Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments

Release 10.2.x
Issue 15
March 2026

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to deploy the Avaya Aura® System Manager *Software-Only ISO image* on a:

- Customer-provided hardware
- Infrastructure as a Service environment

This document is intended for people who deploy and configure System Manager *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.

Changes to platform support

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

Discontinued Platforms:

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

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

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

Prerequisites

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

Knowledge

- Linux® Operating System
- Avaya Aura® System Manager
- 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 20.

Change history

Issue	Date	Summary of changes
15	March 2026	Added the section: Changes to platform support on page 6
14	November 2025	Updated the following sections: • Third-party software requirements on page 19 • Deploying System Manager Software-Only ISO image using the OS console on page 41
13	August 2025	Updated the following section: • Unsupported features of Avaya Aura application on Infrastructure as a Service on page 16
12	July 2025	Updated the following section: • Checklist for deploying ISO on Microsoft Azure on page 29
11	May 2025	Re-organized the following section: • Preparing System Manager for deployment on Cloud by disabling DHCP on page 15

Table continues…

Issue	Date	Summary of changes
10	April 2025	Added the following section: • List of Application-Based RPMs Provided by System Manager on page 74 Updated the following sections: • List of OS-based RPMs on RHEL 8.4 on page 63 • List of OS-based RPMs on RHEL 8.10 on page 68
9	February 2025	Added the following section: • Geographic Redundancy configuration on page 51
8	January 2025	Updated the following section: • List of OS-based RPMs on RHEL 8.4 on page 63 • List of OS-based RPMs on RHEL 8.10 on page 68
7	December 2024	Added the following sections for Release 10.2.1: • List of OS-based RPMs on RHEL 8.10 on page 68 • Uploading the RHEL ISO to Nutanix server on page 78 • Installing RHEL on the Nutanix server on page 79 Updated the following sections for Release 10.2.1: • Third-party software requirements on page 19 • Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 20 • Preparing for software-only deployments on page 37 • Site preparation checklist on page 24 • Creating RHEL instance on Microsoft Azure on page 29 • Software-only environment overview on page 10 • System Manager disk partitioning on page 39
6	May 2024	Updated: • Preparing for software-only deployments on page 37 • Installing the System Manager patch, service pack, or feature pack from CLI on page 49
5	May 2024	Updated: • Software-only environment overview on page 10 • Creating RHEL instance on Microsoft Azure on page 29 • Creating RHEL instance on Google Cloud Platform on page 33 • Preparing for software-only deployments on page 37

Table continues…

Issue	Date	Summary of changes
4	April 2024	Added the section Preparing System Manager for deployment on Cloud by disabling DHCP on page 15.
3	April 2024	Updated: • Deploying System Manager Software-Only ISO image using the OS console on page 41
2	April 2024	Changed hyper-threading to hyperthreading across the document.
1	December 2023	Initial issue of Release 10.2 document.

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 PSN020617u 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 and later
- 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 and G450 Branch 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

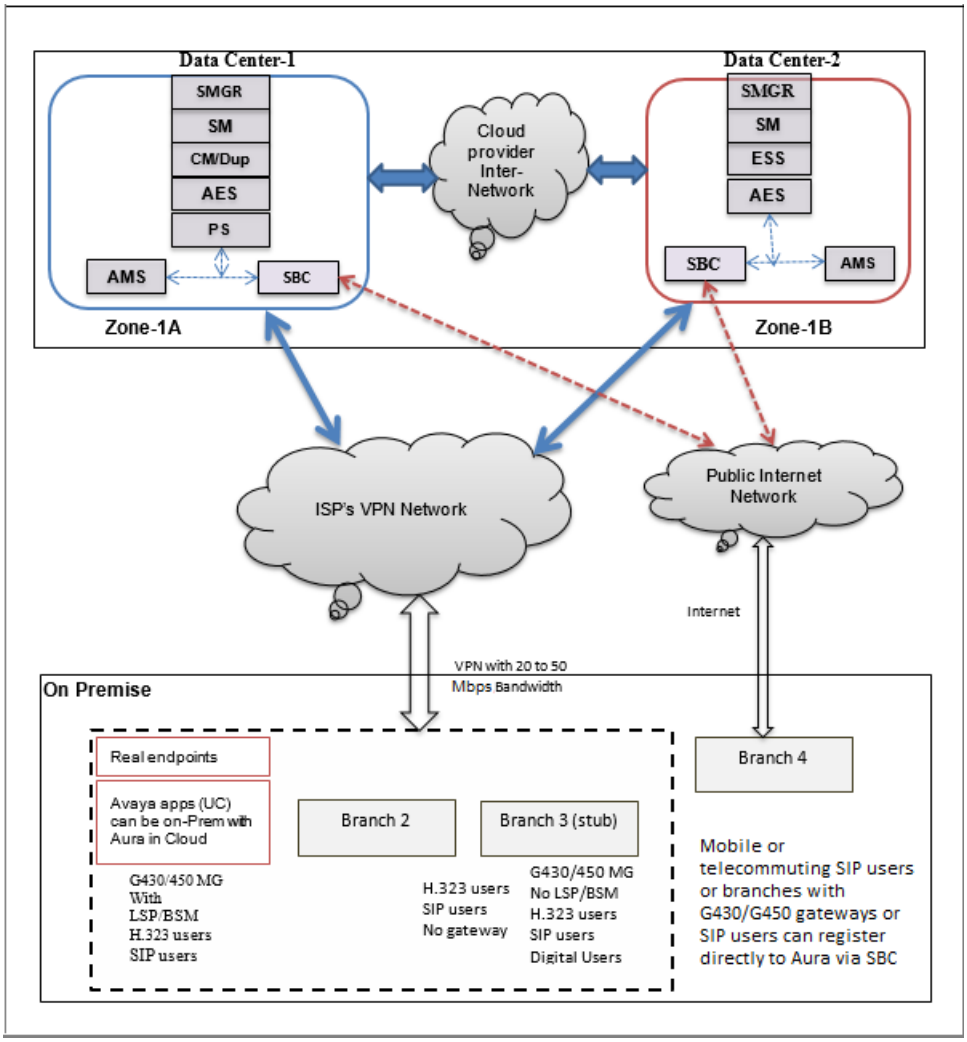
Topology on page 12
Connection types for Infrastructure as a Service on page 13
Networking considerations on page 14
Unsupported features of Avaya Aura application on Infrastructure as a Service on page 16

