Upgrading standalone Avaya WebLM

Release 10.1.x
Issue 9
February 2026

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document describes the procedures for upgrading WebLM from Release 7.x and Release 8.x to Release 10.1.2 on:

- Avaya Solutions Platform 130 (Dell PowerEdge R640) in a Avaya-Supplied VMware ESXi 7.0.
- VMware in customer-provided Virtualized Environment.
- Avaya Solutions Platform 130 Release 6.0 (Avaya supplied KVM on RHEL R8.10) environment.
- Customer provided *Software-Only* environment.
- Amazon Web Services, Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS) in *Software-Only* environment.

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 WebLM.

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”.

Change history

The following changes have been made to this document since the last issue:

Issue	Date	Summary of changes
9	February 2026	Updated the following sections: • Supported servers on page 15 • Supported servers for Avaya Aura applications on page 15 • Software requirements on page 17 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 108 • Calculating space for the clone on page 111 • Validating a Virtual Machine Backup (clone) on page 113
8	October 2025	Updated the following section: • Upgrade sequence for Avaya components on page 19
7	June 2025	Updated the following section for R10.1.3.6: • Supported ESXi version on page 18

Table continues…

Issue	Date	Summary of changes
6	December 2024	Updated the following sections: • Purpose on page 7 • Prerequisites on page 7 • Supported servers on page 15 • Supported servers for Avaya Aura applications on page 15 Added the following sections: • Upgrading RHEL 8.6 to RHEL 8.10 on OVA- based virtual machines on page 60 • Supported footprints of WebLM on KVM on page 24 • Migrating WebLM from VMware to KVM on page 61 • Obtaining existing WebLM details on page 62 • Obtaining existing VMware details on page 61 • Obtaining the license information on page 62 • Shutting down WebLM virtual machine on VMware on page 62 • Installing licences on page 63 • Virtual Machine Backups (clone) as an alternative to snapshots on page 108 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 108 • Calculating space for the clone on page 111 • Validating a Virtual Machine Backup (clone) on page 113 • Rolling back using the Virtual Machine Backup (clone) on page 115
5	March 2024	Spelling update in multiple topics.
4	January 2024	Updated the section: Supported ESXi version on page 18
3	September 2023	Updated the section: Overview on page 10
2	August 2023	For Release 10.1.3.1, updated the section: Installing a WebLM patch, feature pack, or service pack on page 75
1	February 2023	Release 10.1.2 document.

Chapter 2: Upgrade overview

Overview

The document provides procedures for upgrading WebLM from Release 7.x or 8.x to WebLM Release 10.1.2.

- When upgrading to WebLM Release 10.1.2 on VMware, the VMware ESXi version must be 6.7 or 7.0.x.
- From WebLM Release 10.1.2, Appliance Virtualization Platform is no longer available for deploying or upgrading the WebLM applications. To upgrade the WebLM applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.
- From Release 10.1.2, WebLM will no longer have the Amazon Web Services (AWS). Alternately, you can continue to deploy the application by using the software-only offer. For more information, see the *Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environment* guide.

Note:

For upgrading WebLM from Release 6.x to Release 10.1.2, first upgrade WebLM Release 6.x to 8.1.x, and then upgrade to WebLM Release 10.1.2. You cannot directly upgrade the Release 6.x system to Release 10.1.2 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1.2, the upgrade fails.

Important:

- If you are upgrading standalone WebLM using Solution Deployment Manager on the following supported platform, the system preserves the licenses that are available on old WebLM.
  - Appliance Virtualization Platform to VMware
  - VMware to VMware
- If you are upgrading standalone WebLM by using Solution Deployment Manager in Software-only environment, the system does not preserve the licenses that are available on old WebLM.
- If you are upgrading standalone WebLM by using CLI-based procedure without using Solution Deployment Manager, the licenses that were available on the old WebLM server are not preserved as the host id of the new WebLM is different from the old one. In this case you need to rehost the licenses on the new WebLM using the new host id after the upgrade. As part of the CLI restore only the users that were available on the old WebLM are preserved, if supported depending on the upgrade path.

Supported upgrade paths for WebLM

Important:

- Before starting the application upgrade, upgrade the platform and hypervisor.
- To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, 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.

  Software-only upgrade is supported for VMware, KVM, RHVH, Hyper-V, AWS, GoogleCloud, and Azure.

For information about terms used in this table, see “Glossary”.

The following table displays all the upgrade paths from earlier releases to Release 10.1.2:

From offer	From Release	To Software-only 10.1.2 (VMware, KVM, RHVH, OpenStack, Hyper-V, AWS, GoogleCloud, or Azure) 10.1.2 (ISO))	To ASP 130 (OVA)/VMware 10.1.2 (OVA)
AVP	7.x	Migration using SDM	Fully automated upgrade using SDM
	8.x	Migration using SDM	Fully automated upgrade using SDM
VMware	7.x	Migration using SDM	Fully automated upgrade using SDM
	8.x	Migration using SDM	Fully automated upgrade using SDM
KVM	7.1.x	Migration using CLI	Migration using CLI
	8.x	Migration using CLI	Migration using CLI
Software-only	8.x	Migration using SDM	NA
AWS (OVA)	7.1.x	Migration using CLI	Migration using CLI
	8.x	Migration using CLI	Migration using CLI

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

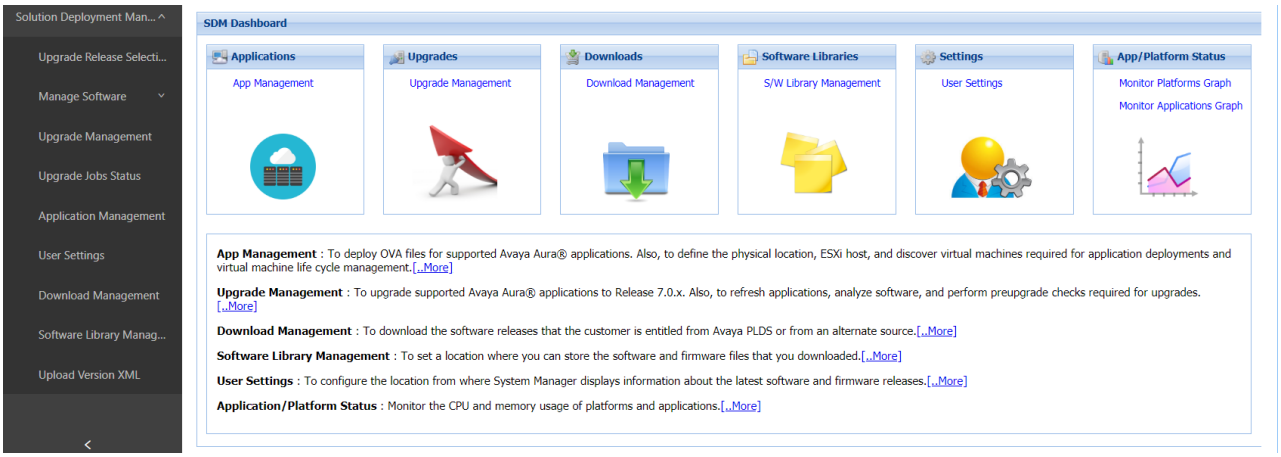
Note:

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

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
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

Table continues…

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
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).

