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

Release 10.2.x
Issue 9
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® Session 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 Session 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 Avaya Aura® application *ISO image*, ensure that you have the following knowledge, skills, and tools.

### Knowledge

- Linux® Operating System
- Avaya Aura® Session 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*.

# Change history

| Issue | Date | Summary of changes |
|---|---|---|
| 9 | March 2026 | Added the section:<br>Changes to platform support on page 7 |
| 8 | August 2025 | Updated the following section:<br>• Unsupported features of Avaya Aura application on Infrastructure as a Service on page 14 |
| 7 | June 2025 | Updated the following section:<br>• Licensing requirements on page 25 |
| 6 | April 2025 | Updated the following section:<br>• Unsupported features of Avaya Aura application on Infrastructure as a Service on page 14 |
| 5 | January 2025 | Updated the following sections:<br>• Supported footprints for Avaya Aura Session Manager on Microsoft Azure on page 19<br>• Appendix A:- List of required RPMs on RHEL 8.4 on page 85<br>• Appendix B:- List of required RPMs on RHEL 8.10 on page 98 |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 4 | December 2024 | Added the following sections for R10.2.1:<br>• Appendix B:- List of required RPMs on RHEL 8.10<br>• Appendix D:- Creating RHEL virtual machine on Nutanix<br>Updated the following sections for R10.2.1:<br>• Third-party software requirements<br>• Supported Red Hat Enterprise Linux operating system versions for Software-only Environment<br>• Site preparation checklist<br>• Creating RHEL instance on Microsoft Azure<br>• Installing Linux for software-only installations<br>• Deploying Avaya Aura® Session Manager or Branch Session Manager in a software-only environment<br>• Troubleshooting installer check<br>• Adding a software-only platform<br>• Session Manager Disk partitioning<br>• Branch Session Manager Disk partitioning<br>• Software-only environment overview- Supported platforms |
| 3 | May 2024 | Updated the following sections:<br>• Software-only environment overview on page 10<br>• Creating RHEL instance on Amazon Web Services on page 27<br>• Creating RHEL instance on Microsoft Azure on page 32<br>• Creating RHEL instance on Google Cloud Platform on page 37 |
| 2 | April 2024 | Updated the following sections:<br>Deploying Avaya Aura Session Manager or Branch Session Manager in a software-only environment on page 49<br>Deploying Avaya Aura Software-Only ISO image using Solution Deployment Manager on page 59 |
| 1 | December 2023 | Release 10.2 |

# 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.

**Note:**

Branch Session Manager is not supported on Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

# 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.

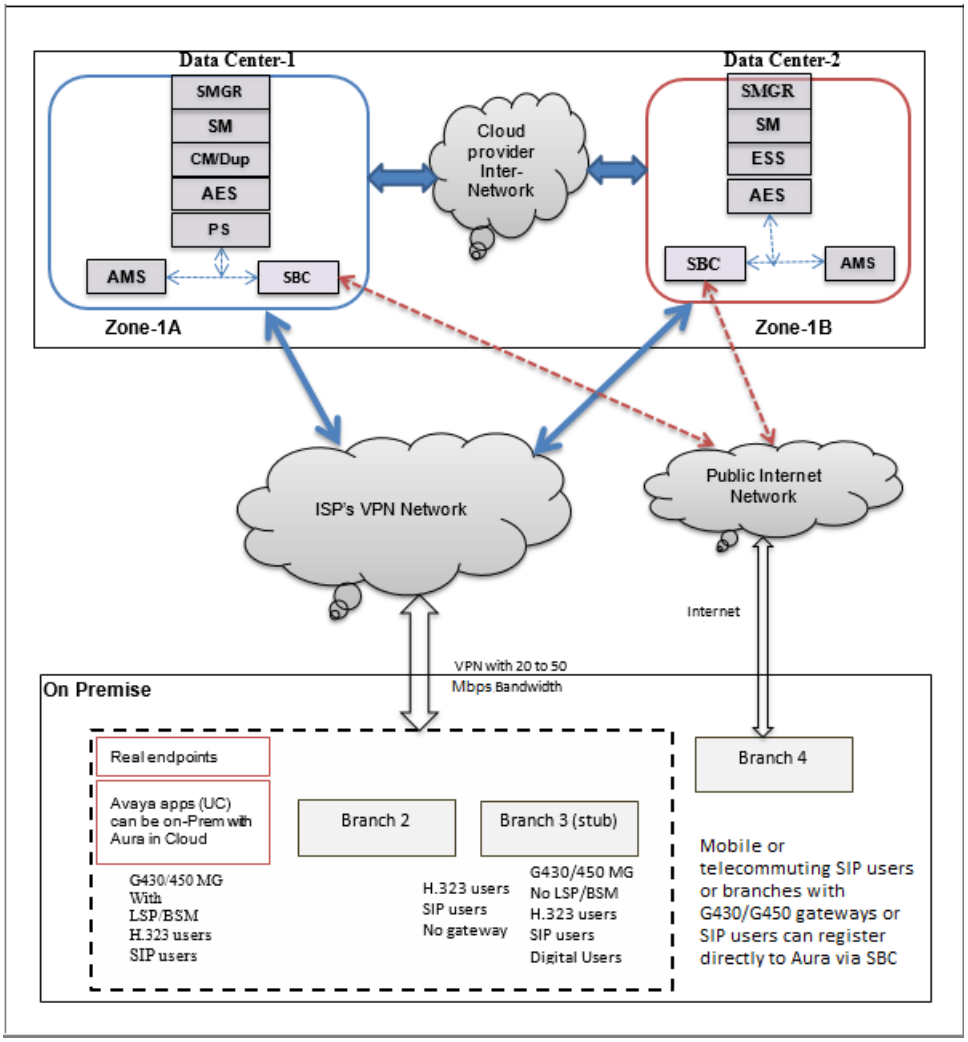
For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

## 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.




# 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”.<br>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”. |

## 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.

## 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 15.

### Amazon Web Services

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes

### Microsoft Azure

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes

### Google Cloud Platform

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes

## Out of Band Management Support Matrix for Avaya Aura® Components

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

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

*Table continues…*

| Product | On-Premise (OVA) | IAAS (SW-Only) | Support OOBM |
|---|---|---|---|
| Avaya Aura® Device Services | No | No | Needs to be on Voice Network and needs VPC Peering in GCP with Voice Network. |

# Chapter 3: Planning and preconfiguration

## 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.<br>**Note:**<br>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:**<br>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 24 | |
| 5 | Register for PLDS and activate license entitlements. | Downloading software from PLDS on page 24 | |
| 6 | Prepare the site. | Site preparation checklist on page 25 | |

## Planning for deploying Software-Only ISO on Amazon Web Services

### Planning checklist

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

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1. | Purchase the required licenses.<br>Register for PLDS and perform the following:<br>• Obtain the license file.<br>• 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 24. | |
| 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. | |

# Supported footprints of Session Manager ISO on Amazon Web Services

**Note:**

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 | AWS instance type | HDD (GiB) | NICs |
|---|---|---|---|
| Profile 1 | • c5.xlarge or higher<br>• c5a.xlarge or higher | 100 | 2 |
| Profile 2 | • c5.2xlarge or higher<br>• c5a.2xlarge or higher | 100 | 2 |
| Profile 3 | • c5.2xlarge or higher<br>• c5a.2xlarge or higher | 135 | 2 |
| Profile 4 | • c5.4xlarge or higher<br>• c5a.4xlarge or higher | 135 | 2 |
| Profile 5 | • c5a.8xlarge or higher | 210 | 2 |
| Profile 6 | • c5.18xlarge or higher<br>• c5a.16xlarge or higher | 210 | 2 |

# Planning for deploying ISO on Microsoft Azure

## Planning checklist

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

| No. | Task | Link/Notes | ✔ |
|---|---|---|---|
| 1. | Purchase the required licenses. Register for PLDS and perform the following<br>• Obtain the license file.<br>• Activate license entitlements in PLDS. | Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/. | |
| 2. | Download the required Avaya Aura® application ISO. | See Downloading software from PLDS on page 24. | |

## Supported footprints for Avaya Aura® Session Manager on Microsoft Azure

| Footprint | Azure instance type | HDD (GiB) | NICs |
|---|---|---|---|
| Profile 1 | Standard B4ms | 100 | 2 |
| Profile 2 | Standard B8ms | 100 | 2 |
| Profile 3 | Standard B8ms | 135 | 2 |
| Profile 4 | Standard B20ms | 135 | 2 |
| Profile 5 | Standard B20ms | 210 | 2 |
| Profile 6 | Standard D64as_v4 | 210 | 2 |

**Note:**

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

# Planning for deploying ISO on Google Cloud Platform

## Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application on Google Cloud Platform:

| No. | Task | Link/Notes | ✔ |
|---|---|---|---|
| 1. | Purchase the required licenses. Register for PLDS and perform the following<br>• Obtain the license file.<br>• Activate license entitlements in PLDS. | Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/. | |
| 2. | Download the required Avaya Aura® application ISO. | See Downloading software from PLDS on page 24. | |

## Supported footprints for Avaya Aura® Session Manager on Google Cloud Platform

| Profile | GCP instance type | HDD (GiB) | NICs |
|---|---|---|---|
| Profile 1 | e2-standard-4 (4 vCPU, 16 GiB memory) | 100 | 2 |
| Profile 2 | e2-standard-8 (8 vCPU, 32 GiB memory) | 100 | 2 |
| Profile 3 | e2-standard-8 (8 vCPU, 32 GiB memory) | 135 | 2 |
| Profile 4 | e2-standard-16 (16 vCPU, 64 GiB memory) | 135 | 2 |
| Profile 5 | e2-standard-32 (32 vCPU, 128 GiB memory) | 210 | 2 |
| Profile 6 | n2-standard-64 (64 vCPU, 256 GiB memory) | 210 | 2 |

**Note:**

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

# Supported footprints of Software-Only ISO image for on-premise

## Supported footprints for Session Manager

The following table summarizes single Session Manager capacities for all Session Manager footprints:

**Note:**

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

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

| Session Manager Device Footprints | Up to 2K Devices | 2K to 4.5K Devices | 4.5K to 7K Devices | 7K to 10K Devices (R1 footprint) | 10K to 23.3K Devices (R2 footprint) | 23.3K to 66.7K Devices |
|---|---|---|---|---|---|---|
| CPU Minimum | 2200MHz | | | | | |
| vCPUs | 3 | 5 | 8 | 12 | 20 | 53 |
| CPU MHz Reservation | 3300 | 5500 | 8800 | 13200 | 22000 | 58300 |
| Memory Reservation | 5132 MiB | 7828 MiB | 10552 MiB | 13368 MiB | 24370 MiB | 74064 MiB |
| SIP Devices[1] (Normal/ Failure)[2] | 2K/2.4K | 4.5K/5K | 7K/8K | 10K/12K | 23.3K/ 25K | 66.7K/72K |
| CC Agents (Normal/Failure) | 1.6K/2K | 3.75K/4166 | 5.8K/6666 | 8333/10K | 18K/21K | 21.6K/25.2K |
| Presence Users (Normal/Failure) | 2K/2.4K | 4.5K/5K | 7K/8K | 10K/12K | 18K/21K | 21.6K/25.2K |
| Sessions (Sec/ Hour/Max) | 20/72K/ 17.9K | 45/162K/ 37.4K | 70/256K/ 59.8K | 100/360K/90 K | 150/540K/ 170K | 180/648K/ 510K |
| HDD for Software-Only ISO (GiB)[3] | 100 | 100 | 135 | 135 | 210 | 210 |

**Note:**

1. SIP devices: It includes all hard endpoints, soft clients, AST/Non-AST SIP endpoints and third-party endpoints.
2. Normal/Failure: Normal refers to capacity of the Session Manager in Sunny Day scenario and Failure refers to capacity of the Session Manager in Rainy Day scenario. A Session Manager in a rainy day scenario can have more number of users registered as it has registrations from the users whose primary Session Manager is down.
3. You can deploy the Session Manager software-only *ISO image* on VMware, KVM, Hyper-V, Amazon Web Services, Google Cloud Platform, and Microsoft Azure platforms.