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 11

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 AWS documentation and search for “VPN connections”.
Direct connection	For more information, see AWS documentation section and search for “Direct connection”.

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 Microsoft documentation and search for “Create a Site-to-Site connection in the Azure portal”. For more information, go to Microsoft documentation and search for “Azure networking”.
Direct connection	For more information, go to Microsoft documentation and search for “ExpressRoute overview”.

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 Google Cloud documentation, and search for “Cloud VPN overview”.
GCN Direct	For more information, go to Google Cloud documentation, and search for “Dedicated Interconnect Overview”.

Related links

Infrastructure as a Service environment overview on page 11

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, refer to the Amazon Web Services documentation and search for relevant term.

For more information about Microsoft Azure VPN connection limits and VPN Gateway, refer to the Microsoft Azure documentation and search for relevant terms.

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 11
Preparing System Manager for deployment on Cloud by disabling DHCP on page 15

Preparing System Manager for deployment on Cloud by disabling DHCP

About this task

Typically, you must configure cloud-provided Red Hat instances before installing the System Manager *Software-Only ISO image*. For example, cloud-provided instances are often deployed with DHCP enabled. System Manager 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 System Manager server.

Related links

Networking considerations on page 14

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 16.

Amazon Web Services

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Changing the IP Address or FQDN using the **changeIPFQDN** command

Microsoft Azure

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Changing the IP Address or FQDN using the **changeIPFQDN** command

Google Cloud Platform

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Changing the IP Address or FQDN using the **changeIPFQDN** command

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
Session Border Controller	Yes	No	Not Supported

Table continues…

Product	On-Premise (OVA)	IAAS (SW-Only)	Support OOBM
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 11

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 System Manager

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) 8.4 or RHEL 8.10 virtual machine.

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		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit			
Linux operating system Release 7.6 with 64-bit	Y		
Linux operating system Release 8.4 with 64-bit		Y	Y
Linux operating system Release 8.10 with 64 bit			Y

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 System Manager *Software-Only ISO image* for on-premise

These footprint values are applicable for Software-Only deployments on VMware, Hyper-V, and KVM.

Note:

Avaya Aura® System Manager 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	CPUs (GHz)	Number of vCPUs	CPU reservation	RAM (GiB)	Memory reservation	HDD (GiB)	NICs
Profile 2	2.29	6	13740	12	12288	170	1
Profile 3	2.29	8	18320	18	18432	270	1
Profile 4	2.29	18	39600	36	39600	850	1

Supported footprints on IaaS

Supported footprints of System Manager on AWS

Note:

Avaya Aura® System Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

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

Footprint	Profile 2	Profile 3	Profile 4
Instance type	m4.2xlarge or higher, m5.2xlarge, m5a.2xlarge, c5a.2xlarge, or c5.2xlarge	m4.2xlarge or higher, m5.2xlarge, m5a.2xlarge, c5a.4xlarge, or c5.2xlarge	m4.10xlarge or higher, m5.8xlarge, m5a.8xlarge, c5.9xlarge, or c5a.8xlarge
HDD (GiB)	170	270	850
NICs	1	1	1

Supported footprints of System Manager ISO on Microsoft Azure

Note:

Avaya Aura® System Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

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

Footprint	Profile 2	Profile 3	Profile 4
Instance type	Standard_D8s_v3	Standard_D8s_v3	Standard_D32s_v3
HDD (GiB)	170	270	850
NICs	1	1	1

Supported footprints of System Manager ISO on Google Cloud Platform

Note:

Avaya Aura® System Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

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

Footprint	Profile 2	Profile 3	Profile 4
vCPU	6	8	18
RAM (GiB)	12	18	36
HDD (GiB)	170	270	850
NICs	1	1	1

Supported number of users on System Manager

The following System Manager resource requirements are based on the profile and are applicable for System Manager deployed on Customer-provided VMware, Avaya-supplied Avaya Solutions Platform 130, or Software-only environment.

Footprint	Max number of users	Max number of Branch Session Managers	Max number of Session Managers	Max number of Breeze	Max number of IP Office Branches
Profile 2	35,000 to 250,000	250	12	12	500
Profile 3	250,000	500	28	28	2000
Profile 4	300,000	5000	28	28	3500

System-wide crypto policy

Red Hat Enterprise Linux 8.x comes with system-wide crypto policies to simplify management of crypto across different supported applications, such as OpenSSL, GnuTLS, Kerberos 5, Bind, NSS, Java, OpenSSH client, OpenSSH server, libssh, libreswan. This supported application list can grow with new RHEL updates.

Software-only System Manager needs system-wide crypto policy to LEGACY to support backward compatibility with older systems. Although, System Manager applications such as Wildfly Application Server, SPIRIT, SystemMonitor, CND, Postgress, OpenSSH client, OpenSSH server, Csync2, rsyslog client override system-wide crypto settings at an application level and ensure a

stronger level of cryptographic strength as compared to RHEL provided LEGACY crypto policy. These applications level overrides are controlled through System Manager commands, and UI options.

