Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environments

Release 10.1.x
Issue 9
August 2025

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 how to deploy the Avaya WebLM *Software-Only ISO image* on a:

- Customer-provided hardware
- Infrastructure as a Service environment

This document is intended for people who install and configure Avaya WebLM *ISO image* at a customer site.

The *Software-Only* offer is for customers who want to deploy the Avaya Aura® applications on their own standard Red Hat Enterprise Linux operating system. Avaya Aura® applications support third party applications only on the *Software-Only* deployments.

Note:

A virtualized environment is required for the software-only deployment.

Prerequisites

Before deploying the Avaya WebLM *ISO image*, ensure that you have the following knowledge, skills, and tools.

Knowledge

- Linux® Operating System
- Avaya Aura® System Manager
- Avaya WebLM
- Infrastructure as a Service
- Virtualized environment

Skills

To administer the Linux server and Avaya Aura® applications.

Tools

For information about tools and utilities, see Configuration tools and utilities on page 16.

Chapter 2: Overview

Software-only environment overview

In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Customers and/or Service Providers must procure a server or virtual machine that meets the recommended hardware requirements and the appropriate version of Red Hat Enterprise Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020558u that Avaya publishes periodically on the Avaya Support website.

Note:

For information about RPM updates for the Red Hat Enterprise Linux operating system and required changes to operating system files on Software only installation, see *Avaya Aura® Software Only White paper* on the Avaya Support website.

Supported platforms

You can deploy the Avaya Aura® application software-only *ISO image* on the following:

- On-premise platforms:
  - VMware
  - Kernel-based Virtual Machine (KVM)
  - Hyper-V

  - Nutanix 6.5 +
- Cloud platforms:
  - Amazon Web Services
  - Google Cloud Platform
  - Microsoft Azure
  - IBM Cloud for VMware Solutions

    Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

    For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Infrastructure as a Service environment overview

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services

  Note:

  With Release 10.1.x and later, Avaya Aura® will no longer have the Amazon Web Services OVA. Deployment on Amazon Web Services is supported through the software only offer.
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud for VMware Solutions

  For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.

- Allows you to stay current with latest security updates provided by the service provider.

You can connect the following applications to the Avaya Aura® IaaS instances from the customer premises:

- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway, G450 Branch Gateway, and G650 Media Gateway

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Related links

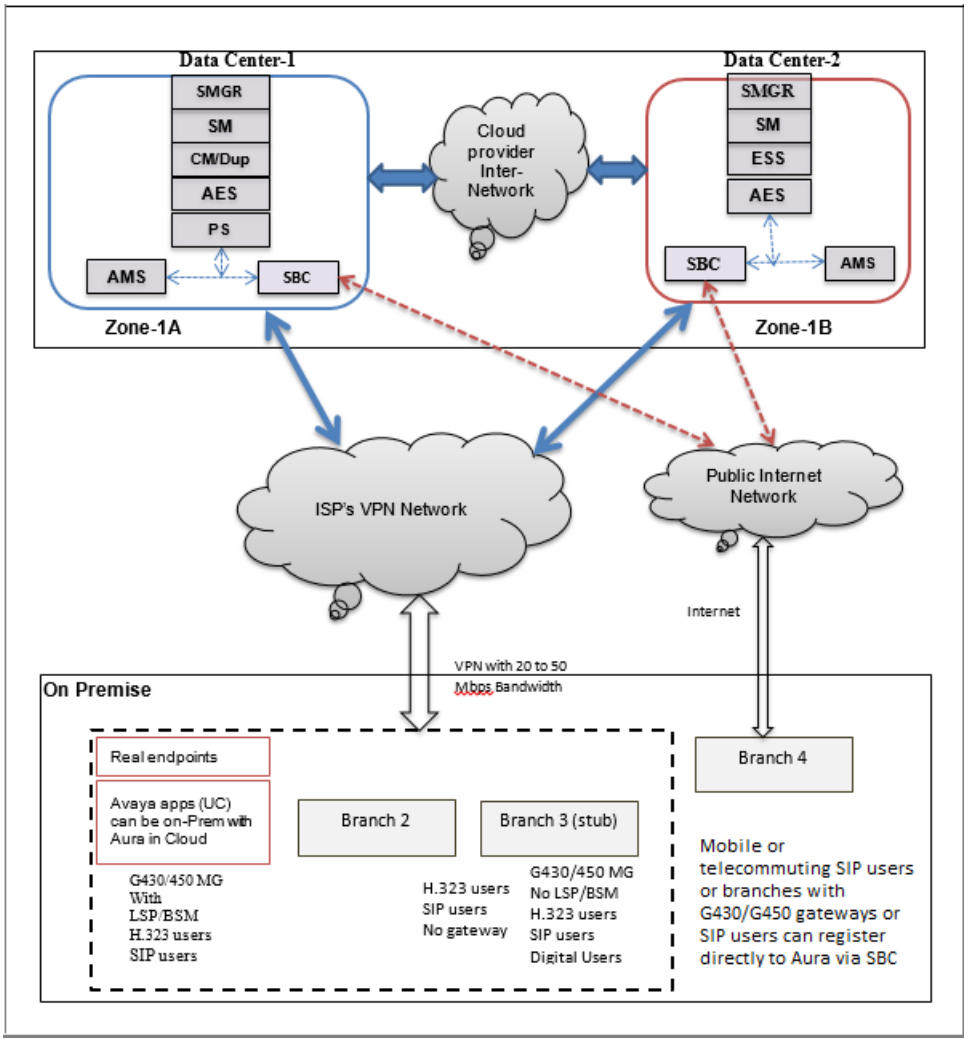
Topology on page 9
Connection types for Infrastructure as a Service on page 10
Networking considerations on page 11
Unsupported features of Avaya Aura application on Infrastructure as a Service on page 12

Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.

Important:

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.



Related links

Infrastructure as a Service environment overview on page 8

Connection types for Infrastructure as a Service

Amazon Web Services

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

Connection type	Resource
VPN connection	For more information, go to https://docs.aws.amazon.com/VPC/ and search for “VPN connections” section.
Direct connection	For more information, see https://aws.amazon.com/directconnect/ section.

Microsoft Azure

You can connect applications in a hybrid network on the Virtual Networks (VNet) in the following ways:

Connection type	Resource
VPN connection	For more information, go to https://docs.microsoft.com/en-us/ and search for “Create a Site-to-Site connection in the Azure portal” section. For more information, go to https://docs.microsoft.com/en-us/ and search for “Azure networking” section.
Direct connection	For more information, go to https://docs.microsoft.com/en-us/ and search for “ExpressRoute overview” section.

Google Cloud Platform

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

Connection type	Resource
VPN connection	For more information, go to https://cloud.google.com/vpn/docs/ and search for “Cloud VPN overview” section.
GCN Direct	For more information, go to https://cloud.google.com/interconnect/docs/ and search for “Dedicated Interconnect Overview” section.

Related links

Infrastructure as a Service environment overview on page 8

Networking considerations

When you deploy an Avaya application at main location or at a branch location on Infrastructure as a Service, ensure that you follow the networking requirements, such as, the WAN network topology, bandwidth and latency of the Avaya applications. You must adhere to the Avaya network recommendations and Infrastructure as a Service networking rules.

Infrastructure as a Service has some limitations for establishing public internet VPNs and direct connections.

For more information about Amazon VPC Limits, see the Amazon Web Services documentation at https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

For more information about Microsoft Azure VPN connection limits and VPN Gateway, see the Microsoft Azure documentation at https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways.

Important:

Avaya recommends the use of direct connection in combination of a private WAN connection with Service Level Agreement that measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between Infrastructure as a Service and customer premises.

Related links

Infrastructure as a Service environment overview on page 8

Unsupported features of Avaya Aura® application on Infrastructure as a Service

The following features are unsupported on the Software-Only Environment.

For more information on Out of Band Management (OOBM) feature support matrix for Avaya Aura® components, refer to section Out of Band Management Support Matrix for Avaya Aura Components on page 12.

Amazon Web Services

The Avaya Aura® application does not support the following features on Amazon Web Services:

- IPv6 addresses
- Data Encryption
- Security Hardening modes

Microsoft Azure

The Avaya Aura® application does not support the following features on Microsoft Azure:

- IPv6 addresses
- Data Encryption
- Security Hardening modes

Google Cloud Platform

The Avaya Aura® application does not support the following features on Google Cloud Platform:

- IPv6 addresses
- Data Encryption
- Security Hardening modes

Out of Band Management Support Matrix for Avaya Aura® Components

The following table provides the information on OOBM support matrix for Avaya Aura® components.

