.

   Any other application running on the platform is automatically discovered and displayed in the **Applications** tab.

   - If the Solution Deployment Manager cannot establish trust, the application is displayed as Unknown.
   - If you add the OS, only **Add** and **Remove** operations are available on the **Platforms** tab. **New** option is enabled on the **Applications** tab. If the application is System Manager, **Update App** is enabled on Solution Deployment Manager Client.

   System Manager displays the added base operating system on the **Platforms** tab.

Shutting down the Appliance Virtualization Platform host

About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions** > **Lifecycle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Shutting down Appliance Virtualization Platform host from CLI

About this task

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh`.

   The system displays `Are you sure you want to stop all VMs and shutdown?`
3. To confirm the shutdown operation, type `Y`.

   The system shuts down Appliance Virtualization Platform host, and stops all virtual machines running on the Appliance Virtualization Platform host. The host does not restart automatically.

   You must manually turn on the Appliance Virtualization Platform server. All virtual machines running on Appliance Virtualization Platform automatically start.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Web Client or through the Solution Deployment Manager client.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
3. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
4. On the confirmation dialog box, click **Yes**.

   The system restarts the host and virtual machines running on the host.

Removing a platform

Procedure

1. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
2. Click **Remove**.
3. On the Delete page, click **Yes**.

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.

Table continues…

Name	Description
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

Button	Description
Save	Saves the host information and returns to the Platforms for Selected Location <location name> section.

Downloading the OVA file to System Manager

About this task

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. Click **Download**.

      The system displays the Upload File page.
5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.

8. Provide a valid file type.

   This system uploads the OVA file from local computer to the designated software library on System Manager.

   Note:

   If the file type is invalid, System Manager displays an error.

Managing the application

Editing an application

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
  - AVP Utilities must be available and must be discovered.
  - If AVP Utilities is discovered, the system must display AVP Utilities in the **App Name** column. If the application name in **App Name** is empty, click **More Actions** > **Re-establish connection** to establish trust between the application and System Manager.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

   The system displays the Edit App section.
3. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

   b. Click **More Actions** > **Refresh App**.

      Note:

      To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

   c. Click **Update IP/FQDN in Local Inventory**.

   d. Click **Update App IP/FQDN**.

   e. Provide the IP address and FQDN of the application.

Update IP/FQDN in Local Inventory updates the IP address or FQDN of the application only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the **Platforms** tab to update the IP address or FQDN of the host.

4. Click **Save**.

Starting an application from Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

   In **Application State**, the system displays `Started`.

Stopping an application from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

   In **Application State**, the system displays `Stopped`.

Restarting an application from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
- Applications must be in the running state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.
4. Click **Restart**.

   In **Application State**, the system displays `Stopped` and then `Started`.

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ().
2. Click **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the **Applications** tab, in the Applications for Selected Location <location name> area, select an application.
5. Click **More Actions** > **Re-establish connection**.
6. Select the release version of the product deployed on the application.

   The options are:

   - **6.3 and below**: When you select this, the system displays the following message:

     `Trust cannot be established for this version VM.`
   - **7.0**
   - **7.1 and above**
   - **others**

   Note:

   When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
7. When you select the version **7.0** or **others**, in **User Name**, type the user name of the application.

8. When you select the version **7.0** or **others**, in **Password**, type the password of the application.
9. Click **Reestablish Connection**.

Common causes for application deployment failure

If the application is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the application to not work properly.
- Chosen a private virtual network.

The following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as `0.0.0.0`.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the **Current Action Status** column on the **Applications** tab.

Reestablish Connection field descriptions

Name	Description
Select Version	Select the required version. The options are: • **6.3 and below** • **7.0** • **7.1 and above** • **others** **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Application Name	The name of the application.
VM IP/FQDN	The IP address or FQDN of the application.

Table continues…

Name	Description
User Name	The user name of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Password	The password of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

Button	Description
Reestablish Connection	Establishes connection between System Manager and the application.
Cancel	Cancels the changes and returns to the previous page.

Managing vCenter

Creating a role for a user

About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**
      - **Datastore cluster**
      - **Distributed switch**
      - **Folder**
      - **Host profile**
      - **Network**

- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

Note:

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

b. In All Privileges, expand **Host**, and select the **Configuration** check box.

Note:

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds them to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, click **Add**.
3. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates.

Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.

- The FQDN value must match the value of the **SAN** field of the vCenter certificate. The FQDN value is case-sensitive.

b. In **User Name**, type the username to log in to vCenter.

c. In **Password**, type the password to log in to vCenter.

d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.

e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

PSC must have a valid certificate.

The system enables **PSC IP or FQDN**, and you must provide the IP or FQDN of PSC.

f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.

4. Click **Save**.
5. On the certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds vCenter.

In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Note:

- System Manager does not support vCenter with Cluster level.
- If there is a large data center with multiple hosts in a vCenter, there can be a delay in discovering all the VMs of those hosts when mapping that vCenter in the Solution Deployment Manager. If you select a smaller number of hosts rather than all hosts, this process can be faster.

Related links

Editing vCenter on page 60
Map vCenter field descriptions on page 61
New vCenter and Edit vCenter field descriptions on page 62

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, select a vCenter server and click **Edit**.

3. In the Edit vCenter section, change the vCenter information as appropriate.
4. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
5. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ( ).
   - Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.
6. Click **Commit** to get an updated list of managed and unmanaged hosts.

   If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
3. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The options are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.

Button	Description
Add	Displays the New vCenter page where you can add a new ESXi host.
Edit	Displays the Edit vCenter page where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Applications pre-upgrade functions

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

Note:

For Branch Session Manager, Session Manager, AES, and other elements (excluding Communication Manager), the user must follow these steps in sequence to ensure that the correct options appear in the **Operation** drop-down menu on the **Upgrade Configuration** page.

1. Refreshing elements on page 64
2. Analyzing software on page 64
3. Performing the preupgrade check on page 67

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions** > **Analyze**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✓, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Download Management**.

   The system displays the File Download Manager page.
3. To change the display settings, click one of the following:
   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.
4. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
5. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

The time to complete the refresh operation depends on the source configuration in **User Settings**.

6. Click **Show Files**.
7. In **Select Files Download Details**, do the following:
   a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.
   b. Select the files that you want to download.
   c. Click **Download**.

      In File Download Status, the system displays the file that you selected for download.

File Download Manager field descriptions

Select Software/Hardware Types

Name	Description
Family Name	The name of the device family.
Hardware/Software	The name of the associated software or hardware.

Select Files Download Details

Name	Description
Source	The source from where Download Manager gets the software or firmware files. The options are: • **Avaya PLDS/Alternate Source** • **My Computer**

Name	Description
File name	The file name.
Version	The file version.
Entitled	The file entitlements.
File Size (in bytes)	The file size in bytes.
Hardware/Software	The name of the hardware or the software.
Family Name	The name of the device family.
Content Type	The type of the content.
Software Library	The status of the file download.
File Description	A description of the file that you download.

Button	Description
Refresh Families	Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page. **Note:** When you add or update details in the `versions.xml` file, you must click **Refresh Families** to get the updated information.
Show Files	Displays the files associated with the element that you selected.

File Download Status

Name	Description
File Name	The file name of the software or firmware file.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.
Status	The status of the download activity.
Scheduled By	The user who scheduled the download job.

Button	Description
Delete	Deletes the files that you have selected.

Performing the preupgrade check

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   Note:

   To upgrade to different server, in **Target Host**, select the target server host.
5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
6. Click **Schedule**.

On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

Preupgrade Configuration field descriptions

Pre upgrade Configuration Parameters

Name	Description
Element name	The name of the application that you want to upgrade.
Parent name	The parent of the application that you want to upgrade.
IP Address	The IP address of the application that you want to upgrade.
Current Version	The current version of the application that you want to upgrade.
Target Platform	The Appliance Virtualization Platform or ESXi host of the virtual machine.
Data Store	The data store. When you set the **Target Host** as **Same Box**, the system enables the **Data Store** field.
New Target Platform	The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine. For upgrades on a different server, add Appliance Virtualization Platform or ESXi host from Application Management.
Upgrade Source	The location where OVA or the software patches are available in the local storage or remote server.
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.

Table continues…

Name	Description
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

Upgrading VMware ESXi version

About this task

If the ESXi upgrade is required for upgrading the application to Release 10.2.x, use the following procedure to upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 21.

Before you begin

Take the backup of the application and keep it on remote servers. For information about creating a data backup on a remote server, see the application-specific document.

Procedure

1. Shut down all the virtual machines that are hosted on the ESXi.
2. Put the ESXi into maintenance mode.

   For information about performing steps on ESXi, see VMware product documentation website.
3. Upgrade ESXi to supported ESXi version.

   For information about upgrading ESXi, see VMware product documentation website.
4. After upgrading the ESXi host, log in to the host UI, and exit from the ESXi maintenance mode.
5. Apply the license key for the upgraded ESXi.
6. Power on the virtual machines.

Chapter 5: Migrating from Vmware to ASP R6.0.x (KVM on RHEL 8.10)

Migrating Application Enablement Services from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to migrate Application Enablement Services R10.2.x on ASP R5.x (VMware) to Application Enablement Services 10.2.x on ASP R6.0 (KVM on RHEL).

When migrating, ensure to match the Application Enablement Services version from backup to restore. Perform the backup and restore on the same Application Enablement Services version.

Procedure

1. Note down the existing VMware details.

   For more information, see Obtaining existing VMware details on page 71.

2. Check encryption status.

   For more information, see Obtaining encryption status on page 72.

3. Note down the existing network details.

   For more information, see Obtaining existing network details on page 72.

4. Check FIPS status.

   For more information, see Checking FIPS status on page 73.

5. Enabling secure boot.

   For more information, see Enabling secure boot on page 73.

6. Back up Application Enablement Services.

   For more information, see Backing up Application Enablement Services on page 74.

7. Shut down VMware.

   For more information, see Shutting down WebLM virtual machine on VMware on page 74.

8. Install ASP R6.0.x (KVM on RHEL 8.10).

   For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.

9. Deploy Application Enablement Services on KVM host.

   For more information, see *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment* and *Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments*.

10. Restore Application Enablement Services back-up.

    For more information, see Restoring Application Enablement Services using the web console on page 74 or Restoring Application Enablement Services using the command line interface on page 75.

11. Check connection between Communication Manager and Application Enablement Services.

    For more information, see Checking the connection between Communication Manager and Application Enablement Services on page 76.

12. Verify that services are online.

    For more information, see Verifying that services are online on page 76.

13. Make test calls.

    For more information, see Making test calls using TSAPI and JTAPI on page 77 and Testing DMCC configuration on page 77.

14. Send test messages.

    For more information, see Sending test messages on page 78.

Obtaining existing VMware details

About this task

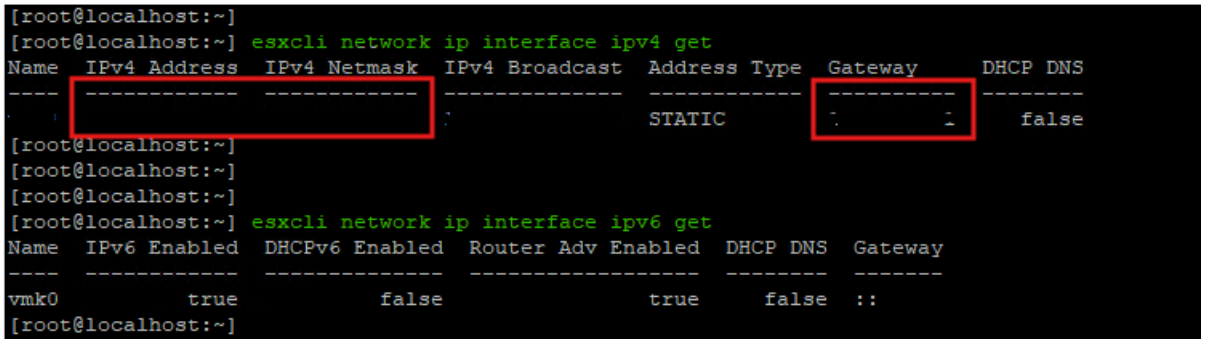
Obtain the configuration details of VMware and use them for ASP R6.0.x (KVM on RHEL 8.10).

For module-specific details, see Obtaining existing network details on page 72.

Use this procedure to obtain the network IP interface details.

Procedure

1. Log in to ESXi CLI, run the following commands:
   - `# esxcli network ip interface ipv4 get`: note down IPv4 network IP interface details.
   - `# esxcli network ip interface ipv6 get`: note down IPv6 network IP interface details.



2. Login to ESXi vSphere or vCenter and note down the VMware License serial number.

Obtaining encryption status

About this task

Use this procedure to make a note of the current encryption status. Configure this status on the upgraded server.

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. To find the Application Enablement Services encryption status, run the command `# encryptionStatus`.

   Example output: `[smsv@test ~]$ encryptionStatus`

   ```
   Data Encryption: enabled
   Local Key Store: disabled
   Encryption passphrase required at Boot-time: yes
   ```

Obtaining existing network details

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. Note-down the configuration details of Application Enablement Services by running the following commands:
   - `hostname -f`: To obtain the Fully Qualified Domain Name (FQDN).