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 18	
5	Register for PLDS and activate license entitlements.	Downloading software from PLDS on page 18	
6	Prepare the site.	Site preparation checklist on page 24	

Verifying if TMOUT variable is not set to read-only

About this task

Ensure that the **TMOUT** variable permission is not set to read-only. Use the following procedure to check if TMOUT is set as read-only.

Procedure

1. Using the SSH client, type `$ export TMOUT=0` command.

   If the system does not return an error, then no further action is required.

2. If the system returns an error, do the following:
   a. Comment out line `#readonly TMOUT(from the profile which sets TMOUT as read-only).`
   b. Close the existing session and open a new SSH session.

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) 8.4 or RHEL 8.10 with **Minimal Install** for the Software-Only deployment.	See Red Hat documentation.	
4	Configure Yum.	See Configuring Yum on RHEL on page 28	

Users and groups

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

Users

Username	Login account	Notes
admin	Yes	Admin user
csadmin	Yes	User needed for SDM access
smgr	Yes	System Manager user
nortel	Yes	Nortel user
init	Yes	Service account (EASG)
inads		
craft	Yes	Service account (EASG)
sroot	Yes	Service account (EASG)

Groups

Group	Description
susers	Members of this group have the necessary privileges needed to operate and maintain the application.

Table continues…

Group	Description
admin	Members of this group have the administrator privileges.
securityadmin	
smgr	
nortel	
csadmin	
logadmin	
cust	
groot	
gadmin	
gsmgr	
gcliuser	
gasguser	
gcacadmin	
gcacnonadmin	

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® System Manager ISO on *Amazon Web Services*.

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 18.	

Table continues…

No.	Task	Link/Notes	✔
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Ensure that you have the required resources.	See Supported footprints of System Manager on AWS on page 21	
5	Create an RHEL instance.	See Creating RHEL instance on Amazon Web Services on page 26	
6	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services on page 28	
7	Configure Yum.	See Configuring Yum on RHEL on page 28	

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 PSN020617u that Avaya publishes periodically on the Avaya Support website.

Also, 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 an Instance**.
4. Under **Name and tags**, for Name, enter a descriptive name for your instance.

   Note:

   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.
5. Under **Application and OS Images (Amazon Machine Image)**, search for the supported RHEL version in **Community AMIs**, and click **Select**.

For the supported RHEL version, see “Third party software requirements” section.

6. Under **Instance type**, select the instance type according to your required footprints.

   For information about instance type, see “Supported footprints for the System Manager on AWS”.

7. Under **Key pair (login)**, select an existing key pair or create a new key pair dialog box using the following options:

   - **Choose an existing key pair**.
   - **Create a new key pair**.

8. If you select the **Choose an existing key pair** option, from the **Select a key pair** drop-down list, and select a key pair.

9. 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 **Create key pair**. The key pair will automatically download to the system after clicking on **Create key pair**.

   c. Save the file in a secure and accessible location.

   Note:

   You will not be able to download the file again.

10. Under **Network settings**, choose **Edit**. For Security group name, select **Create security group** for creating a new security group or **Select existing security group** to select an existing security group.

    If you select an existing security group, from **Common security groups** dropdown, choose your security group from the list of existing security groups.

11. Click **Configure storage**.

    For example, change the size of the default Hard Disk size from 10 to 170 GiB for Profile 1.

12. Review the details of each configuration in the **Summary** panel.

13. Click **Launch Instances**.

    The system creates the RHEL instance.

14. Click on the hyperlink of the instance ID to view the details of your instance.

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

Next steps

[Preparing System Manager for deployment on Cloud by disabling DHCP](#) on page 15

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® System Manager ISO on Microsoft Azure.

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 18.	
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Ensure that you have the required resources.	See Supported footprints of System Manager ISO on Microsoft Azure on page 21	
5	Create an RHEL instance.	See Creating RHEL instance on Microsoft Azure on page 29	
6	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure on page 32	

Creating RHEL instance on Microsoft Azure

Before you begin

Create an account on Microsoft Azure.

Do the following in Microsoft Azure environment:

- Create a resource group.

You must provide the same resource group while creating any resource in Microsoft Azure.

- Create a storage account.
- In the same resource group, create a vNet and create an address space in that vNet with sufficient IP addresses.
- Using the IP address space:
  - Create a subnet for Main interfaces.
  - Create a subnet for duplication link interfaces.
  - Create a subnet for Gateway. For VPN Gateway, VPN gateway will internally use this subnet.

    For more information, see Microsoft Azure documentation and search for VPN Gateway.
  - Create VPN connection between your Azure Private Network and your enterprise premise by creating VPN gateway, Local Gateway, Connection, Shared Key.

    For more information, see Microsoft Azure documentation and search for relevant terms.
  - Create a Network Security group and ensure that the ports are open as per the port matrix guide of respective product.

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 PSN020617u 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 8.4 or Red Hat Enterprise Linux 8.10** from the images list.
   d. In **Size**, select the required details.

      For System Manager Profile 2 and 3, select Standard_D8s_v3.

For System Manager Profile 4, select Standard_D32s_v3.

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**.

For System Manager Profile 2, attach a disk of 128 GiB.

For System Manager Profile 3, attach a disk of 220 GiB.

For information about disk partitions for all profiles, see “System Manager disk partitioning”.

Note:

Disk partitioning is mandatory. You must configure the partition on the RHEL virtual machine as per the disk partitioning table before starting the System Manager installation procedure.

c. On Create a new disk page, click **Change size** and select **55 GiB** from the list.

d. Click **OK**.

A new disk of size 55 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 **Review + create** tab, review the details and click **Create**.

The deployment begins. Wait till the deployment is complete.