Product	On-Premise (OVA)	IAAS (SW-Only)	Support OOBM
Communication Manager	Yes	Yes	Supported
Session Manager	Yes	Yes	Management only runs OOBM.
Media Server	Yes	Yes	Supported

Table continues…

Product	On-Premise (OVA)	IAAS (SW-Only)	Support OOBM
Session Border Controller	Yes	No	Not Supported
System Manager	No	No	Needs VPC Peering with Voice Network in GCP for communicating with AADS.
WebLM	No	No	Needs VPC Peering with Voice Network in GCP if independently installed from SMGR to license AADS or AES.
Application Enablement Services	Yes	No	Needs to be on Voice Network only.
Avaya Aura® Device Services	No	No	Needs to be on Voice Network and needs VPC Peering in GCP with Voice Network.

Related links

Infrastructure as a Service environment overview on page 8

System capacities for applications

For information about the system capacities, such as, number of users, gateways, and endpoints, see the product specific documentation on the Avaya Support website at http://support.avaya.com.

Chapter 3: Planning and preconfiguration

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.

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/.

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.

Third-party software requirements

You can deploy the Avaya Aura® application ISO file on a Red Hat Enterprise Linux (RHEL) 8.6 or RHEL 8.10 virtual machine by using the operating system command line interface or by using Solution Deployment Manager.

Supported Red Hat Enterprise Linux operating system versions for Software-only Environment

The following table lists the supported Red Hat Enterprise Linux operating system versions for deploying or upgrading Avaya Aura® applications in Software-only Environment.

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.0.x	8.1.x	10.1.x
Linux operating system Release 7.4 with 64-bit	Y		
Linux operating system Release 7.6 with 64-bit		Y	
Linux operating system Release 8.6 with 64-bit			Y **Note:** Avaya WebLM Release 10.1.2 supports Linux operating system Release 8.6 with 64-bit.
Linux operating system Release 8.10 with 64-bit			Y **Note:** Avaya WebLM Release 10.1.3.4 supports Linux operating system Release 8.10 with 64-bit.

Configuration tools and utilities

To deploy Avaya Aura® ISO image and to configure the application, you need the following tools and utilities:

- PuTTY and WinSCP
- Solution Deployment Manager Client

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
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

Preconfiguration in Software-Only

Planning checklist

Before creating a virtual machine and installing the operating system, you must perform the following:

No.	Task	Description/Notes	✔
1	Download and install the virtualization software and the operating system. **Note:** The operating system needs to be configured to meet the application's requirement.	Ensure that the virtual environment with required operating system is installed and is available for software-only deployment.	
2	Download the ISO.	**Note:** For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at https://support.avaya.com/.	
3	Install the required third-party software.		
4	Purchase and obtain the required licenses.	Downloading software from PLDS on page 14	
5	Register for PLDS and activate license entitlements.	Downloading software from PLDS on page 14	
6	Prepare the site.	Site preparation checklist on page 18	

Site preparation checklist

Use the following checklist to know the set up required to deploy the application ISO file in the software-only environment:

No.	Task	Description	✔
1	Create a virtual machine on the supported virtualized environment.	See the corresponding virtualized environment documentation.	
2	Subscribe to Red Hat network.		
3	Install the Red Hat Enterprise Linux (RHEL) 8.6 with minimal configuration for the Software-Only deployment.	See Red Hat documentation.	
4	Configure Yum.	See Configuring Yum on RHEL on page 21	

Preconfiguration in Infrastructure as a Service

Preconfiguration for deploying ISO on Amazon Web Services

Checklist for deploying ISO on *Amazon Web Services*

Ensure that you complete the following before deploying Avaya Aura® application ISO on *Amazon Web Services*.

No.	Task	Link/Notes	✔
1	Create a virtual machine.	See Creating RHEL instance on Amazon Web Services on page 18	
2	Assign the required resources to the virtual machine.	See Supported footprints of WebLM Software-Only ISO image on page 16	
3	Copy the ISO to the virtual machine.	See Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services on page 21	

Creating RHEL instance on Amazon Web Services

About this task

Use this procedure to create RHEL virtual machine on Amazon Web Services.

Note:

Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020558u that Avaya publishes periodically on the Avaya Support website.

Also, please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Amazon Web Services documentation.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Compute** > **EC2**.

   The system displays the EC2 Management Console page.
3. Click **Launch Instance**.
4. On the Choose an Amazon Machine Image (AMI) page, search for the supported RHEL version in **Community AMIs**, and click **Select**.

   For the supported RHEL version, see “Third party software requirements” section.
5. On the Choose an Instance Type page, select the instance type according to your required footprints, and click **Next: Configure Instance Details**.
6. Click **Next: Add Storage**.

   Change the size of the default Hard Disk size from 10 to 40 GB.
7. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.

   Remember the name entered for the tag. The name entered for the tag is used to identify the RHEL instance after the instance is created.
8. On the Configure Security Group page, create a new security group or select an existing security group, and click **Review and Launch**.
9. On the Review Instance Launch page, review the details of each configuration, and then click **Launch**.
10. On the Select an existing key pair or create a new key pair dialog box, select one of the following options:
    - **Choose an existing key pair**.
    - **Create a new key pair**.
11. If you select the **Choose an existing key pair** option, perform the following:
    a. From the **Select a key pair** drop-down list, select a key pair.

b. Select the **I acknowledge that I have access to the selected private key file (<example.pem>), and that without this file, I won't be able to log into my instance** check box.

12. If you select the **Create a new key pair** option, perform the following:
    a. In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
    b. Click **Download Key Pair**.
    c. Save the file in a secure and accessible location.

    Note:

    You will not be able to download the file again.
13. Click **Launch Instances**.

    The system creates the RHEL instance.
14. Click **View instance**.

    When the system creates an instance, the **Status Checks** column displays the message: `2/2 checks passed`.

Preparing WebLM for deployment on Cloud by disabling DHCP

About this task

Typically, you must configure cloud-provided Red Hat instances before installing the Avaya WebLM *Software-Only ISO image*. For example, cloud-provided instances are often deployed with DHCP enabled. Avaya WebLM does not support DHCP so you must configure the operating system before running the installer. Perform the steps here to disable DHCP.

Before you begin

Log in to the system as a root user.

Procedure

1. Get the current assigned network information using the command:

   ```
   nmcli device show eth0
   ```
2. From the Command Line Interface (CLI), note the IP4.ADDRESS, IP4.GATEWAY, and IP4.DNS values.
3. Run the following command to access the NetworkManager TUI page:

   ```
   nmtui
   ```

   If the command is unavailable, use Yum to install the NetworkManager-tui package.
4. On the NetworkManager Text-Based Interface (TUI) page, select **Edit a connection**.
5. Select **System eth0** from the Ethernet list and click **Edit**.

   The entry for eth0 is called Wired connection 1 on some platforms.

6. On the Edit Connection page, click **Show** at the IPv4 CONFIGURATION.
7. From the **IPv4 CONFIGURATION** list, select **Manual**.
8. Enter the IP information collected in step 2.b.
9. Select **OK** and then **Back**.
10. On the NetworkManager TUI page, select **Set system hostname**.
11. On the Set Hostname page, enter the hostname and select **OK**.
12. Reboot the Avaya WebLM server.

Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Amazon Web Services

Create a ppk file

Procedure

1. Open WinSCP.
2. From the advance section, choose the authentication and browse to the .ppk file, and click login.
3. Enter the login credentials.
4. Upload the .iso to the virtual machine instance by using the IP address of the virtual machine.

Configuring Yum on RHEL

Before you begin

- Converting the *.pem file to the *.ppk format.
- Configuring PuTTY for an SSH session.
- Find the SSH user name of the instance you deployed.

For more information, see “Appendix”.

Procedure

1. Log on to the RHEL virtual machine using SSH.

   Use the SSH user name to log on.