- `ifconfig -a | grep inet | grep -v 127.0.0.1`: To obtain the IP address and network mask.
- `netstat -nrv | grep '^0.0.0.0'`: To obtain the IP address of the default gateway.
- `cat /etc/resolv.conf`: To obtain the Domain Name System (DNS) search list and DNS server IP address.

Checking FIPS status

About this task

Use this procedure to make a note of the current Federal Information Processing Standards (FIPS) status. Configure this status on the upgraded server.

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. Run the command `# fips-mode-setup --check`

   Example output: `FIPS mode is disabled.`

Enabling secure boot

About this task

Application Enablement Services supports Unified Extensible Firmware Interface (UEFI), which replaces traditional Basic Input/Output System (BIOS) and is more secure.

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. Run the following commands:

   ```
   [ -d /sys/firmware/efi ] && echo UEFI || echo BIOS
   ```

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

   Example output: `SecureBoot enabled`

Backing up Application Enablement Services

Before you begin

Log on to the Application Enablement Services web console with administrator privilege credentials.

About this task

Use this procedure to back up Application Enablement Services. Application Enablement Services supports encryption for backups. For more information on encryption, see *Administering Avaya Aura® Application Enablement Services*.

Procedure

1. In the navigation pane, navigate to **Maintenance** > **Server Data** > **Backup**.
2. Click **Continue** and click **Apply**.
3. Click **Here** to download the backup file.

   Example filename: `aes123-456_10.2.1.0.0.425-0_aesvcsdb15102024.tar.gz`
4. **(Optional)** If encryption is configured, make a note of the encryption password.

   You require the encryption password when you restore Application Enablement Services.

Shutting down WebLM virtual machine on VMware

About this task

Use this procedure to shut down VMware.

Procedure

1. Log in to VMware.
2. Shut down the virtual machine.

Restoring Application Enablement Services using the web console

Before you begin

Log on to the Application Enablement Services web console with administrator privilege credentials.

About this task

Use this procedure to restore Application Enablement Services. If the configuration file is large, see Restoring Application Enablement Services using the command line interface on page 75.

Procedure

1. In the navigation pane, navigate to **Maintenance** > **Server Data** > **Restore**.
2. Click **Choose File** and select an Application Enablement Services back-up file.

   Example filename: `aes123-*.tar.gz`
3. Click **Restore** to restore the back-up file.
4. Click **Restart** and wait for five minutes.

   Application Enablement Services restores to the server.

Restoring Application Enablement Services using the command line interface

About this task

Use the Command Line Interface (CLI) to restore the server data when the size of a backup file is greater than 10 MB.

Note:

Remove the Geo Redundant High Availability (GRHA) configuration before restoring the database backup. If you restore the backup when GRHA is enabled, GRHA might not work properly. If this happens, remove GRHA and then reconfigure.

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. To copy the backup file to the `/tmp` directory, use the following command:

   ```
   cp <backup file> to /tmp
   ```
3. To restore the server data, do the following:
   - Run the following command to restore with the GRHA configuration:

     ```
     /opt/mvap/bin/Restore.sh -L </path/to/LargeAESBackupFIle.tar.gz>
     ```
   - Run the following command to restore without the GRHA configuration:

     ```
     /opt/mvap/bin/Restore.sh -L -n </path/to/LargeAESBackupFIle.tar.gz>
     ```
4. Run the following commands to restart the services:

   ```
   systemctl restart DBService
   systemctl restart aesvcs
   systemctl restart sohd
   systemctl restart nftables
   ```

```
systemctl restart httpd
systemctl restart tomcat
systemctl restart snmpd
systemctl restart subagent1
systemctl restart subagent2
```

Note:

Restart if both GRHA and sohd are running.

Checking the connection between Communication Manager and Application Enablement Services

Before you begin

Log on to the Application Enablement Services web console with administrator privilege credentials.

About this task

Use this procedure to restore verify that Application Enablement Services can communicate with Communication Manager.

Procedure

1. In the navigation pane, navigate to **Communication Manager Interface** > **Switch Connection**.
2. Verify the number of active connections.
3. In the navigation pane, navigate to **Status** > **Status and Control** > **Switch Conn Summary**.
4. Verify the **Switch Conn State** as **Talking**.
5. In the navigation pane, navigate to **AES Services** > **TSAPI** > **TSAPI Links**.
6. Verify that the Computer Telephony Integration (CTI) link is established and the Application Specific A Interface (ASAI link) is configured.

Verifying that services are online

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. Run the command: `$ statapp`

   The CLI interface returns a list of services with the status **Running**.

Making test calls using TSAPI and JTAPI

About this task

Use this procedure to verify the end-to-end connectivity of Application Enablement Services.

Before you begin

You must be familiar with the following applications:

- TSAPI Exerciser: Telephony Services API is a C- language based API for third-party call and device control, and based on CSTA standards. TSAPI Exerciser is an application that enables you to send CSTA requests across a TSAPI CTI link and view the exchange of messages between the TSAPI Exerciser and the AE Services Server.
- JTAPI Exerciser: Java Telephony Application Programming Interface is a Java-based API that enables telephony applications to interact with telephony services. JTAPI provides a standardized way to access telephony features across different platforms.

Procedure

1. Place a call using TSAPI.
   a. Navigate to **Start** > **All Programs** > **Avaya AE Services** > **SDKs** > **TSAPI**.
   b. Select **TSAPI Exerciser**.

      Windows opens the TSAPI Exerciser. For more information about using the TSAPI Exerciser, see TSAPI Exerciser Help, which is included with the TSAPI Exerciser.
   c. Place a call using the steps in TSAPI Exerciser Help and TSAPI Exerciser Scripting Instructions.

   For more information, see the following:

   - *Avaya Aura® Application Enablement Services TSAPI for Avaya Communication Manager Programmer's Reference*
   - *Application Enablement Services TSAPI Programmer's Reference*
2. Place a call using JTAPI.

   For more information, see the following:

   - *Avaya Aura® Application Enablement Services JTAPI Programmers Guide*
   - *Avaya Aura® Application Enablement Services JTAPI Programmer's Reference*

Testing DMCC configuration

About this task

Make first-party and third-party calls to test DMCC configuration for a sample application.

Procedure

1. On the AE Services management console, go to **Utilities > Diagnostics > AE Service > DMCC Test**.
2. On the DMCC Test page, in **User**, type the user ID.
3. In **User Password**, type the user password.
4. Clear the **TLS** check box.
5. In **Switch Name**, select the required switch.
6. **(Optional)** In **Switch IP**, select the IP address of the switch.
7. In **Caller Extension**, type the caller extension.
8. In **Caller Extension Password**, type the password for the caller extension.
9. In **Callee Extension**, type the extension that receives the call.
10. In **Callee Extension Password**, type the password for the extension that receives the call.
11. Do one of the following:
    - To make a first-party call, click **Make First Party Call**.

      AE Services displays the test results on the First Party Call Test Result page.
    - To make a third-party call, click **Make Third Party Call**.

      AE Services displays the test results on the Third Party Call Test Result page.

Sending test messages

About this task

This proccedure uses Short Message Service (SMS) protocol.

Procedure

1. In a Web browser, enter the following syntax:

   `<https://<AES IP Address>>/sms/sms_test.php`
2. In the **CM Login ID** field, type a login name.

   Example input: `cust@<Communication Manager IP Address>`
3. In the **Password** field, type a password.
4. Select your choice of request parameters.
5. Click **Submit Request**.
6. Verify that the response parameters match your request parameters.

Chapter 6: Upgrading AE Services to Release 10.2.x on Avaya Solutions Platform 130 or on VMware

Upgrading AE Services by using System Manager Solution Deployment Manager

Upgrading Application Enablement Services to Release 10.2.x using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade AE Services to Release 10.2.x from:

- Release 8.1.x running on Appliance Virtualization Platform, VMware, or ASP 130.
- Release 10.1.x running on VMware, or ASP 130.

The procedure covers upgrades on the same and different servers.

Before you begin

- Ensure that all the pre-requisite patches are installed.

  For more information about the patches, see Avaya Aura® Release Notes on Avaya Support Website at http://support.avaya.com.
- Ensure that System Manager is running on Release 10.2.
- Add a location.

  For more information about adding a new location, see Adding a location on page 45.
- Add the ESXi, vCenter, Appliance Virtualization Platform, or Avaya Solutions Platform 130 host.

  For information about adding the host, see “Managing the platform”.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 59.

Important:

- If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

  For information about the supported ESXi version, see Supported ESXi version on page 21.

  For information about upgrading ESXi, see the VMware product documentation.
- If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
- If the application is running on the server that is not supported with Release 10.2.x, then deploy Avaya Solutions Platform 130.

  For information about supported servers, see Supported servers for Avaya Aura applications on page 18.

- Select the AE Services virtual machine and click **More Actions** > **Re-establish connection** to establish trust.
- Obtain the AE Services software. See “Software details of Application Enablement Services”.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select AE Services, and then click **Pre-Upgrade Actions** > **Refresh Element(s)**.
4. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
5. After refresh is done, click **Pre-Upgrade Actions** > **Analyze**.
6. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
7. After analyze is done, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
8. On the Pre-upgrade Configuration page, do the following:
   a. Do one of the following:
      - For same server, provide the mandatory parameters along with the same target host information.
      - For different server, provide the mandatory parameters along with different target host information.
   b. In the Job Schedule section, click **Schedule**.

      You can schedule the job now or for a later time.
9. Select the AE Services application.
10. Click **Upgrade Actions** > **Upgrade/Update**.

11. **(Optional)** On the Upgrade Configuration page, select **Override preupgrade check**.

    When you select the check box, the upgrade process continues even when the recommended checks fail in pre-upgrade check.

12. To provide the upgrade configuration details for AE Services, click **Edit**.

13. On the Edit Upgrade Configuration page, do the following:

    a. Do one of the following:

       - For the same server, provide the mandatory parameters and the same target host information, latest patch file, and credentials
       - For different server, provide the mandatory parameters along with different target host information, the latest patch file, and credentials

       For information about parameters, see Edit Upgrade Configuration field descriptions on page 86.

    b. Complete the details, and click **Save**.

14. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.

15. Click **Save**.

16. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.

17. On the Upgrade Configuration page, click **Upgrade**.

18. On the Job Schedule page, click one of the following:

    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.

19. Click **Schedule**.

20. Click **Upgrade**.

21. On the Upgrade Management page, click .

    The **Last Action** column displays **Upgrade**, and **Last Action Status** column displays .

22. To Commit or Rollback, do the following:

    a. On the Upgrade Management page, select the element.

    b. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.

       The system displays the Job Schedule page.

    c. Select the action to be performed under the **Upgrade Action** column.

    d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.

e. Click **Schedule**.

When you commit the changes, the system deletes the old virtual machine.

When you rollback, the system deletes the newly-created virtual machine and starts the old virtual machine.

23. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In **Job Type**, click **Upgrade**.
    c. Click the upgrade job that you want to view.
24. Once the upgrade is successful, wait for 5 minutes before accessing the AE Services OAM page.
25. Verify that the upgrade of the AE Services application is successful.

Note:

Occasionally, after upgrading AE Services from 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to 10.2 by using Solution Deployment Manager, the DMCC service fails to activate. Verify if the DMCC port 4721 or 4722 is in LISTEN state using `netstat -nap | grep 4722` or `netstat -nap | grep 4721`. If the ports are not in LISTEN state, perform one of the following steps to restart the service:

- Through the CLI, run the command `systemctl restart aesvcs`.
- If you are authorized to perform AE Services OAM administration, log into the AE Services server and click **Maintenance** > **Service Controller** > **Restart AE Server**.

Next steps

Important:

When AE Services is upgraded to Release 8.1.2.1 and later, the Host ID utilized by the embedded Avaya WebLM server will change. The original license will not be valid since it is based on a different Host ID and the system will enter into a 30 day license error grace period. Hence, a new license must be created based on the new Host ID. To obtain a new license, see Obtaining the AE Services license file on page 138. For more information on this issue, see PSN020518u on Avaya support site at https://support.avaya.com.

For information about AE Services Release 10.2 logs rotation and **Security** > **PAM** > **Password Management** issues, see Avaya Product Support Notice.

Upgrade Management field descriptions

You can apply filters and sort each column in the devices list.

Name	Description
Name	The name of the device that you want to upgrade.

Table continues…

Name	Description
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board.
Sub-Type	The sub type of the device. For example, TN2302AP.
IP Address	The IP address of the device.
Release Status	The release status of the device. The upgrade status can be: For upgrade: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed
Update Status	The update status of the device. The upgrade status can be: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.

Table continues…

Name	Description
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • : Mandatory checks and recommended checks passed • : Mandatory checks are successful, but recommended checks failed. • : Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
Location	The location of the device.

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/Rollback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.

Table continues…

Button	Description
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download > **Download**	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Download > **Bulk Import Spreadsheet**	Downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, CommunicationManager_123.
Type	The device type.
IP Address	The IP Address of the device.
Current Version	The release status of the device.
Override Preupgrade Check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.