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.

Supported ESXi version

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

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

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

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

Note:

- Please check the release notes for the availability of 8.1 and 10.1.

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 18.

For information about the supported KVM version, see Supported KVM version on page 19.

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
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.

Software details of WebLM

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

Downloading software from PLDS

When you order for an Avaya Product Licensing and Delivery System (PLDS)-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from https://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

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

Procedure

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

Note:

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

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

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

Supported footprints of WebLM on VMware

These footprints are common for VMware and Avaya Solutions Platform 130 Release 5.x.

Note:

- WebLM supports VMware hosts with Hyperthreading enabled at the BIOS level.
- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware*.

  Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

Resource	Profile 1	Profile 2
vCPU	1	1
CPU reservation	**Avaya Solutions Platform 130 and VMware:** 2185 MHz	**Avaya Solutions Platform 130 and VMware:** 2185 MHz
Memory reservation	1GiB	2GiB
Storage reservation	40GiB	40GiB
Shared NICs	1	1

Note:

If you use the WebLM server to acquire licenses for more than 5000 clients, use Profile 2.

Supported footprints of WebLM on KVM

These footprints are common for KVM and Avaya Solutions Platform 130 Release 5.x.

Note:

- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware*.

  Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

Resource	Profile 1	Profile 2
vCPU	1	1
CPU reservation	**Avaya Solutions Platform 130 and KVM:** 2185 MHz	**Avaya Solutions Platform 130 and KVM:** 2185 MHz
Memory reservation	1GiB	2GiB
Storage reservation	40GiB	40GiB
Shared NICs	1	1

Note:

If you use the WebLM server to acquire licenses for more than 5000 clients, use Profile 2.

Supported footprints of WebLM *Software-Only ISO image*

These footprints are common for deploying Avaya WebLM *Software-Only ISO image* on VMware, KVM, Hyper-V, AWS, GCN, Azure, or Nutanix:

Note:

WebLM supports VMware hosts with Hyperthreading enabled at the BIOS level.

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.

Footprint	Profile 1	Profile 2
AWS instance type for ISO	t2.medium, c5.large, c5a.large, m5.large, or m5a.large	t2.medium, c5.large, c5a.large, m5.large, or m5a.large
Azure instance type	D2s_v3 (Standard)	D2s_v3 (Standard)
vCPU	1	1

Table continues…

Footprint	Profile 1	Profile 2
CPU reservation	2290 MHz	2290 MHz
RAM (GiB)	1 GiB	2 GiB
Memory Reservation	1 GiB	2 GiB
HDD (GiB)	40	40
NICs	1	1

Customer configuration data for WebLM

The following table identifies the key customer configuration information that you must provide throughout the deployment and configuration process.

Required data	Description	Example value for the system	✔
IP address	The IP address of the WebLM interface.	For IPv4: 10.10.x.x For IPv6: 2001:0db8::a	
Netmask	The network address mask.	255.255.0.0	
Default Gateway	The default network traffic gateway.	For IPv4: 10.16.x.x For IPv6: 2001:0db8::1	
DNS IP Address	The IP address of the primary DNS server.	For IPv4: 10.x.x For IPv6: 2001:0db8::5	
Domain Name	The domain name which must be a fully qualified domain name.	abc.mydomain.com	
Short HostName	-	weblm	
Default Search List	The domain name string that is used for default search.	abc.mydomain.com	
NTP Server	The IP address of the NTP server. The application supports only the NTP server. It does not support the NTP pool.	For IPv4: 10.16.x.x For IPv6: 2001:0db8::b	
Time Zone	The time zone you want to choose.	America/Denver	
CLI User details	The command-line interface user details.	abcd	
Admin UI password	The admin UI password.		

Table continues…

Required data	Description	Example value for the system	✔
EASG	Enhanced Access Security Gateway		
Customer root account details	The customer root account details.		

Supported browsers

The following are the minimum tested versions of the supported browsers:

Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Chapter 4: Preupgrade tasks

Viewing license options

Viewing the license capacity and utilization of the product features

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View license capacity**.

View License Capacity field descriptions

Name	Description
License File Host IDs	The host ID of the license file.

The following fields are applicable for the Solution license:

Name	Description
Active License Mode	The type of license active on WebLM. The default value is **Avaya Subscription**. The WebLM server can have Avaya Subscription and Standard (Perpetual) licenses installed. However, at a time only one license can be active. These licenses are used while switching between two modes.
License State	The status of the Avaya Subscription license. The default value is **Granted**.

Table continues…

Name	Description
Avaya Subscription License Available	The availability status of the Avaya Subscription license on WebLM. The default value is **Yes**.
Standard License Available	The availability status of the standard license on WebLM. The default value is **No**.

Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Expiration Date	The date on which the feature license expires.
Licensed capacity	The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file. For the Solution license, the value is **Metered**.
Currently Used	The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays *Not counted*.

Acquired Licenses

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

Name	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Acquirer ID	The unique identifier of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

Viewing peak usage for a licensed product

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View peak usage**.

View Peak Usage field descriptions

You can view information about the usage of feature licenses of a licensed application at different time intervals.

For the Solution license, the usage fields shows the number of used license file, but not the percentage (%) of usage.

Name	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Currently Allocated	The number of feature licenses purchased by the organization. For the Solution license, the value is **Metered**.
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage. For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%.
Peak Usage (today): qty	The highest number of feature licenses for each licensed feature used for the day.
Peak Usage (Last 7 days): qty/%	The highest number of feature licenses for each licensed feature used in the last seven days. For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%.
Peak Usage (Last 30 days): qty/%	The highest number of feature licenses for each licensed feature used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.
Time of Query	The date and time when the last usage query for WebLM was executed.
Status	The success or failure of the last usage query executed for the WebLM server.

Button	Description
Back	Cancels the action and returns to the previous page.

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.

- Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- 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

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. 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 System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. 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.
4. Click **Save**.

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

Related links

New and Edit location field descriptions on page 32

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 32

Deleting a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. 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.
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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a 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 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.
5. Click **Save**.
6. 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.
7. To view the discovered application details, such as name and version, do the following to establish trust between the application and System Manager:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.

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

   Important:

   To change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure it is available.
8. On the **Platforms** tab, select the required platform and click **Refresh Host**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of the **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

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.
8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.
   c. Click **More Actions** > **Refresh App**.
9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

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

2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. 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.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. 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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. 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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. 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 System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. 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.
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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. 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.

4. 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.
5. 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.
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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. 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.
5. Click **Save**.
6. 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 47
Map vCenter field descriptions on page 48
New vCenter and Edit vCenter field descriptions on page 48

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. 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**.
7. 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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. 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.

Table continues…

Name	Description
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.

Installing the Solution Deployment Manager client on your computer

About this task

When the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches of only System Manager and hypervisor patches of Appliance Virtualization Platform.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

Solution Deployment Manager must be used to deploy or upgrade Avaya Aura® applications on Avaya Aura® Appliance Virtualization Platform.

Note:

Solution Deployment Manager is not supported for Avaya Solutions Platform R6.0 (KVM on RHEL 8.10).

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at https://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Product Support** > **Downloads**, and type the product name as **System Manager**, and Release as **10.2.x**.