2. Switch to root user by using the following command: `sudo su`
3. Check if the BaseOS and AppStream repos are enabled.

```
Repo ID:rhel-8-for-x86_64-baseos-rpms
Repo Name:Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
```

```
Repo URL:https://cdn.redhat.com/content/dist/rhel8/$releasever/x86_64/baseos/os
Enabled: 1
```

and

```
Repo ID:rhel-8-for-x86_64-appstream-rpms
Repo Name:Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
Repo URL:https://cdn.redhat.com/content/dist/rhel8/$releasever/x86_64/appstream/os
Enabled:1
```

4. Enable the CodeReady Builder repository:

```
subscription-manager repos --enable codeready-builder-for-rhel-8-x86_64-rpms
```

5. Install the EPEL repository:

```
dnf install: https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

Preconfiguration for deploying ISO on Microsoft Azure

Checklist for deploying ISO on Microsoft Azure

Ensure that you complete the following before deploying Avaya Aura® application ISO on Microsoft Azure.

No.	Task	Link/Notes	✔
1	Create a virtual machine.	See Creating RHEL instance on Microsoft Azure on page 22	
2	Assign the required resources to the virtual machine.	See Supported footprints of WebLM Software-Only ISO image on page 16	
3	Copy the ISO to the virtual machine.	See Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure on page 24	

Creating RHEL instance on Microsoft Azure

Before you begin

Create an account on Microsoft Azure.

Important:

Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020558u that Avaya publishes periodically on the Avaya Support website.

Note:

Please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Microsoft Azure documentation.

Procedure

1. Log on to the Azure portal.
2. In the search box, type virtual machine, and click **Virtual machines**.
3. On the Virtual machines page, click on the **+ Create** link and select **+ Virtual machine**.

   The system displays the Create a virtual machine page.
4. In the **Basics** tab, do the following:
   a. In **Project details**, select the **Resource group**.
   b. In **Instance details**, provide the **Virtual machine name** and select the **Region**.
   c. In **Image**, select **Red Hat Enterprise Linux 8.6** from the images list.
   d. In **Size**, select the required details.
   e. From **Administrator account**, in **Authentication type**, select **Password**, and enter the required credentials.

      Ensure that you select authentication type as **password** instead of **SSH public key**.
   f. Optional: Select the required **Inbound port rules**.
   g. Click **Next: Disks**.
5. In the **Disks** tab, do the following:
   a. From **Disk options**, select the required **OS disk type** and **Encryption type**.

      Caution:

      Do not use temporary disk for application configuration. It might lead to loss of data.
   b. In **Data disks for 'undefined'**, click **Create and attach a new disk**.
   c. On Create a new disk page, click **Change size** and select **128 GiB** from the list.
   d. Click **OK**.

      A new disk of size 128 GiB is created.
   e. Click **Next: Networking**.
6. In the **Networking** tab, from **Network interface** select the required **Virtual network**, **Subnet**, and **Public inbound ports**.

   Select other fields on that page, if required.
7. In the **Management**, **Advanced**, and **Tags** tabs, fill the details, if required.
8. In the **Size** tab, select the profile as B2s, and click **Select**.

9. In the **Review + create** tab, review the details and click **Create**.

   The deployment begins. Wait till the deployment is complete.

10. Change the hard disk size from 32 GB to 40 GB and save the configuration.

Next steps

Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure

Before you begin

Create RHEL virtual machine instance on Microsoft Azure.

Procedure

1. Open WinSCP session with your RHEL machine on Microsoft Azure by using the user ID and password that you provided at the time of creating the virtual machine.
2. From the advance section, choose the authentication and browse to the .ppk file, and click **login**.
3. Enter the login credentials.
4. Upload the .iso file to the virtual machine instance.

Preconfiguration for deploying ISO on Google Cloud Network

Checklist for deploying ISO on Google Cloud Network

Ensure that you complete the following before deploying Avaya Aura® application ISO on Google Cloud Network.

No.	Task	Link/Notes	✔
1	Create a virtual machine.	See Creating RHEL instance on Google Cloud Platform on page 25	
2	Assign the required resources to the virtual machine.	See Supported footprints of WebLM Software-Only ISO image on page 16	
3	Copy the ISO to the virtual machine.	See Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform on page 26	

Creating a PPK file

Procedure

1. Open puttygen file, and click **Load**.
2. Under the **Parameters** section, select SSH-2 RSA.

3. Under **Actions** section, click **Generate**.

   You will be instructed to move the mouse cursor around within the PuTTY Key Generator window as a randomizer to generate the private key.

4. Enter a value in the **Key passphrase** and enter the same value in the **Confirm passphrase** field to protect the private key.
5. Click **Save private key**, and save the file to your local computer.
6. The box under **Public key for pasting into OpenSSH authorized_keys file:** contains the public key.
7. Copy the public key.
8. Open a text editor and paste the public key into the text editor and save the file.

Creating RHEL instance on Google Cloud Platform

Before you begin

- Create an account on the Google Cloud Platform
- Create a ppk file.

Important:

Installing only the required RPMs to the system for security and stability. Do not install a complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020558u that Avaya publishes periodically on the Avaya Support website.

Note:

Please note that the steps provided in this section are for reference. For the most up-to-date information, see the Google Cloud Platform documentation.

Procedure

1. Log on to the Google Cloud Platform.
2. Go to **Compute Engine** > **VM Instances**.
3. On the VM Instances page, click **CREATE INSTANCE**
4. On the **Create an instance** page, update the following fields:
   a. In **Name**, enter your product name.
   b. In **Region**, select the required region.
   c. In **Zone**, select the required zone.
   d. Under **Machine configuration**, in **Series**, select **E2**.
5. Under the **Boot disk** section, click **Change** and do the following:
   a. Select the appropriate RHEL image. For the supported RHEL version, see the “Third party software requirements” section.

b. In **Size (GB)**, enter the required disk size and click **Select**.

6. Click **Networking** > **Networking interfaces**, and update the following fields:
   a. In **Network**, select the VPC network.
   b. In **Subnetwork**, select an appropriate subnet.
   c. In **Primary Internal IP**, select Ephemeral Custom.
   d. In **Custom ephemeral IP address**, enter an IP address that is within the range of your network.
   e. In **External IP**, select an appropriate option.
7. Click **Done**.
8. Click **Security**.
9. Click **Create**.

   A Virtual machine instance is deployed and it appears under the VM instances page.

Next steps

Uploading the ISO to the RHEL virtual machine instance.

Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Google Cloud Platform.

Reuse the PPK file that was created earlier.

Procedure

1. Open WinSCP and enter the login credentials.
2. Click **Advanced**, and select **Advanced**.
3. In the left pane of the Advanced Site Settings window, click **Authentication**.
4. In the right pane, click the browse icon under the **Private key file** field and browse to the .ppk file.
5. Click **OK**, and click **Login**.
6. Upload the .iso to the virtual machine instance.

Chapter 4: Deploying the Avaya WebLM ISO image in Software-Only Environment using the Operating System Console

Preparing for software-only deployments

About this task

Use this procedure to prepare the setup for software-only deployments.

Before you begin

1. Create an RHEL instance with required resources and do the following:
   a. Ensure that the system is configured with RHEL 8 yum repository.

      For information about configuring the yum repository, see Red Hat documentation.

   b. **Important:**

      Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

      In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020558u that Avaya publishes periodically on the Avaya Support website.

   c. Ensure that the network interface naming convention is configured to old network scheme names.

      WebLM requires old network scheme eth0.

      Note:

      If you do not configure the old network scheme names, the deployment fails.

      For more information about creating RHEL instance, see the Red Hat documentation.

      For more information about the required resources, see Supported footprints information for respective environments.

Procedure

1. Log in to the RHEL instance as a default user and switch to the root account. To create a directory, run the following command:

   ```
   mkdir /var/installer
   ```

2. Download the Avaya Aura® application ISO to the RHEL instance.
3. To mount the ISO, run the following command:

   ```
   mount -o loop AvayaAuraWebLM_10.1.2.x.x-xxxxx_xx.iso /mnt
   ```

4. To copy the ISO content to the directory, run the following command:

   ```
   cp -rvf /mnt/* /var/installer
   ```

5. Run the following command to unmount the `/mnt` directory:

   ```
   umount /mnt
   ```

6. Go to `vim /etc/profile`, and enter the following command to set `Java_home`:

   ```
   export JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk
   ```

   ```
   export PATH=$JAVA_HOME/bin:$PATH
   ```

7. Delete the downloaded ISO file.
8. To install dependencies, run the following command:

   ```
   yum install -y WebLM-Dependencies-0.1-1.noarch.rpm --nogpgcheck
   ```

9. Set the **umask** to `0022`.
10. Ensure that the `Defaults requiretty` setting is not available in the `/etc/sudoers` file.
11. Ensure that the `log_group` permission is set to admin in the `/etc/audit/auditd.conf` file.
12. To configure the python to version 3 in RHEL 8, run the following command:

    ```
    alternatives --set python /usr/bin/python3
    ```

    The default python is python3.

    If the **alternatives** command fails, then use the following commands to set the python3 link:

    a. **unlink /usr/bin/python**

    b. **ln -s /usr/bin/python3 /usr/bin/python**

13. Set the system-wide crypto policy to LEGACY on the RHEL 8.x and later operating system by running the following command.

    ```
    update-crypto-policies --set LEGACY
    ```

    WebLM requires system-wide crypto policy to LEGACY:

    - To support backward compatible with product systems having older WebLM client.

- In case any WebLM client communication has key size less than 1023 to get license from WebLM Server.
- In case TLSv1 and TLSv1.1 communication is required. You can change the TLS version from the WebLM command-line interface.

If system-wide crypto policy is not set to Legacy, WebLM applies the default crypto policy settings that comes as part of OS installation.

14. Disable SELinux, if already enabled.

    For disabling SELinux, see the Red Hat documentation.

15. To remove cloud-init package for AWS, run the following command:

```
systemctl stop cloud-init
systemctl disable cloud-init
yum remove cloud-init -y
```

16. Reboot the system.

Next steps

Check the environment.

Avaya WebLM disk partitioning

Use the following table to refer to the recommended values for disk size and partition.

The disk partitioning is recommended. Alternatively, a single root partition can be used as long as it meets the minimum total disk size for the profile.

Partition	Profile 1	Profile 2
/	4 GB	4 GB
/tmp	1.5 GB	1.5 GB
/var	4.5 GB	4.5 GB
/opt	19 GB	19 GB
/var/log	1.8 GB	1.8 GB
/home	1.8 GB	1.8 GB
/var/log/audit	1.8 GB	1.8 GB
/boot	512 MB	512 MB
/boot/efi	512MB	512MB
swap	4 GB	4 GB
Minimal disk size	40 GB	40 GB

Note:

If you are planning to use an antivirus or another approved third party application, you must add the disk space required by the third party application to the values in the above table.

Checking the environment

Before you begin

- Create an RHEL instance.
- Create a user before running the installer.
- Install required RPMs.
- The procedure below is an important mandatory procedure: Configure the Java path as an environment variable and reboot the WebLM Server VM.

Procedure

1. Log in to the RHEL instance as a default user and switch to the root account.

   You must run the installer as a root user.

2. Go to `cd /var/installer`.
3. To check for installer environment check, do one of the following:
   - For profile 1, type the following command:

     ```
     ./Install_WebLM_10.1.2.0.x-xxxxx -c -p profile1
     ```

   - For profile 2, type the following command:

     ```
     ./Install_WebLM_10.1.2.0.x-xxxxx -c -p profile2
     ```

   The system checks for the environment against the installer. During this time, you cannot perform any other action.

   If the check fails, take necessary steps to fix errors and perform the installer check again.

Deploying Avaya WebLM in a software-only environment

Before you begin

- Create a user before running the installer.
- Create a RHEL instance with the required resources for software-only installation. For creating a RHEL instance, refer to the corresponding Red Hat documentation.
- Ensure that yum repository is configured on the RHEL instance. For more information, see Red Hat documentation.

- Ensure that SELinux is disabled. For more information, see Red Hat documentation.
- Download the application ISO file to the RHEL instance.

Procedure

1. Log in to the system as a root user.
2. Go to the `/var/install` directory.
3. Run the following installation script as a root user:

   ```
   /Install_WebLM_10.1.2.0.x-xxxx
   ```

4. Press **Enter** to continue the installation.
5. Type `y` to accept the EULA.
6. To specify configuration details, type `y`.
7. In **IP Address**, type the IP address of the WebLM instance.
8. In **Gateway**, type the gateway IP address of the WebLM instance.
9. In **IP Address of DNS Server**, type the domain name of the primary, secondary, and WebLM instances.

   Separate the IP addresses with commas (,).
10. In **Short Hostname**, type the hostname of the WebLM instance.

    The value of the WebLM hostname is case-sensitive. The restriction applies only during the upgrade of WebLM.
11. In **Domain Name**, type the domain name of the WebLM instance.
12. **(Optional)** In **Default Search List**, type the search list of domain names.
13. **(Optional)** In **NTP Server IP or FQDN**, type the IP address or FQDN of the NTP server.

    Separate the IP addresses with commas (,).
14. In **Time Zone Detail**, select the timezone where the WebLM instance is located.

    The system displays a list of available continents and countries.
15. At the **WebLM CLI USER** prompt, perform the following:
    a. In **WebLM command line user name**, type the username of the WebLM CLI user.

       Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
    b. In **WebLM command line user password**, type the password for the WebLM CLI user.
    c. In **Confirm Password**, retype the password to confirm the WebLM CLI user authentication.

16. At the **WebLM UI Password for User - admin** prompt, perform the following:
    a. In **WebLM UI admin user password**, type the password for the WebLM UI user.
    b. In **Confirm Password**, retype the password to confirm the WebLM UI user authentication.
17. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and do one of the following:

    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.
    ```

    - Select 1 to enable EASG.
    - Select 2 to disable EASG.

    Avaya recommends that you enable EASG.

    You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.
18. To confirm the WebLM Configuration parameters, type `Y`.
19. After the installation is successful, log in to the WebLM user interface to check the Avaya Aura® application version. For more information, see Verifying the WebLM software version on page 48.

Users and groups

The following tables list all the users and groups added by the installer.

Users

Username	Login account	Notes
inads	Yes	<>
csadmin	Yes	User needed for SDM access
admin	Yes	Admin user
init	Yes	Service account (EASG)
craft	Yes	Service account (EASG)
sroot	Yes	Service account (EASG)

Groups

Group
admin
securityadmin
csadmin
logadmin
cust
groot
gadmin
gsmgr
gcliuser
gasguser
gcacadmin
gcacnonadmin

Chapter 5: Deploying Avaya WebLM ISO image in Software-Only Environment using SDM Client

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager supports migration of Virtualized Environment-based 8.1.x or 10.1.x applications to Release 10.2.x in the customer's Virtualized Environment. For migrating to Release 10.2.x and later, you must use Solution Deployment Manager Release 10.2.x and later.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.
- Avaya Solutions Platform 130: Avaya Aura® applications are deployed on the Avaya provided hardware.

Note:

- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

With Solution Deployment Manager, you can do the following in Virtualized Environment, Avaya Solutions Platform 130, and Avaya Aura® Virtualized Appliance Release 8.x or earlier models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

Note:

When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

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

- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, and media modules
  - Session Manager
  - Branch Session Manager
  - AE Services

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 10.2.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Installing the Solution Deployment Manager client

Prerequisites for installing the Solution Deployment Manager client

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel** > **Programs** > **Programs and Features**.

   For information about uninstalling the Solution Deployment Manager client, see “Uninstalling the Solution Deployment Manager client”.

2. Ensure that Windows 8.1 64-bit, Windows 10 64-bit, Windows 11 64-bit, Windows Server 2016 64-bit, Windows Server 2019 64-bit, or Windows Server 2022 64-bit operating system is installed on the computer.

Tip:

On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

3. Ensure that at least 5 GB of disk space is available to install the client. To deploy applications, you must have additional 15 GB of disk space on your system.

   Tip:

   Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space.

4. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client and use the Solution Deployment Manager functionality.

   Note:

   System Manager 10.2.x Port Matrix lists all the ports and protocols that System Manager uses. You can access the System Manager 10.2.x Port Matrix document on the Avaya Support website at https://support.avaya.com/ by using valid credentials.

6. Ensure that ports support Avaya Aura® 10.2.x supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

   Tip:

   On **Computer**, right-click properties, and perform the following:

   a. In the left navigation pane, click **Advanced system settings**.
   b. On the System Properties dialog box, click the **Advanced** tab, and click **Environment Variables**.
   c. Verify the system variables.

9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

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.

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 **Support by Products** > **Downloads**, and type the product name as **System Manager**, and Release as **10.1.x**.
3. Click the **Avaya Aura® System Manager Release 10.1.x SDM Client Downloads,10.1.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*.

Adding a location

About this task

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

Procedure

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

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

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 10.2.x, the System Manager system supports the Red Hat Enterprise Linux Release (RHEL) 8.6 or RHEL 8.10 (64-bit) operating system.

Before you begin

Add a location.

Procedure

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

4. In **User Name**, type the username of the base operating system.

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

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

   If the platform has some applications running, the system automatically discovers those applications and displays the applications in the **Applications** tab.

   - If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
   - If you are adding OS, only **Add** and **Remove** operations are available on the **Platforms** tab. You cannot perform any other operations. On the **Applications** tab, the system enables the **New** option. If the application is System Manager, the system enables **Update App** on Solution Deployment Manager Client.

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

Deploying Avaya WebLM in a software-only environment using Solution Deployment Manager

About this task

Use this procedure to deploy Avaya WebLM ISO in a software-only environment using Solution Deployment Manager.

Before you begin

- Install the Solution Deployment Manager client if System Manager is unavailable.
- Add a location.
- Add a platform.

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 location.
4. On the **Applications** tab, click **New**.

   The system displays the Application Deployment dialog box.
5. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location if not already selected.
   b. In **Select Platform**, select a platform to deploy the *Software-Only ISO image*.

      The system displays the IP Address and FQDN of the platform in the **Platform IP** and **Platform FQDN** fields.
6. 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**.
7. Click **Next**.
8. 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.

     Remote library is not supported for software-only deployment.
   - **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.
9. In **Flexi Footprint**, select the footprint size for the application.
10. 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.

Note:

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

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

    The system displays the Environment Check Output window.

12. Click **Next**.
13. On the Configuration Parameters page, provide all the information required.

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

14. Click **Deploy**.
15. On the EULA Acceptance window, click **Accept**.

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

16. To continue with the deployment, click **Accept**.

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

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

Next steps

This is an important mandatory step: Configure the Java path as an environment variable and reboot the WebLM Server VM.

Chapter 6: Configuration

Configuring the Avaya WebLM instance

About this task

Use the following procedure for the WebLM first boot configuration.

Before you begin

Download and install the WebLM license file.

Procedure

1. Log in to the WebLM command line interface as admin.

   For example: ssh admin@<IP Address>

   At your first login, the system prompts you to change your admin password.
2. To configure the WebLM network and other parameters, run the command: **`WebLMSetup`**.
3. Read the End User License Agreement (EULA).
4. To accept the EULA, in **Do you accept the Avaya Software License Terms? (Y)es/(N)o**, type `Y`.

   The system displays the message: `Starting WebLM post-install first boot.`
5. To specify configuration details, type `y`.
6. In **IP Address**, type the IP address of the WebLM instance.
7. In **Gateway**, type the gateway IP address of the WebLM instance.
8. In **IP Address of DNS Server**, type the domain name of the primary, secondary, and WebLM instances.

   Separate the IP addresses with commas (,).
9. In **Short Hostname**, type the host name of the WebLM instance.

   The value of the WebLM hostname is case-sensitive. The restriction applies only during the upgrade of WebLM.
10. In **Domain Name**, type the domain name of the WebLM instance.
11. **(Optional)** In **Default Search List**, type the search list of domain names.
12. **(Optional)** In **NTP Server IP or FQDN**, type the IP address or FQDN of the NTP server.

Separate the IP addresses with commas (,).

13. In **Time Zone Detail**, select the timezone where the WebLM instance is located.

    The system displays a list of available continents and countries.

14. At the **WebLM CLI USER** prompt, perform the following:

    a. In **WebLM command line user name**, type the user name of the WebLM CLI user.

       Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.

    b. In **WebLM command line user password**, type the password for the WebLM CLI user.

    c. In **Confirm Password**, retype the password to confirm the WebLM CLI user authentication.

15. At the **WebLM UI Password for User - admin** prompt, perform the following:

    a. In **WebLM UI admin user password**, type the password for the WebLM UI user.

    b. In **Confirm Password**, retype the password to confirm the WebLM UI user authentication.

16. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and do one of the following:

    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.
    ```

    - Select 1 to enable EASG.
    - Select 2 to disable EASG.

    Avaya recommends that you enable EASG.

You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.

17. To confirm the WebLM Configuration parameters, in **Do you want to continue**, type `Y`.

    The system starts the configuration of the network parameters. The deployment process takes about 10–15 minutes to be completed.

    Do not reboot the system until the configuration is complete.

Application Deployment field descriptions

Configuration Parameters

Note:

The master WebLM server and the local WebLM server must be in the same IP mode either IPv4 or IPv6.

Name	Description
IPv4 Address	The IPv4 address of the WebLM virtual machine.
Netmask	The IPv4 subnetwork mask to assign to the WebLM virtual machine.
IPv4 Default Gateway	The gateway IPv4 address to assign to the WebLM virtual machine.
IP Address of DNS Server	The DNS IPv4 address to assign to the WebLM virtual machine. Separate the IP addresses with commas (,).
Short Hostname	The short hostname to assign to the WebLM virtual machine.
IPv6 Address	The IPv6 address of the WebLM virtual machine.
IPv6 Network Prefix	The IPv6 subnetwork mask to assign to the WebLM virtual machine.
IPv6 Gateway	The gateway IPv6 address to assign to the WebLM virtual machine.
Domain Name	The domain name of the WebLM virtual machine.
Default Search List	The short hostname to assign to the WebLM virtual machine.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Timezone	The timezone where the WebLM virtual machine is located. A list is available where you select the name of the continent and the name of the country.

WebLM CLI USER

Name	Description
WebLM command line user name	Specifies the WebLM command line user name. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel. Do not use the user names, such as, admin and csadmin.
WebLM command line user password	Specifies the WebLM command line user password.
Confirm Password	Re-type the WebLM command line user password.

WebLM UI Password for User - admin

Name	Description
WebLM UI admin user Password	Specifies the WebLM admin user password. **Note:** Do not use the default password for admin.
Confirm Password	Re-type the WebLM admin user password.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends that you enable EASG. You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.

Button	Description
Deploy	Displays the EULA acceptance screen. To accept EULA and start the deployment process, click **Accept**.

Chapter 7: Post-deployment verifications

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
```