Next steps

Prepare for software-only deployment.

Related links

Preparing for software-only deployments on page 37

System Manager disk partitioning on page 39

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 Platform

Checklist for deploying ISO on Google Cloud Platform

Ensure that you complete the following before deploying Avaya Aura® System Manager ISO on Google Cloud Platform.

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 18.	
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Create a PPK file.	See Creating a PPK file on page 33	

Table continues…

No.	Task	Link/Notes	✔
5	Ensure that you have the required resources.	See Supported footprints of System Manager ISO on Google Cloud Platform on page 22	
6	Create an RHEL instance.	See Creating RHEL instance on Google Cloud Platform on page 33	
7	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform on page 36	

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 PSN020617u 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**.
    e. In **Machine type**, select **Custom** and then select the number of vCPUs and memory needed for your deployment.

        Note:

        Select the **Custom** option for the supported Google Cloud Platform Machine type. Select the number of vCPUs and memory details based on the System Manager profile.

        For example, the corresponding mapping information for Profile 2 is shown in the screenshot:

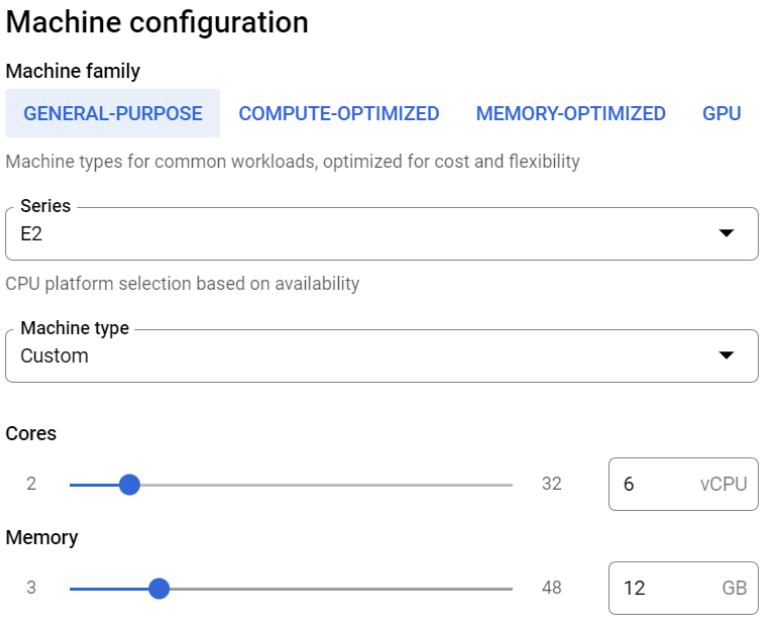


Figure 1: Custom machine type and Profile 2 vCPU and memory details

Use the required CPUs only. For CPU, memory, and hard disk details, see the Supported footprints of System Manager ISO on Google Cloud Platform on page 22.

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 (GiB)**, enter the required disk size and click **Select**.

   For more information about the disk size requirements, see Supported footprints of System Manager ISO on Google Cloud Platform on page 22.
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. Under the **SSH Keys** section, click **ADD ITEM**.
10. In **SSH key 1**, copy the public SSH key details along with the username.

11. 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.

Next steps

Prepare for software-only deployment.

Related links

Preparing for software-only deployments on page 37

Chapter 4: Deploying the System Manager Software-Only ISO image using 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 PSN020617u that Avaya publishes periodically on the Avaya Support website.

   c. Create the required disk partitions.

      You must have the following partitions:

      - `/var/lib/pgsql/data`
      - `/emdata`
      - `/perfdata`
      - `/swlibrary`

      For information about the partitions, see “System Manager disk partitioning”.

   d. Ensure that the `/etc/cron.deny` file is available on the System Manager system. Do the following:

      a. If the `/etc/cron.allow` file is available, then delete it.

      b. If the `/etc/cron.deny` is not available, then create the `/etc/cron.deny` file on the System Manager system.

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

System Manager requires old network scheme eth0 and eth1.

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 supported Red Hat Enterprise Linux operating system versions, see Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 20.

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

Procedure

1. For deploying System Manager 10.2 ISO, run the following command to install the openjdk libraries before installing the actual System Manager dependencies RPM to be consistent with 10.2.0.0 OVA patch.

   yum install java-1.8.0-openjdk-1.8.0.342.b07-2.el8_6.x86_64 java-1.8.0-openjdk-headless-1.8.0.342.b07-2.el8_6.x86_64 java-1.8.0-openjdk-devel-1.8.0.342.b07-2.el8_6.x86_64