3. Click the **Avaya Aura® System Manager Release 10.2.x SDM Client Downloads,10.2.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.

4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

     If the `C:\Program Files\Avaya\AvayaSDMClient` directory is not empty, the installer displays the following message: `To install the SDM client, select an empty directory or manually delete the files from the installation directory.`

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.

   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.

8. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:

   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

   b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

      The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

      You can save the artifacts in the specified directory.

   c. In **Data Port No**, select the appropriate data port.

      The default data port is 1527. The data port range is from 1527 through 1627.

d. In **Application Port No**, select the appropriate application port.

The default application port is 443. If this port is already in use by any of your application on your system, then the system does not enable you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

Note:

After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

e. **(Optional)** Click **Reset All to Default** to reset all values to default.

10. Click **Next**.
11. On the Summary and Validation page, verify the product information and the system requirements.

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the user must make the required disk space, memory, and the ports available to start the installation process again.
12. Click **Install**.
13. On the Install Complete page, click **Done** to complete the installation of Solution Deployment Manager Client.

    After the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.
14. To start the client, click the Solution Deployment Manager client icon, .

Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

  For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

Applications pre-upgrade functions

Refreshing elements

Before you begin

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

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.

Table continues…

Name	Description
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.

Table continues…

Name	Description
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.
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 18.

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.

Upgrading Avaya Solutions Platform 130 from Release 4.0 to 5.0 with WebLM 8.1.x

About this task

Use the following procedure to upgrade the Avaya Solutions Platform 130 from Release 4.0 (Avaya Supplied ESXi 6.5) to Release 5.0 (Avaya Supplied ESXi 7.0) with WebLM Release 8.1.x installed on it.

Procedure

1. Take the backup of WebLM and keep it on remote servers.

   For information about creating a backup, see “Performing WebLM backup”.
2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:
   a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

The system displays the following message:

```
Are you sure you want to shut down <virtual_machine_name>.
```

b. To proceed, click **Yes**.

Note:

If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.

3. Upgrade Avaya Solutions Platform 130 from Release 4.0 to 5.0.

   For information about upgrading Avaya Solutions Platform 130 from Release 4.0 to 5.0, see Avaya Solutions Platform 130 Series: Upgrading to ESXi 7.0 u2 from ESXi 6.5.x.

   - If the Avaya Solutions Platform 130 upgrade is successful, power on the WebLM application and ensure WebLM is up and running.

     If the WebLM application is not up and running, go to step 4.

   - If the Avaya Solutions Platform 130 upgrade fails:

     a. Do the fresh deployment of Avaya Solutions Platform 130 Release 5.0.

        For information about installing Avaya Solutions Platform 130, see “Installing the Avaya Solutions Platform 130 Series”.

     b. Deploy WebLM at the same version that was before the Avaya Solutions Platform upgrade.

        Restore the backup taken at step1 and ensure everything is working fine.

        For information about restoring the backup, see “Performing WebLM restore”.

4. **(Optional)** If the WebLM application is not up and running:

   a. Do the fresh deployment of WebLM at the same version that was before the Avaya Solutions Platform 130 upgrade.

   b. Restore the backup that is taken at step1 and ensure everything is working fine.

      For information about restoring the backup, see “Performing WebLM restore”.

Note:

If multiple applications are on the same server, follow the upgrade order for restoring the backup.

Upgrading RHEL 8.6 to RHEL 8.10 on OVA- based virtual machines

About this task

You can upgrade RHEL 8.6 to RHEL 8.10 using the following **av-upgrade-os** command. The **av-upgrade-os** command is available when WebLM R10.1.x is installed.

Before you begin

1. Install WebLM R10.1.x.

   To view the current version of WebLM, run the following command: **swversion -s**.

2. Install the latest WebLM patch, such as 10.1.3.4 or later. For more information, see Installing a WebLM patch, feature pack, or service pack on page 75.

3. 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**

4. Verify the current version of RHEL on which WebLM is running.

   To view the current RHELversion, run any of the following commands:

   - **cat /etc/redhat-release**
   - **av-version**

5. Download WebLM RHEL 8.10 Operating System bundle on WebLM R10.1.x virtual machine.

Procedure

1. Log in to WebLM CLI.
2. To upgrade from RHEL 8.6 to RHEL 8.10, run the following command: **av-upgrade-os <AV-WEBLM10.1-RHEL8.10-OSUpdate-003.tar.bz2>**.
3. After successful upgrade to RHEL 8.10, reboot the WebLM virtual machine.
4. Log in to WebLM CLI.
5. To verify that RHEL 8.10 is upgraded successfully, run any of the following commands:

   - **cat /etc/redhat-release**
   - **av-version**

Chapter 5: Migrating from VMware to KVM

Migrating WebLM from VMware to KVM

About this task

Use this procedure to migrate WebLM R10.1.3.x on ASP R5.x (VMware) to WebLM R10.1.3.x on ASP R6.0 (KVM on RHEL). When migrating, ensure that you match the WebLM version. That is to say, the restore has to be performed on the exact same WebLM version as the backup.

Procedure

1. Note down the existing VMware details.

   For more information, see Obtaining existing VMware details on page 61.

2. Note down the existing WebLM details.

   For more information, see Obtaining existing WebLM details on page 62.

3. Note down license information.

   For more information, see Obtaining the license information on page 62.

4. Shut down VMware.

   For more information, see Shutting down WebLM virtual machine on VMware on page 62.

5. 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.

6. Deploy WebLM on KVM host.

   For more information, see *Deploying standalone Avaya WebLM in Virtualized Environment*.

7. Install the WebLM licenses.

   For more. information, see Installing licences on page 63.

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).

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 existing WebLM details

Procedure

Log in to WebLM CLI, run the following commands:

- `# swversion -s`: Note down the WebLM version and profile.
- `#EASGStatus` : Note down the Enhanced Access Security Gateway (EASG) status.

Obtaining the license information

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.

About this task

Use this procedure to view all product licenses.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Note down the existing product licenses.

   You require these license to complete the migration.

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.

Installing licences

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. Restore the product licenses.

   For more information, see Rehosting license files on page 82.
2. Verify the product licenses.

   For more information, see Obtaining the license information on page 62.

Chapter 6: Upgrading WebLM to Avaya Solutions Platform 130 and VMware

Upgrading WebLM to Release 10.1.2 by using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade Appliance Virtualization Platform or VMware based WebLM Release 7.x or 8.x to Release 10.1.2 on Avaya Solutions Platform 130 or on VMware.

Note:

For upgrading WebLM from Release 6.x to Release 10.1.2, first upgrade WebLM Release 6.x to 8.1.x, and then upgrade to WebLM Release 10.1.2. You cannot directly upgrade the Release 6.x system to Release 10.1.2 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1.2, the upgrade fails.

Before you begin

- Install Solution Deployment Manager client.

  For information, see Installing the Solution Deployment Manager client on your computer on page 50.
- Ensure that System Manager is running on Release 10.2.x.
- Add a location.

  For information, see Adding a location on page 31.
- Add the required host.

  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host on page 33.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 45.

  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 18.

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 15.

- Select the WebLM virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For information, see Re-establishing trust for Solution Deployment Manager elements on page 42.