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

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

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

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the

given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge or response.

Managing site certificates

Before you begin

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

Procedure

1. 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 8: 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: Appendix

Configuring PuTTY

Converting the *.pem file to the *.ppk format

Before you begin

Download the PuTTYGen software.

Procedure

1. Double-click the downloaded `puttygen.exe` file.
2. In the PuTTY Key Generator dialog box, click **Conversions** > **Import key**.
3. On Load private key, select a `.pem` file from your local computer, and click **Open**.

   The system displays the key in the **Key** section.
4. Click **Generate**.

   The system takes a few minutes.
5. Click **Save private key**.

Configuring PuTTY for an SSH session

Before you begin

Convert the `*.pem` file to the `*.ppk` format.

Procedure

1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click **Connections** > **SSH** > **Auth**.
3. In the **Authentication parameters** section, click **Browse**.
4. On **Select a private key**, select a `.ppk` file from your local computer, and click **Open**.

Signing in to the Amazon EC2 virtual server instance

Before you begin

- Convert the `*.pem` file to the `*.ppk` format.
- Configure PuTTY for an SSH session

Procedure

1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click **Session**.
3. In **Host Name (or IP Address)**, type `admin@<IP_Address>`, where `<IP_Address>` is the IP address of the Amazon EC2 virtual server instance.
4. Click **Open**.

Identifying the SSH user name of the RHEL instance on AWS

About this task

You will require the user name to login to the RHEL instance. This is applicable for software-only deployments.

Before you begin

Create RHEL instance on Amazon Web Services.

Procedure

1. Log on to the Amazon Web Services management console.
2. Click **Servers** > **EC2**.
3. In the right-pane, select the RHEL instance you created.
4. On the top of the page, click **Actions** > **Connect**.

   In the page that opens, under the **Example**, user name of the RHEL instance appears. For example: **`ssh -i "<Key_Pair.pem>" abc-user@<IP address>`**. In this example, “abc-user” is the user name to login to the RHEL instance using SSH.