Table continues…

Name	Description
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system deletes the old virtual machine after the upgrade check.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. • : Configuration incomplete. • : Configuration complete.

Button	Description
Import Configuration(s)	Imports the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. The system displays the Upload Xlsx File Configuration dialog box to upload the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.
Save Configuration	Saves the upgrade configuration. **Note:** The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page.
Upgrade	Commits the upgrade operation.

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- **Element Configuration**
- **AVP Configuration**

Element Configuration: General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update

Table continues…

Name	Description
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/ Platform	The new target host on which you want to run the device.
Migrate With AVP Install	The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.
Service/Feature Pack for auto-install after upgrade/ migration	The service pack or feature pack that you want to install.

Element Configuration: Upgrade Configuration Details

The page displays the following fields when you upgrade application and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

Name	Description
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.
Hostname	The IP address of the virtual machine.
DNS Search Path	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Password for cust	The password of the cust user.
Password for root	The password of the root user.
Timezone	The timezone of the virtual machine.

Table continues…

Name	Description
NTP server(s)	The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,). The application supports only the NTP server. It does not support the NTP pool.
EASG User Access	**Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. **Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled. Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Public IP Address	The IP Address of AE Services virtual machine.
Public Netmask	The network mask of AE Services virtual machine.
Private IP Address	This field is optional and can be configured to be used for private network.
Private Netmask	This field is optional, and can be configured to be used for private network.
Out of Band Management Netmask	The subnet mask of the virtual machine for out of band management.
Out of Band Management IP Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.

Table continues…

Name	Description
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: Data Encryption

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.

Table continues…

Name	Description
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Element Configuration: End User License Agreement

Name	Description
I Agree to the above end user license agreement	The end user license agreement. You must select the check box to accept the license agreement.

AVP Configuration: Existing Machine Details

Name	Description
Source IP	The source IP address.
Source Administrative User	The source user name with appropriate admin privileges.

Table continues…

Name	Description
Source Administrative Password	The source password of the administrator.
Source Root User	The source user name with appropriate root privileges.
Source Root Password	The source password of the root.

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. **Note:** IPv6 is only supported in a dual stack configuration.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.

Table continues…

Name	Description
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

Table continues…

Name	Description
Enhanced Access Security Gateway (EASG)	**Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. **Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled. Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Save	Saves the changes that you made to the Edit Upgrade Configuration page.
Cancel	Cancels the changes that you made to the Edit Upgrade Configuration page.

Upgrade Management field descriptions

Name	Description
Application Name	The application name displayed on the Add Element page.

Deploy OVA

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.

Table continues…

Name	Description
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is ✔.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see the latest System Manager release notes.

Configuration Parameters

The system populates most of the fields depending on the OVA file. You must provide information, such as password, FQDN, and timezone.

Management Network Settings

Name	Description
Out of Band Management IPv4 Address	The IPv4 address of the Application Enablement Services application for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Out of Band Management Netmask	The Out of Band Management subnetwork mask to assign to the Application Enablement Services application.
Management Gateway	The Management Gateway address to assign to the Application Enablement Services application.
Private Netmask	The private Netmask address to assign to the Application Enablement Services application.
Private IP Address	The private IP address to assign to the Application Enablement Services application.
Public Netmask	The IPv4 subnetwork mask to assign to Application Enablement Services application. The field is optional.

Table continues…

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
DNS	The DNS IP addresses to assign to the primary, secondary, and other applications. Separate the IP addresses with commas (,).
Default Gateway	The default Gateway address to assign to the Application Enablement Services application.
Application Name	The application name displayed on the Add Element page.
Hostname	The Hostname address to assign to the Application Enablement Services application.
DNS Search path	The DNS search path to locate and assign to the Application Enablement Services application.
Password for cust	The root password for the application
Confirm Password	The root password for the application
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the Application Enablement Services application is located. A list is available where you select the name of the continent and the name of the country.

Network Parameters

Name	Description
Out of Band Management IP Address	The IP address of the Application Enablement Services application that is mapped to the out of band management.
Public	The port number that you must assign to public port group. The field is optional.

Button	Description
Upgrade	Displays Upgrade Management page. Click on **Upgrade Actions** > **Upgrade/Update**, Upgrade Configuration page displays. Click on **Edit**. Edit Update Configuration page displays. Check EULA: Global and Root agreement. Click **Save**.

Installing software patches by using Solution Deployment Manager

About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Note:

- When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions** > **Installed Patches** on the Upgrade Management page, then perform the following:
  1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
  2. Refresh the element.

Before you begin

- Perform refresh and analyze operations.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.

13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display ✓.
15. To view the update status, click ✓.

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

    When the update is complete, the **Update status** and **Last Action Status** fields displays ✓.
16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display ✓.

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Related links

Installed Patches field descriptions on page 97

Installed Patches field descriptions

Name	Description
Commit	The option to select the patches that you can commit.
Uninstall	The option to select the patches that you can uninstall.
Rollback	The option to select the patches that you can rollback.
Show All	The option to display all the available options.

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.
Patch Type	The type of the software patch. The options are: • service pack or feature pack or software patch • Security
Patch State	The state of the software patch. The options are: • Active (when patch is activated) • Installed (when patch is unpacked) • Pending (when patch is pending a commit)

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

Related links

Installing software patches by using Solution Deployment Manager on page 95

Installing custom software patches

About this task

The custom patching option is for advanced administrators so that they can fully control the installation of hot fixes, patches, service pack, and feature packs.

While installing custom patches, you do not need to perform the analyze and preupgrade check options that are available under **Pre-upgrade Actions** on the Upgrade Management page. Performing the preupgrade check while using Custom patches will result in a failure.

Use this procedure to install a single software file, such as software patch, service pack, or a feature pack to an Avaya Aura® application.

You can install custom patches for the following Avaya Aura® applications:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- Communication Manager Messaging
- WebLM
- Application Enablement Services

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays  .

    If the field displays  , review the information on the Edit Upgrade Configuration page.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.

15. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display ✓.

16. To view the update status, click ✓.

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

    When the update is complete, the **Update status** and **Last Action Status** fields displays ✓.

17. Click **Upgrade Actions** > **Installed Patches**.
18. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

19. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.

20. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.

21. Ensure that **Update status** and **Last Action Status** fields display ✓.

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Upgrading AE Services using backup and restore

Upgrading AE Services from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to 10.2.x by using backup and restore

About this task

Use the following procedure for migrating the AE Services virtual appliance:

Procedure

1. Back up the current AE Services database.

For information about the database backup, see Backing up the AE Services server data on page 40.

Note:

7.1.3.x version is only supported in the transient period when upgrading the Avaya Aura® solution.

2. Shut down the AE Services virtual machine.
3. Install the AE Services 10.2 OVA.

   Ensure that the IP and Network parameters information of the new AE Services virtual machine is the same as it was on the existing AE Services virtual machine.
4. Restore the AE Services database backup to the AE Services virtual machine.

   For information about the restoring the database backup, see:

   - Restoring the AE Services server data using AE Services Management Console on page 101
   - Restoring Application Enablement Services using the command line interface on page 75
5. After the restore is complete, verify that the AE Services application is operational.

Restore AE Services server data

You can restore the AE Services server data by using one of the following methods:

1. AE Services Management Console
2. Command line interface (CLI)

Note:

When restoring using OAM if the restore file size exceeds 10 MB, it is recommended to restore AE Services server data using CLI.

Restoring the AE Services server data using AE Services Management Console

About this task

Note:

- The database backup file includes the license file in the preserved server data. If a restore is made on a newer AE Services major release than the release in the database backup file (older releases to 7.0), you must remove the license file restored from the previous release.
- Remove the Geo Redundant High Availability (GRHA) configuration before restoring the database backup. If you restore the backup when GRHA is enabled, GRHA might not work properly. If this happens, remove GRHA and then reconfigure.

Procedure

1. Log in to AE Services Management Console.
2. From the main menu, select **Maintenance** > **Server Data** > **Restore**.
3. On the Restore Database Configuration page, click **Browse**.
4. Select the appropriate AE Services backup file, and click **Restore**.

   If the backup file is encrypted, the **Password** box appears on the Restore Database Configuration page.
5. In the **Password** box, type the password for the backup file, and then click **Continue**.

   On the Restore Database Configuration page, AE Services displays the following message:

   ```
   A database restore is pending. You must restart the Database
   Service and the AE Server for the restore to take effect. To
   restart these services now, click the Restart Services button
   below.
   ```
6. Click **Restart Services**.

   Caution:

   If you make any changes in the interval between clicking **Restore** and **Restart Services**, these changes will be lost.

Restoring Application Enablement Services using the command line interface

About this task

Use the Command Line Interface (CLI) to restore the server data when the size of a backup file is greater than 10 MB.

Note:

Remove the Geo Redundant High Availability (GRHA) configuration before restoring the database backup. If you restore the backup when GRHA is enabled, GRHA might not work properly. If this happens, remove GRHA and then reconfigure.

Procedure

1. Log in to the Application Enablement Services CLI as a cust user, then log in as a root user using the command `su -root`.
2. To copy the backup file to the `/tmp` directory, use the following command:

   ```
   cp <backup file> to /tmp
   ```
3. To restore the server data, do the following:
   - Run the following command to restore with the GRHA configuration:

     ```
     /opt/mvap/bin/Restore.sh -L </path/to/LargeAESBackupFIle.tar.gz>
     ```

- Run the following command to restore without the GRHA configuration:

```
/opt/mvap/bin/Restore.sh -L -n </path/to/LargeAESBackupFIle.tar.gz>
```

4. Run the following commands to restart the services:

```
systemctl restart DBService
systemctl restart aesvcs
systemctl restart sohd
systemctl restart nftables
systemctl restart httpd
systemctl restart tomcat
systemctl restart snmpd
systemctl restart subagent1
systemctl restart subagent2
```

Note:

Restart if both GRHA and sohd are running.

Upgrading AE Services standby and active servers in the Geographical Redundancy High Availability setup

About this task

Use this procedure to upgrade the standby and active servers, when the AE Services server is configured with Geographical Redundancy High Availability (GRHA).

The following upgrade procedure is applicable only for the major release upgrades. If you are upgrading to a Feature Pack (FP) or a service pack, install the FP on the active AE Services server and the same configuration will be applied to the standby server.

In GRHA using Virtual IP, if AE Services is upgraded to Release 10.1 and later, the Host ID utilized by the embedded WebLM server will change. Hence, a new license must be created based on the new Host ID. To obtain a new license, see Obtaining the AE Services license file on page 138. For more information on this issue, see PSN020518u on Avaya support site at https://support.avaya.com.

Procedure

1. Using the AE Services Management Console, remove High Availability on the active server.
2. Perform a backup of the AE Services server data for the active server.
3. Delete the active and standby AE Services servers.
4. Install the new active and standby AE Services servers.
5. Restore the data for the active AE Services server.
6. Using the AE Services Management Console, configure and start High Availability on the active server.

Note:

- For GRHA configuration both active and standby servers must be on the same platform and profile.

  For example, if the active AE Services is on VMware with profile 1, the active AE Services server must also be on VMware with profile 1.
- To improve the performance of the GRHA, use profiles 2 and 3.

Upgrading AE Services active and standby servers with a SSP patch in the Geographical Redundancy High Availability setup

Procedure

1. Using the CLI, install the SSP patch on the standby server.
2. Reboot the AE Services server and wait till the state of **AESVCS** service changes to active.
3. Synchronize the data between the active and standby AE Services servers.
4. Perform interchange or failover from active server to the standby server.
5. Using the CLI, install the SSP patch on the recently added standby server.
6. Reboot the AE Services server and wait till the state of **AESVCS** service changes to active.
7. Perform interchange or failback from active server to the standby server.

Chapter 7: Upgrading AE Services on Infrastructure as a Service environment

Upgrade path for AWS

You can upgrade to AE Services Release 10.2 on AWS from the following:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 8.0.x or 8.1.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.

Upgrade path for Google Cloud Network

You can upgrade to AE Services Release 10.2 on Google Cloud Network from the following:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 8.0.x or 8.1.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 7.1.3.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or Software-only Environment.

Upgrade path for Microsoft Azure

You can upgrade to AE Services Release 10.2 on Microsoft Azure from the following:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.

- Release 8.0.x or 8.1.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 7.1.3.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or Software-only Environment.

Upgrading to Release 10.2.x on Infrastructure as a Service environment

Before you begin

- Ensure that all the pre-requisite patches are installed.

  For more information about the patches, see Avaya Aura® Release Notes on Avaya Support Website at http://support.avaya.com.

Procedure

1. Log in to the AE Services Management Console with the appropriate user account and password.
2. Create a backup of the system and copy it to the remote server.

   Note:

   7.1.3.x version is only supported in transient period when upgrading the Avaya Aura® solution.
3. Deploy the Release 10.2 ISO on your target Infrastructure as a Service environment.

   For more information about deploying AE Services on Infrastructure as a Service environment, see *Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment*.