  Note:

  For WebLM Release 6.x on VMware, trust establishment is not required.

- Obtain the WebLM software. See “Software details of WebLM”.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select WebLM, 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, select **Pre-Upgrade Actions** > **Analyze**.
6. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
7. After refresh 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.

      For information about parameters, see Preupgrade Configuration field descriptions on page 56.
   b. In the Job Schedule section, click **Schedule**.

      You can schedule the job now or for a later time.

9. Select WebLM.
10. Click **Upgrade Actions** > **Upgrade/Update**.
11. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

    When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.
12. To provide the upgrade configuration details, click **Edit**.
13. On the Edit Upgrade Configuration page, perform the following:
    a. Do one of the following:
       - For same server, provide the mandatory parameters along with same target host information, latest patch file, and credentials
       - For different server, provide the mandatory parameters along with different target host information, latest patch file, and credentials

       For information about parameters, see Edit Upgrade Configuration field descriptions on page 67.
    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 the **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.

Next steps

Verify the version of the WebLM to ensure that the upgrade is successful.

Related links

Verifying the WebLM software version on page 82

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
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

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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

Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:**
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.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.

Table continues…

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.
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

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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.

Upgrading WebLM by using CLI

About this task

Use the following procedure to upgrade WebLM manually.

Note:

When you manually upgrade WebLM without using Solution Deployment Manager, the WebLM host id changes.

Note:

For upgrading WebLM from Release 6.x to Release 10.1.2, first upgrade WebLM Release 6.x to 8.1.x, and then upgrade to WebLM Release 10.1.2. You cannot directly upgrade the Release 6.x system to Release 10.1.2 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1.2, the upgrade fails.

Procedure

1. Take the backup of the old WebLM server.

   For information about taking the backup, see Performing WebLM backup on page 93.
2. Turn off the old WebLM server in case you are deploying WebLM by using the same IP Address.
3. Deploy the latest WebLM Release.
4. Apply the latest WebLM patch, if required.

   For information about applying the patch file, see Installing a WebLM patch, feature pack, or service pack on page 75.
5. Restore the backup on the new WebLM server.

   For information about restoring the backup, see Performing WebLM restore on page 93.
6. Generate new licenses and install on new WebLM.
7. Ensure new WebLM is operational.
8. Delete the old version of the WebLM server.

Next steps

After upgrading the system:

- Regenerate the license files because the host ID changes.
- Recreate the users to administrate the WebLM web console, if required.

Installing a WebLM patch, feature pack, or service pack

Before you begin

- Create backup of WebLM.
- Check the installed WebLM software version. For more information, see “Verifying the WebLM software version”.
- Copy the patch file, feature pack file, or the service pack file to the WebLM server in the `/var/WebLMPatch` folder.

Note:

If you have older WebLM 10.1.2 OVA (`WebLM-10.1.2.0.0-39162-e70-64.ova`) deployed, then it is recommended to re-deploy WebLM using the new re-spun OVA (`WebLM-10.1.2.0.0-39457-e70-72.ova`). For more details about the WebLM 10.1.2 re-spun OVA, see PSN006085u.

If you copy the WebLM patch file in a folder other than `/var/WebLMPatch` and initiate the patch installation, WebLM stops the patch execution and displays the following message:

```
Verifying the patch binary.....
The patch bin file needs to be copied under /var/WebLMPatch/
folder.
```

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Verify the MD5 checksum of the patch file.
3. Type `WebLMPatchdeploy <absolute path to the WebLM feature pack file>`.

   For example, `WebLMPatchdeploy /var/WebLMPatch/VEWebLM_10.1.x.x_xxx.bin`.

   WebLM installs the patch file.
4. To accept the license terms, read the End User License Agreement carefully and type `Y`.

   The patch installation takes about 10–15 minutes to complete. You can view to monitor the WebLM patch progress status from the `/var/log/Avaya/WebLM_Patch.log` file.

If the installation is successful, the system displays a warning message on the dashboard and on the command line interface to restart WebLM if kernel is updated.

5. After patch installation is successful, relogin to CLI to check if the updated kernel is running.
6. Restart the standalone WebLM.

Next steps

If the patch or service pack installation fails, perform a snapshot restore to go to the previous version of WebLM.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Related links

Verifying the WebLM software version on page 82

Chapter 7: Upgrading WebLM to Software-only environment

Migration path for Software-only environment

You can migrate to WebLM Release 10.1.2 on Software-only environment from the following:

- 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.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or on AWS.

Note:

For upgrading WebLM from Release 6.x to Release 10.1.2, first upgrade WebLM Release 6.x to 8.1.x, and then upgrade to WebLM Release 10.1.2. You cannot directly upgrade the Release 6.x system to Release 10.1.2 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1.2, the upgrade fails.

Upgrading to Software-only environment using manual backup and restore method

You can upgrade Standalone WebLM to Release 10.1.2 on Software-only environment by performing fresh deployment of the application. For detailed information, see the *Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environment* document.

For information about upgrading the system using CLI, see Upgrading WebLM by using CLI on page 74.

Upgrading from AVP or VMware based WebLM to Software-only environment by using System Manager Solution Deployment Manager

About this task

The procedure describes the steps to upgrade Appliance Virtualization Platform or VMware based WebLM Release 7.x or 8.x to WebLM Release 10.1.2 on Software-only environment.

Note:

Follow this procedure to upgrade to Release 10.1.2 on Hyper-V systems.

Before you begin

- Ensure that System Manager is running on Release 10.2.x.
- Add a location.

  For information, see Adding a location on page 31.
- Add the ESXi, vCenter, or Appliance Virtualization Platform host from the Application Management page.
- Select the WebLM application and click **More Actions** > **Re-establish connection** to establish the trust. For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
- Obtain the WebLM application ISO for Software-only environment and the latest service or feature pack file.

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, select the WebLM virtual machine.
4. Click **Upgrade**.
5. On **Select Platform**, select the **Software Only** check box.
6. Click **Continue**.

   Solution Deployment Manager takes the backup and shuts down the virtual machine.
7. Click the Refresh  icon until the **Upgrade Status** changes to **Upgrading (PAUSED)...RESUME** state.
8. Manually install and configure the RHEL OS with the same IP address of the old WebLM virtual machine.
9. Once the RHEL system is configured and running, access Solution Deployment Manager, and go to **Add Platform** to add the newly added Software-only platform.

10. On the **Add Platform** dialog box, configure the following options:
    - **Platform Name**: Type the name of the platform.
    - **Platform FQDN or IP**: Type the FQDN or IP address of the platform, that is, the RHEL system created for software-only.
    - **User Name**: Type the user name to access the platform.
    - **Password**: Type the password to access the platform.
    - **Platform Type**: Select platform type as **OS** for Software-only upgrade.
11. Click **Save**.
12. Click **Upgrade Management** > **Upgrade Elements** and, then click **RESUME** displayed under the **Upgrade Status** column.
13. In the Provide admin and root Credentials section, do the following:
    a. In **Admin User of OS**, type the admin user name.
    b. In **Admin Password of OS**, type the admin user password.
    c. In **Root User of OS**, type the root user name.
    d. In **Root Password of OS**, type the root user password.
    e. **(Optional)** Click **Test Connection**.