Appendix B: List of required RPMs on RHEL 8.6

The following are lists of required RPMs on RHEL 8.6 for Avaya WebLM Software-Only environment:

A

abrt	abrt-addon-ccpp	abrt-addon-coredump-helper	abrt-addon-kerneloops
abrt-addon-pstoreoops	abrt-addon-vmcore	abrt-addon-xorg	abrt-cli
abrt-dbus	abrt-libs	abrt-tui	acl
aide	alsa-lib	at	atk
audit	audit-libs	augeas-libs	authselect
authselect-compat	authselect-libs	autogen-libopts	avahi-libs

B

basesystem	bash	bash-completion	bc
bind	bind-export-libs	bind-libs	bind-libs-lite
bind-license	bind-utils	binutils	biosdevname
blktrace	boost-date-time	boost-system	boost-thread
brotli	bubblewrap	bzip2	bzip2-libs

C

ca-certificates	cairo	c-ares	checkpolicy
chkconfig	chrony	clevis	clevis-dracut
clevis-luks	clevis-systemd	copy-jdk-configs	coreutils
coreutils-common	cpio	cracklib	cracklib-dicts
cronie	cronie-anacron	crontabs	crypto-policies
crypto-policies-scripts	cryptsetup	cryptsetup-libs	cups-libs
curl	cyrus-sasl	cyrus-sasl-lib	

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts
desktop-file-utils	device-mapper	device-mapper-event	device-mapper-event-libs
device-mapper-libs	device-mapper-persistent-data	dhcp-client	dhcp-common
dhcp-libs	diffutils	dmidecode	dnf
dnf-data	dnf-plugins-core	dnf-plugin-spacewalk	dos2unix
dosfstools	dracut	dracut-config-rescue	dracut-network
dracut-squash			

E

e2fsprogs	e2fsprogs-libs	efibootmgr	efi-filesystem
efivar	efivar-libs	elfutils	elfutils-default-yama-scope
elfutils-libelf	elfutils-libs	emacs-filesystem	ethtool
expat	expect		

F

file	file-libs	filesystem	findutils
firewalld	firewalld-filesystem	fontconfig	fontpackages-filesystem
freetype	fribidi	fstrm	fuse
fuse-common	fuse-libs	fwupd	

G

gawk	gc	GConf2	gdb
gdb-headless	gdbm	gdbm-libs	gdk-pixbuf2
gettext	gettext-common-devel	gettext-devel	gettext-libs
giflib	glib2	glibc	glibc-all-langpacks
glibc-common	gmp	gnupg2	gnutls
gobject-introspection	gpgme	gpm-libs	graphite2
grep	groff-base	grub2-common	grub2-efi
grub2-tools	grub2-tools-extra	grub2-tools-minimal	grubby
gssproxy	gtk-update-icon-cache	guile	gzip

H

harfbuzz	haveged	hostname	hunspell
hunspell-en	hunspell-en-GB	hunspell-en-US	hwdata

I

ima-evm-utils	info	initscripts	insights-client
ipcalc	iproute	iprutils	ipset
ipset-libs	iptables	iptables-ebtables	iptables-libs
iputils	irqbalance		

J

jansson	java-1.8.0-openjdk	java-1.8.0-openjdk-devel	java-1.8.0-openjdk-headless
javapackages-filesystem	jbigkit-libs	jose	jq
json-c	json-glib		

K

kbd	kbd-legacy	kbd-misc	kernel-core
kexec-tools	keyutils	keyutils-libs	kmod
kmod-libs	krb5-libs	ksh	

L

ledmon	less	libacl	libaio
libarchive	libassuan	libatomic_ops	libattr
libbabeltrace	libbasicobjects	libblkid	libbsd
libcap	libcap-ng	libcollection	libcom_err
libcomps	libcroco	libcurl	libdaemon
libdatrie	libdb	libdbi	libdb-utils
libdnf	libdrm	libedit	libestr
libevent	libfastjson	libfdisk	libffi
libfontenc	libgcab1	libgcc	libgcrypt
libgomp	libgpg-error	libgudev	libgusb
libibverbs	libicu	libIDL	libidn2
libini_config	libipt	libjose	libjpeg-turbo
libkcapi	libkcapi-hmaccalc	libksba	libluksmeta
libmaxminddb	libmbim	libmetalink	libmnl
libmodman	libmodulemd	libmount	libmspack
libndp	libnetfilter_conntrack	libnfnetlink	libnfsidmap
libnftnl	libnghttp2	libnl3	libnl3-cli
libnsl2	libpath_utils	libpcap	libpciaccess
libpipeline	libpkgconf	libpng	libpq

Table continues…

libproxy	libpsl	libpwquality	libqmi
libref_array	librepo	libreport	libreport-cli
libreport-filesystem	libreport-plugin-kerneloops	libreport-plugin-logger	libreport-plugin-reportuploader
libreport-plugin-rhtsupport	libreport-plugin-ureport	libreport-rhel	libreport-web
libretls	librhsm	librsync	libseccomp
libselinux	libselinux-utils	libsemanage	libsepol
libsigsegv	libsmartcols	libsmbios	libsmi
libsolv	libss	libssh	libssh-config
libsss_idmap	libsss_nss_idmap	libstdc++	libsysfs
libtalloc	libtar	libtasn1	libteam
libtevent	libthai	libtiff	libtirpc
libtool-ltdl	libunistring	libusal	libusb
libusbx	libuser	libutempter	libuuid
libverto	libverto-libevent	libX11	libX11-common
libXau	libxcb	libXcomposite	libxcrypt
libXcursor	libXdamage	libXext	libXfixes
libXfont2	libXft	libXi	libXinerama
libxml2	libxmlb	libXrandr	libXrender
libxslt	libXtst	libyaml	libzstd
linux-firmware	lksctp-tools	lm_sensors-libs	logrotate
lsof	lua	lua-libs	luksmeta
lvm2	lvm2-libs	lz4	lz4-libs
lzo			

M

mailcap	man-db	mariadb-connector-c	mariadb-connector-c-config
microcode_ctl	mlocate	ModemManager-glib	mokutil
mozjs60	mpfr		

N

nano	ncurses	ncurses-base	ncurses-libs
netcat	nettle	net-tools	NetworkManager
NetworkManager-config-server	NetworkManager-libnm	NetworkManager-team	NetworkManager-tui
newt	nfs-utils	nftables	npth

Table continues…

nspr	nss	nss-softokn	nss-softokn-freebl
nss-sysinit	nss-util	numactl-libs	

O

oniguruma	openldap	openscap	openscap-scanner
openssh	openssh-askpass	openssh-clients	openssh-server
openssl	openssl-libs	open-vm-tools	os-prober

P

p11-kit	p11-kit-trust	pam	pango
parted	passwd	pciutils	pciutils-libs
pcre	pcre2	perl-Carp	perl-Compress-Raw-Bzip2
perl-Compress-Raw-Zlib	perl-constant	perl-Data-Dump	perl-Data-Dumper
perl-Data-OptList	perl-DB_File	perl-DBI	perl-Digest
perl-Digest-HMAC	perl-Digest-MD5	perl-Digest-SHA	perl-Digest-SHA1
perl-Encode	perl-Encode-Locale	perl-Errno	perl-Exporter
perl-File-Listing	perl-File-Path	perl-File-Temp	perl-Getopt-Long
perl-HTML-Parser	perl-HTML-Tagset	perl-HTTP-Cookies	perl-HTTP-Date
perl-HTTP-Message	perl-HTTP-Negotiate	perl-HTTP-Tiny	perl-interpreter
perl-IO	perl-IO-Compress	perl-IO-HTML	perl-IO-Socket-INET6
perl-IO-Socket-IP	perl-IO-Socket-SSL	perl-IO-Tty	perl-IPC-Run
perl-IPC-Run3	perl-libnet	perl-libs	perl-libwww-perl
perl-LWP-MediaTypes	perl-macros	perl-MIME-Base64	perl-Module-Pluggable
perl-Module-Runtime	perl-Net-DNS	perl-Net-HTTP	perl-Net-SSLeay
perl-NTLM	perl-Params-Util	perl-parent	perl-PathTools
perl-Pod-Escapes	perl-podlators	perl-Pod-Perldoc	perl-Pod-Simple
perl-Pod-Usage	perl-Scalar-List-Utils	perl-SelfLoader	perl-Socket
perl-Socket6	perl-Storable	perl-Sub-Install	perl-Switch
perl-Sys-Syslog	perl-Term-ANSIColor	perl-Term-Cap	perl-TermReadKey
perl-Text-ASCIITable	perl-Text-Balanced	perl-Text-ParseWords	perl-Text-Tabs+Wrap
perl-threads	perl-threads-shared	perl-TimeDate	perl-Time-Local
perl-Try-Tiny	perl-Unicode-Normalize	perl-URI	perl-WWW-RobotRules
perl-XML-LibXML	perl-XML-NamespaceSupport	perl-XML-Parser	perl-XML-SAX
perl-XML-SAX-Base	perl-XML-Writer	pinfo	pixman
pkgconf	pkgconf-m4	pkgconf-pkg-config	platform-python