2. 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 /swlibrary/installer
   ```

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

   ```
   mount -o loop AvayaAuraSystemManager-10.2.x.0.xxxxxx_vxx.iso /mnt
   ```

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

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

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

   ```
   umount /mnt
   ```

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

   ```
   yum install SMGR-Dependencies-0.1-1.noarch.rpm -y
   ```

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
    ```

    For details, see “System-wide crypto policy”.

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.

Related links

Checking the environment on page 40

System Manager 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.

Note:

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

Partition	Profile 2	Profile 3	Profile 4
/	5 GiB	16 GiB	16 GiB
/emdata	15 GiB	20 GiB	20 GiB

Table continues…

Partition	Profile 2	Profile 3	Profile 4
/perfdata	25 GiB	30 GiB	29 GiB
/swlibrary	50 GiB	50 GiB	155 GiB
/var	6 GiB	18 GiB	40 GiB
/var/lib/pgsql/data	15 GiB	51 GiB	460 GiB
/var/opt/nortel/cnd	1 GiB	1 GiB	1 GiB
/var/log	15 GiB	22.5 GiB	36.5 GiB
/var/log/audit	5 GiB	9 GiB	25 GiB
/home	5 GiB	7.5 GiB	9.5 GiB
/opt	20 GiB	34 GiB	45 GiB
/tmp	3 GiB	6 GiB	20 GiB
swap	4 GiB	4 GiB	8 GiB
/boot	0.5 GiB	0.5 GiB	0.5 GiB
/boot/efi	0.5 GiB	0.5 GiB	0.5 GiB
Minimal disk size	170 GiB	270 GiB	867 GiB

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.

  For more information on supported Red Hat Enterprise Linux operating system versions, see Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 20.
- Create a user before running the installer.
- Install required RPMs.
- Ensure that you have configured Java path as an environment variable.

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 /swlibrary/installer`.

3. To check for installer environment check, do one of the following:
   - For profile 2, type the following command:

     ```
     ./Install_System_Manager_10.2.0.0.xxxxxx -c -p 250Kuser
     ```
   - For profile 3, type the following command:

     ```
     ./Install_System_Manager_10.2.0.0.xxxxxx -c -p 250Kuser-prof3
     ```
   - For profile 4, type the following command:

     ```
     ./Install_System_Manager_10.2.0.0.xxxxxx -c -p 300Kuser-prof4
     ```

   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 System Manager *Software-Only ISO image* using the OS console

About this task

Use this procedure to deploy the System Manager *ISO image* in a *Software-Only* environment.

Note:

The deployment of Avaya Aura® applications as software only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as software only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Before you begin

- Create an operating system instance.

  For information, see “Preparing for software-only deployments”.
- Copy the installer and check the environment.

  For information, see “Checking the environment”.

Procedure

1. Log on to the RHEL instance.

   Ensure that you use the bash shell for installation.
2. Go to the `/swlibrary/installer` directory.
3. Run the following installation script as a root user:

   ```
   ./Install_System_Manager_10.2.0.0.xxxxxx
   ```

   The system runs the command and displays the system changes.

Note:

When you install the System Manager *ISO image* on RHEL 8.10, the following warning message is displayed. You can ignore this warning message and proceed to the next step:

```
WARNING: OS version detected is 8.10. Supported version is 8.4.
But Installer will continue..
```

4. Press `Enter` to continue.

   The installer checks the package and environment settings.

   The System Manager system displays the following message:

   ```
   A reboot will be required in order to complete this. Please exit
   any other sessions before continuing.
   ```

5. Press `Enter` to continue.
6. In the Enter profile field, check the message and type the required System Manager profile from the following:
   - Press `1` for profile 2
   - Press `2` for profile 3
   - Press `3` for profile 4
7. Press `Enter` on the End User License Agreement page.
8. Press `Space` to read the license agreement.
9. Press `Y` to accept the license terms.

   The installation process begins.

   The system starts the installation and prompts you to configure the System Manager configuration and network parameters before proceeding to the next step. For more information about configuration and network parameters, see Network and configuration field descriptions on page 44.
10. At the Enhanced Access Security Gateway (EASG) prompt, read the EASG information, and do one of the following:
    - To enable EASG (Recommended), type `1`.
    - To disable EASG, type `2`.
11. Select the required Backup definition parameter for System Manager schedule backup.
12. Verify the configuration details and press **Enter** to continue.
13. At the Do you want to continue prompt, type `y`.

    After the installation is complete the system reboots.
14. To verify the post installation status, type the following command:

    ```
    tail -f /var/log/Avaya/PostDeployLogs/post_install_sp.log
    ```

On successful post installation, System Manager displays a message.

For example: `exit status of eject command is....`

15. Delete the `/swlibrary/installer` directory.
16. Access System Manager web console using IP address or FQDN.

    If installation is successful, System Manager displays the following message:

    `Installation of latest System manager patch is mandatory`

    For information about patch installation, see “Installing the System Manager patch, service pack, or feature pack from CLI ”.

Chapter 5: Configuration

Network and configuration field descriptions

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application for Out of Band Management. This field is an optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager application.
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. This field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. This field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. This field is optional.
Default Search List	The search list of domain names. This field is optional.

Note:

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.

Table continues…

Name	Description
Public Netmask	The IPv4 subnetwork mask to assign to System Manager application. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager application. The field is optional.
Public FQDN	The FQDN to assign to the System Manager application. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager application. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.

Table continues…

Name	Description
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **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.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.

Table continues…

Name	Description
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Out of Band Management	The port number that you must assign to the Out of Band Management port group. The field is mandatory.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description

Table continues…

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`**.

Installing the System Manager patch, service pack, or feature pack from CLI

About this task

Note:

- If you upgrade System Manager from an older release like 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x, and the goal is to apply the latest Feature Pack or Service pack of 10.2.x, then you can install the latest service pack or feature pack of System Manager Release 10.2.x as part of the migration process. For an upgrade/migration, you should not install the mandatory patch manually. The data migration utility prompts you to install the mandatory patch or the latest service pack

  For example, if you upgrade System Manager from Release 10.1.x to Release 10.2.x, then you can directly apply the Release 10.2.x patch as part of data migration. You do not need to apply the 10.2 GA patch (`System_Manager_10.2.0.0_GA_Patch_rxxxxxxxxx.bin`) in the intermediate step.
- If you perform the fresh deployment of System Manager Release 10.2 and the goal is to be on the latest Feature Pack or Service Pack of 10.2.x that is available, then after deploying the Release 10.2 OVA you can directly install the latest feature pack or service pack of System Manager Release 10.2.x. You do not have to install the 10.2 GA patch first.
- After enabling data encryption and installing the System Manager 8.1.2 and later patch, if the local or remote key store is not enabled, the Data Encrypted server prompts for the encryption passphrase. After you enter the encryption passphrase, System Manager automatically reboots. This happens only after the first reboot and prompts you to add the encryption passphrase again.

Before you begin

- Ensure that System Manager is running on Release 10.2.
- Download the System Manager patch bin file from the Avaya Support website at https://support.avaya.com/ and copy the file to the `/swlibrary` location on System Manager.

Procedure

1. Log in to the System Manager command-line interface with administrator privilege credentials.
2. Create a snapshot of the System Manager application.

   This activity might impact the service.
3. Type the following: `SMGRPatchdeploy <absolute path to the patch, service pack, or feature pack for System Manager>`

   If you do not provide the name of the patch, service pack, or feature pack, the console displays menu items. Provide the absolute path to the System Manager patch, service pack, or feature pack.

   System Manager displays the license information.
4. Read the End User License Agreement carefully, and to accept the license terms, type `Y`.

   The patch installation takes about 45 minutes to complete.

   If the installation is successful, the system displays a warning message on the dashboard and on the command line interface to restart System Manager, if the kernel is updated.
5. Perform one of the following:
   - If the patch installation is successful, remove the patch bin file, log off from the system, and remove the snapshot.

     Note:

     Snapshots occupy the system memory and degrade the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.
   - If the patch installation fails, first collect logs and then use the snapshot to restore the system to the original state.

     To collect logs, you can run the **`collectLogs`** command. The system creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file in the `/swlibrary` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to the remote server and share the file with Avaya Support Team.

Next steps

Note:

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

Log on to the System Manager web console. At your first login, change the System Manager web console credentials.

Rebooting the System Manager virtual machine through command-line interface