       The system logs in to the platform by using the credentials to test the platform connectivity. If connectivity is established, the system displays the message: `Test Connection Successful.`
    f. Click **OK**.
14. Click **Next**.
15. To select the required application, on the **ISO** tab, click one of the following:
    - **SW Library** / **Select from software library**: Select the local library where the *ISO image* is available.

      If you are deploying the *ISO image* from the Solution Deployment Manager client, you can use the default software library that is set during the Solution Deployment Manager Client installation.
    - **Browse**: Select the *ISO image* from your local computer, and click **Submit File**.
    - **URL**: Click URL and provide the path to the *ISO image*.

    Select the required application, click **Submit**.

    If the application *ISO image* supports the patch deployment, the system enables the **Service or Feature Pack** tab.
16. To apply the latest patch file for the application, click **Service or Feature Pack**, and enter the appropriate parameters.
    a. Click **URL**, and provide the absolute path to the latest service or feature pack.

b. Click **SW Library** / **Select from software library**, and select the latest service or feature pack.

c. Click **Browse**, and select the latest service or feature pack.

17. Click **Next**.
18. In **Flexi Footprint**, select the footprint size for the application.
19. In Test Your Operating System Compatibility Against Element Software Package, click **Test Environment Compatibility**.

    The installer checks if the platform has all the dependent RPMs, network, CPU, memory, and hard disk configuration as specified for the element. This process takes about 4-5 minutes. After the process starts, you cannot proceed further until the process is complete. If you get any error or warning, make the necessary changes before the next steps. After the check is completed successfully, the system displays a message “Environment check is successful”.

    Note:

    If the browser hangs, the system provides the option to end the script or wait. Always click **Wait**.

20. **(Optional)** To view the installer compatibility results in a separate window, click **View Output**.

    The system displays the Environment Check Output window.

21. Click **Next**.
22. On the Configuration Parameters page, provide all the information required.

    For a *Software-Only* application upgrade, the **Network Parameters** tab is disabled.

23. Click **Upgrade**.
24. On the EULA Acceptance window, click **Accept**.

    After accepting EULA, the system displays Software only Installation Warning for software-only application upgrade.

25. To continue with the upgrade, click **Accept**.

    The system displays the upgrade status in the **Current Action Status** column and the upgraded application on the **Applications** tab.

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

Chapter 8: Post-upgrade verifications

Post-upgrade checklist

Sr. No.	Tasks	Links/Notes	✔
1	Log on to the WebLM web console and verify the WebLM *<version_number>*.	See Logging on to the WebLM web console on page 81.	
2	Rehost the license file that you generated on the WebLM server. **Note:** If you had upgraded the application by using Solution Deployment Manager client, you do not need to rehost the license file separately.	See Rehosting license files on page 82. For more details, see *Administering standalone Avaya WebLM*.	
3	Configure the EASG settings, if required.	See Enhanced Access Security Gateway (EASG) overview on page 86.	
4	Rollback the upgrade in case the upgrade fails.	See Rolling back an upgrade on page 86.	
5	Delete the virtual machine snapshots, if required.	-	

Logging on to the WebLM web console

About this task

The WebLM web console is the main interface of Avaya WebLM. You must log on to the WebLM web console to perform any task. The WebLM home page displays the navigation menu that provides access to shared services to perform operations that WebLM supports.

Before you begin

Get a user account to log on to the WebLM web console. To create a new account, go to the Avaya Support website at https://support.avaya.com.

Procedure

1. On a web browser, type the WebLM URL: `https://<IP Address or Fully Qualified Domain Name>/WebLM` or `https://<IP Address or Fully Qualified Domain Name>/`.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Click **Log On**.

   WebLM validates the credentials with the WebLM user account and displays the home page with the WebLM <*version_number*>. If the credentials fail, WebLM displays an error message and prompts you to reenter the credentials.

Rehosting license files

Procedure

1. On the WebLM console, click **Server Properties**.
2. On the Server Properties page, note the WebLM server host ID.
3. Go to the PLDS website regenerate the license file for your product using the same host ID.
4. Install the license file that you generated on the WebLM server.

   For more information about installing a license file, see *Administering standalone Avaya WebLM*.

Verifying the WebLM software version

About this task

To verify the WebLM version, perform the following procedure after you deploy or upgrade WebLM.

- On the WebLM console, do the following:
  1. Log on to the WebLM web console with administrator privilege credentials.
  2. On the home page, click **About**.

     WebLM displays the About WebLM window with the build details.
  3. Verify the software version of WebLM.

- On the WebLM command line interface, do the following:

  1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
  2. Do one of the following:

  - Type **swversion**.

    WebLM displays the following message:

```
**********************************************
StandAlone WebLM Software Information

**********************************************
Standalone WebLM on VMware 10.1.0.0 Build Number 10.1.0.0.0.xxxxx
Patch 10.1.0.0 Build Number 10.1.2.0.0.xxxxx

**********************************************
Operating System Information

**********************************************
Red Hat Enterprise Linux release 8.6 (Ootpa)
Linux weblm50.avaya.com 4.18.0-372.19.1.el8_6.x86_64 #1 SMP Mon
Jul 18 11:14:02 EDT 2022 x86_64 x86_64 x86_64 GNU/Linux

**********************************************
JAVA Version

openjdk version "1.8.0_342"
OpenJDK Runtime Environment (build 1.8.0_342-b07)

OpenJDK 64-Bit Server VM (build 25.342-b07, mixed mode)
```

  - Type **swversion -s**.

    Note:

    The output varies based on the application deployment and the virtualization environment.

    - Following is an example of VMware deployment using profile1:

```
Application Name: WebLM
Application Version: 10.1.2.0.0.xxxxx
Application Deployment: Virtual Machine
Virtualization Environment: VMware
Current application size: profile1
```

    - Following is an example of *Software-Only* deployment using profile2:

```
Application Name: WebLM
Application Version: 10.1.2.0.0.xxxxx
Application Deployment: Software Only
Virtualization Environment: AWS
Current application size: profile2
```

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**.

Enhanced Access Security Gateway

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

Log in to the application CLI interface.

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. 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.
2. 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.
3. 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.

Chapter 9: Maintenance

This chapter describes the procedures to change the WebLM IP address, FQDN, and other parameters from Command Line Interface (CLI). This chapter also provides information about performing backup and restore of WebLM.

Note:

The existing license files become invalid when you:

- change the WebLM IP address
- perform a WebLM update
- clone a virtual machine

When you redeploy the WebLM, then you must reinstall a new license file to match the new Host ID generated in the WebLM server.

Changing the IP, FQDN, DNS, Gateway, or Netmask addresses

Before you begin

Log in to the WebLM command line interface with administrator privilege CLI user credentials.

Important:

Ensure that WebLM maintenance is not in progress.

Procedure

1. Type `changeIPFQDN –IP <IP Address> –FQDN <FQDN> –GATEWAY <Gateway address> –NETMASK <Netmask address> –dns <dns address> –SEARCH <search list for DNS>`.

   Warning:

   Do not change the IP address settings from VMware tools when WebLM is in the **Power Off** state.

Note:

After a WebLM IP/FQDN change, the licenses become invalid. You must re-host the licenses. The license data varies based on the installed license as part of the license re-host.