Table continues…

platform-python-pip	platform-python-setuptools	plymouth	plymouth-core-libs
plymouth-scripts	policycoreutils	policycoreutils-python-utils	polkit
polkit-libs	polkit-pkla-compat	popt	procmail
procps-ng	protobuf-c	psmisc	publicsuffix-list
python2-pip-wheel	python2-setuptools-wheel	python3	python36
python3-abrt	python3-abrt-addon	python3-audit	python3-augeas
python3-bind	python3-cffi	python3-chardet	python3-configobj
python3-cryptography	python3-dateutil	python3-dbus	python3-decorator
python3-dmidecode	python3-dnf	python3-dnf-plugins-core	python3-dnf-plugin-spacewalk
python3-firewall	python3-gobject-base	python3-gpg	python3-hawkey
python3-hwdata	python3-idna	python3-iniparse	python3-libcomps
python3-libdnf	python3-librepo	python3-libreport	python3-libs
python3-libselinux	python3-libsemanage	python3-libxml2	python3-linux-procfs
python3-lxml	python3-magic	python3-netaddr	python3-netifaces
python3-newt	python3-nftables	python3-perf	python3-pip
python3-pip-wheel	python3-ply	python3-policycoreutils	python3-psutil
python3-psycopg2	python3-pwquality	python3-pycparser	python3-pycurl
python3-pyOpenSSL	python3-pysocks	python3-pyudev	python3-pyyaml
python3-requests	python3-rhn-check	python3-rhn-client-tools	python3-rhnlib
python3-rpm	python3-schedutils	python3-setools	python3-setuptools
python3-setuptools-wheel	python3-six	python3-slip	python3-slip-dbus
python3-subscription-manager-rhsm	python3-syspurpose	python3-systemd	python3-urllib3

Q

quota	quota-nls		

R

rdma-core	readline	redhat-logos	redhat-release
redhat-support-lib-python	redhat-support-tool	rhn-check	rhn-client-tools
rootfiles	rpcbind	rpm	rpm-build-libs
rpm-libs	rpm-plugin-selinux	rsync	rsyslog
rsyslog-gnutls	ruby	ruby-libs	

S

satyr	scap-security-guide	sed	selinux-policy
selinux-policy-targeted	sendmail	setools-console	setup
sg3_utils-libs	sgml-common	shadow-utils	shared-mime-info
shim	sqlite-libs	squashfs-tools	sssd-client
strace	subscription-manager-rhsm-certificates	sudo	systemd
systemd-libs	systemd-pam	systemd-udev	

T

tar	tcl	tcpdump	teamd
time	tpm2-tools	tpm2-tss	traceroute
ttmkfdir	tuned	tzdata	tzdata-java

U

unzip	util-linux	uuid	

V

vim-common	vim-enhanced	vim-filesystem	vim-minimal
virt-what			

W

wget	which	wireshark	words

X

xdg-utils	xfsprogs	xml-common	xmlrpc-c
xmlrpc-c-client	xmlsec1	xmlsec1-openssl	xorg-x11-fonts-Type1
xorg-x11-font-utils	xz	xz-libs	

Y

yum	yum-utils		

Z

zip	zlib		

Appendix C: List of required RPMs on RHEL 8.10

The following are lists of required RPMs on RHEL 8.10 for Avaya WebLM Software-Only environment:

A

acl	aide	alsa-lib	at
atk	audispd-plugins	audit	audit-libs
augeas-libs	authselect	authselect-compat	authselect-libs
autogen-libopts	avahi-libs	avaya-os-tools	

B

basesystem	bash	bash-completion	bc
bind	bind-export-libs	bind-libs	bind-libs-lite
bind-license	bind-utils	binutils	biosdevname
blktrace	boost-date-time	boost-system	boost-thread
brotli	bubblewrap	bzip2	bzip2-libs

C

ca-certificates	cairo	c-ares	checkpolicy
chkconfig	chrony	clevis	clevis-dracut
clevis-luks	clevis-systemd	copy-jdk-configs	coreutils
coreutils-common	cpio	cpp	cracklib
cracklib-dicts	cronie	cronie-anacron	crontabs
crypto-policies	crypto-policies-scripts	cryptsetup	cryptsetup-libs
cups-libs	curl	cyrus-sasl	cyrus-sasl-lib

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts

Table continues…

desktop-file-utils	device-mapper	device-mapper-event	device-mapper-event-libs
device-mapper-libs	device-mapper-persistent-data	dhcp-client	dhcp-common
dhcp-libs	diffutils	dmidecode	dnf
dnf-data	dnf-plugins-core	dnf-plugin-spacewalk	dnf-plugin-subscription-manager
dos2unix	dosfstools	dracut	dracut-config-rescue
dracut-network	dracut-squash		

E

e2fsprogs	e2fsprogs-libs	easg	efibootmgr
efi-filesystem	efivar	efivar-libs	elfutils-debuginfod-client
elfutils-default-yama-scope	elfutils-libelf	elfutils-libs	emacs-filesystem
ethtool	expat	expect	

F

fapolicyd	fapolicyd-selinux	file	file-libs
filesystem	findutils	firewalld	firewalld-filesystem
fontconfig	fontpackages-filesystem	freetype	fribidi
fstrm	fuse	fuse-common	fuse-libs
fwupd			

G

gawk	gc	gcc	gcc-gdb-plugin
GConf2	gdb	gdb-headless	gdbm
gdbm-libs	gdisk	gdk-pixbuf2	gdk-pixbuf2-modules
genisoimage	geolite2-city	geolite2-country	gettext
gettext-common-devel	gettext-devel	gettext-libs	giflib
glib2	glibc	glibc-all-langpacks	glibc-common
glibc-devel	glibc-gconv-extra	glibc-headers	glibc-langpack-en
gmp	gnupg2	gnupg2-smime	gnutls
gobject-introspection	gpgme	gpm-libs	graphite2
grep	groff-base	grub2-common	grub2-efi-x64
grub2-tools	grub2-tools-extra	grub2-tools-minimal	grubby
gssproxy	gtk2	gtk-update-icon-cache	guile
gzip			

H

hardlink	harfbuzz	haveged	hdparm
hicolor-icon-theme	hostname	hunspell	hunspell-en
hunspell-en-GB	hunspell-en-US	hwdata	

I

ima-evm-utils	info	initscripts	insights-client
ipcalc	iproute	iprutils	ipset
ipset-libs	iptables	iptables-ebtables	iptables-libs
iputils	irqbalance	isl	

J

jansson	jasper-libs	java-1.8.0-openjdk	java-1.8.0-openjdk-devel
java-1.8.0-openjdk-headless	javapackages-filesystem	jbigkit-libs	jose
jq	json-c	json-glib	

K

kbd	kbd-legacy	kbd-misc	kernel
kernel-core	kernel-headers	kernel-modules	kernel-tools
kernel-tools-libs	kexec-tools	keyutils	keyutils-libs
kmod	kmod-libs	kpartx	krb5-libs
ksh			

L

langpacks-en	ledmon	less	libacl
libaio	libarchive	libassuan	libatasmart
libatomic_ops	libattr	libbabeltrace	libbasicobjects
libblkid	libblockdev	libblockdev-crypto	libblockdev-fs
libblockdev-loop	libblockdev-mdraid	libblockdev-part	libblockdev-swap
libblockdev-utils	libbpf	libbytesize	libcap
libcap-ng	libcollection	libcom_err	libcomps
libcroco	libcurl	libdaemon	libdatrie
libdb	libdb-utils	libdnf	libdrm
libedit	libestr	libevent	libfastjson
libfdisk	libffi	libfontenc	libgcab1
libgcc	libgcrypt	libgomp	libgpg-error