About this task

When you start the reboot process, you cannot access the System Manager web console.

Important:

If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.

Procedure

1. Log in to the System Manager command-line interface.
2. Type **`rebootVM`** and press **Enter**.
3. At the **Do you want to continue ? .. (Yes/No)** prompt, type **Yes** and press **Enter**.

   System Manager starts the reboot process.

Dual data center configuration

For configuring the applications in a dual data center environment, the instances must be configured in the same network region in two zones on the same Virtual Private Cloud (VPC).

Geographic Redundancy configuration

For more information about Geographic Redundancy configuration, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.

Chapter 6: Post-installation verification

Post-installation steps

Procedure

Recreate all licenses with the new host ID format, and install the new license files.

System Manager uses a new host ID format for Avaya WebLM server. Therefore, all previously installed licenses become invalid. For instructions to install the license file, see Managing licenses in *Administering Avaya Aura® System Manager*.

Verifying the installation of System Manager

About this task

Perform the following verification procedure after installing the System Manager patch and configure System Manager.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`.
2. To log on to the System Manager web console, do the following:
   a. In **User ID**, type the default user name “admin”.
   b. In **Password**, type the default password “admin123”.
   c. Click **Log On**.
3. On the Password Change page, do the following:
   a. In **User ID**, type the default user name.
   b. In **Current password**, type the default password.
   c. In **New password**, type a new password.
   d. In **Confirm new password**, retype the new password.
   e. Click **Save**.

      System Manager displays the following confirmation message:

      `User (admin) password changed successfully.`

4. Click the **Primary Login** link.
5. On the System Manager log on page, type the user name and new password.
6. On the upper-right corner, click  and click **About**.

   The system displays a pop up window with the build details.
7. Verify the System Manager version number.

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

Note:

After installing the language pack, you cannot uninstall the language pack.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `locate LocalizationScript.sh`, and press `Enter`.

   System Manager displays the path of the localization script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/script/LocalizationScript.sh`
3. Type `locate FrenchResourceBundle.zip`, and press `Enter`.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path; the path might vary based on actual path that you get.
4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.
5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
6. If you are installing the language pack through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

Note:

During this activity, System Manager restarts the Application server. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode, then apply these steps on the secondary System Manager server also after secondary server is active.

7. Change the browser language setting to French.

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 product certificate expiration

The Avaya Aura® application raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

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 7: Resources

System Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

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 on the Avaya Learning website at http://www.avaya-learning.com. After you login to the website, enter the course code or the title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 61

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.

- Links to other pertinent information.

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

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

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

Related links

Support on page 61

Appendix A: List of OS-based RPMs on RHEL 8.4

The following is a list of OS-based RPMs required on RHEL 8.4 for Avaya Aura® System Manager Software-Only environment:

A

acl	alsa-lib	atk	audit
audit-libs	authselect	authselect-libs	avahi-libs

B

basesystem	bash	biosdevname	brotli
bubblewrap	bzip2-libs		

C

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

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts
device-mapper	device-mapper-event	device-mapper-event-libs	device-mapper-libs
device-mapper-persistent-data	diffutils	dmidecode	dnf
dnf-data	dnf-plugins-core	dnf-plugin-subscription-manager	dosfstools
dracut	dracut-config-rescue	dracut-network	dracut-squash

E

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

F

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

G

gawk	gdbm	gdbm-libs	gdisk
gdk-pixbuf2	gdk-pixbuf2-modules	gettext	gettext-libs
glib2	glibc	glibc-common	glibc-gconv-extra
glibc-langpack-en	gmp	gnupg2	gnupg2-smime
gnutls	gobject-introspection	gpgme	gpg-pubkey
gpg-pubkey	gpm-libs	graphite2	grep
groff-base	grub2-common	grub2-efi-x64	grub2-tools
grub2-tools-extra	grub2-tools-minimal	grubby	gtk2
gtk-update-icon-cache	gzip		

H

hardlink	harfbuzz	hdparm	hicolor-icon-theme
hostname	hwdata		

I

ima-evm-utils	info	initscripts	insights-client
iproute	iprutils	ipset	ipset-libs
iptables	iptables-ebtables	iptables-libs	iputils
irqbalance	iwl100-firmware	iwl1000-firmware	iwl105-firmware
iwl135-firmware	iwl2000-firmware	iwl2030-firmware	iwl3160-firmware
iwl5000-firmware	iwl5150-firmware	iwl6000-firmware	iwl6000g2a-firmware
iwl6050-firmware	iwl7260-firmware		

J

jansson	jasper-libs	java-1.8.0-openjdk	java-1.8.0-openjdk-devel

Table continues…

java-1.8.0-openjdk-headless	javapackages-filesystem	jbigkit-libs	json-c
json-glib			

K

kernel	kernel-core	kernel-modules	kernel-tools
kernel-tools-libs	keyutils-libs	kmod	kmod-libs
kpartx	krb5-libs	kexec-tools	

L

langpacks-en	less	libacl	libaio
libarchive	libassuan	libatasmart	libattr
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	libdhash
libdnf	libdrm		

M

man-db	mdadm	memstrack	microcode_ctl
mokutil	mozjs60	mpfr	

N

ncurses	ncurses-base	ncurses-libs	nettle
NetworkManager	NetworkManager-libnm	NetworkManager-team	NetworkManager-tui
newt	nftables	npth	nspr
nss	nss-softokn	nss-softokn-freebl	nss-sysinit
nss-util	numactl-libs		

O

openldap	openssh	openssh-clients	openssh-server
openssl	openssl-libs	openssl-pkcs11	open-vm-tools
os-prober			

P

p11-kit	p11-kit-trust	pam	pango

Table continues…

parted	passwd	pciutils	pciutils-libs
pcre	pcre2	pigz	pinentry
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
prefixdevname	procps-ng	psmisc	publicsuffix-list-dafsa
python3-audit	python3-chardet	python3-cloud-what	python3-dateutil
python3-dbus	python3-decorator	python3-dnf	python3-dnf-plugins-core
python3-ethtool	python3-firewall	python3-gobject-base	python3-gpg
python3-hawkey	python3-idna	python3-iniparse	python3-inotify
python3-libcomps	python3-libdnf	python3-librepo	python3-libs
python3-libselinux	python3-libsemanage	python3-linux-procfs	python3-magic
python3-nftables	python3-perf	python3-pip-wheel	python3-policycoreutils
python3-pysocks	python3-pyudev	python3-pyyaml	python3-requests
python3-rpm	python3-setools	python3-setuptools-wheel	python3-six