2. To add more than one IP address for the DNS server, type `changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPaddress....” to “changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPaddress.`

   You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN –dns 10.14.16.2,14.17.13.5.`

   The system takes a few seconds to apply the DNS changes to the network.

   Note:

   The command to configure multiple DNS IP addresses overrides all the previous DNS IP address entries.

Related links

Rehosting license files on page 82
WebLM CLI operations on page 95

Configuring multiple DNS IP addresses

Before you begin

- Deploy the WebLM application.
- Start the WebLM virtual machine.

  When you power on WebLM for the first time after you deploy the WebLM application, the system applies the network configurations that you provided during the deployment of the WebLM application.

Note:

The command to configure multiple DNS IP addresses overrides all the previous DNS IP address entries.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.

   Important:

   Ensure that WebLM maintenance is not in progress.

2. Check the existing DNS IP address of WebLM.

3. To add more than one IP address for the DNS server, type `changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPaddress....” to “changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPaddress`.

   You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN -dns 10.14.16.2,14.17.13.5`.

   The system takes a few seconds to apply the DNS changes to the network.
4. Log on to the WebLM web console with administrator privilege credentials.
5. Ensure that the system displays the multiple DNS IP addresses.

Related links

WebLM CLI operations on page 95

Configuring the time zone

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type `configureTimeZone`.
3. Select the time zone from the list.

   For example, America/Denver.

Related links

WebLM CLI operations on page 95

Configuring the NTP server

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type `configureNTP <IP address of the NTP server>`.

   The system configures the NTP server.

Related links

WebLM CLI operations on page 95

Resetting the WebLM password through CLI

About this task

Any CLI user who is part of the gcliuser and admin groups created during deployment can run the command to reset the WebLM password through CLI.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type the **`weblm_password`** command and press `Enter`.
3. In **Enter new WebLM UI Admin Password**, type a new password.

   The password must be 6-14 characters long.
4. In **Re-enter new WebLM UI Admin Password**, type the new password again.

   WebLM successfully resets the password. You can log in to the WebLM UI with user 'admin' and the new password.

Performing WebLM backup

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type **`WebLMBackup <backup_location>`**.

   Where: <backup_location> is the absolute path of the backup file.

   You can copy the backup files to a remote computer or to an external storage device.

Performing WebLM restore

About this task

WebLM restores user, data, and license information from the backup based on the data available in the backup file.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type **`WebLMRestore <Full path where the Backup files have been saved>`**.

Where, **<Full path where the Backup files have been saved>** is the absolute path of the backup file.

WebLM restores required details from the specified backup file location.

Creating a snapshot backup

About this task

Important:

Do not perform any activity on WebLM until the snapshot backup is complete.

To create the snapshot backup, use the vSphere Web client.

Procedure

1. From the list of virtual machines, right-click the required WebLM virtual machine, and select **Snapshot**.
2. Click **Take Snapshot**.
3. In the **Name** and **Description** fields, enter a name and the description for the snapshot.
4. Set the following Snapshot options:
   a. Enable **Snapshot the virtual machine's memory**.
   b. Enable **Quiesce guest file system (Needs VMware Tools installed)**.

   Note:

   Quiescing indicates pausing or altering the state of running processes, particularly the processes that might modify the information stored on disk during a backup. Quiescing ensures a consistent and usable backup.
5. Click **OK**.
6. In the Recent Tasks window, ensure that the status of the **Create virtual machine snapshot** task is **Completed**.

Creating a snapshot restore

About this task

Important:

Do not perform any activity on WebLM until the snapshot restore is complete.

Performing the VMware snapshot restore is not the same as application specific restore.

To restore the snapshot backup, use the vSphere Web client.

Procedure

1. From the list of virtual machines, select the deployed WebLM virtual machine, and right-click and select **Snapshot**.
2. Open **Snapshot Manager**.
3. Select the snapshot version that you want to restore.
4. Click **Go to**.
5. In the Recent Tasks window, verify whether the **Status** of the **Revert snapshot** task is **Completed**.

WebLM CLI operations

Note:

Any CLI user who is part of the gcliuser, and admin groups created at the time of deployment can execute the following commands:

#	Command	Parameters	Description	Usage
1.	`changeIPFQDN`	• IP < new IP address for WebLM > • FQDN < new fully qualified domain name of WebLM > • GATEWAY < new gateway address for WebLM > • NETMASK < new netmask address for WebLM > • dns < new DNS address for WebLM > • SEARCH < new search list for DNS addresses >	Updates the IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• changeIPFQDN -IP < new IP address > • changeIPFQDN -FQDN < new fully qualified domain name > • changeIPFQDN -IP < new IP address > -GATEWAY < new gateway address for WebLM > -SEARCH < new search list for DNS addresses >
2.	`configureNTP`	< IP address of the NTP server >	Configures the NTP server details.	configureNTP < IP address of the NTP server > Separate the IP addresses or the host names of the NTP servers with commas (,).

Table continues…

#	Command	Parameters	Description	Usage
3.	**configureTimeZone**	< Time zone that you want to select >	Configures the time zone with the value that you select.	Select a time zone. For example, America/Denver
4.	**WebLMPatchdeploy**	< absolute path to the WebLM service pack, feature pack, or the software patch >	Installs the software patch, the service pack, or the feature pack for WebLM.	WebLMPatchdeploy <absolute path to `home/admin/< WebLM FeaturepackName >` **Note:** Copy the WebLM feature pack or patches that you install to `/home/admin/`.
5.	**weblm_password**		Resets the WebLM password through CLI. Any CLI user who is part of the gcliuser and admin groups, created at the time of deployment can execute the command.	
6.	**configureTLS**	• -ENABLE_TLS_VERSIONS TLSv1.3 • -ENABLE_TLS_VERSIONS TLSv1.2 • -ENABLE_TLS_VERSIONS TLSv1.1 • -ENABLE_TLS_VERSIONS TLSv1.0	Configures the TLS version.	Type one of the following options: • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.3** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.2** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.1** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.0**
7.	**collectLogs**		Collects the WebLM logs in the `/tmp/WebLM_Logs_DDMonYY_XXXXXXXXXXXXXXX.zip` file.	
8.	**swversion**		Verifies the WebLM software version.	