## Supported footprints of Branch Session Manager on VMware

The following table summarizes single Branch Session Manager capacities for all Branch Session Manager footprints.

**Note:**

Avaya Aura® Session 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 = $1000^3$.

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

| Branch Session Manager Device Footprints | Up to 1K Devices | 1k to 5K Devices |
|---|---|---|
| CPU Minimum | 2200 MHz | |
| vCPUs | 2 | 4 |
| CPU MHz Reservation | 2200 | 4400 |
| Memory Reservation | 3164 MiB | 4952 MiB |
| CC Agents Max | 583 | 4167 |
| Sessions (Sec/Hour/Max) | 3/10.8K/4.8K | 30/108K/35K |
| HDD (GiB) | 50 | 50 |

# 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 (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site 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 need to download and install any updates or patches.

**Important:**

The customer is responsible for updates to the virtual environment and the operating system. Avaya is only responsible for Avaya Aura® application updates in the software-only deployment. You must refer to the appropriate PSN for Avaya approved software-only updates.

# Software details of Session Manager and Branch Session Manager

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

# 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 by using the operating system command line interface or by using Solution Deployment Manager.

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

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

| Red Hat Enterprise Linux operating system | Avaya Aura® Release | | |
|---|---|---|---|
| | 8.1.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<br>**Note:**<br>Session Manager Release 8.1.1 and later support the Red Hat Enterprise Linux operating system Release 7.6 through 7.9 with 64-bit. | | |
| Linux operating system Release 8.4 with 64-bit | | Y | Y |
| Linux operating system Release 8.10 with 64 bit | | | Y |

# 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.

# 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 30 | |

# Configuration tools and utilities

To deploy Avaya Aura® ISO for the software-only environment and to configure the application, you need the following tools and utilities:

- PuTTY and WinSCP
- SDM Client (Optional)

# Licensing requirements

For licensing, Branch Session Manager and core Session Manager require:

- Product Licensing and Delivery System (PLDS) for license entitlement management, license activation, and license file delivery.
- Web License Manager (WebLM). Use WebLM that is embedded in System Manager.

You can download the license file from PLDS and install the license. Avaya or an authorized Business Partner can also download and install the license file.

Software licenses for upgrades to major releases of Session Manager are chargeable. Software licenses for upgrades to the next minor upgrade release are not chargeable.

The Session Manager license file contains the total number of authorized Session Manager licenses available for the enterprise. With Session Manager you can monitor the Session Manager licenses used in the system, based on the instance counts. Session Manager raises an alarm when the number of licenses used exceeds the number of authorized Session Manager licenses available for the system. The system does not block the calls or disable the feature. You can:

- Purchase additional Session Manager licenses from Avaya.
- Analyze the Session Manager license usage and reschedule the planned usage of the system.

**Note:**

Licensing provides a 30–day grace period for all license errors, including no license file present on initial installation, before applying any license enforcement.

### Backward compatibility and upgrade for licensing

The types of licensing are:

- Session Manager connection licensing. This licensing is deprecated from Release 7.0 onwards.
- Session Manager instance licensing. This licensing is introduced in Release 7.0 onwards.

For Licensing, the recommended upgrade order is:

1. Upgrade System Manager to the Release 10.2.
2. Install Session Manager 10.2 license file on System Manager Release 10.2.
3. Upgrade Session Manager to Release 10.2.

## Installing the license file

### Procedure

1. On the home page of the System Manager web console, click **Services** > **Licenses**.
2. In the navigation pane, click **Install license**.
3. Click **Browse** to specify the location of the Session Manager license file on your computer.
4. Click **Accept the License Terms & Conditions**.
5. Click **Install**.

   The System Manager web console displays Session Manager in the **Licensed products** section.

# Pre-deployment configuration in Infrastructure as a Service

## Preconfiguration for deploying ISO on Amazon Web Services

### Predeployment checklist for Amazon Web Services

Perform the following tasks to deploy Avaya Aura® application ISO on Amazon Web Services.

| Task | Link/Notes | ✔ |
|---|---|---|
| Create a virtual machine. | See Creating RHEL instance on Amazon Web Services on page 27. | |
| Assign the required resources to the virtual machine. | See Session Manager Disk partitioning on page 46. | |
| Prepare Session Manager for cloud deployment. | See Preparing Session Manager for deployment on Cloud on page 29. | |
| Copy the ISO to the virtual machine. | See Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services on page 30. | |
| Configure Yum. | See Configuring Yum on RHEL on page 30. | |
| Validate the installer. | See Validating the installer ISO file on page 31. | |
| Deploy Avaya Aura® application. | See Deploying Avaya Aura application ISO on Infrastructure as a Service on page 42. | |

### 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.
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. In the Network interfaces section, do the following:
    a. Assign an IP address for the first interface eth0.
    b. Click **Add Device** to add a new interface eth1.

**Note:**

IP address needs to be assigned only for the first interface (eth0), not for the second one (eth1).

12. Click **Configure storage**.
13. On the Configure Storage page, do the following:
    a. Add partitions according to the profiles.
    b. Select **Delete on Termination** check box for all the profiles.

    **Note:**

    The previous step ensures the disks are removed from the storage array when the VM is deleted.
14. Review the details of each configuration in the **Summary** panel.
15. Click **Launch Instances**.

    The system creates the RHEL instance.
16. 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`.

## Preparing Session Manager for deployment on Cloud

### About this task

Cloud-provided Red Hat instances typically require additional configuration before installing Session Manager Software-only ISO. For example, cloud provided instances often are deployed with DHCP enabled. Session Manager currently does not support DHCP so the OS needs to be configured before running the installer. This procedure covers the required changes to cloud-provided instances.

**Important:**

If net-snmp RPMs are installed before deploying the Session Manager Software Only ISO, remove net-snmp RPMs. If you do not remove net-snmp RPMs, the Session Manager Software Only ISO cannot install the Avaya custom net-snmp rpm and alarming does not work.

### Procedure

1. Log in to the system as a root user.
2. Run the following command to remove the packages that conflict with Session Manager:

   ```
   yum erase cloud-init google-compute-engine net-snmp-libs net-snmp-utils
   ```
3. To disable DHCP, do the following:
   a. Get the currently assigned network information with the command:

      ```
      nmcli device show eth0
      ```
   b. From the CLI, note the IP4.ADDRESS, IP4.GATEWAY, and IP4.DNS values.
   c. Run the following command to access the NetworkManager TUI page:

```
nmtui
```

If the command is not available, use yum to install the NetworkManager-tui package.

d. On the NetworkManager TUI page, select **Edit a connection**.

e. Select **System eth0** from the **Ethernet** list and click **Edit**.

The entry for eth0 might be called *Wired connection 1* on some platforms.

f. On the Edit Connection page, click **Show** against the **IPv4 CONFIGURATION**.

g. From the **IPv4 CONFIGURATION** list, select **Manual**.

h. Enter the IP information collected in step 3.b.

i. Select **OK** and then **Back**.

j. On the NetworkManager TUI page, select **Set system hostname**.

k. On the Set Hostname screen, enter the hostname and select **OK**.

l. Reboot Session Manager.

## 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
   ```

## Validating the installer ISO file

### About this task

Use this procedure to validate the Session Manager installer ISO, which is signed using Avaya File Signing Authority (AFSA). For a software-only installation, you must validate the ISO manually. You can also validate ISO by checking the checksum on the image and by comparing the values provided on PLDS.

### Before you begin

Download the Avaya Product Root CA, for example, `AvayaRootCert.pem`, and add Root CA to the Session Manager trusted list. To create the file `AvayaRootCert.pem`, use the file present in the “Appendix B Avaya root certificate” section of this document.

For more information on adding Root CA to the Session Manager trusted list, see *Administering Avaya Aura® Session Manager*.

### Procedure

1. Run the following command to mount the installer ISO:

   ```
   mount -o loop,ro Session_Manager_10.2.0.0.*.iso /mnt
   ```

2. Run the following command to validate the certificate file by using the root CA:

   ```
   openssl verify -CAfile <directory_name>/AvayaRootCert.pem /mnt/SM-10.2.0.0.*.cert
   ```

3. Run the following command to extract the public key:

   ```
   openssl x509 -in /mnt/SM-10.2.0.0.*.cert -pubkey -noout > /tmp/key
   ```

4. Run the following command to check the signature of the manifest file:

   ```
   openssl dgst -sha256 -verify /tmp/key -signature /mnt/*.cert /mnt/SM-10.2.0.0.*.mf
   ```

   This command must return `Verified OK`.

5. Run the following command to validate manifest files:

   ```
   cd /mnt
   sha256sum -c SM-10.2.0.0.*.mf
   ```

   After you run the command, an output of `OK` indicates that the ISO file is signed and verified.

**Related links**

Avaya root certificate on page 105

## Configuring password authentication for Amazon Web Services

### Procedure

1. Login to Amazon Web Services as a “ec2-user”.
2. Switch to root by using `sudo su`.
3. Edit `/etc/ssh/sshd_config` and set **PasswordAuthentication** to yes.

# Preconfiguration for deploying ISO on Microsoft Azure

## Predeployment checklist for Microsoft Azure

Perform the following tasks to deploy Avaya Aura® application ISO on Microsoft Azure.

| Task | Link/Notes | ✔ |
|---|---|---|
| Create a virtual machine. | See Creating RHEL instance on Microsoft Azure on page 32. | |
| Assign the required resources to the virtual machine. | See Session Manager Disk partitioning on page 46. | |
| Prepare Session Manager for cloud deployment. | See Preparing Session Manager for deployment on Cloud on page 29. | |
| Copy the ISO to the virtual machine. | See Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure on page 35. | |
| Validate the installer. | See Validating the installer ISO file on page 31. | |
| Deploy Avaya Aura® application. | See Deploying Avaya Aura application ISO on Infrastructure as a Service on page 42. | |

## Creating RHEL instance on Microsoft Azure

### Before you begin

Create an account on Microsoft Azure.

**Important:**

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

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the 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.
   e. From **Administrator account**, in **Authentication type**, select **Password**, and enter the required credentials.

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

      **Caution:**

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

9. Change the hard disk size from 32 GiB to 40 GiB and save the configuration.

### Next steps

## Preparing Session Manager for deployment on Cloud

### About this task

Cloud-provided Red Hat instances typically require additional configuration before installing Session Manager Software-only ISO. For example, cloud provided instances often are deployed with DHCP enabled. Session Manager currently does not support DHCP so the OS needs to be configured before running the installer. This procedure covers the required changes to cloud-provided instances.

**Important:**

If net-snmp RPMs are installed before deploying the Session Manager Software Only ISO, remove net-snmp RPMs. If you do not remove net-snmp RPMs, the Session Manager Software Only ISO cannot install the Avaya custom net-snmp rpm and alarming does not work.

### Procedure

1. Log in to the system as a root user.
2. Run the following command to remove the packages that conflict with Session Manager:

   ```
   yum erase cloud-init google-compute-engine net-snmp-libs net-snmp-utils
   ```

3. To disable DHCP, do the following:
   a. Get the currently assigned network information with the command:

      ```
      nmcli device show eth0
      ```

   b. From the CLI, note the IP4.ADDRESS, IP4.GATEWAY, and IP4.DNS values.
   c. Run the following command to access the NetworkManager TUI page:

      ```
      nmtui
      ```

      If the command is not available, use yum to install the NetworkManager-tui package.

   d. On the NetworkManager TUI page, select **Edit a connection**.
   e. Select **System eth0** from the **Ethernet** list and click **Edit**.

The entry for eth0 might be called *Wired connection 1* on some platforms.

f. On the Edit Connection page, click **Show** against the **IPv4 CONFIGURATION**.

g. From the **IPv4 CONFIGURATION** list, select **Manual**.

h. Enter the IP information collected in step 3.b.

i. Select **OK** and then **Back**.

j. On the NetworkManager TUI page, select **Set system hostname**.

k. On the Set Hostname screen, enter the hostname and select **OK**.

l. Reboot Session Manager.

## 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.

## Validating the installer ISO file

### About this task

Use this procedure to validate the Session Manager installer ISO, which is signed using Avaya File Signing Authority (AFSA). For a software-only installation, you must validate the ISO manually. You can also validate ISO by checking the checksum on the image and by comparing the values provided on PLDS.

### Before you begin

Download the Avaya Product Root CA, for example, `AvayaRootCert.pem`, and add Root CA to the Session Manager trusted list. To create the file `AvayaRootCert.pem`, use the file present in the “Appendix B Avaya root certificate” section of this document.

For more information on adding Root CA to the Session Manager trusted list, see *Administering Avaya Aura® Session Manager*.

### Procedure

1. Run the following command to mount the installer ISO:

```
mount -o loop,ro Session_Manager_10.2.0.0.*.iso /mnt
```

2. Run the following command to validate the certificate file by using the root CA:

   ```
   openssl verify -CAfile <directory_name>/AvayaRootCert.pem /mnt/SM-10.2.0.0.*.cert
   ```

3. Run the following command to extract the public key:

   ```
   openssl x509 -in /mnt/SM-10.2.0.0.*.cert -pubkey -noout > /tmp/key
   ```

4. Run the following command to check the signature of the manifest file:

   ```
   openssl dgst -sha256 -verify /tmp/key -signature /mnt/*.cert /mnt/SM-10.2.0.0.*.mf
   ```

   This command must return `Verified OK`.

5. Run the following command to validate manifest files:

   ```
   cd /mnt
   sha256sum -c SM-10.2.0.0.*.mf
   ```

   After you run the command, an output of `OK` indicates that the ISO file is signed and verified.

**Related links**

Avaya root certificate on page 105

# Preconfiguration for deploying ISO on Google Cloud Platform

## Predeployment checklist for Google Cloud Platform

Perform the following tasks to deploy Avaya Aura® application ISO on Google Cloud Platform.

| Task | Link/Notes | ✔ |
|---|---|---|
| Create a PPK file. | See Creating a PPK file on page 37. | |
| Create RHEL virtual machine instance. | See Creating RHEL instance on Google Cloud Platform on page 37. | |
| Assign the required resources to the RHEL virtual machine instance. | See Session Manager Disk partitioning on page 46. | |
| Prepare Session Manager for cloud deployment. | See Preparing Session Manager for deployment on Google Cloud Platform on page 38. | |
| Copy the ISO to the RHEL virtual machine instance. | See Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform on page 39. | |
| Validate the installer. | See Validating the installer ISO file on page 31. | |
| Deploy Avaya Aura® application. | See Deploying Avaya Aura application ISO on Infrastructure as a Service on page 42. | |

# 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**.

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**.

6. Click **Networking** > **Networking interfaces**, and update the following fields:

   a. In **Network**, select the VPC network.

   b. In **Subnetwork**, select an appropriate subnet.

   c. In **Primary Internal IP**, select Ephemeral Custom.

   d. In **Custom ephemeral IP address**, enter an IP address that is within the range of your network.

   e. In **External IP**, select an appropriate option.

7. Click **Done**.

8. Click **Security**.

9. Click **Create**.

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

### Next steps

Uploading the ISO to the RHEL virtual machine instance.

## Preparing Session Manager for deployment on Google Cloud Platform

### About this task

Cloud-provided Red Hat instances require additional configuration before installing Session Manager Software-only ISO. For example, cloud-provided instances often are deployed with DHCP enabled. Session Manager currently does not support DHCP, so the OS must be configured before running the installer. This procedure covers the required changes to cloud-provided instances.

**Important:**

If net-snmp RPMs are installed before deploying the Session Manager Software Only ISO, remove net-snmp RPMs. If you do not remove net-snmp RPMs, the Session Manager Software Only ISO cannot install the Avaya custom net-snmp rpm and alarming does not work.

### Procedure

1. Log in to the system as a root user.

2. Run the following command to remove the packages that conflict with Session Manager:

   ```
   yum erase cloud-init google-compute-engine net-snmp-libs net-snmp-utils
   ```

3. If present, remove eth1 address from `/etc/hosts`.
4. To disable DHCP, do the following:
    a. Get the currently assigned network information with the command:

       ```
       nmcli device show eth0
       ```

    b. From the CLI, make note of the IP4.ADDRESS, IP4.GATEWAY, and IP4.DNS values.
    c. Run the following command to access the NetworkManager TUI page:

       ```
       nmtui
       ```

       If the command is not available, use yum to install the NetworkManager-tui package.
    d. On the NetworkManager TUI page, select **Edit a connection**.
    e. Select **System eth0** from the **Ethernet** list and click **Edit**.

       The entry for eth0 might be called *Wired connection 1* on some platforms.
    f. On the Edit Connection page, click **Show** against the **IPv4 CONFIGURATION**.
    g. From the **IPv4 CONFIGURATION** list, select **Manual**.
    h. Enter the IP information collected in step 4.b.
    i. Select **OK** and then **Back**.
    j. On the NetworkManager TUI page, select **Set system hostname**.
    k. On the Set Hostname screen, enter the hostname and select **OK**.
    l. Use the following command to rename the network interface name from “Wired_connection_1” to “eth0”:

       ```
       mv /etc/sysconfig/network-scripts/ifcfg-
       Wired_connection_1 /etc/sysconfig/network-scripts/ifcfg-eth0
       ```

    m. Reboot Session Manager.

## 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.

## Validating the installer ISO file

### About this task

Use this procedure to validate the Session Manager installer ISO, which is signed using Avaya File Signing Authority (AFSA). For a software-only installation, you must validate the ISO manually. You can also validate ISO by checking the checksum on the image and by comparing the values provided on PLDS.

### Before you begin

Download the Avaya Product Root CA, for example, `AvayaRootCert.pem`, and add Root CA to the Session Manager trusted list. To create the file `AvayaRootCert.pem`, use the file present in the “Appendix B Avaya root certificate” section of this document.

For more information on adding Root CA to the Session Manager trusted list, see *Administering Avaya Aura® Session Manager*.

### Procedure

1. Run the following command to mount the installer ISO:

   ```
   mount -o loop,ro Session_Manager_10.2.0.0.*.iso /mnt
   ```

2. Run the following command to validate the certificate file by using the root CA:

   ```
   openssl verify -CAfile <directory_name>/AvayaRootCert.pem /mnt/SM-10.2.0.0.*.cert
   ```

3. Run the following command to extract the public key:

   ```
   openssl x509 -in /mnt/SM-10.2.0.0.*.cert -pubkey -noout > /tmp/key
   ```

4. Run the following command to check the signature of the manifest file:

   ```
   openssl dgst -sha256 -verify /tmp/key -signature /mnt/*.cert /mnt/SM-10.2.0.0.*.mf
   ```

   This command must return `Verified OK`.

5. Run the following command to validate manifest files:

   ```
   cd /mnt
   sha256sum -c SM-10.2.0.0.*.mf
   ```

   After you run the command, an output of `OK` indicates that the ISO file is signed and verified.

### Related links

Avaya root certificate on page 105

## Adding a swap space for Google Cloud Network

### About this task

By default, Google instances do not have swap space allocated. Session Manager requires swap space from time to time. So, swap space needs to be added before installing the Session Manager ISO.

### Procedure

1. As a root user, run the following command:

   ```
   dd if=/dev/zero of=/swapfile bs=1M count=8192
   ```

2. Run the following command to format the swap space:

   ```
   mkswap /swapfile
   ```

3. Run the following command to turn on the swap:

   ```
   swapon /swapfile
   ```

4. Run the following command to make the change permanent by adding the following command to `/etc/fstab`:

   ```
   /swapfile swap swap defaults 0 0
   ```

# Required RPMs

A complete list of required RPMs is packaged in the `Dependencies.txt` file of the ISO.

To see the list of required RPMs, see List of required RPMs on RHEL 8.4 on page 85

# Users and groups

The following tables list all the users and groups added by the Session Manager installer:

### Users

| User name | Login account | Notes |
|---|---|---|
| CDR_User | Yes | The CDR user.<br>This account is created only if CDR is enabled. |
| wsadmin | No | The WebSphere application user. |
| jboss | No | The JBoss application user. |
| postgres | No | The database application user. |
| asset | No | The Security Module user. |

*Table continues…*

| User name | Login account | Notes |
|---|---|---|
| csadmin | Yes | The user required for SDM access. |
| cassandra | No | The Cassandra application user. |
| spirit | No | The SAL- Agent application user. |
| ncs | No | The Nortel application user. |
| nginx | No | The nginx application user. |
| init | Yes | The Service account (EASG). |
| craft | Yes | The Service account (EASG). |
| sroot | Yes | The Service account (EASG). |

### Groups

| Group | Description |
|---|---|
| susers | Members of this group have the necessary privileges required to operate and maintain the application. |
| CDR_User | This is a group for CDR_User. This account is created only if CDR is enabled. |
| custadmins | This group is for System Administrator roles. |
| custusers | This group is for Auditor roles. |
| avusers | This group is for Avaya Services Maintenance role. |
| avrusers | This group is for Avaya Services Administrator role. |
| sshusers | This group determines which login accounts can access SSH commands. |
| nginx | This group is for nginx application roles. |
| spirit | This group is for AL- Agent application roles. |
| asset | This group is for the Security Module roles. |
| cassandra | This group is for Cassandra application roles. |
| wsuser | This group is for WebSphere application roles. |
| jboss | This group is for JBoss application roles. |
| postgres | This group is for database application roles. |
| csadmin | This group is for roles required to access SDM . |

# Deploying Avaya Aura® application ISO on Infrastructure as a Service

You can deploy the Avaya Aura® application on Infrastructure as a Service by using the following methods:

- Bash CLI

- Avaya SDM client

# Chapter 4: Deploying Session Manager

## Installing Linux for software-only installations

### About this task

Use this procedure to install Linux for software-only installations.

**Important:**

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

**Important:**

Changes to the default kernel boot time parameters can result in an unstable or inoperable behavior of Avaya Aura® application. You must take care when altering the RHEL Kernel boot options. If issues arise with Avaya Aura® application where kernel boot options have been customized, Avaya recommends to restore the kernel options to the defaults to determine if the customization of kernel boot options are the cause of any undesired behavior.

**Important:**

Session Manager supports running with SELinux set to enforcing. SELinux can be enabled prior to installing Session Manager or after installation.

**Warning:**

Additional SELinux rules, besides the default one included by Red Hat, may cause Session Manager not to work properly. Avaya should be consulted prior to adding any additional SELinux rules.

### Before you begin

Create a virtual machine for software-only installation. For creating a virtual machine, see the third-party documentation for the corresponding virtualized environment.

### Procedure

1. Start the virtual machine.
2. Boot your Linux installation media and follow the instructions of the installation utility.
3. Disable the new naming scheme of network interfaces to use eth0 and eth1 network device names:
    a. On the command prompt, select **Install Red Hat Enterprise Linux 8.4 or Red Hat Enterprise Linux 8.10**, and press **E**.

b. On the command line, append `net.ifnames=0` to the existing line and press **Control+X**.

**Note:**

Avaya requires exclusive usage of eth0 and eth1.

4. Select your language and keyboard type.
5. On the SOFTWARE SELECTION page, select **Minimal Install**
6. On the Network & Host Name screen, do the following:
   a. In the **Host Name** field, type the host name and click **Apply**.
   b. In the **Network Connection** field, click **eth0**, and click **Configure**.
   c. On the Editing eth0 page, in the **IPv4 Settings** tab, provide the required IPv4 information, configure DNS settings, and click **Save**.

      **Note:**

      IPv4 is required. You can optionally add IPv6.

   d. Verify that the eth0 is enabled.
7. On the Linux installation Console, do the following:
   a. In the Date & Time section, select the required time zone.
   b. To configure NTP, click the **Settings** icon.
   c. On the Add and mark for usage NTP servers page, clear all the non-working NTP servers.

      **Note:**

      Avaya strongly recommends to configure NTP servers.

   d. To add a new NTP server, click the plus **(+)** sign and then click **OK**.
   e. Click **Done**.
8. On the Linux installation Console, click **Installation Destination**.
9. On the Installation Destination page, in the **Storage Configuration** area, select **Custom**.
10. Select **Click here to create them automatically**.

    For partitioning details, see *Disk Partitioning*.
11. Click **Done**.
12. When prompted, click **Accept Changes**.
13. On the next page, click **Root Password**, and type the root password when prompted.
14. **(Optional)** To create a user do the following steps:
    a. On the Create User page, enter the user name and password for the new user.

b. Select the following check boxes:

- **Make this user administrator**
- **Require a password to use this account**

15. On the Linux installation Console, click **Begin Installation**.
16. After the installation is complete, reboot the virtual machine when prompted.

# Session Manager Disk partitioning

Partitions are strongly recommended; however: a single partition can be used as long as it meets the minimum total disk size for the profile.

Use the following table for the required disk size and minimal sizes for each partition. Any additional partitions or applications will require enough disk space to meet the directory requirements for Session Manager.

**Note:**

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

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

| Partition | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 |
|---|---|---|---|---|---|---|
| /boot | 1 GiB | 1 GiB | 1 GiB | 1 GiB | 1 GiB | 1 GiB |
| /boot/efi[1] | 200 MiB | 200 MiB | 200 MiB | 200 MiB | 200 MiB | 200 MiB |
| / | 15 GiB | 15 GiB | 15 GiB | 15 GiB | 15 GiB | 15 GiB |
| /home | 10 GiB | 10 GiB | 10 GiB | 10 GiB | 10 GiB | 10 GiB |
| /tmp | 10 GiB | 10 GiB | 10 GiB | 10 GiB | 10 GiB | 10 GiB |
| /var[2] | 3 GiB | 3 GiB | 3 GiB | 3 GiB | 3 GiB | 3 GiB |
| /var/log | 22 GiB | 22 GiB | 36 GiB | 36 GiB | 67 GiB | 67 GiB |
| /var/log/audit | 3 GiB | 3 GiB | 4 GiB | 4 GiB | 7 GiB | 7 GiB |
| /data | 30 GiB | 30 GiB | 50 GiB | 50 GiB | 90 GiB | 90 GiB |
| swap | 8 GiB | 8 GiB | 8 GiB | 8 GiB | 8 GiB | 8 GiB |
| Minimal disk size | 100 GiB | 100 GiB | 135 GiB | 135 GiB | 210 GiB | 210 GiB |

**Note:**

1. Only needed if EFI boot is used (recommended).
2. Do not create a separate `/var/lib/pgsql` partition. Creating such a directory leads to Session Manager installation failure.

Regardless of partitioning, the directories in the table below must have a minimum space as given in the table for respective profiles.

| Directory | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 |
|---|---|---|---|---|---|---|
| /opt | 8 GiB | 8 GiB | 8 GiB | 8 GiB | 8 GiB | 8 GiB |
| /data | 12 GiB | 12 GiB | 14 GiB | 14 GiB | 22 GiB | 22 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.

# Branch Session Manager Disk partitioning

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

| Branch Session Manager Device Footprints | Up to 1K Devices | 1K to 5K Devices |
|---|---|---|
| /boot | 1 GiB | 1 GiB |
| /boot/efi[1] | 200 MiB | 200 MiB |
| /[2] | 17 GiB | 17 GiB |
| /var/log | 18 GiB | 22 GiB |
| /data | 12 GiB | 30 GiB |
| swapp | 2 GiB | 2 GiB |
| HDD (GiB) | 50 GiB | 50 GiB |

1. Only needed if EFI boot is used (recommended).
2. Do not create a separate `/var/lib/pgsql` partition. Creating such a directory leads to Branch Session Manager installation failure.

**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.

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

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

# Validating the installer ISO file

## About this task

Use this procedure to validate the Session Manager installer ISO, which is signed using Avaya File Signing Authority (AFSA). For a software-only installation, you must validate the ISO manually. You can also validate ISO by checking the checksum on the image and by comparing the values provided on PLDS.

## Before you begin

Download the Avaya Product Root CA, for example, `AvayaRootCert.pem`, and add Root CA to the Session Manager trusted list. To create the file `AvayaRootCert.pem`, use the file present in the “Appendix B Avaya root certificate” section of this document.

For more information on adding Root CA to the Session Manager trusted list, see *Administering Avaya Aura® Session Manager*.

## Procedure

1. Run the following command to mount the installer ISO:

   ```
   mount -o loop,ro Session_Manager_10.2.0.0.*.iso /mnt
   ```

2. Run the following command to validate the certificate file by using the root CA:

   ```
   openssl verify -CAfile <directory_name>/AvayaRootCert.pem /mnt/SM-10.2.0.0.*.cert
   ```

3. Run the following command to extract the public key:

   ```
   openssl x509 -in /mnt/SM-10.2.0.0.*.cert -pubkey -noout > /tmp/key
   ```

4. Run the following command to check the signature of the manifest file:

   ```
   openssl dgst -sha256 -verify /tmp/key -signature /mnt/*.cert /mnt/SM-10.2.0.0.*.mf
   ```

   This command must return `Verified OK`.

5. Run the following command to validate manifest files:

   ```
   cd /mnt
   sha256sum -c SM-10.2.0.0.*.mf
   ```

   After you run the command, an output of `OK` indicates that the ISO file is signed and verified.

**Related links**

Avaya root certificate on page 105

# Deploying Avaya Aura® Session Manager or Branch Session Manager in a software-only environment

## About this task

**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 a new virtual machine for the software-only installation. For creating a virtual machine, refer to the corresponding third-party documentation.
- Install Linux on the virtual machine.
- Ensure that TMOUT variable is not set to read-only.
- Ensure that yum is configured on the virtual machine. For more information, see Red Hat documentation.
- Deploy System Manager. For more information, see the specific System Manager deploying guide on Avaya Support website.
- Download the application ISO file to the virtual machine.

## Procedure

1. Log in to the system as a root user.
2. Run the following command to mount the ISO file:

   ```
   mount -o loop,ro Session_Manager_10.2.x.x.xxxx.iso /mnt
   ```

3. Run the following command to remove the cloud-init packages:

   ```
   yum erase cloud-init google-compute-engine
   ```

   Some of these packages are installed only on cloud based installations such as AWS.

4. Run the following command to install the required RPMs:

   ```
   yum install /mnt/avaya-sm-setup-10.2.x.x.xxxx-1.noarch.rpm
   ```

   The `avaya-sm-setup` RPM is an empty RPM that lists the required RPMs for Session Manager.

   For the list of tested Avaya Aura® Software-Only RPMs, see Avaya PSN020361u at PSN020361u.

   **Important:**

   The PSN PSN020361u provides details of the latest RPMs tested with Avaya applications. These RPM versions should be used when installing and updating the

operating system. Using the RPM versions that are not tested might result in an operational impact to the Avaya application.

5. Run the following command to start the installation:

   ```
   /mnt/install-SM
   ```

   The installer performs the following checks to verify that the environment is suitable for Session Manager:

   - The version of Red Hat is at least 8.4.
   - The environment is virtual and not baremetal.
   - All the RPM dependencies are installed.
   - The number of processors meets the provided profile. If a profile is not specified, then Profile 1 CPU requirements are used.
   - The amount of memory for the provided profile. If a profile is not specified, then Profile 1 memory requirements are used.
   - The amount of disk space available on the root partition.
   - The amount of disk space available on the `/var/lib` directory. This check is skipped if the operating system is configured with only one partition.
   - All users can read the `/opt` directory (755 permissions).
   - Root user is being used to run the installer.
   - IPv6 is enabled in the kernel.
   - No other Avaya applications are installed.
   - Remote syslog is running.
   - Minimum 2 network interfaces exist.
   - The network interfaces are named eth0 and eth1.
   - Network interface eth1 configuration does not exist.
   - Identify any port conflicts.
   - The installer can write in the home directory.

   If any check fails, refer to the troubleshooting section.

6. If `net.ifnames=0` is not specified during the Linux installation, enter `Y` to allow the installer to automatically rename the interfaces and repeat Step 2 and Step 5 after reboot.
7. On the End User License Agreement page, click **Accept**.
8. On the System Configuration page, read the warning, and click **Accept**.
9. Click **Continue** to acknowledge system reboot after installation.
10. On the Please select installation type window, select the required installation type.

**Important:**

The installation type must match the profile values used while creating the virtual machine. If the virtual machine is configured with the Session Manager profile, you must select the Core Session Manager. If the virtual machine is configured with the Branch Session Manager profile, you must select the Branch Session Manager as a required installation type.

11. Enter the IP address of the primary System Manager and click **OK**.
12. In the **Enrollment password** field, type the enrollment password.
13. In the **Confirm Password** field, re-enter the enrollment password and click **OK**.
14. On the Enhanced Access Security Gateway (EASG) page, read the EASG information, and click **OK**.
15. Select one of the following and then click **OK**:
    - **Enable EASG (Recommended)**
    - **Disable EASG**
16. In the **Enter Login ID to use for the customer account** field, type a new username to use as a customer account, and click **OK**.
17. In the **Enter password** field, type the customer account password.
18. In the **Confirm Password** field, re-enter the customer account password and click **OK**.
19. On the Verify Settings page, confirm all the settings and click **Continue**.

    After the installation is completed, reboot the virtual machine.

**Note:**

Session Manager supports running with FIPS enabled. FIPS should be enabled after installing Session Manager. Session Manager provides **`fips_mode.sh`** for enabling FIPS. To enable FIPS, run:

```
fips_mode.sh enable
```

# Troubleshooting installer check

The Session Manager installer performs the following checks to verify if the environment is suitable for Session Manager software-only deployment. Use the following table if any of the test fails:

**Note:**

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

| No. | Installer checks | Solution |
|---|---|---|
| 1 | Checking for RHEL version | Session Manager requires at least version 8.4 of Red Hat Enterprise Linux. Re-install the virtual machine with a supported version of Linux. |
| 2 | Checking virtualization environment | Session Manager supports deployment in a virtualized environment. Session Manager does not support deployment on baremetal. Use a virtual machine to install Session Manager. |
| 3 | Checking RPM dependencies | Failure of this test indicates that the RPMs currently installed does not meet Session Manager requirements. |
| 4 | Checking number of processors | If a profile is passed to the installer, the installer checks the number of CPUs versus the required amount by the profile. If no profile is supplied, the installer uses Session Manager Profile 1 (3 CPUs). Ensure that the number of CPUs assigned to the virtual machine meets the desired profile. |
| 5 | Checking memory | If a profile is passed to the installer, the installer checks the amount of memory versus the required amount by the profile. If no profile is supplied, the installer uses Session Manager Profile 1 (5132 MB). Ensure that the amount of memory assigned to the virtual machine meets the desired profile. |
| 6 | Checking available disk space on root partition | Session Manager requires at least 8 GiB of free disk space on the root partition for the installer to run. Clear some space and re-run the installer. |
| 7 | Checking available disk space on `/var/lib` directory (if applicable) | Session Manager needs at least 12 GiB of free disk space in `/var/lib` for profiles 1 & 2, 15 GiB for profiles 3 & 4, and 22 GiB for profiles 5 & 6. Clear or add some space under `/var/lib` and re-run the installer. |
| 8 | Checking user permissions | You must run the installer as a root user. Re-run the installer as a root user. |
| 9 | Checking IPv6 | Session Manager requires IPv6 be enabled even if IPv6 is not used. Make sure that kernel option `ipv6.disable=1` is not present and re-run the installer. |
| 10 | Checking installed Avaya applications | Do not install other Avaya applications on the virtual machine created for deploying Session Manager. |

*Table continues…*

| No. | Installer checks | Solution |
|---|---|---|
| 11 | Checking rsyslog status | Enable Syslog service to generate installation logs. Start rsyslog prior to running the installer (**`systemctl start rsyslog`**). |
| 12 | Checking network interfaces | Session Manager requires two network interfaces:<br>• Out of Band Management<br>• Public (SIP/HTTP)<br>Reconfigure the virtual machine for two network interfaces. |
| 13 | Checking network naming | Session Manager requires the network interface names as eth0 and eth1. If this test fails, allow the installer to rename the network interfaces. |
| 14 | Checking eth1 configuration | Session Manager takes control of eth1 interface for the SIP networks and overwrites any existing configuration. This is a warning only. If the install continues, then Session Manager overwrites the existing eth1 configuration. |
| 15 | Checking Listening ports | Resolve any port conflicts re-run the installer. Refer the port matrix document for the ports necessary for Session Manager's correct operation. |
| 16 | Checking `/home` directory access | The Session Manager installer creates several new users. Many of these users require a home directory. If the `/home` directory is not accessible (for example, configured with autofs) then the installer will not be able to create the users. If `/home` is not available for new users, then update `/etc/defaults/useradd` to a writable home directory. |

# Chapter 5: Deploying Session Manager by using Solution Deployment Manager

## Installing the Solution Deployment Manager client

### Prerequisites for installing the Solution Deployment Manager client

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

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

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

   **Tip:**

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

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

   **Note:**

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

   **Tip:**

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

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

**Tip:**

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

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

   **Note:**

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

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

   **Tip:**

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

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

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

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

# Installing the Solution Deployment Manager client on your computer

## About this task

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

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

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

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

**Note:**

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

## Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at https://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Product Support** > **Downloads**, and type the product name as **System Manager**, and Release as **10.2.x**.
3. Click the **Avaya Aura® System Manager Release 10.2.x SDM Client Downloads,10.2.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

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

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

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

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. On the Pre-Installation Summary page, review the information, and click **Next**.

9. On the User Input page, perform the following:
    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
    b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

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

       You can save the artifacts in the specified directory.
    c. In **Data Port No**, select the appropriate data port.

       The default data port is 1527. The data port range is from 1527 through 1627.
    d. In **Application Port No**, select the appropriate application port.

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

       **Note:**

       After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
    e. **(Optional)** Click **Reset All to Default** to reset all values to default.
10. Click **Next**.
11. On the Summary and Validation page, verify the product information and the system requirements.

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

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

## Next steps

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

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

# Adding a location

### About this task

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

### Procedure

1. On the desktop, click the SDM icon (  ), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
4. Click **Save**.

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

# Adding a software-only platform

### About this task

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

### Before you begin

Add a location.

### Procedure

1. On the desktop, click the SDM icon (  ), and then click **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the username of the base operating system.

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

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

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

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

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

# Deploying Avaya Aura® *Software-Only ISO image* using Solution Deployment Manager

### About this task

Use this procedure to deploy the Avaya Aura® application *ISO image* file 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

- Add a location.

  For more information, see “Adding a location using Solution Deployment Manager”.
- Add a platform

  For more information, see “Adding a platform for software-only”.
- Add an Operating System user on RHEL instance.

  For example, you can add a user using the following commands: **`adduser <username>`**, **`passwd <username>`**.
- Set the password for the root user.

  For example, you can set the password using the following command: **`passwd <root>`**

### Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or click the SDM (  ) icon on the desktop.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, click **New**.

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

      The system displays the IP Address and FQDN of the platform in the **Platform IP** and **Platform FQDN** fields.

   Avaya recommends to keep the FQDN value short because when the FQDN of RHEL system on Google Cloud Platform is greater than 45 characters, the HTTPD service of Application Enablement Services fails to start. If the FQDN in the /etc/hosts file becomes more than 45 characters, you must remove the FQDN from the file, restart the system, and then install Application Enablement Services.
6. In the Provide admin and root Credentials section, do the following:
   a. In **Admin User of OS**, type the admin user name.
   b. In **Admin Password of OS**, type the admin user password.
   c. In **Root User of OS**, type the root user name.
   d. In **Root Password of OS**, type the root user password.
   e. **(Optional)** Click **Test Connection**.

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

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

- **URL**: Click URL and provide the path to the *ISO image*.

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

If the application *ISO image* supports the patch deployment, the system enables the **Service or Feature Pack** tab.

9. **(Optional)** To install the patch file for the application, click Service or Feature Pack, and enter the appropriate parameters.
   a. Click **URL**, and provide the absolute path to the latest service or feature pack.
   b. Click **SW Library** / **Select from software library**, and select the latest service or feature pack.
   c. Click **Browse**, and select the latest service or feature pack.

   You can install the Avaya Aura® application Release 10.2 bin file now or after completing the Avaya Aura® application deployment.

   If you do not provide the Avaya Aura® application Release 10.2 bin file at the time of deploying the Avaya Aura® application, the system displays the following message:

   ```
   Installation of the latest <application> patch is mandatory. Are you sure you want to skip the patch installation? If Yes, ensure to manually install the <application> patch later.
   ```

10. In **Flexi Footprint**, select the footprint size for the application.
11. In Test Your Operating System Compatibility Against Element Software Package, click **Test Environment Compatibility**.

    The installer checks if the platform has all the dependent rpms, network, cpu, memory, and hard disk configuration as specified for the element. This process takes about 4-5 minutes. After the process starts, you cannot proceed further until the process is complete. If you get any error or warning, make the necessary changes before the next steps.

    **Note:**

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

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

    The system displays the Environment Check Output window.

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

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

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

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

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

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

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

# Chapter 6: Configuration

## Allocating dedicated hosts

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Instances** > **Dedicated Hosts**.
3. Click **Allocate a Host**.

   The system displays the Allocate Dedicated Host page.
4. In the **Instance type** field, select **c5.xlarge** or **c5a.xlarge** instance.
5. In the **Availability Zone** field, select the appropriate zone.
6. In the **Quantity** field, type `2`.
7. Click **Allocate host**.

## 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).

# Chapter 7: Post-installation verification

## Post-deployment checklist

Do the following to verify that the Avaya Aura® Session Manager ISO is deployed successfully in the software-only environment:

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Verify the connections of the deployed Session Manager. | See Verifying the connections on page 64. | |
| 2 | Run the maintenance tests on the deployed Session Manager. | See Running maintenance tests on page 65. | |
| 3 | Verify data replication. | See Verifying data replication on page 65 | |
| 4 | Generate a test alarm. | See Generating a test alarm on page 66 | |

## Verifying the connections

### About this task

Verify the connections of the deployed Session Manager.

### Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.
2. Verify **Security Module state** is **Up** for Session Manager.
3. Verify the Service State of the Session Manager instance is **Accept New Service**. If the service state is not **Accept New Service**:
   a. Select the Session Manager instance.
   b. Click **Service State** > **Accept New Service**.

# Running maintenance tests

### About this task

Use this procedure to run maintenance tests on System Manager or any configured Session Manager or Branch Session Manager.

### Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager**, a Session Manager instance, or a Branch Session Manager instance.
3. Do one of the following:
   - To run all the tests, select **Execute All Tests**.
   - To run specific tests, select the tests you want to run, and click **Execute Selected Tests**.
4. Verify that the tests pass.

# Verifying data replication

### Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. Select the appropriate **Replica Group** field and click **View Replica Nodes**.
3. Confirm that the selected **Replica Group Host Name** is synchronized.

   The synchronized replica group host name is indicated in green.
4. If the selected **Replica Group Host Name** is not synchronized:
   a. Select the appropriate **Replica Group Host Name**.
   b. Click **Repair**.

# Troubleshooting Data Replication

### Procedure

1. On the home page of the System Manager Web console, under **Services**, click **Replication**.
2. If the status for the replica group is not **Synchronized**:
   a. Select the affected replica group.
   b. Click **View Replica Nodes**.

c. Verify that an instance exists in the replica group under **Replica Group Host Name**.
d. Select the appropriate instance under **Replica Group Host Name**.
e. Click **View Details**.
f. Under the Synchronization Statistics section, wait until the **Pending Batches** value is zero. Refresh the page as necessary by clicking **Refresh**.

3. If the **Pending Batches** value does not change to zero:
   a. Click **Done**.
   b. On the **Replica Group** page, click **Repair**.
   c. Click **OK** in the dialog box.
4. Wait until the status of the replica group changes to **Synchronized**. Refresh the page as necessary.

# Generating a test alarm

### About this task

Generate a test alarm to the targets assigned to the serviceability agent. These targets can include:

- A SAL Gateway

  The alarm is forwarded to ADC
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

### Procedure

1. If using the Session Manager CLI:
   a. Login to the Session Manager server.
   b. Run the Session Manager CLI command `generateTestAlarmSM.sh`.
2. If using the **Generate Test Alarm** button on the Serviceability Agents screen:
   a. On the System Manager web console, click **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
   b. Select a hostname from the list and click **Generate Test Alarm**.

3. To verify that the System Manager received the test alarm message, do one of the following:
   a. On the System Manager web console, click **Services** > **Events** > **Alarms**.
   b. Check that the system displays the message **Test alarm for testing only, no recovery action necessary** in the **Description** column.
4. If the serviceability agent is configured with other targets, verify that the other targets also received the test alarm and also verify the clearing of the alarm.

**Note:**

The test alarms are not generated when Session Manager is in Maintenance Mode.

# Chapter 8: Maintenance and administration procedures

## Adding Session Manager or Branch Session Manager as SIP entity

### About this task

Use the following procedure to add a Session Manager or Branch Session Manager instance as a SIP entity. It should be noted that eth1 configuration on Session Manager or Branch Session Manager is reserved for SIP and should not be modified at the OS level.

### Procedure

1. On the home page of the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter the name of the Session Manager or Branch Session Manager instance.
4. In the **IP Address Family** field, click the address types that the SIP entity supports.

   For administering SIP entities by using IPv6 address, ensure that the **Enable IPv6** check box is selected on the Global Settings page. If IPv6 is not enabled, the IPv6 and Both options are not available.

   Depending on the IP Address Family that you select, the system displays:

   - For IPv4 IP address family: **FQDN or IPv4 Address** field.
   - For IPv6 IP address family: **FQDN or IPv6 Address** field.
   - For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields.

     For SIP entities other than Session Manager, if the FQDNs for IPv4 and IPv6 are separate, specify both fields with the corresponding IPv4 and IPv6 FQDNs.

     If one FQDN resolves to IPv4 and IPv6 addresses, fill the **FQDN or IPv4 Address** field. You can leave the **FQDN or IPv6 Address** field blank.

     For Session Manager SIP entities, specify only IP addresses.

   Session Manager supports a mixture of FQDN and IPv6 addresses for SIP entities other than Session Manager.

5. In the **FQDN or IPv4 Address** or **FQDN or IPv6 Address** field, enter the IP address of the Session Manager or Branch Session Manager Security Module.

   This IP address is not the management IP address.

6. In the **Type** field, set the type of Session Manager.
7. In the Listen Ports section, click **Add**.
8. Add the **Listen Ports**, **Protocol**, **Default Domain** entries and select the **Endpoint** check box for each port and protocol on which Session Manager or Branch Session Manager listens for SIP traffic.

   Add failover ports if the SIP entity is a failover group member. For more information about Failover Groups, see *Administering Avaya Aura® Session Manager*.

9. Click **Commit**.

# Accepting new service

### About this task

Use this procedure to change the state of a new service to accept.

**Note:**

Even though Security Module displays the status as Up, the Security Module might take 5 to 10 minutes to begin routing calls.

### Procedure

1. On the home page of the System Manager web console, click **Elements** > **Session Manager** > **Dashboard**.
2. On the Session Manager Dashboard page, select the appropriate Session Manager or Branch Session Manager instance in the **Session Manager Instances** table.
3. In the **Service State** field, click **Accept New Service**.
4. Click **Confirm**.

# Denying new service

### About this task

Use this procedure to change the status of a service to deny new service.

When you change the state of the selected Session Manager to **Deny New Service**, the system denies any new call attempts and service requests. Existing calls remain in effect until the users terminate the calls.

### Procedure

1. On the home page of the System Manager web console, click **Elements** > **Session Manager** > **Dashboard**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager instance in the **Session Manager Instances** table.
3. In the **Service State** field, click **Deny New Service**.
4. Click **Confirm**.

# Session Manager Backup and Restore

Use the native System Manager backup and restore function for the long-term backup and recovery of the entire cluster of Session Manager.

**backupSM** and **backupSM -e** commands create backup files called `Session_Manager_backup.tgz (non-encrypted)` and `Session_Manager_backup.zip (encrypted)` respectively, and stores it in the home directory of the account running the command. For example, if the **cust** user runs the command then Session Manager stores the backup file in `/home/cust`.

**Note:**

When using **encrypt** option, ensure that you make a note of the `passphrase` used during the backup.

**restoreSM** command requires the path to the backup file created during backup.

For more information about Session Manager backup and restore, see *Administering Avaya Aura® Session Manager* on the Avaya support website at https://support.avaya.com.

**Note:**

This procedure only backs up administration data.

## Using CLI to backup and restore Session Manager

### About this task

Use the procedure below to create and restore encrypted or non-encrypted Session Manager backup files using CLI commands.

### Procedure

1. To back up Session Manager from the CLI interface, do one of the following steps:
   a. To create a non-encrypted Session Manager backup, run the following command:

      ```
      # backupSM
      ```

This command creates a backup file called `Session_Manager_backup.tgz` and places it in the home directory of the system.

b. To create an encrypted Session Manager backup, run the following command:

**# backupSM -e**

**Note:**

Make a note of the passphrase used while creating the backup.

This command creates a backup file called `Session_Manager_backup.zip` and places it in the home directory of the system.

2. Run the following command to restore Session Manager:

**# restoreSM <path to backup file>**

**Note:**

- The **restoreSM** command requires the path to the backup file created in the previous step.
- To restore encrypted backup enter the passphrase used during backup.

# Preparing for Software-Only RPM updates

## About this task

Use this procedure as a pre-requisite for updating non-critical RPMs.

## Procedure

1. On the home page of the System Manager web console, click **Elements** > **Session Manager** > **Dashboard**.
2. On the Session Manager Dashboard page, click the required Session Manager instance.
3. Click **Service State** > **Deny New Service**.
4. On the Confirmation page, click **Confirm**.
5. On the Session Manager Dashboard page, wait until the **Active Call Count** is zero and refresh the screen to update the count.
6. Take a snapshot of the virtual machine before making any changes.
7. Log in to the Session Manager command line interface as a root user.
8. Run the following command to stop Session Manager:

```
stop -ac
```

9. Configure yum to point to the Red Hat 8 repository containing updates. For more information, see Red Hat documentation.

# Verifying Active Call Count

### About this task

Use this procedure to verify Active Call Count.

The Active Call Count value indicates the number of active calls on the Session Manager instance. Active calls are calls that were already active before the Session Manager was placed in the denial state. When you change the state to **Deny New Service**, the application does not drop calls that are currently processed.

To prevent any impact on calls that are active, the **Active Call Count** must be zero before proceeding with the Session Manager upgrade. If the administrator decides to continue the upgrade and if the active call count is not zero, the active calls are dropped.

### Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.
2. Wait until the value in **Active Call Count** is zero.
3. Refresh the screen to update the count.

# Viewing the Security Module status

### About this task

Use this procedure to view the security module status.

Possible causes for the security module status to be **Down** include:

- The security module might have recently been reset. A reset can take several minutes to complete.
- The security module might not have received security module configuration information from System Manager.

### Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.
2. If the security module state of Session Manager does not display as **Up**:
    a. Click the status text of the security module for Session Manager to display the Security Module Status page.
    b. Verify that the IP address of Session Manager is correct.
    c. Select the Session Manager instance.
    d. Click **Synchronize**.
    e. If the status remains **Down**, click **Reset**.

**Warning:**

Session Manager cannot process calls while the security module is being reset.

## Troubleshooting Security Module Sanity failure

### Procedure

1. On the System Manager Web Console, select **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
2. Select **Refresh** to display the current status.
3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.
5. If the status is selected as **Down**, reset the security module:
   a. Select the appropriate Session Manager instance from the table.
   b. Click **Reset**.

   **Warning:**

   Session Manager cannot process calls while the system resets the security module.
6. Select **Refresh** to display the current status.

# Configuring custom firewall rules

### About this task

Session Manager allows you to configure additional firewall rules over and above the set of rules that are provided and configured at system startup and dynamically at runtime. Use the procedure listed below, to retain the firewall rules after system restart and upgrade. The custom rules are set after Session Manager's default rules are set, but before the dynamic runtime rules.

### Before you begin

Prior knowledge of linux command line utility for configuring firewall rules, **`nft`**, is required. Session Manager provided utility, **`snfw`** is a wrapper script for **`nft`** that also stores the rules that can be reconfigured on system reboots and upgrades. You can view the help for this feature by running **`snfw --help`**.

**Note:**

Please validate your firewall rule using **`nft`** before using **`snfw`**.

### Procedure

1. To add a rule, use the **`--nft-custom-add`** option.

For example, the following command opens port 12345 for TCP at a priority of 0 on eth0 in the output chain:

```
snfw --nft-custom-add inet filter output oif "eth0" tcp dport 12345 counter accept
```

2. To list all the custom rules that are configured on the system, use the **`--nft-custom-list`** option.

   For example,

   ```
   snfw --nft-custom-list
   ```

3. To remove a rule, use the **`--nft-custom-remove`** option.

   For example, the following command removes the rule added in step 1:

   ```
   snfw --nft-custom-delete inet filter output oif \"eth0\" tcp dport 12345 counter
   accept
   ```

# Viewing the Session Manager entity link connection status

## About this task

Use this procedure to view Session Manager entity link connection status.

**Note:**

Entity Monitoring does not apply to a Branch Session Manager. The monitoring status of a Branch Session Manager is always unknown (---).

An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all the connections are up, then the Entity Link status is **up**. If one or more connections are down but at least one connection is up, the link status is **partially down**. If all the connections are down, the Entity Link status is **down**.

On the Session Manager dashboard page, the number of down links and total links are shown in the **Entity Monitoring** column. The values have the format **# of Down links / # of Total links**.

## Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.
2. Under the **Entity Monitoring** column, red values indicate that at least one entity link is down. Click the red values link to display the Session Manager Entity Link Connection Status page.

   The Session Manager Entity Link Connection Status page displays the details for each link. If a link is down, the page displays a reason code.

3. To view the SIP Entity Link Monitoring Status Summary page, click **Summary View**.

# Viewing the SIP Monitoring Status Summary page

### About this task

Use this procedure to view the status of the entity links for all the administered Session Manager instances.

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all the administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager server and a SIP entity.

### Procedure

On the System Manager web console, click **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**.

# Enhanced Access Security Gateway

Session Manager supports Enhanced Access Security Gateway (EASG), an authentication interface that secures the system administration and logins on the system. EASG provides a secure method for Avaya services personnel to access the Avaya Aura® applications 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.

EASG uses a challenge and response protocol to confirm the validity of a user. This process reduces the opportunity for unauthorized access.

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

## Checking EASG status

### Before you begin

Log in to the application with the customer account.

### Procedure

1. On the command line interface, type `EASGStatus`.
2. Press `Enter`.

   The system displays one of the following:

   - **`EASG is enabled`** — if EASG is enabled.
   - **`EASG is disabled`** — if EASG is disabled.

# Enabling and disabling EASG using CLI

## About this task

Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements and allowing Avaya to resolve product issues in a timely manner. See the Avaya support site for additional information for registering products and establishing remote access and alarming.

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

## Before you begin

Log in to the application with the customer account.

## Procedure

1. On the command line interface, do one of the following:
   - To enable EASG, type `EASGManage --enableEASG`.
   - To disable EASG, type `EASGManage --disableEASG`.

   The system displays the message **`Do you want to continue [yes/no] ?`**
2. Type `yes` or `no`.
3. Press `Enter`.

# Enabling and disabling EASG through System Manager

## About this task

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

## Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.
2. In the navigation pane, click **Dashboard**.
3. Click the **EASG** field.
4. Click one of the following:
   - **Enable EASG**.
   - **Disable EASG**.
5. Click **Confirm**.

# EASGManage

Use **EASGManage** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

### Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--
userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

| | |
|---|---|
| **--enableEASG** | Enables Enhanced Access Security Gateway (EASG) authentication. |
| **--disableEASG** | Disables EASG authentication. |
| **--enable** | Enables EASG authentication only for the Avaya Services logins specified in the *user* variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft. |
| **--disable** | Disables EASG authentication only for the Avaya Services logins specified in the *user* variable. |
| **--userStatus** | Displays the EASG status of the user specified in the *user* variable. |
| **--listUsers** | Lists the available EASG users. |
| **--f** | Forces the enable or disable action to run without prompts. |
| **--printDisableWarning** | Displays the warning message for disabling EASG on the system. |
| **--printEnableWarning** | Displays the warning message for enabling EASG on the system. |

# Loading and managing site certificate

### About this task

Site certificates are used by the onsite technicians not having access to the Avaya network to generate a response to the Enhanced Access Security Gateway (EASG) challenge. The technician will generate and provide the site certificate to the customer. The customer must load this site certificate on each server (AVP Host) and virtual machine that the technician needs to access. Once this is done the technician can use EASG Site Manager to login with the EASG challenge. After the technician is done the customer can remove the site certificate from the server or they will be removed by the EASG software after the site certificate expires (~15 days later).

You can load a site certificate using `EASGSiteCertManage --add <pkcs7_file_path>`. You will need to specify a Site Authentication Factor (SAF). The SAF must be provided to the technician and is also used by EASG Site Manager to generate a response to the EASG challenge.

### Before you begin

Customers must complete the following before loading and managing site certificates:

- Have a valid login and password.
- Use a tool such as WinSCP. Log in using a customer login, for example `cust`. Copy the certificate to `/home/cust directory` (where `cust` is the customer directory).
- Use a 10 to 20 character Site Authentication Factor (SAF) for instance 12345abcwxyz.
- Be familiar with CLI type shell commands.

### Procedure

1. Log in to a Linux® shell by using the customer account.

   The customer account is created during the deployment procedure.

2. To manage site certificates, type the following command:

```
[cust@host ~]$  EASGSiteCertManage --add johndoe.p7b
You are about to install this site certificate into your trusted repository:
Technician Name: johndoe
Expiration Date: Nov 10 17:02:15 2016 GMT
Do you want to continue [yes/no]? yes
Please enter a site authentication factor (SAF) for the technician to use
when getting access to your machine. The SAF is alphanumeric with at least 10
characters and no more than 20 characters.
  Please enter your SAF:  Site Authentication Factor
  Please confirm your SAF: Site Authentication Factor
Site Certificate installed successfully.
```

   Save the Site Authentication Factor to share with the technician once on site.

3. To display information about a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --show johndoe.p7b
Subject:        CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
User Name:      johndoe
Expiration:     Nov 10 17:02:15 2016 GMT
Trust Chain:
    1. O=Avaya, OU=IT, CN=AvayaITrootCA2
    2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
    3. O=Avaya LLC, OU=EASG, CN=EASG Intermediate CA
    4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya LLC
    5. CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
```

4. To remove a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
Successfully removed Site Cert: johndoe.p7b
```

# Chapter 9: Resources

## Session Manager documentation

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

| Title | Description | Audience |
|---|---|---|
| Overview | | |
| *Avaya Aura® Session Manager Overview and Specification* | Describes the key features of Session Manager. | System administrators |
| *Avaya Aura® Session Manager Security Design* | Describes the security considerations, features, and solutions for Session Manager. | Network administrators, services, and support personnel |
| Implementation | | |
| *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment* | Describes how to deploy the Session Manager virtual application in a virtualized environment. | Services and support personnel |
| *Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment* | Describes how to deploy the Session Manager in the Software-Only and Infrastructure as a Service (IaaS) environment. | Services and support personnel |
| *Routing Web Service API Programming Reference* | Describes how to use the System Manager Routing Web Service API for Session Manager. | Services and support personnel |
| *Avaya Aura® Session Manager Element Manager Web Service API Programming Reference* | Describes how to get programmatic access to Session Manager Dashboard and User Registration status data. | Services and support personnel |
| Administration | | |
| *Administering Avaya Aura® Session Manager* | Describes the procedures to administer Session Manager using System Manager. | System administrators |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| *Avaya Aura® Session Manager Data Privacy Guidelines* | Describes how to administer Session Manager to fulfill Data Privacy requirements. | System administrators, Network administrators, services, and support personnel |
| Installation and upgrades | | |
| *Upgrading Avaya Aura® Session Manager* | Describes the procedures to upgrade Session Manager to the latest software release. | Services and support personnel |
| Maintaining and Troubleshooting | | |
| *Maintaining Avaya Aura® Session Manager* | Contains the procedures for maintaining Session Manager. | Services and support personnel |
| *Troubleshooting Avaya Aura® Session Manager* | Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware. | Services and support 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 table contains courses that are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

| Course code | Course title |
|---|---|
| 71201V | Integrating Avaya Aura® Core Components |
| 72201V | Supporting Avaya Aura® Core Components |
| 61131V | Administering Avaya Aura® System 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.

## Using the Avaya InSite Knowledge Base

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

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

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

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

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

# Appendix A: List of required RPMs on RHEL 8.4

The following are the lists of the required RPMs on 8.4 RHEL for Session Manager in the Software-Only environment:

**A**

| | | | |
|---|---|---|---|
| aide | augeas-libs | authselect | avahi-libs |

**B**

| | | | |
|---|---|---|---|
| bash | bash-completion | bind | bind-libs |
| bind-utils | boost-serialization | | |

**C**

| | | | |
|---|---|---|---|
| chrony | clevis-luks | copy-jdk-configs | cronie |

**D**

| | | | |
|---|---|---|---|
| dbxtool | dialog | dmidecode | dos2unix |
| dosfstools | dracut-network | | |

**E**

| | | | |
|---|---|---|---|
| efibootmgr | efivar | efivar-libs | efi-filesystem |
| ethtool | | | |

**G**

| | | | |
|---|---|---|---|
| gd | glibc | glibc.i686 | glibc-common |
| grub2-efi-x64 | | | |

**H**

| |
|---|
| hdparm |

**I**

| |
|---|
| iputils |

### J

| | | | |
|---|---|---|---|
| java-1.8.0-openjdk-devel | jpackage-utils | json-c | |

### L

| | | | |
|---|---|---|---|
| less | libgcc | libgcc.i686 | libicu |
| libjpeg-turbo | libkcapi-hmaccalc | libstdc++ | libstdc++.i686 |
| libwebp | libXpm | lksctp-tools | lsof |

### M

| |
|---|
| mokutil |

### N

| | | | |
|---|---|---|---|
| net-tools | network-scripts | NetworkManager | nftables |
| nss | nss-softokn-freebl | | |

### O

| | | | |
|---|---|---|---|
| openssl | openssh-clients | openssh-server | |

### P

| | | | |
|---|---|---|---|
| parted | passwd | patch | pcre-cpp |
| perf | perl | perl-Data-Dumper | perl-Sys-Syslog |
| plymouth | postgresql-libs | psmisc | policycoreutils-python-utils |
| python2 | python3 | python3-augeas | python3-lxml |
| python3-netifaces | python3-policycoreutils | python3-psutil | python3-pwquality |
| python3-psycopg2 | python3-requests | | |

### R

| |
|---|
| rsyslog-gnutls |

### S

| | | | |
|---|---|---|---|
| selinux-policy | selinux-policy-targeted | setools-console | shim-x64 |
| sssd-client | sudo | sysstat | |

### T

| | | | |
|---|---|---|---|
| tmux | traceroute | tzdata-java | |

### U

| | | | |
|---|---|---|---|
| unzip | uuid | | |

**V**

| | | | |
|---|---|---|---|
| vim-common | vim-minimal | virt-what | |

**W**

| | | | |
|---|---|---|---|
| wireshark-cli | wget | | |

**Y**

| | | | |
|---|---|---|---|
| yum | yum-utils | | |

**Z**

| | | | |
|---|---|---|---|
| zip | zlib.i686 | | |

**Related links**

Example kickstart template for BSM Software-only deployments on page 87
Core Session Manager kickstart example for software-only deployments on page 92

# Example kickstart template for BSM Software-only deployments

To use this template, replace all uppercase values surrounded by < >.

Also uncomment the desired profile disk configuration.

```
auth --enableshadow --passalgo=sha512

# Use network installation

url --url=<HTTP_PATH_TO_REPOSITORY>

# Use text install

text

# network settings

network --bootproto=static --device='eth0' --ip=<IP> --gateway=<GATEWAY>
--netmask=<NETMASK> --nameserver=<DNS_SERVERS> --ipv6=auto --
hostname=<FQDN> --activate

network --device=eth1 --onboot=no

reboot --eject

# Keyboard layouts

keyboard --vckeymap=us --xlayouts='us'

# System language

lang en_US.UTF-8
```

```
# set SELinux state
selinux --enforcing
# Root password
rootpw --iscrypted <ENCRYPTED_HASH_PASSWORD>
# System services
services --enabled="chronyd"
# System timezone
timezone America/Denver --isUtc --ntpservers=<NTP_SERVERS>
# System bootloader configuration
bootloader --append="crashkernel=auto" --location=mbr --boot-drive=sda
clearpart --all --initlabel
part /boot/efi --fstype="vfat" --size=200 --ondisk=sda
part /boot/ --size=1024 --ondisk=sda
part pv.01 --size=1 --grow --ondisk=sda
volgroup sysvg pv.01
# Disk partitioning information
logvol swap --fstype="swap" --size=2048 --name=lv_swap --vgname=sysvg
logvol / --vgname=sysvg --size=17408 --name=lv_root
logvol /data --vgname=sysvg --size=12288 --name=lv_data --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev
logvol /var/log --vgname=sysvg --size=1 --grow --name=lv_var_log --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev
%packages
aide
audit
audit-libs
augeas-libs
authselect-compat
avahi-libs
bash
bash-completion
bind
bind-libs
bind-utils
```

boost-serialization
chrony
cronie
clevis-luks
copy-jdk-configs
dbxtool
dialog
dmidecode
dos2unix
dosfstools
dracut-network
efibootmgr
efivar-libs
efi-filesystem
efivar
ethtool
gd
glibc
glibc.i686
glibc-common
grub2-efi-x64
hdparm
java-1.8.0-openjdk-devel
less
jpackage-utils
json-c
libgcc
libgcc.i686
libicu
libjpeg-turbo
libkcapi-hmaccalc
libstdc++
libstdc++.i686

- libwebp
- libXpm
- lksctp-tools
- iputils
- lsof
- mokutil
- net-tools
- network-scripts
- nftables
- nss
- nss-softokn-freebl
- NetworkManager
- openssl
- openssh-clients
- openssh-server
- parted
- passwd
- patch
- pcre-cpp
- perf
- perl
- perl-Data-Dumper
- perl-Sys-Syslog
- plymouth
- postgresql-libs
- psmisc
- policycoreutils-python-utils
- python2
- python3
- python3-augeas
- python3-lxml
- python3-netifaces
- python3-policycoreutils

python3-psutil
python3-pwquality
python3-psycopg2
python3-requests
rsyslog-gnutls
selinux-policy
selinux-policy-targeted
setools-console
shim-x64
sssd-client
sudo
sysstat
tmux
traceroute
tzdata-java
unzip
uuid
vim-common
vim-minimal
virt-what
wireshark-cli
wget
yum
yum-utils
zip
zlib.i686

```
%end
%post
%end
```

**Related links**

List of required RPMs on RHEL 8.4 on page 85

# Core Session Manager kickstart example for software-only deployments

To use this template, replace all uppercase values surrounded by < >.

Also uncomment the desired profile disk configuration.