   Ensure that the IP and Network parameters information of the new AE Services virtual machine is the same as it was on the existing AE Services virtual machine.
4. Log in to the new AE Services Management Console.
5. Configure the server.
6. Restore the data backup on the new system.
7. Verify the software version of the new system.

Next steps

Important:

When AE Services is upgraded to Release 8.1.2.1 and later, the Host ID utilized by the embedded Avaya WebLM server will change. The original license will not be valid since it is based on a different Host ID and the system will enter into a 30 day license error grace period.

Hence, a new license must be created based on the new Host ID. To obtain a new license, see Obtaining the AE Services license file on page 138. For more information on this issue, see PSN020518u on Avaya support site at https://support.avaya.com.

License management

Following are the use cases for managing licenses when an application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 8.0 and later, Software-only Environment supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment, but only the applications move to Software-only Environment, then you do not have to regenerate the license for those applications that move to Software-only Environment.
- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to Software-only Environment, then all the licenses need to migrate to the centralized System Manager Release 8.0 and later with integrated WebLM in AWS and the applications that move need to regenerate the license files.

Chapter 8: Upgrading AE Services on Software-Only environment

Upgrade checklist for Software-Only environment

Use the following checklist to monitor your progress as you perform an upgrade.

#	Description	Notes	✔
1	Gather the prerequisites.	See Prerequisites for an upgrade or update to AE Services on page 109.	
2	Record the local IP settings	See Recording the local IP settings on page 113.	
3	Back up the AE Services server hard drive.	**Important:** Important: Avaya recommends that you backup the entire contents of the AE Services server drive.	
4	Back up the AE Services server data.	See Backing up the AE Services server data on page 40.	
5	Install Linux® Operating System RHEL 8.4 or RHEL 8.10 (64 Bit) with all security updates applied.	See Installing the Red Hat Enterprise Linux software for AE Services on page 110.	
6	Install the AE Services 10.2.x Software-only offer.	See Upgrading to AE Services Release 10.2.x on page 114.	
7	Validate the configuration settings.	See Validating the configuration settings on page 118.	
8	Uninstall the license file, if you are upgrading from a one major release to another release.	See Uninstalling the AE Services license on page 138.	
9	Install the new license.	See Installing the AE Services license on page 135.	

Note:

In Software-Only environment, AE Services does not support upgrade from Release 8.1.x to Release 10.1 and later using Solution Deployment Manager.

Prerequisites for an upgrade or update to AE Services

From Release 10.1 onwards, the default Communication Manager identity certificate signed by the SIP Product Certificate Authority is not accepted due to security hardening. So, install a third-party CA certificate on AE Services and an identity certificate on Communication Manager.

The public key of the CA and identity certificates should not be less than 2048 bits. You must install the certificates on AE Services and Communication Manager before upgrading to AE Services Release 10.2.

Before you start the upgrade, make sure you have the following items:

- Administrative workstation.
- (Optional) A program to back up the AE Services server drive: Use a program that enables you to copy the entire content of the AE Services server drive. Avaya recommends creating a backup of the AE Services server drive before upgrading the AE Services software.
- AE Services Release 10.2.x software that includes pre-upgrade patch files and features or service pack files.

  To upgrade AE Services from Release 8.0.x and later to Release 10.2.x, use the following options:

  - You can download the ISO file of the Application Enablement Services software for Release 10.2 and create an installation DVD.
  - You can mount the ISO file on the file system and then use the file to install the server.
- The Linux® Operating System RHEL 8.4 or RHEL 8.10 (64 Bit) has received all security updates. For more information, see the “Hardware Requirements” section.
- AE Services Release 10.2.x license file: A new license is required to upgrade AE Services from an earlier major release. For example, in AE Services 8.1.x., uninstall the license file if you are upgrading from a major release to another release. To obtain a license file, see Obtaining the AE Services license file on page 138.

  Note:

  Release 7.1.3.x version is supported only during the transient period while upgrading the Avaya Aura® solution.

  Important:

  Ensure you request the license file a day before you upgrade.
- (Optional) Release Notes: To obtain the release notes, visit the Avaya Support site at https://support.avaya.com.

Installing the Red Hat Enterprise Linux software for AE Services

Before you begin

- You must install the Red Hat Enterprise Linux (RHEL) *before* you install the AE Services software because the AE Services installation script also configures RHEL for AE Services.

  Note:

  Avaya does not provide RHEL installation media with the AE Services Software-Only offer. This document assumes that you have obtained Linux® Operating System RHEL 8.4 or RHEL 8.10 (64-bit) with all security updates applied.

  Refer to the RHEL Installation Guide when you install RHEL. The following steps provide a high-level summary of the installation with a few specific instructions for installing AE Services.

- Perform the installation using the graphical user interface (GUI) installation program. In general, you can use the default options. However, when you install the Software Packages, Avaya recommends that you customize the software selection instead of installing the default packages, as described in this procedure.

Procedure

1. Boot to your RHEL installation media. Follow the instructions of the installation utility.
2. In the RHEL installation program, follow these steps to set up a `/var` partition.

   Note:

   Although you can use the RHEL default partitioning, Avaya recommends that you set up the `/var` directory as a file system (partition) to improve system reliability. This change prevents the AE Services root directory from becoming filled with log messages.

   a. On the **Disk Partition Setup** screen, select the partition method you prefer, such as **Automatically partition**.

   b. On the next screen, click **New**.

   c. Name the partition `/var` and complete the screen.

   d. Allocate about 40 percent of the disk drive space to create the `/var` partition if available.

      - The `/var` partition must be at least 9.5 GiB in size.
      - On the Firewall Configuration screen, the Security Enhanced Linux (SELinux) features are active by default. You must disable SELinux or AE Services will not work correctly.
      - Avaya recommends separating `/var/log/` partition to avoid system instability in case the partition fills up due to large log files.

- The `/var/log/` partition must be at least 18.5 GiB in size.

3. On the Software Selection page, in the Base Environment and Add-Ons for Selected Environment sections, keep the default selections.

   In the Base Environment section, the Minimal Install option is selected by default and in the Add-Ons for Selected Environment section, all the options are cleared by default.

4. Complete the RHEL installation and reboot the server.

   The time required for the software installation depends on the options you selected and the server processing power. Allow several minutes.

   Note:

   See Configuring Linux OS on page 111 before installing AE Services Software-Only offer.

5. For security purposes, enable only the specific ports you require.

   Include all the ports that the AE Services software uses. For a list of required ports, see the Port Matrix for Avaya Aura® Application Enablement Services 10.2 and *Whitepaper on Security in Avaya Aura® Application Enablement Services*. The Port Matrix and Whitepaper are available with the AE Services customer documents on the Avaya Support website at http://www.avaya.com/support.

Configuring the Linux operating system for AE Services *Software-Only* installation on on-premise

About this task

Use this procedure to configure the Linux operating system for software-only installation on on-premise.

Before you begin

- Log in to Linux using the root credentials.
- Back up the following files and folders (if present), before installing AE Services:
  - `/etc/openldap`
  - `/etc/sssd`
  - `/etc/ssh`
  - `/etc/pam.d`
  - `/etc/ldap.conf`
  - `/etc/nslcd.conf`
  - `/etc/resolv.conf`

- /etc/hosts

Procedure

1. In the /etc/sysconfig/network-scripts/ifcfg-ensXXX or /etc/sysconfig/network-scripts/ifcfg-eth0, set the ONBOOT file attribute to Yes.
2. If the network interface is not currently set to eth0, use **GRUB Changes** to rename network interface to eth0.
   a. Type vi /etc/default/grub.
   b. Look for the line GRUB_CMDLINE_LINUX and add the following:

      ```
      net.ifnames=0 biosdevname=0 (with example)
      (GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/
      swap rhgb quiet net.ifnames=0 biosdevname=0")
      ```

   c. Click **Save**.
   d. Type grub2-mkconfig -o /boot/grub2/grub.cfg.
   e. If you have not specified names for the interface files during the installation, rename **/etc/sysconfig/network-scripts/ifcfg-*** to **/etc/sysconfig/network-scripts/ifcfg-eth0** using the below command:

      ```
      mv /etc/sysconfig/network-scripts/ifcfg-ens  /etc/sysconfig/network-scripts/
      ifcfg-eth0
      ```

      - Open /etc/sysconfig/network-scripts/ifcfg-eth0.
      - Update *DEVICE* and *NAME* value from esn* to eth0.
3. Disable the firewall by entering the command:

   ```
   systemctl disable firewalld
   ```

   Warning:

   This is a slow process and affects system performance when logging is enabled.
4. Disable journaling for *systemd* as follows:

   ```
   systemctl disable systemd-journald.service
   systemctl disable systemd-journald.socket
   ```

   Make sure you see the line SELINUX=disabled in the /etc/selinux/config file.
5. Do the following to create entries in the /etc/hosts file and edit the **/etc/hosts** command:
   a. Make sure IPv4 and IPv6 loopback entries are added in the /etc/hosts file. The loopback entries must be in the following formats:
      - **127.0.0.1 localhost.localdomain localhost**
      - **::1 localhost6.localdomain6 localhost6**

Caution:

If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

Only IPv6 is not supported.

b. Edit **/etc/hosts** and add an entry for your server. For example: `ipAddress fqdn hostname`.

6. In `/etc/resolv.conf` edit **nameserver**. If **nameserver** is not present, add it.
7. Run `hostname <hostname>`, where <hostname> is the host name entry you added.
8. Run `shutdown -r now`

Recording the local IP settings

About this task

This procedure is recommended for upgrading all releases.

Recording the local IP settings refers to maintaining a record of the settings that appear on the Local IP screen in the AE Services Management Console interface. You can manually record the settings on paper, or you can create an electronic file and either type in the information or capture the screen.

For AE Services, local IP settings are the IP addresses you have assigned to the Ethernet interfaces on the AE Services server. It is recommended that you record them, and then verify them after the upgrade is complete.

Procedure

1. From your browser, log in to the AE Services Management Console with the appropriate user account and password. See Logging into the Management Console on page 123 for more information.
2. From the CTI OAM home page, select **Networking > AE Service IP (Local IP)**.
3. From the Local IP page, record the local IP settings for the Ethernet interfaces (Client connectivity, Switch connectivity, and Media connectivity).

Upgrading the Red Hat Enterprise Linux software

About this task

To install or upgrade Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10, see http://www.redhat.com/en.

Note:

Perform a backup and restore of the LDAP database, if required. For more information, see http://www.redhat.com/en.

Upgrading to AE Services Release 10.2.x

About this task

Follow this procedure to upgrade an AE Services Software-only server running AE Services Release 7.1.3.x or 8.x to AE Services 10.2.x from a DVD-ROM or ISO image.

Note:

- 7.1.3.x version is only supported in the transient period when upgrading the Avaya Aura® solution.
- If you are upgrading from an AE Services minor release to AE Services Release 10.2.x, see Prerequisites for an upgrade or update to AE Services on page 109.
- In Software-only environment, AE Services does not support upgrade from Release 8.1.x to Release 10.2.x using Solution Deployment Manager (SDM).

If you are upgrading from an AE Services minor release to AE Services Release 10.2.x, see Prerequisites for an upgrade or update to AE Services on page 109.

Before you begin

- Take the AE Services backup.
- Ensure that all the pre-requisite patches are installed.

  For more information about the patches, see Avaya Aura® Release Notes on Avaya Support Website at http://support.avaya.com.
- Complete and configure Operating System installation.

Procedure

1. Install Linux® Operating System RHEL 8.4 or RHEL 8.10 (64 Bit) with all security updates applied. See Installing the Linux software for AE Services on page 110.
2. Open an ssh session to the AE Services server and access an account with root privileges.
3. If you are installing from a DVD, insert the disk into the DVD drive on the AE Services server.
   - If the Autorun RPM is installed and configured on the server, the installation program starts automatically and the Navigating the dialog boxes screen is displayed. Continue with Step 7.
   - If the installation program does not start automatically, mount the DVD by entering the command `mount mountpoint/install` where *mountpoint* is the name of the media directory. For example, `mount /media/cdrom`.

     The Navigating the dialog boxes screen is displayed. Continue with Step 7.

4. If you are installing from an ISO image, download the ISO image to the `/tmp` directory of the AE Services server and then do one of the following:
   - Mount the image using the **`mount`** command. For example, `mount -t iso9660 -o loop /tmp/swonly-<build-number>.iso` *`mountpoint`* where, *mountpoint* is the name of the media directory, for example, `/media/cdrom`.
   - Start the installation program manually by typing the following command (assuming the *mountpoint* is `/media/cdrom`): `/media/cdrom/install-10.2.x.0.0.x-0`.

   The Navigating the dialog boxes screen is displayed. Continue with Step 7.
5. Press **Enter** to continue with the server software installation.
6. If a previous release of AE Services software is detected, the Uninstall Previous AES Release screen is displayed.
7. Press **Enter** to select **Yes**.

   Note:

   If you select **No**, the installation terminates.