Table continues…

#	Command	Parameters	Description	Usage
9.	**swversion -s**		Verifies the WebLM software version and also displays information about the application name, profile, and deployment type.	**swversion -s** **Note:** The output varies based on the application deployment and the virtualization environment.
10.	**WebLMBackup**	<backup_location>	Performs the WebLM backup.	**WebLMBackup <backup_location>** **Note:** You can copy the backup files to a remote computer or to an external storage device.
11.	**WebLMRestore**	<Full path where the Backup files have been saved>	WebLM restores user, data, and license information from the backup based on the data available in the backup file.	**WebLMRestore <Full path where the Backup files have been saved>**
12.	**configureCiphersList**	• 1: To view the configured cipher suites. • 2: To configure relaxed cipher suites. • 3: To configure strict cipher suites.	You can toggle between the Relaxed cipher suites or Strict cipher suites.	
13.	**weblmStart**		Starts the WebLM Application server.	**weblmStart**
14.	**weblmStatus**		Checks the status of the WebLM Application server.	**weblmStatus**
15.	**weblmStop**		Stops the WebLM Application server.	**weblmStop**
16.	**weblmRestart**		Restarts the WebLM Application server.	**weblmRestart**

Table continues…

#	Command	Parameters	Description	Usage
17.	**manageWebLMCertificate**	• -display • -replace • -generateSelfSigned	Allows you to view a WebLM certificate, replace a WebLM certificate with a third-party certificate, and generate a self-signed WebLM certificate.	Type one of the following options: • **manageWebLMCertificate -display** • **manageWebLMCertificate -replace -certpath <file> -password <password>** • **manageWebLMCertificate -generateSelfSigned**
18.	**manageCACertificates**	• -list • -add • -remove	Allows you to view, add, and delete CA imported certificates in the WebLM server truststore.	Type one of the following options: • **manageCACertificates -list** • **manageCACertificates -add -certpath <file> -alias <alias>** • **manageCACertificates -remove -alias <alias>**

Table continues…

#	Command	Parameters	Description	Usage
19.	**setWebLMClientAuth**	• 1: Displays existing WebLM client certificate authentication configuration. • 2: Enables WebLM client certificate authentication. • 3: Disables WebLM client certificate authentication.	Allows you to manage the client certificate authentication for WebLM port 52233. **Note:** From 10.1.3.3 onwards, the WebLM client certificate authentication configuration is ON by default and you need to setup WebLM client certificate for communication with WebLM server for licensing to work. You must disable client certificate authentication if you do not require it (WebLM client certificate for communication). You can re-enable it once the WebLM client certificate for communication is configured.	

Table continues…

#	Command	Parameters	Description	Usage

20	**toggleOldWebLMClientCommunication**	Run this utility as the following:
		• Type `1` to check the old WebLM client communication status
		• Type `2` to enable the old WebLM client communication status
		• Type `3` to disable the old WebLM client communication status
		Note:
		The user can enter the values specified above based on their usage.
			This utility is used to check, enable, and disable the old WebLM client communication status with releases 10.1.3.1 and later. For the older WebLM client communication, the default status is ENABLED.	• Type `1` to check the old WebLM client communication status.
				• Type `2` to enable the old WebLM client communication status.
				• Type `3` to disable the old WebLM client communication status.
				If your input is 1 and the current status is enabled, the message
				`Old WebLM client communication status is ENABLED`
				is displayed.
				If the current status is disabled, the message
				`Old WebLM client communication status is DISABLED`
				is displayed.
				If your input is 2, the message
				`Old WebLM client communication is now ENABLED`
				is displayed.
				If your input is 3, the message
				`Old WebLM client communication is now DISABLED`
				is displayed.

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the desktop, click the SDM icon (), and then click **Application Management**.
3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

   The page displays the details of jobs that you selected.

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Name	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Platforms**.
3. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Chapter 10: Resources

Avaya WebLM documentation

The following table lists the documents related to Avaya WebLM. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Implementing		
Deploying standalone Avaya WebLM in Virtualized Environment	Deploy the application in virtualized environment.	Implementation personnel
Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environment	Deploy the application on software-only environment and cloud services.	Implementation personnel
Upgrading standalone Avaya WebLM	Upgrade the application.	Implementation personnel
Administering		
Administering standalone Avaya WebLM	Perform administration tasks	System administrators

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.

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**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.

- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available at http://www.avaya-learning.com/. To search for the course, enter the course code in the **Search** field and click **Go**.

Course code	Course title
71201V	Integrating Avaya Aura® Core Components

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: 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.

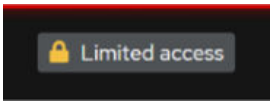


Figure 1: Limited access button

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`**.

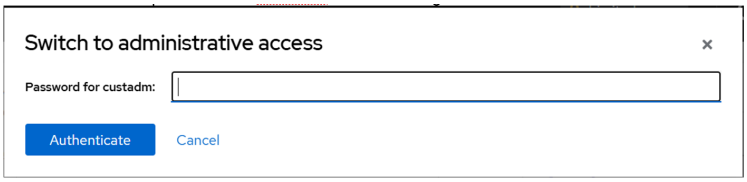


Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

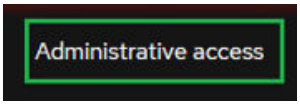


Figure 3: Administrative access button

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.

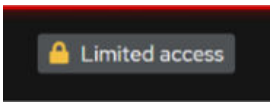


Figure 4: Limited access button

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`**.

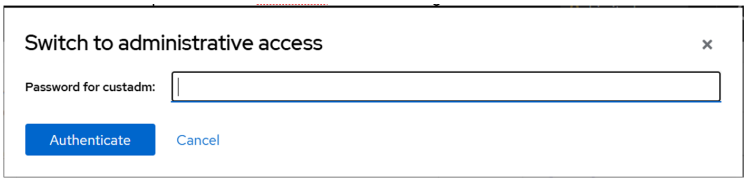


Figure 5: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

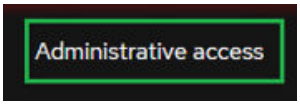


Figure 6: Administrative access button

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%).

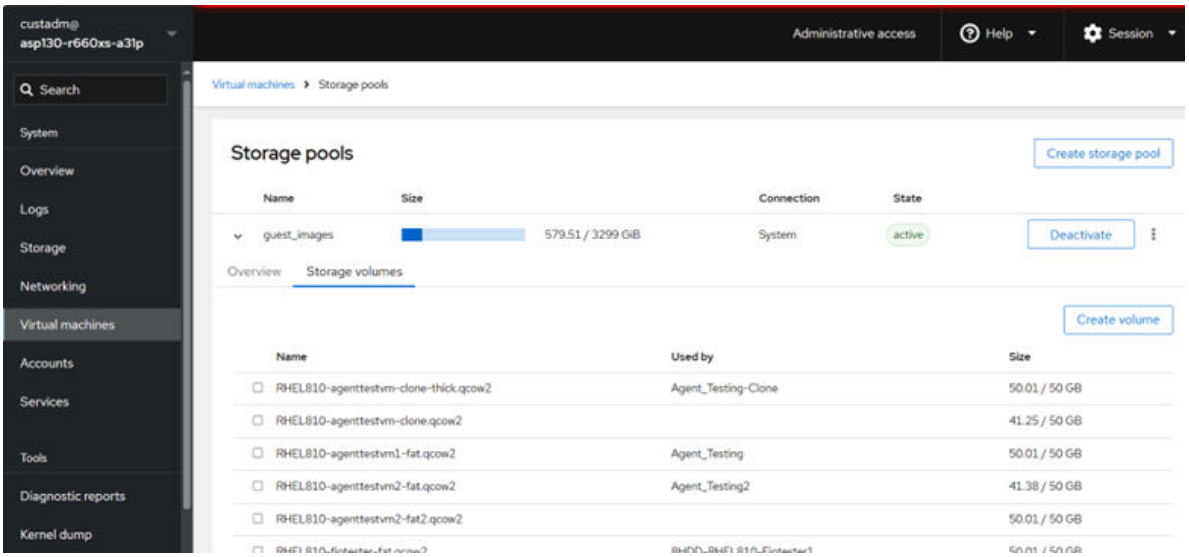


Figure 7: Example size

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.