Table continues…

libgudev	libgusb	libibverbs	libicu
libIDL	libidn2	libini_config	libipt
libjose	libjpeg-turbo	libkcapi	libkcapi-hmaccalc
libksba	libluksmeta	libmaxminddb	libmetalink
libmnl	libmodman	libmodulemd	libmount
libmpc	libmspack	libndp	libnetfilter_conntrack
libnfnetlink	libnfsidmap	libnftnl	libnghttp2
libnl3	libnl3-cli	libnsl2	libpath_utils
libpcap	libpciaccess	libpipeline	libpkgconf
libpng	libpq	libproxy	libpsl
libpwquality	libref_array	librepo	libreport
libreport-cli	libreport-filesystem	libreport-plugin-kerneloops	libreport-plugin-logger
libreport-plugin-reportuploader	libreport-plugin-rhtsupport	libreport-plugin-ureport	libreport-web
librhsm	librsync	libseccomp	libsecret
libselinux	libselinux-utils	libsemanage	libsepol
libsigsegv	libsmartcols	libsmbios	libsmi
libsolv	libss	libssh	libssh-config
libsss_idmap	libsss_nss_idmap	libstdc++	libsysfs
libtalloc	libtar	libtasn1	libteam
libtevent	libthai	libtiff	libtirpc
libtool-ltdl	libudisks2	libunistring	libusal
libusb	libusbx	libuser	libutempter
libuuid	libverto	libverto-libevent	libX11
libX11-common	libXau	libxcb	libXcomposite
libxcrypt	libxcrypt-devel	libXcursor	libXdamage
libXext	libXfixes	libXft	libXi
libXinerama	libxkbcommon	libxml2	libxmlb
libXrandr	libXrender	libxslt	libXtst
libyaml	libzstd	linux-firmware	lksctp-tools
lm_sensors-libs	lmdb-libs	logrotate	lsof
lua	lua-libs	luksmeta	lvm2
lvm2-libs	lz4	lz4-libs	lzo

M

mailcap	man-db	mariadb-connector-c	mariadb-connector-c-config
mdadm	memstrack	microcode_ctl	mlocate
mokutil	mozjs60	mpfr	

N

nano	ncurses	ncurses-base	ncurses-libs
net-snmp	net-snmp-agent-libs	net-snmp-libs	nettle
net-tools	NetworkManager	NetworkManager-config-server	NetworkManager-libnm
NetworkManager-team	NetworkManager-tui	newt	nfs-utils
nftables	nmap-ncat	npth	nspr
nss	nss-softokn	nss-softokn-freebl	nss-sysinit
nss-util	numactl-libs		

O

oddjob	oddjob-mkhomedir	oniguruma	openldap
openssh	openssh-askpass	openssh-clients	openssh-server
openssl	openssl-libs	openssl-pkcs11	open-vm-tools
os-prober			

P

p11-kit	p11-kit-trust	pam	pango
parted	passwd	pciutils	pciutils-libs
pcre	pcre2	perl-Carp	perl-Compress-Raw-Bzip2
perl-Compress-Raw-Zlib	perl-constant	perl-Data-Dump	perl-Data-Dumper
perl-Data-OptList	perl-DB_File	perl-DBI	perl-Digest
perl-Digest-HMAC	perl-Digest-MD5	perl-Digest-SHA	perl-Encode
perl-Encode-Locale	perl-Errno	perl-Exporter	perl-File-Listing
perl-File-Path	perl-File-Temp	perl-Filter	perl-Getopt-Long
perl-HTML-Parser	perl-HTML-Tagset	perl-HTTP-Cookies	perl-HTTP-Date
perl-HTTP-Message	perl-HTTP-Negotiate	perl-HTTP-Tiny	perl-interpreter
perl-IO	perl-IO-Compress	perl-IO-HTML	perl-IO-Socket-IP
perl-IO-Socket-SSL	perl-IO-Tty	perl-IPC-Run	perl-IPC-Run3
perl-IPC-SysV	perl-libnet	perl-libs	perl-libwww-perl
perl-LWP-MediaTypes	perl-macros	perl-Math-BigInt	perl-Math-Complex

Table continues…

perl-MIME-Base64	perl-Module-Pluggable	perl-Module-Runtime	perl-Mozilla-CA
perl-Net-DNS	perl-Net-HTTP	perl-Net-SSLeay	perl-NTLM
perl-Params-Util	perl-parent	perl-PathTools	perl-Pod-Escapes
perl-podlators	perl-Pod-Perldoc	perl-Pod-Simple	perl-Pod-Usage
perl-Scalar-List-Utils	perl-SelfLoader	perl-Socket	perl-Socket6
perl-Storable	perl-Sub-Install	perl-Switch	perl-Sys-Syslog
perl-Term-ANSIColor	perl-Term-Cap	perl-TermReadKey	perl-Text-ASCIITable
perl-Text-Balanced	perl-Text-ParseWords	perl-Text-Tabs+Wrap	perl-threads
perl-threads-shared	perl-TimeDate	perl-Time-HiRes	perl-Time-Local
perl-Try-Tiny	perl-Unicode-Normalize	perl-URI	perl-WWW-RobotRules
perl-XML-LibXML	perl-XML-NamespaceSupport	perl-XML-Parser	perl-XML-SAX
perl-XML-SAX-Base	perl-XML-Writer	pigz	pinentry
pinfo	pixman	pkgconf	pkgconf-m4
pkgconf-pkg-config	platform-python	platform-python-pip	platform-python-setuptools
plymouth	plymouth-core-libs	plymouth-scripts	policycoreutils
policycoreutils-python-utils	polkit	polkit-libs	polkit-pkla-compat
popt	procmail	procps-ng	protobuf-c
psmisc	publicsuffix-list-dafsa	python36	python3-audit
python3-augeas	python3-beautifulsoup4	python3-bind	python3-cffi
python3-chardet	python3-cloud-what	python3-cryptography	python3-cssselect
python3-dateutil	python3-dbus	python3-decorator	python3-dmidecode
python3-dnf	python3-dnf-plugins-core	python3-dnf-plugin-spacewalk	python3-ethtool
python3-firewall	python3-gobject-base	python3-gpg	python3-hawkey
python3-html5lib	python3-hwdata	python3-idna	python3-iniparse
python3-inotify	python3-jwt	python3-libcomps	python3-libdnf
python3-librepo	python3-libreport	python3-libs	python3-libselinux
python3-libsemanage	python3-libxml2	python3-linux-procfs	python3-lxml
python3-magic	python3-netaddr	python3-netifaces	python3-newt
python3-nftables	python3-perf	python3-pexpect	python3-pip
python3-pip-wheel	python3-ply	python3-policycoreutils	python3-psutil
python3-psycopg2	python3-ptyprocess	python3-pwquality	python3-pycparser
python3-pycurl	python3-pyOpenSSL	python3-pysocks	python3-pyudev
python3-pyyaml	python3-requests	python3-rhn-check	python3-rhn-client-tools

Table continues…

python3-rhnlib	python3-rpm	python3-setools	python3-setuptools
python3-setuptools-wheel	python3-six	python3-slip	python3-slip-dbus
python3-subscription-manager-rhsm	python3-syspurpose	python3-systemd	python3-unbound
python3-urllib3	python3-webencodings		

Q

quota	quota-nls		

R

readline	redhat-logos	redhat-release	redhat-release-eula
redhat-support-lib-python	redhat-support-tool	rhn-check	rhn-client-tools
rootfiles	rpcbind	rpm	rpm-build-libs
rpm-libs	rpm-plugin-fapolicyd	rpm-plugin-selinux	rpm-plugin-systemd-inhibit
rsync	rsyslog	rsyslog-gnutls	

S

satyr	sed	selinux-policy	selinux-policy-targeted
sendmail	setools-console	setup	sg3_utils-libs
sgml-common	shadow-utils	shared-mime-info	shim-x64
slang	snappy	sqlite	sqlite-libs
squashfs-tools	sssd-client	strace	subscription-manager
subscription-manager-rhsm-certificates	sudo	systemd	systemd-libs
systemd-pam	systemd-udev		

T

tar	tcl	tcpdump	teamd
time	timedatex	tmux	tpm2-tools
tpm2-tss	traceroute	trousers	trousers-lib
ttmkfdir	tuned	tzdata	tzdata-java

U

udisks2	unbound-libs	unzip	usermode
util-linux	uuid		

V

vim-common	vim-enhanced	vim-filesystem	vim-minimal
virt-what	volume_key-libs		

W

wget	which	words	

X

xdg-utils	xfsprogs	xkeyboard-config	xmlrpc-c
xmlrpc-c-client	xmlsec1	xmlsec1-openssl	xorg-x11-fonts-Type1
xorg-x11-font-utils	xz	xz-libs	

Y

yum	yum-utils		

Z

zip	zlib		

Appendix D: Creating RHEL virtual machine on Nutanix

Uploading the RHEL ISO to Nutanix server

About this task

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

Note:

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

Procedure

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

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

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

Next steps

Installing RHEL on Nutanix 6.5 and later.

Installing RHEL on the Nutanix server

Before you begin

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

Procedure

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

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

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

d. Click **Add**.

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

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

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

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

    b. Click **Save**.

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

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

    Note:

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

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

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

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

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

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

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

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

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

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

    h. Click **Done**.

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

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

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

Index

K

L

N

O

P

R

S

T

U

V

W