   The installation program uninstalls the previous release of AE Services.
8. Press **Enter** to continue.
9. In the Select Installation Media screen, highlight **OK**, and press **Enter**.
10. Enter a selection to enable (recommended) or disable Avaya Login access for Enhanced Access Security Gateway (EASG). For additional information about how to enable or disable EASG after initial deployment or mange the EASG site certificate, see *Administering Avaya Aura® Application Enablement Services*.

    Note:

    Enable:(Recommended):

    By enabling Avaya Logins, you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

    In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

    Disable:

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

    Enter `1` to Enable EASG (Recommended), or enter `2` to Disable EASG.

Note:

All earlier AE Services releases require a new license file when upgrading to AE Services 8.0 and later.

11. Select the media from which to install, then highlight **OK** and press **Enter**.
12. In the Enter RPM URL screen, type the path name you used in Step 6, for example:

    `/media/cdrom`
13. Highlight **OK** and press **Enter**.
14. In the Select Release Version screen, verify the release you are installing; then highlight **OK** and press **Enter**.
15. In the Co-residency warning screen, highlight **Yes** and press **Enter**.
16. In the Choose Installation Method screen, verify that **Install Install/Update** is selected; then highlight **OK** and press **Enter**.

    The Choose Installation Packages screen is displayed with the following packages selected:

    - MVAP Avaya AE Services
    - Third Party Third_Party_Packages
17. Highlight **OK** and press **Enter**.

    The Optional Packages screen is displayed with the following packages selected:

    - aesvcs-linux-config – The Linux Configuration Package for AE Services.
    - cs-cusldap – The LDAP Configuration Package for AE Services.
    - cs-service – The Avaya Services package.
18. Select the optional packages that you want to install.

    - **`aesvcs-linux-config`** - The Linux configuration package (selected by default). Avaya strongly recommends that you accept the default.
    - **`cs-cusldap`** - Configures a Lightweight Directory Access Protocol (LDAP) directory in the default location of /etc/openldap (selected by default). Unless you are installing AE Services on a server that already has an implementation of LDAP installed, Avaya recommends that you accept the default.

      Caution:

      If you are using your own implementation of LDAP, clear this selection. (Selecting the cs-cusldap option will overwrite your existing LDAP directory). To use your existing LDAP directory with AE Services you will need to manually configure your LDAP implementation for compatibility with AE Services User Management. For this procedure, see Configuring the LDAP server on page 118.

- **cs-service** - The Avaya Services package. Select this option only if you have a technical support contract with Avaya. This package provides tools and information, including a Services login, for Avaya support personnel (not selected by default).

  The Last chance to abort -- Ready to Proceed? window appears.

19. Verify the installation command. If all options are correct, press **Enter** to select **Yes**.

    The software installation proceeds. The time required to install the software varies depending on the packages you selected and the server processing power. Allow 5 to 10 minutes for the installation. When the installation is complete, the system displays the following message:

    ```
    Success, Installation/Update completed
    ```

20. After the installation is complete, press **Enter** to exit.

    - If the installation is successful, the system displays the following message:

      ```
      Installation Successful — Install/Upgrade log file is
      in /var/log/avaya
      ```

    - If the installation is unsuccessful, the system displays the following message:

      ```
      Installation/Update failed
      ```

      Check the installation log files.

21. Press **Enter** to select **OK**.
22. Reboot the server.
23. If you ran the AE Services installation from a DVD-ROM, remove the DVD ROM, or DVD as applicable.
24. Restore the database. See Restoring the Database on page 101.
25. Remove the old AE Services license file. See Uninstalling the AE Services license on page 138.

    When AE Services is upgraded to Release 8.1.2.1 and later, the Host ID utilized by the embedded Avaya WebLM server will change. The original license will not be valid since it is based on a different Host ID and the system will enter into a 30 day license error grace period. Hence, a new license must be created based on the new Host ID. For more information, see the latest Product Support Notices (PSNs) on Avaya support site at https://support.avaya.com.

26. Obtain the new AE Services license file. See Obtaining the AE Services license file on page 138.
27. Install the new AE Services license file. See Installing the AE Services license on page 135.

Validating the configuration settings

About this task

This procedure is required for all upgrades.

Follow this procedure to verify the upgrade. Recall that when the upgrade script completes and the AE Services server reboots, your administrative workstation loses its connection to the AE Services server. You must open an ssh session to the AE Services server.

Procedure

1. Open an ssh session to the AE Services server, and access the root account. See Opening an ssh session to AE Services on page 122 for more information.
2. From the command line, run the command **`swversion`** and verify that the version number and build number are correct.

   Caution:

   If the version number and build number are not correct, do not continue with this procedure. Troubleshoot your installation, and determine if you need to repeat the upgrade procedure.
3. From your browser, log in to AE Services Management Console as a user with System Administration privileges.
4. From the main menu, select **Networking > AE Service IP (Local IP)**.
5. Compare the settings on the AE Service IP (Local IP) page with the settings you recorded in Recording the local IP settings on page 113.
6. From the main menu, select **Networking > Network Configure**, and verify that the NIC configuration settings are correct for AE Services.
7. From the main menu, step through the following menu items and verify that all services are running and properly configured: AE Services, Communication Manager Interface, Licensing, Maintenance, Security, Status, and User Management.

Configuring the LDAP server

About this task

Use this procedure to manually configure your LDAP server for User Management.

Procedure

1. Copy the mvapus schema file named `mvapus.schema` from `/var/mvap/config/cus` to the LDAP schema directory at `/etc/openldap/schema`.

2. Edit the `core.schema` file at `/etc/openldap/schema/` as follows:
   a. Locate the **userid** attribute specification section.
   b. Type `ORDERING caseIgnoreOrderingMatch` after the line **EQUALITY caseIgnoreMatch**.
   c. Save the schema file.
3. Edit the `slapd.conf` file at `/etc/openldap/` as follows:
   a. Type the following include statement to the already existing set of \include statements: include `/etc/openldap/schema/mvapus.schema`
   b. Note the suffix value used in the current `slapd.conf` file.
   c. Save and close the `slapd.conf` file.
4. Modify the `init.ldif` file to match the chosen **organizationalUnit** for the \users and the existing suffix used by the enterprise as follows:
   a. Delete the first entry in the `init.ldif` file.
   b. Update the second entry to reflect the desired **organizationalUnit**.

      For example, ou=users
   c. Update the **DN** attribute of the next two entries to reflect the chosen **organizationalUnit** and suffix in use in the enterprise.
   d. Save and close the `init.ldif` file.
5. Restart the LDAP server.
6. Use the ldapadd tool or equivalent to add the entries in the `ldif.init` file into the LDAP server.

   For example, `ldapadd -x -D` *`bind credentials DN`* `-W -f init.ldif`

Chapter 9: AE Services updates and patches

AE Services updates and patches

Avaya periodically provides updates and patches for the AE Services software.

- An update provides new features or enhancements to the AE Services system. An update might also include bug fixes. Avaya releases updates only on an as-needed basis for critical fixes. Updates are effected by the **`update`** command.
- A patch addresses a specific issue related to a specific component or a set of components in the AE Services system.

When you install an update or patch:

- The install script installs the new version of the RPMs in `/var/disk/software`.
- The update script backs up the current RPM before installing the new version of the RPM.

The /var/disk/software directory also contains all of the previous versions of the RPMs. To see all updates or patches installed on a server, use the **`swversion -a`** command.

Note:

When updates and patch releases become available, see the Release Notes for a particular update or patch release.

Installing AE Services updates and patches using CLI

About this task

AE Services updates and patches consist of .bin files of RPMs. You can apply multiple updates or patches to the system. To see all the updates or patches installed on the server, use the **`swversion -a`** command.

Updates and patches are available on the following Web sites:

- Avaya Support Web site: http://www.avaya.com/support
- Avaya Product Licensing and Delivery System (PLDS) Web site: https://plds.avaya.com.

Check these sites periodically to see if there is a new patch that applies to your system.

Caution:

Always use the procedure described in this book, *not* an RPM command, to install AE Services updates or patches.

Procedure

1. From the AE Services Management Console, back up the server data before you install an update. See Backing up the AE Services server data on page 40.
2. Download any new patch or update files to the current directory on the AE Services server.
3. To provide executable permission to the patch file, run the command **`chmod +x <xxxx>`** where *xxxx* is the name of the downloaded file.
4. Open an ssh session to the AE Services server and access an account with root privileges. See Opening an ssh session to AE Services on page 122 for more information.
5. From the command line, type `./xxxx.bin` where *xxxx* is the name of the downloaded file.

   The system displays the update or patch ID and the RPMs contained in the package. The system then prompts you to confirm the installation of the RPMs.

   - If you type `y`, the installation of the update or patch proceeds. The system:
     - Stops AE Services, Tomcat service, and DBService.
     - Installs the RPMs contained in the package.
     - Restarts AE Services, Tomcat service, and DBService.
     - Once the upgrade is successful, wait for 5 minutes before accessing the AE Services OAM page.
   - If you type `n`, the installation of the update or patch terminates.
6. To verify the version of the AE Services application, run the command **`swversion`**.
7. To reconfigure AIDE, run the following command:

   ```
   /opt/mvap/bin/setAIDE configure
   ```

Chapter 10: Post-upgrade verification

Post-upgrade checklist

Sr. No.	Task	Link/Notes	✔
1	Verify the software version of Avaya Aura® Application Enablement Services.	-	
2	Install the license file.	See Installing the AE Services license on page 135.	
3	Click the **AE Services** link from the navigation bar and verify the following columns next to the required services: • Status • State • License Mode Ensure there is no license specific error.	-	
4	Verify old configurations and ensure they are correct after the upgrade.	-	
5	Click **Status** > **Status and Control** on the navigation bar and verify detailed status of individual links.	-	
6	Configure the EASG settings, if required.	See Enhanced Access Security Gateway (EASG) overview on page 124.	
7	Rollback the upgrade in case the upgrade fails.	See Rolling back an upgrade on page 129.	

Opening an ssh session to AE Services

About this task

This procedure assumes that you have a secure shell (ssh) client, such as PuTTY or PuTTYtel running on your administrative workstation.

Procedure

1. Start your ssh client, and complete the information in the dialog box that it presents to open a session. For example, specify the following information to open a session to the AE Services server.
   - Host Name (or IP address) - enter the host name or IP address of your AE Services server, for example, `aeserver.example.com`.
   - Port - enter `22`.
   - Connection type - enter `SSH`.
   - Click **Open**.

   Note:

   The server displays the PuTTY Security Alert window the first time you connect to the SAMP. If you see this window, click **Yes** to accept the server's host key.

   The system displays the PuTTY window.
2. If you are an Avaya service technician or Business Partner, log in as follows:
   a. At the login as: prompt, type `craft`.
   b. At the prompt, type the challenge/password.
   c. At the command prompt, type `su - sroot`.
   d. At the prompt, type the challenge/password.
3. If you are a customer, log in as follows:
   a. At the login as: prompt, type `cust`.
   b. At the password prompt, type the password for the cust account.
   c. At the command prompt, type `su - root`.
   d. At the password prompt, type the password for the root account.

Logging on to the AE Services Management web console

About this task

Important:

You cannot log in to the AE Services Management web console with root credentials.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name/IP address>`, the AE Services URL.

   For example: `https://aserver.example.com`

If you are accessing the AE Services server for the first time, the browser displays a security alert for an SSL certificate.

If the SSL certificate is not presented, verify that the address bar on your browser displays https and the fully qualified domain name or IP address of the AE Services server.

2. On the Security alert window, click **Yes** to accept the certificate.
3. On the Application Enablement Services welcome page, click **Continue To Login**.
4. On the Application Enablement Services Management web console login page, in **Username** , type the login ID.
5. Click **Continue**.
6. In **Password**, type the password.

   When logged in as a service technician, and if the Enhanced Access Security Gateway (EASG) is present, your login ID is challenged by EASG. You must enter a proper response in the **Response** field to log in successfully.

   For customer user login credentials, these options are not presented.
7. Click **Login**.

   The browser displays the Application Enablement Services Management web console. The main menu is in the left pane and the welcome page is in the right pane.

   Note:

   If you are logging in for the first time, AE Services displays the End User License Agreement page.

Enhanced Access Security Gateway (EASG) overview

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

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, remove, restore or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message:

      ```
      By enabling Avaya Services Logins you are granting Avaya access
      to your system. This is required to maximize the performance
      and value of your Avaya support entitlements, allowing Avaya to
      resolve product issues in a timely manner.

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the
      Avaya support site (https://support.avaya.com/ registration)
      for additional information for registering products and
      establishing remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled.`

3. To disable EASG, do the following:

   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message:

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

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is disabled.`

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **`EASGProductCert --certInfo`**.

   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge or response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. Log in to the AE Services CLI interface as an administrator associated with the Linux group, easg.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate, run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates currently installed on the system.

Upgrade job status

Upgrade job status

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job.

You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s)**: To get the latest data like version data for the applications in the system.
2. **Analyze**: To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check**: To evaluate an application that completed the Analyze job.
4. **Upgrade**: To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit**: To view commit jobs.
6. **Rollback**: To view rollback jobs.
7. **Uninstall**: To view uninstall jobs.

Viewing the Upgrade job status

Procedure

1. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

   System Manager displays the status of the upgrade job type that you selected.