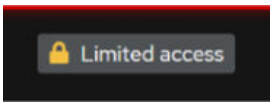


Figure 8: Limited access button

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**.

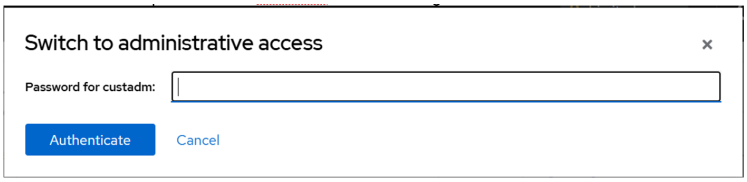


Figure 9: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

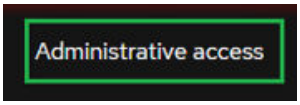


Figure 10: Administrative access button

8. Navigate to **System** > **Virtual Machines**.

9. View the cloned virtual machine in the virtual machines list.

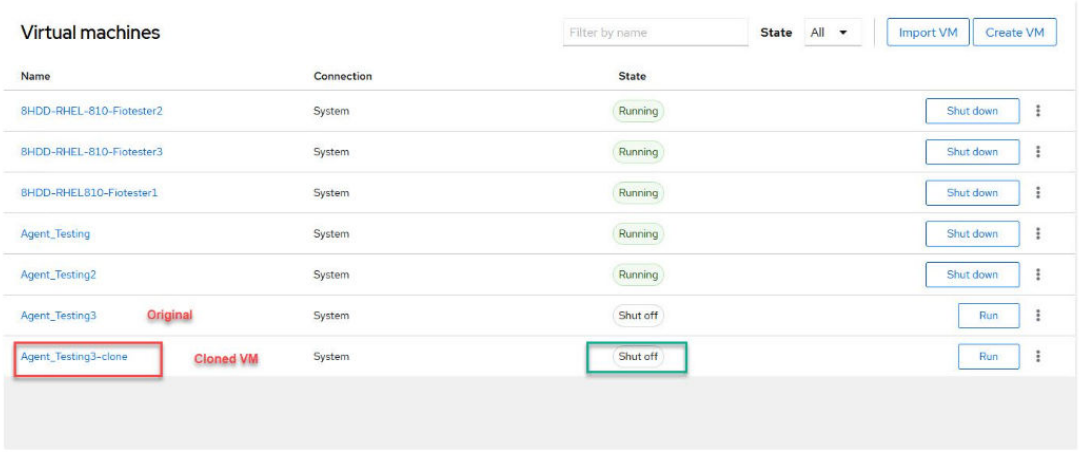


Figure 11: Virtual machines list

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.

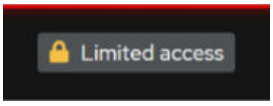


Figure 12: Limited access button

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`**.

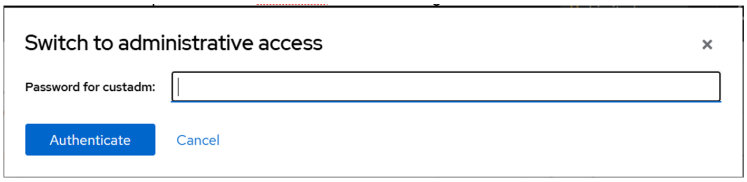


Figure 13: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

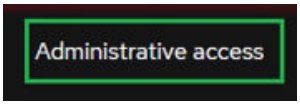


Figure 14: Administrative access button

4. Navigate to **System** > **Virtual Machines**.
5. Shut down the original virtual machine.
6. Rename the original virtual machine.

   For example: `Virtual_Machine_Broken`

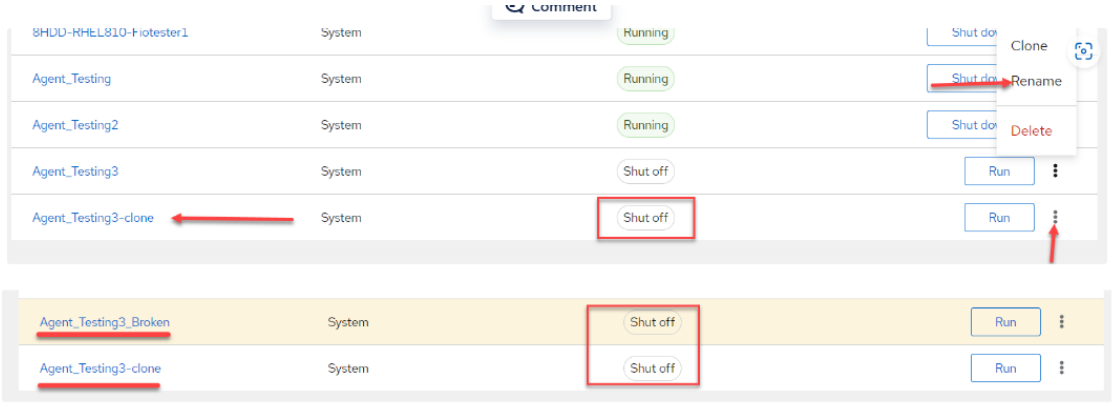


Figure 15: Roll back VM backup

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.

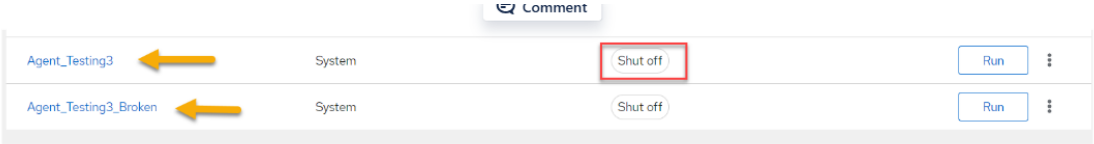


Figure 16: Edit Virtual Machine name

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`

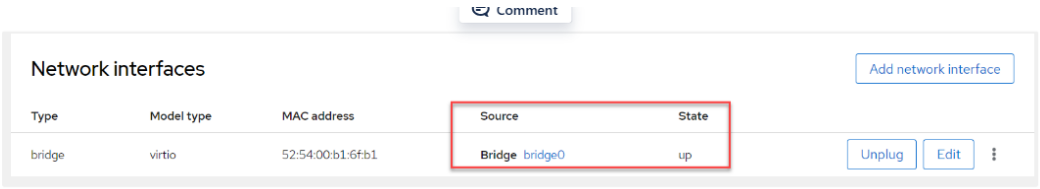


Figure 17: Network interfaces

9. Power on the virtual machine that you renamed in step 5.

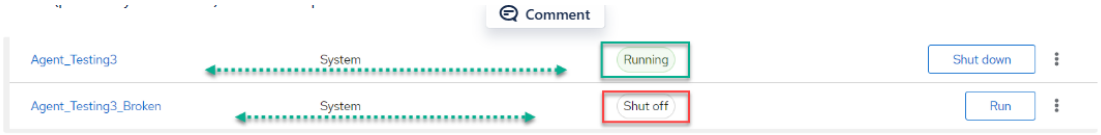


Figure 18: Power on

10. Delete any unused backups.

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.
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

F

G

H

I

J

K

L

M

N

P

R

S

T

U

V

W