python3-slip	python3-slip-dbus	python3-subscription-manager-rhsm	python3-syspurpose
python3-systemd	python3-unbound	python3-urllib3	

R

readline	redhat-release	redhat-release-eula	rhc
rootfiles	rpm	rpm-build-libs	rpm-libs
rpm-plugin-selinux	rpm-plugin-systemd-inhibit	rsyslog	

S

sed	selinux-policy	selinux-policy-targeted	setup
sg3_utils	sg3_utils-libs	shadow-utils	shared-mime-info
shim-x64	slang	snappy	sqlite-libs
squashfs-tools	sssd-client	sssd-common	sssd-kcm
sssd-nfs-idmap	subscription-manager	subscription-manager-rhsm-certificates	sudo
systemd	systemd-libs	systemd-pam	systemd-udev

T

tar	teamd	tpm2-tss	trousers
trousers-lib	ttmkfdir	tuned	tzdata
tzdata-java			

U

udisks2	unbound-libs	usermode	util-linux

V

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

W

wget	which		

X

xfsprogs	xkeyboard-config	xmlsec1	xmlsec1-openssl
xorg-x11-fonts-Type1	xorg-x11-font-utils	xz	xz-libs

Y

yum			

Z

zlib			

Appendix B: List of OS-based RPMs on RHEL 8.10

The following is a list of OS-based RPMs required on RHEL 8.10 for Avaya Aura® System Manager Software-Only environment:

A

acl	alsa-lib	atk	audit
audit-libs	authselect	authselect-libs	avahi-libs

B

basesystem	bash	biosdevname	brotli
bubblewrap	bzip2-libs		

C

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

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts
device-mapper	device-mapper-event	device-mapper-event-libs	device-mapper-libs
device-mapper-persistent-data	diffutils	dmidecode	dnf
dnf-data	dnf-plugins-core	dnf-plugin-subscription-manager	dosfstools
dracut	dracut-config-rescue	dracut-network	dracut-squash

E

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

F

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

G

gawk	gdbm	gdbm-libs	gdisk
gdk-pixbuf2	gdk-pixbuf2-modules	gettext	gettext-libs
glib2	glibc	glibc-common	glibc-gconv-extra
glibc-langpack-en	gmp	gnupg2	gnupg2-smime
gnutls	gobject-introspection	gpgme	gpg-pubkey
gpg-pubkey	gpm-libs	graphite2	grep
groff-base	grub2-common	grub2-efi-x64	grub2-tools
grub2-tools-extra	grub2-tools-minimal	grubby	gtk2
gtk-update-icon-cache	gzip		

H

hardlink	harfbuzz	hdparm	hicolor-icon-theme
hostname	hwdata		

I

ima-evm-utils	info	initscripts	insights-client
iproute	iprutils	ipset	ipset-libs
iptables	iptables-ebtables	iptables-libs	iputils
irqbalance	iwl1000-firmware	iwl100-firmware	iwl105-firmware
iwl135-firmware	iwl2000-firmware	iwl2030-firmware	iwl3160-firmware
iwl5000-firmware	iwl5150-firmware	iwl6000-firmware	iwl6000g2a-firmware
iwl6050-firmware	iwl7260-firmware		

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	json-c
json-glib			

K

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

L

langpacks-en	less	libacl	libaio
libarchive	libassuan	libatasmart	libattr
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	libdhash
libdnf	libdrm	libedit	libestr
libevent	libfastjson	libfdisk	libffi
libfontenc	libgcab1	libgcc	libgcrypt
libgomp	libgpg-error	libgudev	libgusb
libibverbs	libidn2	libini_config	libjpeg-turbo
libkcapi	libkcapi-hmaccalc	libksba	libldb
libmetalink	libmnl	libmodulemd	libmount
libmspack	libndp	libnetfilter_conntrack	libnfnetlink
libnfsidmap	libnftnl	libnghttp2	libnl3
libnl3-cli	libnsl2	libpath_utils	libpcap
libpciaccess	libpipeline	libpkgconf	libpng
libpsl	libpwquality	libref_array	librepo
libreport-filesystem	librhsm	libseccomp	libsecret
libselinux	libselinux-utils	libsemanage	libsepol
libsigsegv	libsmartcols	libsmbios	libsolv

Table continues…

libss	libssh	libssh-config	libsss_autofs
libsss_certmap	libsss_idmap	libsss_nss_idmap	libsss_sudo
libstdc++	libsysfs	libtalloc	libtasn1
libtdb	libteam	libtevent	libthai
libtiff	libtirpc	libtool-ltdl	libudisks2
libunistring	libusbx	libuser	libutempter
libuuid	libverto	libX11	libX11-common
libXau	libxcb	libXcomposite	libxcrypt
libXcursor	libXdamage	libXext	libXfixes
libXft	libXi	libXinerama	libxkbcommon
libxml2	libxmlb	libXrandr	libXrender
libxslt	libXtst	libyaml	libzstd
linux-firmware	lksctp-tools	lmdb-libs	logrotate
lshw	lsscsi	lua	lua-libs
lvm2	lvm2-libs	lz4-libs	lzo

M

man-db	mdadm	memstrack	microcode_ctl
mokutil	mozjs60	mpfr	

N

ncurses	ncurses-base	ncurses-libs	nettle
NetworkManager	NetworkManager-libnm	NetworkManager-team	NetworkManager-tui
newt	nftables	npth	nspr
nss	nss-softokn	nss-softokn-freebl	nss-sysinit
nss-util	numactl-libs		

O

openldap	openssh	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	pigz	pinentry
pixman	pkgconf	pkgconf-m4	pkgconf-pkg-config

Table continues…

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
prefixdevname	procps-ng	psmisc	publicsuffix-list-dafsa
python3-audit	python3-chardet	python3-cloud-what	python3-dateutil
python3-dbus	python3-decorator	python3-dnf	python3-dnf-plugins-core
python3-ethtool	python3-firewall	python3-gobject-base	python3-gpg
python3-hawkey	python3-idna	python3-iniparse	python3-inotify
python3-libcomps	python3-libdnf	python3-librepo	python3-libs
python3-libselinux	python3-libsemanage	python3-linux-procfs	python3-magic
python3-nftables	python3-perf	python3-pip-wheel	python3-policycoreutils
python3-pysocks	python3-pyudev	python3-pyyaml	python3-requests
python3-rpm	python3-setools	python3-setuptools-wheel	python3-six
python3-slip	python3-slip-dbus	python3-subscription-manager-rhsm	python3-syspurpose
python3-systemd	python3-unbound	python3-urllib3	

R

readline	redhat-release	redhat-release-eula	rhc
rootfiles	rpm	rpm-build-libs	rpm-libs
rpm-plugin-selinux	rpm-plugin-systemd-inhibit	rsyslog	

S

sed	selinux-policy	selinux-policy-targeted	setup
sg3_utils	sg3_utils-libs	shadow-utils	shared-mime-info
shim-x64	slang	snappy	sqlite-libs
squashfs-tools	sssd-client	sssd-common	sssd-kcm
sssd-nfs-idmap	subscription-manager	subscription-manager-rhsm-certificates	sudo
systemd	systemd-libs	systemd-pam	systemd-udev

T

tar	teamd	tpm2-tss	trousers
trousers-lib	ttmkfdir	tuned	tzdata
tzdata-java			

U

udisks2	unbound-libs	usermode	util-linux

V

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

W

wget	which		

X

xfsprogs	xkeyboard-config	xmlsec1	xmlsec1-openssl
xorg-x11-fonts-Type1	xorg-x11-font-utils	xz	xz-libs

Y

yum			

Z

zlib			

Appendix C: List of Application-Based RPMs Provided by System Manager

The following is a list of Application-Based RPMs for Avaya Aura® System Manager Software-Only environment:

A

avaya-os-tools	avaya-smgr-awtun	account-sync-rpm	

C

cs1000-csoneksvrmgr	collaboration-environment	cs1000-dmWeb	cs1000-ipsec
cs1000-patchWe	cs1000-sysmgr-numgrp		

E

easg	ep-account-registry-rpm	ep-account-rpm	ep-callpilot-registry-rpm
ep-callpilot-rpm	ep-cs1k-rpm		

I

iptcm-khoj			

M

MGMTREPORTS			

N

net-snmp	nortel-redhat8-cnd		

P

password-sync-rpm	postgresql13	postgresql13-contrib	postgresql13-libs
postgresql13-server			

S

smem	SMGR-Dependencies smgr_pam	sdm-api-installer	

U

upm-cndsync-rpm			

Appendix D: 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 E: 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.

   For more information about the required CPU, see footprint profile on page 20.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.

   For more information about the required resources, see footprint profile on page 20.
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.

   System Manager requires additional disks. For more information, see footprint profile on page 20.
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.

       For information on disk partitions and size, see Disk Partitioning on page 39.
    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

W