Editing an upgrade job

Before you begin

Upgrade job status must be in pending state.

Procedure

1. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

   System Manager displays the status of the upgrade job type that you selected.
4. Select a pending upgrade job to edit.

5. Click **Edit Configuration**.

   System Manager displays the Upgrade Configuration page.
6. Edit the required fields.

Deleting Upgrade Jobs

Procedure

1. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

   System Manager displays the status of the upgrade job type that you selected.
4. Click **Delete**.

   System Manager updates the Upgrade Job Status page.

Upgrade Job Status field descriptions

Name	Description
Job Type	The upgrade job type. The options are: • **Refresh Element(s)**: To view refresh elements jobs. • **Analyze**: To view analyze jobs. • **Pre-Upgrade Check**: To view preupgrade check jobs. • **Upgrade**: To view upgrade jobs. • **Commit**: To view commit jobs. • **Rollback**: To view rollback jobs. • **Uninstall**: To view uninstall jobs.
Job Name	The upgrade job name.
Start Time	The time when the system started the job.
End Time	The time when the system ended the job.
Status	The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.
% Complete	The percentage of completion of the upgrade job.
Element Records	The total number of elements in the upgrade job.
Successful Records	The total number of times that the upgrade job ran successfully.
Failed Records	The total number of times that the upgrade job failed.

Button	Description
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Rollback process

Upgrade rollback

The upgrade rollback is initiated in two cases:

- Upgrade process of an element fails: Administrator need not rollback upgrade of all the elements. When the element upgrade fails, the system stops the entire upgrade process and displays the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- Upgrade process of the entire system fails: Admin specifies rollback all when the system upgrade fails. The system stops the upgrade and rolls back the overall upgrade process.

Rolling back an upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.

   The system selects the parent of the application that you select and all child applications of the parent.
4. Click **Upgrade Actions** > **Rollback**.

Related links

Rolling back the SMS RPMs manually on page 129

Rolling back the SMS RPMs manually

About this task

When you are rolling back from Release 10.2.x to any previous release AE Services server, SMS RPMs are not downgraded to the previous release versions automatically. Use the following procedure to downgrade the SMS RPMs manually.

Procedure

1. Log in to the AE Services CLI interface and switch to root user.

2. Run the following commands to get the release-id string of the aesvcs-sms rpm:

```
cd /var/disk/rpms
```

```
ls | grep aesvcs-sms
```

   Single or multiple rows are displayed.

3. Select the RPM release-id that matches with the current AE Services version.
4. Run the following command with the release-id replaced with the text that you got from step 2:

```
rpm -U --oldpackage --force /var/disk/rpms/aesvcs-sms-<release-id>-0.noarch.rpm --nodeps
```

Related links

Rolling back an upgrade on page 129

Chapter 11: AE Services licensing

Application Enablement Services license requirements

To get the full functionality for Application Enablement Services, you must install the Application Enablement Services product license. The product license specifies the features you are permitted to use. For more information about licensed features, see *Avaya Aura® Application Enablement Services Overview and Specification*.

Licensing overview

Use this overview to learn about the licensing cycle and when licensing events take place.

- Obtain the license from the Avaya Product Licensing and Delivery System (PLDS) website.
- After you install the AE Services software, log in to the AE Services Management Console to access the Avaya Web License Manager (WebLM).
- Use WebLM to install the license.
- After you install the license file, you must reboot the AE Services server.
- When the license file is installed, you will have access to the AE Services software.

Embedded Avaya WebLM server

Embedded Avaya WebLM Server and AE Services

This feature is supported on all AE Services offers. The license file is deployed inside a AE Services server running on Tomcat.

The license file installed on the embedded Avaya WebLM server uses the AE Services host ID.

Note:

If the eth0 IP address is changed, you must obtain a new license file.

Embedded Avaya WebLM Server and Geographic Redundancy

Obtain the Avaya WebLM host ID from both AE Services servers prior to configuring Geographic Redundancy.

- For the Geographic Redundancy feature to be activated, the license file generated for embedded Avaya WebLM server requires host IDs of both AE Services servers within the license file.
- If Geographic Redundancy is already configured, disable HA to get the Avaya WebLM host ID from each AE Services server.

Embedded Avaya WebLM support by release

Embedded Avaya WebLM is supported on all AE Services Software-Only offers.

From Release 7.0.1 and later, AE Services VMware offer supports Embedded Avaya WebLM.

Extended Avaya WebLM service feature

Extended Avaya WebLM service supports Avaya WebLM service deployed on System Manager or standalone Avaya WebLM server.

Enterprise Wide Licensing

In pooled mode, multiple AE Services servers share a pool of licenses installed on an external master Avaya WebLM server.

In allocation mode, a pool of licenses are subdivided and distributed to a local (or embedded) Avaya WebLM server from a master Avaya WebLM.

For a more responsive AE Services server, use allocation mode with embedded Avaya WebLM servers.

HTTPS, WebLM, and AE Services

HTTPS is used for connecting a Master Avaya WebLM server and the AE Services Avaya WebLM client or embedded Local Avaya WebLM. The Master Avaya WebLM server can operate in an allocation mode or a pooled mode or both. For the allocation mode, the Master Avaya WebLM server acts as a client of the AE Services embedded Avaya WebLM to establish an HTTPS session and push a license file down to the AE Services embedded Local Avaya WebLM. For the pooled mode, the AE Services C++ and Java Avaya WebLM clients establish an HTTPS session to the Master Avaya WebLM server or the AE Services embedded Local Avaya WebLM to acquire a license.

During the TLS handshake, for an HTTPS client-server session, the server must send its identity certificate to the client and the client must validate the server's identity certificate. For example, the Not Before date and the Not After date timeframe is valid, and the server identity certificate was signed by a trusted Certificate Authority (CA) known by the client. If the client is unable to validate the server's identity certificate, the handshake connection is terminated.

Note:

- For the pooled mode, the Master Avaya WebLM CA certificates must be imported into the AE Services Trusted Certificate store using the AE Services Management Console.

- For the allocation mode, the AE Services Apache Web server CA certificates must be imported into the Master Avaya WebLM trust store.

While attempting to connect to Avaya WebLM from the AE Services server or from a Master Avaya WebLM to the AE Services embedded Local Avaya WebLM, the connection might not get established. The following are some troubleshooting suggestions:

- Pooled mode: Using the Management Console, verify that the CA certificate used to sign the Master Avaya WebLM server's identity certificate is in the AE Services Trusted Certificate store. For a default System Manager installation where the Master Avaya WebLM is also embedded, the System Manager's embedded CA is used to sign the System Manager server identity certificate. Each System Manager deployment creates its own unique CA certificate with the same Common Name. Therefore, when validating whether the System Manager CA certificate is installed on the AE Services server, ensure that the System Manager CA certificate Serial ID matches the Serial ID of the System Manager CA certificate in the AE Services trust store.
- Allocation mode: Verify that the CA certificate used to sign the AE Services server identity certificate is in the Master Avaya WebLM trust store.
- Verify that the port is not blocked by a firewall.
- Verify that the Avaya WebLM server identity certificate has not expired.
- Check the AE Services log files for a TLS/SSL connection error, for example, using an unknown certificate.

Connecting to Avaya WebLM server

About this task

Use this procedure to specify the IP address and port number of the Avaya WebLM server that Application Enablement Services uses for licensing.

From the AE Services Release 7.1.3, do not enter Avaya WebLM credentials to log in to the Embedded Avaya WebLM interface. The change password link on the Avaya WebLM user interface does not work. if you changed the password, log out and log in again to Avaya WebLM. The Avaya WebLM login credentials are required only to log in to the external WebLM.

Procedure

1. On your web browser, log in to AE Services Management Console.
2. On the AE Services Management Console main menu, click **Licensing** > **WebLM Server Address**.
3. In the **WebLM IP Address** field, enter the IPv4 address of the remote Avaya WebLM server to point your AE Services server to the Avaya WebLM server.

   If AE Services requires to use the embedded Avaya WebLM server, enter the IP address `127.0.0.1`.
4. Select the **SSL** check box to specify the appropriate setting for SSL.

   By default the **SSL** check box is selected.

5. In the **WebLM Port** field, enter the port number of the WebLM server.

   Note:

   If System Manager WebLM server is used, import the System Manager CA certificate.

   The configuration for Secondary WebLM is optional.

   AE Services uses secondary WebLM server for licensing only if the primary WebLM server is not available and you have configured the **Secondary WebLM IP Address**.

6. In the **Secondary WebLM IP Address** field, enter the IPv4 address of the secondary WebLM server to point your AE Services server to the WebLM server.
7. Select the **Secondary SSL** check box to specify the appropriate setting for SSL.
8. In the **Secondary WebLM Port** field, enter the port number of the secondary WebLM server.

Logging in to WebLM and creating a WebLM password

About this task

The Web License Manager (WebLM) provides you with the ability to install and manage Avaya product licenses. The first time you run a WebLM session, you must create a new WebLM password.

Note:

Before you start this procedure, make sure your browser allows pop-up windows from avaya.com.

Note:

This procedure is not applicable for Embedded WebLM as no password is required to login in Embedded WebLM.

Follow this procedure to access WebLM from the Application Enablement Services Management Console.

Procedure

1. In the address bar of your browser, type `https://`*`fully-qualified domain name or IP address of the AE Services server`* and press ENTER.
2. From the Application Enablement Services welcome page, click **Continue to Login**.
3. From the Application Enablement Services Management Console log in page, type your user name and password, and click **Login**.

Important:

You cannot log in to the Application Enablement Services Management Console as the root user. Avaya service technicians should log in as craft. Customers should log in as cust.

Your browser displays the Application Enablement Services Management Console. The main menu is in the left pane and the welcome page is in the right pane.

4. From the main menu, select **Licensing > WebLM Server Access**.
5. Follow these steps to complete the Web License Manager Logon screen.
   a. In the User Name field, type `admin`, the default WebLM User name.
   b. In the Password field, type `weblmadmin`, the default WebLM password.
   c. Click the arrow.

      The first time you log in to WebLM, the server displays the **Change Password** page.
6. Complete the fields on the Change Password page and click **Submit**.

   Your browser displays the login page again.
7. Log in as `admin` with the password you just created.

Installing the AE Services license

About this task

To get the full functionality for AE Services you must install the AE Services license. Avaya sends the AE Services license file in an email message. If you did not receive a license file from Avaya, see Obtaining the AE Services license file on page 138. If you are upgrading from AE Services 6.x and you already have a license on a remote WebLM server (for example, the license was installed on a standalone WebLM server or System Manager), you need another license file. Uninstall the license file if you are upgrading from a major release to another release.

All earlier AE Services releases require a new license file when upgrading to AE Services.

Note:

By default, the AE Services server has a 30-days grace period. If a license file is not installed, the AE Services server enters in License Error mode. In License Error mode, you have 30-days in which to install a valid license file for AE Services. Error mode may also occur if an invalid (expired or incorrect) license file has been installed.

Procedure

1. Log on to the AE Services Management Console and click **Licensing** > **WebLM Server Access**.
2. On the Web License Manager Logon page, type your WebLM user name and password, and click the arrow.

3. On the WebLM Install License page, click **Browse**.
4. Locate the AE Services license file, and select it.
5. With the license file name displaying in the text box, click **Install**.

   WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message **License file installed successfully**.

   Note:

   If you do not receive this message, see Troubleshooting licensing error messages on page 137.
6. Verify that the license settings.
   a. Click **Licensed Products** > **Application_Enablement**.
   b. Verify that the correct license settings are enabled.
7. Click **Logout**.
8. Restart AE Services.

   See Restarting AE Services from the AE Services Management Console on page 137 or Restarting AE Services from the Linux command line on page 136.

Restarting AE Services from the Linux command line

About this task

You must restart AE Services to use the capabilities of the license. You can restart AE Services from the command line or through the Application Enablement Services Management Console, the web-based administrative interface.

Follow this procedure to restart AE Services from the command line.

Procedure

1. Open an ssh session to the AE Services server, using either of the following methods.
   - Customers using the Avaya Services package: Log in as cust, and access the root account by using the **`su - root`** command.
   - Avaya service technicians: Log in as craft, and access the root account by using the **`su - sroot`** command.
2. Restart AE Services using the following command: **`systemctl restart aesvcs.service`**.

Result

The **`restart`** command stops AE Services, configures them, and then starts the services. The restart process takes from 3 to 10 minutes.

Restarting AE Services from the AE Services Management web console

About this task

Use this procedure to restart AE Services through the AE Services Management console to use the capabilities of the new license. You can also restart AE Services from the command line interface.

Procedure

1. Log in to the AE Services Management web console.
2. On the AE Services Management web console, click **Maintenance** > **Service Controller**.
3. On the Service Controller page, click **Restart AE Server**.
4. On the Restart AE Server page, click **Restart**.

   After a pause, the AE Services server returns to the Service Controller page. A restart can take several minutes.
5. Verify that all the correct licensed services are running.

Troubleshooting licensing error messages

If your browser displays an error message, try to resolve the problem as shown in the following table. If you cannot resolve the problem, contact your Avaya representative.

Error message	Explanation
`License file is invalid or not created for this server. License file was NOT installed.`	The file is corrupt or the Host ID in the license file does not match the Host ID in the server. For more information, see Identifying the Host ID using WebLM on page 138.
`Attempting to install a license file that is currently installed. License file was NOT installed`	This license is already active.
`More than one license exists, the AE Server will not be started. Please have only one valid license and delete other licenses.`	A valid license already exists due to an upgrade from an earlier release. You must remove the old license before you install the new license for the latest major release. See Uninstalling the AE Services license on page 138.

Table continues…

Error message	Explanation
`No valid license file found`	WebLM might display this message on the main page after AE Services reports "`License file installed successfully`". To resolve this problem: 1. Verify you are using the AE Services server host name, and not the IP address. 2. If the host name is correct, contact your Avaya representative.

Obtaining the AE Services license file

Procedure

1. Determine the Host ID of the first NIC on the server.

   See Identifying the Host ID using WebLM on page 138.
2. Log in to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
3. Provision the license file.
4. Download the license file.

Identifying the Host ID using WebLM

About this task

If AE Services software is already installed, you can use WebLM to identify the Host ID.

Procedure

1. Navigate to WebLM.
2. On the WebLM Home page, click **Server properties**.
3. On the Server Properties page, locate the value for Primary Host ID.

Uninstalling the AE Services license

Procedure

1. Navigate to WebLM.

2. From the main menu, click **Uninstall License**.
3. From the Uninstall License page, select the check box for the Application_Enablement license, and click **Uninstall**.

   Your browser displays a message asking if you want to continue.
4. Click **OK**.

Chapter 12: Resources

Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Application Enablement Services Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide	Installing TSAPI and CVLAN Client and SDK	Customers and sales, services, and support personnel
Using		
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administering Avaya Aura® Application Enablement Services	Administering Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel
Avaya Aura® Application Enablement Services Data Privacy Guidelines	Describes how to administer Application Enablement Services to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation		
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in Software-Only and Infrastructure as a Service Environments	Implementation personnel
Maintenance and Troubleshooting		

Table continues…

Title	Description	Audience
Maintaining Avaya Aura® Application Enablement Services	Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 141
Accessing the port matrix document on page 141
Avaya Documentation Center navigation on page 142

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

Application Enablement Services documentation on page 140

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

Application Enablement Services documentation on page 140

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

Application Enablement Services documentation on page 140

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
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

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

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

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

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Related links

Using the Avaya InSite Knowledge Base on page 145

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 144

Chapter 13: Appendix

Avaya Aura® Security Service Packs overview

With Avaya Aura® Release 10.1.x, Avaya introduced a common version of Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 to its Avaya Aura® platform. With the common versions of RHELs, Avaya has also changed how it provides and installs Security Service Packs (SSPs). Following Avaya Aura® applications support RHEL:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services

Note:

- Beginning with Communication Manager Release 10.1, security updates (Linux and Kernel) are provided in an SSP. There is no longer a separate Kernel Service Pack (KSP).
- Beginning with Application Enablement Services Release 10.1, Linux Security Updates (LSU) are now provided in an SSP. LSU is no longer available.

SSPs are cumulative for each release. The current SSP for a release includes the fixes from all previous SSPs for that release.

SSPs are applicable for Avaya Aura® Release 10.2.x running on:

- Avaya Solutions Platform 130 Release 5.1.x
- Avaya Solutions Platform S8300 Release 5.1 (For Communication Manager or Branch Session Manager)
- Avaya Solutions Platform 130 Release 6.0 (KVM on RHEL 8.10)
- Customer-provided VMware® certified hardware

Note:

SSPs are not applicable for Software-Only deployments.

SSPs are applicable to Avaya Aura® OVA-based 10.2.x deployments.

SSP file format and command

File format of SSP is as follows:

`AV-<product name><mainline release version>-RHEL<number>-SSP-<SSP #>-<build #>.tar.bz2`

Where:

- **<product name>:** Name of the application.

  For example:

<product name>	Application
CM	Communication Manager
SMGR	System Manager
SM	Session Manager
AES	Application Enablement Services

- **<Mainline release version>:** Mainline release version for the application. For example, 10.1.
- **RHEL <number>:** RHEL version used in the Avaya Aura® application. For example, RHEL 8.4 or RHEL 8.10.
- **SSP-<SSP #>:** A three-digit number that defines the SSP version. For example, the first SSP # is 001.
- **<build #>:** Build number associated with the SSP version. For example, `AV-CM10.2-RHEL8.X-SSP-001-05.tar.bz2`.

You can use the **`av-update-os`** command to install SSP and the **`av-version`** command to view the SSP version running on the application.

SSPs product change notice (PCN) reference

- For more information about Avaya Aura® System Manager 10.2.x SSP - S2 - Software, see PCN2163S.
- For more information about Avaya Aura® Session Manager 10.2.x SSP - S2 - Software, see PCN2161S.
- For more information about Avaya Aura® Communication Manager 10.2.x SSP - S2 - Software, see PCN2159S.
- For more information about Avaya Aura® Application Enablement Services 10.2.x SSP - S2 - Software, see PCN2165S.
- For more information about Avaya Aura® WebLM 10.2.x SSP - S2 - Software, see PCN2167S (For future use upon the release of Avaya Aura® WebLM R10.2.x.)

Appendix A: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10)

Virtual Machine Backups (clone) as an alternative to snapshots

Avaya Aura® documentation refers to snapshots at the application level for various procedures. Snapshots apply to a VMware environment.

With the introduction of the alternative hypervisor in Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), RHEL 8.10 does not support snapshots and Linux does not support issues relating to the use of snapshots.

Virtual machine backup is a similar feature to snapshots. Virtual machine backups use the cloning feature. Use virtual machine backups in place of snapshots for ASP R6.0.x (KVM on RHEL 8.10).

You should only keep backups for a maximum 48 hours in order to ensure sufficient storage is available. You may need to remove them earlier.

Note:

The images and screenshots in this document are for illustration purposes only. The actual user interface may slightly vary due to updates and design changes.

Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to create a clone for backup purposes.

Before you begin

- Ensure there is sufficient space to create the Virtual Machine Backup (clone). Clones are created as “thick provisioned” and require the same size as the virtual machine you are cloning.

- Refer to application documentation for guidelines on storage requirements for different application profiles.
- Shut down the virtual machine for which you are creating a backup (clone). This is a service impacting activity. Perform these steps within a customer-approved maintenance window.

Note:

You must be root or use `sudo` with `custadm` account for CLI commands, and you must enable Administrative access when using the Cockpit user interface.

Note:

These clones must be created through the CLI as the Cockpit UI does not support the necessary required options.

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

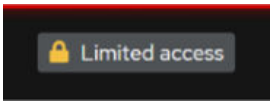


Figure 1: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.

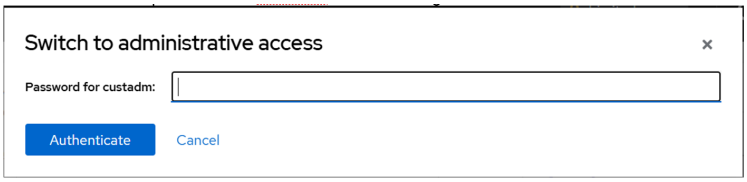


Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

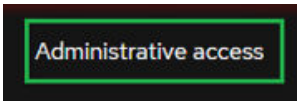


Figure 3: Administrative access button

4. Navigate to **System** > **Virtual Machines** > **Storage Pools**.

The Name guest_images is a label for `/var/lib/libvirt/images`. If you select guest_images, you can see additional information. If you select Storage Volumes, you can view all images in the `/var/lib/libvirt/images` directory.

5. Review the images and remove any of them that you no longer use.

   Images that do not have a 'Used by' value are typically safe to remove.

6. Confirm that you have the necessary space for your clone.
7. Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Run the following command to obtain a list of all virtual machines:

   ```
   sudo virsh list --all
   ```

   Example output:

   ```
   [custadm@asp130-r660xs-a31p ~]# sudo virsh list --all

   Id          Name                                State9
   ----------------------------------------------------------
   1           8HDD-RHEL-810-Fiotester2         running
   2           8HDD-RHEL810-Fiotester1          running
   -           8HDD-RHEL-810-Fiotester3         shut off
   -           8HDD-RHEL-810-Fiotester3-Clone   shut off
   -           8HDD-RHEL-810-Fiotester3-clone   shut off
   -           Agent_Testing                    shut off
   -           Agent_Testing-Clone              shut off
   -           Agent_Testing2                   shut off
   -           Agent_Testing3                   shut off
   ```

   In this example, the virtual machine Agent_Testing3 is shut off state, ready for backup (clone).

9. Run the following command to backup (clone) the virtual machine. You must use the nonsparse option to ensure the clone is created as thick provisioned.

   ```
   sudo virt-clone --original <Domain-to-be-cloned> --auto-clone --
   nonsparse
   ```

   Example output:

   ```
   sudo virt-clone --original Agent_Testing3 --auto-clone --nonsparse

   Allocating 'RHEL810-agenttestvm3-fat-clone.qcow2' | 50 GB 00:01:06

   Clone 'Agent_Testing3-clone1' created successfully.
   ```

   This command creates a backup (clone) with default values. You can create a clone with any name for the virtual machine and QCOW2 labels by specifying a full path and using the following command:

   ```
   sudo virt-clone --original <VM Domain> --name <Clone VM Label> --
   file /var/lib/libvirt/images/<VM Domain QCOW2 file name>.qcow2 --
   nonsparse
   ```

   Example for single QCOW2 image:

```
sudo virt-clone --original RHEL810-fiotester1 --name RHEL810-
fiotester2 --file /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
--nonsparse
```

Example for multiple QCOW2 images:

```
sudo virt-clone --original Duplex_Active_974
--name Duplex_Active_974_CloneTest --file /var/lib/
libvirt/images/Duplex_Active_974_CloneTest_system.qcow2
--nonsparse --file /var/lib/libvirt/images/
Duplex_Active_974_CloneTest_Var_Disk.qcow2 --nonsparse
```

Note:

Completion time varies depending on the size of original virtual machine disk.

Calculating space for the clone

About this task

Use this procedure to figure out if you have the necessary space for the clone. This example refers to System Manager but the same information applies to all Avaya Aura® components.

You can use the Cockpit user interface to calculate this information. You can also use the Command Line Interface (CLI). The units of measure may differ. The Cockpit user interface (UI) uses International Electrotechnical Commission (IEC) values, such as Gibibyte. The CLI uses International System of Units (SI) values, such as Gigabyte.

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

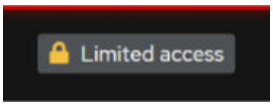


Figure 4: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.

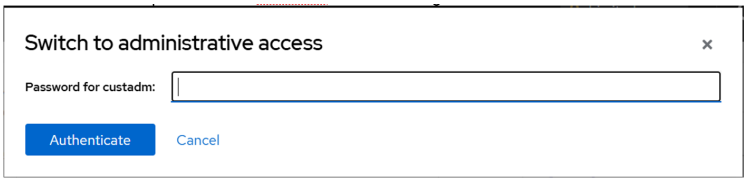


Figure 5: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

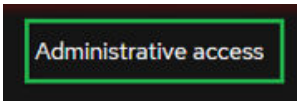


Figure 6: Administrative access button

4. Navigate to **System** > **Virtual Machines** > **Storage Pools**.
5. View the information on the **Storage Pools** screen.
6. Divide the amount of used and available space to get the percentage.

   In this example, approximately 18% of the available storage is used (579.51/3299 ~ 18%).

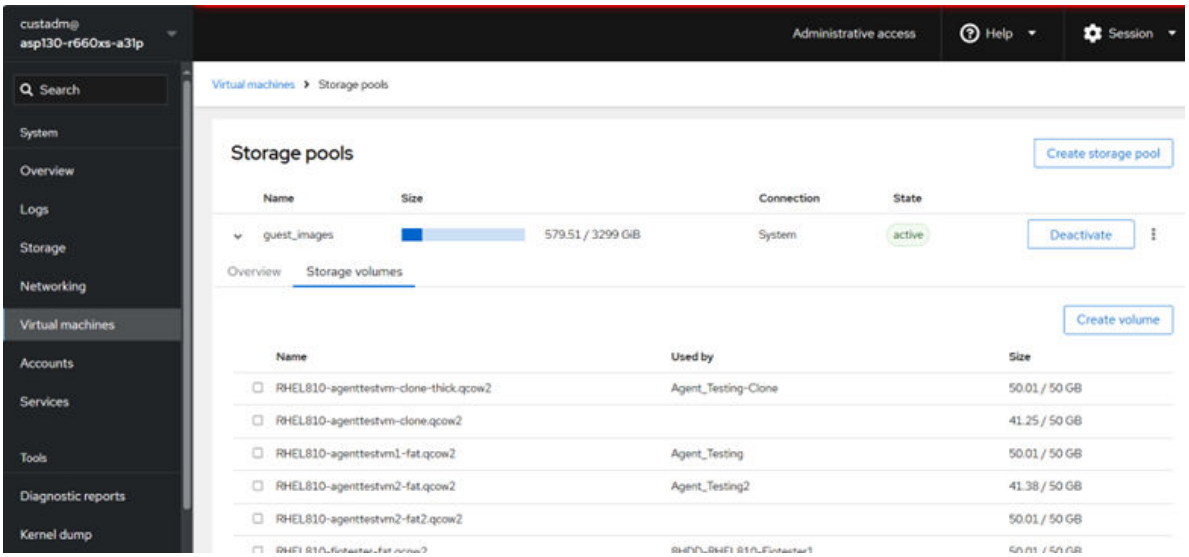


Figure 7: Example size

7. **(Optional)** Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Change the directory to `/var/lib/libvirt/images` and identify the available space.

   In the example below, 18% of available storage is being used on the host.

   Example output:

```
[custadm@asp130-r660xs-a31p ~]$ cd /var/lib/libvirt/images
[custadm@asp130-r660xs-a31p images]$ df -h .
```

```
Filesystem                          Size    Used    Avail   Use%  Mounted on
dev/mapper/vg_system-lv_libvirt     3.3T    580G    2.7T    18%   /var/lib/libvirt
```

Validating a Virtual Machine Backup (clone)

Procedure

1. Login to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
2. Run the following command to validate the backup (clone):

   ```
   sudo virsh list --all
   ```

   Example output:

   ```
   [custadm@asp130-r660xs-a31p ~]# sudo virsh list --all

   Id      Name                                State9
   ----------------------------------------------------------
   1       8HDD-RHEL-810-Fiotester2            running
   2       8HDD-RHEL810-Fiotester1             running
   -       8HDD-RHEL-810-Fiotester3            shut off
   -       8HDD-RHEL-810-Fiotester3-Clone      shut off
   -       8HDD-RHEL-810-Fiotester3-clone      shut off
   -       Agent_Testing                       shut off
   -       Agent_Testing-Clone                 shut off
   -       Agent_Testing2                      shut off
   -       Agent_Testing3                      shut off
   -       Agent_Testing3-clone                shut off
   ```

   In this example, the virtual machine Agent_Testing3-clone is the cloned virtual machine.
3. Confirm that the clone is thick provisioned by running the following command on the clone and ensuring that the virtual size is the same as the disk size:

   ```
   cd /var/lib/libvirt/images

   sudo qemu-img info <clone name>
   ```

   Example output:

   ```
   cd /var/lib/libvirt/images

   sudo qemu-img info Agent_Testing3-clone.qcow2

   image: Agent_Testing3-clone.qcow2

   file format: qcow2

   virtual size: 50 GiB (53687091200 bytes)

   disk size: 50 GiB

   cluster_size: 65536

   Format specific information:

   compat: 1.1
   ```

```
compression type: zlib
lazy refcounts: true
refcount bits: 16
corrupt: false
extended l2: false
```

4. Run the following command to ensure that the virtual machine is cloned with the same disk name that is provided during the backup (clone):

   ```
   sudo virsh domblklist <cloned VM name>_8_1
   ```

   For example, the output of the command appears as follows:

   ```
   hda /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
   ```

5. Log in to the KVM Cockpit web console as **custadm** in the following format: https://*<IP address or FQDN of KVM host>*:9090.
6. For administration actions, on the top-right of the window, click on the **Limited access** button.

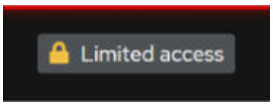


Figure 8: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

7. In the Switch to administrative access window, enter the password for **custadm**.

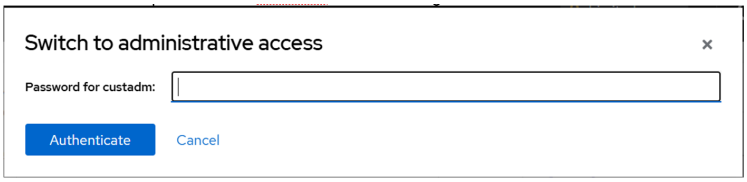


Figure 9: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

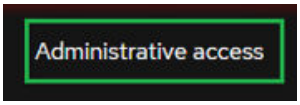


Figure 10: Administrative access button

8. Navigate to **System** > **Virtual Machines**.

9. View the cloned virtual machine in the virtual machines list.

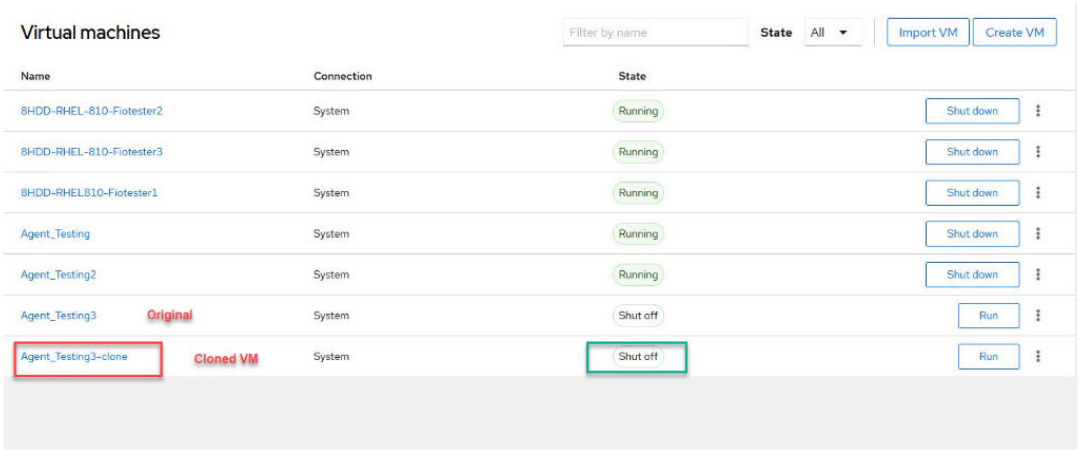


Figure 11: Virtual machines list

Rolling back using the Virtual Machine Backup (clone)

About this task

If you experience a problem during an upgrade, you can roll back to a state using the cloned virtual machine.

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

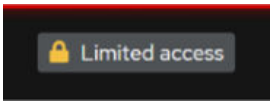


Figure 12: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.

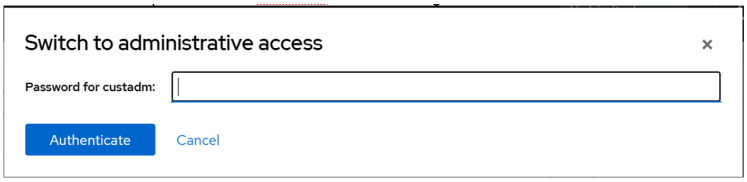


Figure 13: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

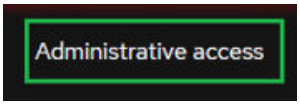


Figure 14: Administrative access button

4. Navigate to **System** > **Virtual Machines**.
5. Shut down the original virtual machine.
6. Rename the original virtual machine.

   For example: `Virtual_Machine_Broken`

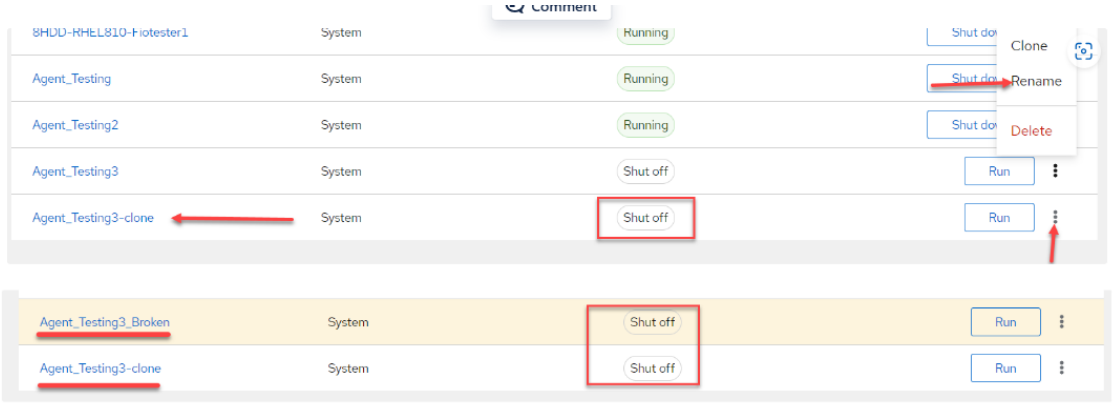


Figure 15: Roll back VM backup

7. While still in a power off state, edit the virtual machine clone Label to match the original virtual machine label. This ensures that the cloned virtual machine becomes the original virtual machine.

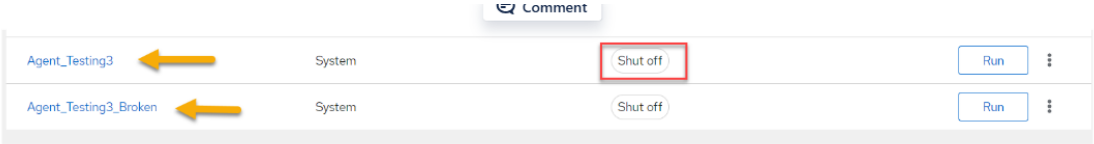


Figure 16: Edit Virtual Machine name

8. Configure the virtual machine that you renamed in step 5 to ensure the network interfaces and state match the broken virtual machine.

For example: `bridge0 and state = up`

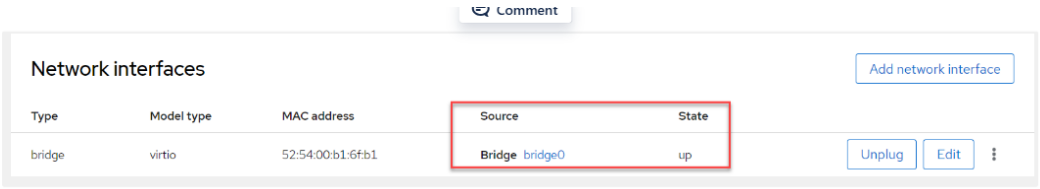


Figure 17: Network interfaces

9. Power on the virtual machine that you renamed in step 5.

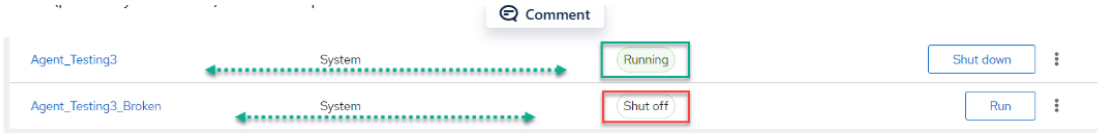


Figure 18: Power on

10. Delete any unused backups.

Appendix B: Upgrading RHEL

Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based Virtual Machines

About this task

You can upgrade RHEL 8.4 to RHEL 8.10 using the following **av-upgrade-os** command. The **av-upgrade-os** command is available when AE Services R10.2.1 is installed.

Before you begin

1. Install AE Services R10.2.1.

   To view the current version of AE Services, run the following command: **update_show**.

2. Verify that **av-upgrade-os** command is available.

   To verify if the **av-upgrade-os** command is available, run the following command: **which av-upgrade-os**

3. Verify the current version of RHEL on which AE Services is running.

   To view the current RHELversion, run any of the following commands:

   - **cat /etc/redhat-release**
   - **av-version**

4. Download AE Services RHEL 8.10 Operating System bundle on AE Services R10.2.1 virtual machine.

Procedure

1. Login to AE Services CLI.
2. To upgrade from RHEL 8.4 to RHEL 8.10, run the following command: **av-upgrade-os <AES RHEL OS Bundle>**

   For example, run **av-upgrade-os AV-AES10.2-RHEL8.10-OSUpdate-001.tar.bz2**

3. After successful upgrade to RHEL 8.10, reboot the AE Services virtual machine.
4. Login to AE Services CLI.
5. To verify that RHEL 8.10 is upgraded successfully, run any of the followig commands:

   - **cat /etc/redhat-release**
   - **av-version**

Glossary

Fully automated upgrade using Solution Deployment Manager	The fully automated upgrade process includes upgrading a product from earlier release to the latest release by using either Solution Deployment Manager Client or System Manager Solution Deployment Manager. In fully automated upgrade all subsequent steps are executed as a single process, including tasks such as backup, deploy, and post upgrade tasks such as applying patches or service packs. For fully automated upgrade using Solution Deployment Manager, the system does not allow to change the IP Address of the application. Alternatively, you can use the Migration using CLI method. To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.
Migration	The migration process includes changing the hypervisor or hardware while upgrading the application. • **Migration using SDM:** Migration using Solution Deployment Manager is supported using same IP Address. For example, from AVP to VMware. To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager. If you want to migrate using different IP Address for the application, use the CLI method. • **Migration using AE Services Management Console:** During migration, you need to perform backup and restore operations.
Update	The update process includes installing patches of an application. For example, security patches, hotfixes, service packs, and feature packs.
Upgrade using CLI	The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W