```
auth --enableshadow --passalgo=sha512

# Use network installation

url --url=<HTTP_PATH_TO_REPOSITORY>

# Use text install

text

# network settings

network --bootproto=static --device='eth0' --ip=<IP> --gateway=<GATEWAY>
--netmask=<NETMASK> --nameserver=<DNS_SERVERS> --ipv6=auto --
hostname=<FQDN> --activate

network --device=eth1 --onboot=no

reboot --eject

# Keyboard layouts

keyboard --vckeymap=us --xlayouts='us'

# System language

lang en_US.UTF-8

# set SELinux state

selinux --enforcing

# Root password

rootpw --iscrypted <ENCRYPTED_HASH_PASSWORD>

# System services

services --enabled="chronyd"

# System timezone

timezone America/Denver --isUtc --ntpservers=<NTP_SERVERS>

# System bootloader configuration

bootloader --append="crashkernel=auto" --location=mbr --boot-drive=sda

clearpart --all --initlabel

part /boot/efi --fstype="vfat" --size=200 --ondisk=sda

part /boot --size=1024 --ondisk=sda

part pv.01 --size=1 --grow --ondisk=sda
```

```
volgroup sysvg pv.01

# Configure the disk based on profile

Common partitioning

logvol swap --fstype="swap" --vgname=sysvg --size 8192 --name=lv_swap

logvol / --vgname=sysvg --grow --size=15360 --name=lv_root

logvol /home --vgname=sysvg --grow --size=10240 --name=lv_home --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /tmp --vgname=sysvg --grow --size=10240 --name=lv_tmp --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var --vgname=sysvg --grow --size=3072 --name=lv_var --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

Disk partitioning information (Profiles 1 & 2)

logvol /data --vgname=sysvg --grow --size=30720 --name=lv_data --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log/audit --vgname=sysvg --
grow --size=2560 --name=lv_var_log_audit --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log --vgname=sysvg --grow --percent=100 --name=lv_var_log --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

Disk partitioning information (Profiles 3 & 4)

logvol /data --vgname=sysvg --grow --size=51200 --name=lv_data --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log/audit --vgname=sysvg --
grow --size=4096 --name=lv_var_log_audit --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log --vgname=sysvg --grow --percent=100 --name=lv_var_log --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

Disk partitioning information (Profiles 5 & 6)

logvol /data --vgname=sysvg --grow --size=92160 --name=lv_data --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log/audit --vgname=sysvg --
grow --size=7168 --name=lv_var_log_audit --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

logvol /var/log --vgname=sysvg --grow --percent=100 --name=lv_var_log --
fsoptions=rw,nosuid,noexec,auto,nouser,async,noatime,nodev

%packages

aide

audit
```

audit-libs
augeas-libs
authselect-compat
avahi-libs
bash
bash-completion
bind
bind-libs
bind-utils
boost-serialization
chrony
cronie
clevis-luks
copy-jdk-configs
dbxtool
dialog
dmidecode
dos2unix
dosfstools
dracut-network
efibootmgr
efivar-libs
efi-filesystem
efivar
ethtool
gd
glibc
glibc.i686
glibc-common
grub2-efi-x64
hdparm
java-1.8.0-openjdk-devel
less

jpackage-utils
json-c
libgcc
libgcc.i686
libicu
libjpeg-turbo
libkcapi-hmaccalc
libstdc++
libstdc++.i686
libwebp
libXpm
lksctp-tools
iputils
lsof
mokutil
net-tools
network-scripts
nftables
nss
nss-softokn-freebl
NetworkManager
openssl
openssh-clients
openssh-server
parted
passwd
patch
pcre-cpp
perf
perl
perl-Data-Dumper
perl-Sys-Syslog
plymouth

- postgresql-libs
- psmisc
- policycoreutils-python-utils
- python2
- python3
- python3-augeas
- python3-lxml
- python3-netifaces
- python3-policycoreutils
- python3-psutil
- python3-pwquality
- python3-psycopg2
- python3-requests
- rsyslog-gnutls
- selinux-policy
- selinux-policy-targeted
- setools-console
- shim-x64
- sssd-client
- sudo
- sysstat
- tmux
- traceroute
- tzdata-java
- unzip
- uuid
- vim-common
- vim-minimal
- virt-what
- wireshark-cli
- wget
- yum
- yum-utils

```
zip
zlib.i686
%end
%post
%end
```

**Related links**

List of required RPMs on RHEL 8.4 on page 85

# Appendix B: List of required RPMs on RHEL 8.10

The following are the lists of the required RPMs on RHEL 8.10 for Session Manager in the Software-Only environment:

**A**

| | | | |
|---|---|---|---|
| acl | aide | alsa-lib | asset |
| asset-hpm | atk | audit | audit-libs |
| augeas-libs | authselect | authselect-compat | authselect-libs |
| avahi-libs | avaya-common-arbiter | avaya-common-drs | avaya-common-jboss |
| avaya-common-mgmt | avaya-common-platform | avaya-common-postgres | avaya-common-tools |
| avaya-common-trustmgmt | avaya-common-websphere | avaya-ncs | avaya-os-tools |
| avaya-sm-appliance | avaya-sm-callp | avaya-sm-cassandra | avaya-sm-cdr |
| avaya-sm-easg | avaya-sm-mgmt | avaya-sm-platform | avaya-sm-ppm |
| avaya-sm-sdm | avaya-sm-spirit | avaya-sm-ustore | avaya-vm-tools |

**B**

| | | | |
|---|---|---|---|
| basesystem | bash | bash-completion | bc |
| bind | bind-export-libs | bind-libs | bind-libs-lite |
| bind-license | bind-utils | boost-serialization | brotli |
| bubblewrap | bzip2 | bzip2-libs | |

**C**

| | | | |
|---|---|---|---|
| ca-certificates | cairo | c-ares | checkpolicy |
| chkconfig | chrony | clevis | clevis-dracut |
| clevis-luks | clevis-systemd | copy-jdk-configs | coreutils |
| coreutils-common | cpio | cracklib | cracklib-dicts |
| cronie | cronie-anacron | crontabs | crypto-policies |
| crypto-policies-scripts | cryptsetup | cryptsetup-libs | cups-libs |
| curl | cyrus-sasl-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 | dhcp-client | dhcp-common | dhcp-libs |
| dialog | diffutils | dmidecode | dnf |
| dnf-data | dnf-plugins-core | dos2unix | dosfstools |
| dracut | dracut-network | dwz | |

## E

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

## F

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

## G

| | | | |
|---|---|---|---|
| gawk | gd | gdbm | gdbm-libs |
| gdisk | gdk-pixbuf2 | gdk-pixbuf2-modules | genisoimage |
| gettext | gettext-libs | ghc-srpm-macros | giflib |
| glib2 | glibc | glibc-common | glibc-gconv-extra |
| glibc-langpack-en | gmp | gnupg2 | gnupg2-smime |
| gnutls | go-srpm-macros | gpgme | gpg-pubkey |
| graphite2 | grep | groff-base | grub2-common |
| grub2-efi-x64 | grub2-tools | grub2-tools-efi | grub2-tools-extra |
| grub2-tools-minimal | grubby | gsoap | gtk2 |
| gtk-update-icon-cache | gzip | | |

## H

| | | | |
|---|---|---|---|
| hardlink | harfbuzz | haveged | hdparm |
| hicolor-icon-theme | hostname | hwdata | |

## I

| | | | |
|---|---|---|---|
| ima-evm-utils | info | initscripts | ipcalc |
| iproute | iptables-libs | iputils | |

## J

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

## K

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

## L

| | | | |
|---|---|---|---|
| langpacks-en | less | libacl | libaio |
| libarchive | libassuan | libatasmart | libattr |
| libbabeltrace | libblkid | libblockdev | libblockdev-crypto |
| libblockdev-fs | libblockdev-loop | libblockdev-mdraid | libblockdev-part |
| libblockdev-swap | libblockdev-utils | libbpf | libbytesize |
| libcap | libcap-ng | libcom_err | libcomps |
| libcroco | libcurl | libdatrie | libdb |
| libdb-utils | libdnf | libdrm | libedit |
| libestr | libevent | libfastjson | libfdisk |
| libffi | libfontenc | libgcab1 | libgcc |
| libgcrypt | libgomp | libgpg-error | libgudev |
| libgusb | libibverbs | libicu | libidn2 |
| libjose | libjpeg-turbo | libkcapi | libkcapi-hmaccalc |
| libksba | libluksmeta | libmaxminddb | libmbim |
| libmetalink | libmnl | libmodulemd | libmount |
| libmspack | libndp | libnftnl | libnghttp2 |
| libnl3 | libnsl2 | libpcap | libpciaccess |
| libpkgconf | libpng | libpq | libpsl |
| libpwquality | libqmi | librepo | libreport-filesystem |
| librhsm | libseccomp | libsecret | libselinux |
| libselinux-utils | libsemanage | libsepol | libsigsegv |

*Table continues…*

| | | | |
|---|---|---|---|
| libsmartcols | libsmbios | libsmi | libsolv |
| libss | libssh | libssh-config | libsss_idmap |
| libsss_nss_idmap | libstdc++ | libtasn1 | libthai |
| libtiff | libtirpc | libtool-ltdl | libtraceevent |
| libudisks2 | libunistring | libusal | libusbx |
| libuser | libutempter | libuuid | libverto |
| libwebp | libX11 | libX11-common | libXau |
| libxcb | libXcomposite | libxcrypt | libXcursor |
| libXdamage | libXext | libXfixes | libXft |
| libXi | libXinerama | libxkbcommon | libxml2 |
| libxmlb | libXpm | libXrandr | libXrender |
| libxslt | libXtst | libyaml | libzstd |
| linux-firmware | lksctp-tools | lm_sensors-libs | logrotate |
| lsof | lua | lua-libs | luksmeta |
| lvm2 | lvm2-libs | lz4-libs | |

**M**

| | | | |
|---|---|---|---|
| mdadm | memstrack | ModemManager-glib | mokutil |
| mozjs60 | mpfr | | |

**N**

| | | | |
|---|---|---|---|
| ncurses | ncurses-base | ncurses-libs | net-snmp |
| nettle | net-tools | NetworkManager | NetworkManager-initscripts-updown |
| NetworkManager-libnm | network-scripts | nftables | nginx |
| npth | nspr | nss | nss-softokn |
| nss-softokn-freebl | nss-sysinit | nss-util | numactl-libs |

**O**

| | | | |
|---|---|---|---|
| ocaml-srpm-macros | oddjob | oddjob-mkhomedir | oniguruma |
| openblas-srpm-macros | 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 | patch | pciutils |

*Table continues…*

| | | | |
|---|---|---|---|
| pciutils-libs | pcre | pcre2 | pcre-cpp |
| perf | perl | perl-Algorithm-Diff | perl-Archive-Tar |
| perl-Archive-Zip | perl-Attribute-Handlers | perl-autodie | perl-B-Debug |
| perl-bignum | perl-Carp | perl-Compress-Bzip2 | perl-Compress-Raw-Bzip2 |
| perl-Compress-Raw-Zlib | perl-Config-Perl-V | perl-constant | perl-CPAN |
| perl-CPAN-Meta | perl-CPAN-Meta-Requirements | perl-CPAN-Meta-YAML | perl-Data-Dumper |
| perl-Data-OptList | perl-Data-Section | perl-DB_File | perl-devel |
| perl-Devel-Peek | perl-Devel-PPPort | perl-Devel-SelfStubber | perl-Devel-Size |
| perl-Digest | perl-Digest-MD5 | perl-Digest-SHA | perl-Encode |
| perl-Encode-devel | perl-Encode-Locale | perl-encoding | perl-Env |
| perl-Errno | perl-experimental | perl-Exporter | perl-ExtUtils-CBuilder |
| perl-ExtUtils-Command | perl-ExtUtils-Embed | perl-ExtUtils-Install | perl-ExtUtils-MakeMaker |
| perl-ExtUtils-Manifest | perl-ExtUtils-Miniperl | perl-ExtUtils-MM-Utils | perl-ExtUtils-ParseXS |
| perl-File-Fetch | perl-File-HomeDir | perl-File-Path | perl-File-Temp |
| perl-File-Which | perl-Filter | perl-Filter-Simple | perl-Getopt-Long |
| perl-HTTP-Tiny | perl-inc-latest | perl-interpreter | perl-IO |
| perl-IO-Compress | perl-IO-Socket-IP | perl-IO-Socket-SSL | perl-IO-Zlib |
| perl-IPC-Cmd | perl-IPC-System-Simple | perl-IPC-SysV | perl-JSON-PP |
| perl-libnet | perl-libnetcfg | perl-libs | perl-Locale-Codes |
| perl-Locale-Maketext | perl-Locale-Maketext-Simple | perl-local-lib | perl-macros |
| perl-Math-BigInt | perl-Math-BigInt-FastCalc | perl-Math-BigRat | perl-Math-Complex |
| perl-Memoize | perl-MIME-Base64 | perl-Module-Build | perl-Module-CoreList |
| perl-Module-CoreList-tools | perl-Module-Load | perl-Module-Load-Conditional | perl-Module-Loaded |
| perl-Module-Metadata | perl-Mozilla-CA | perl-MRO-Compat | perl-Net-Ping |
| perl-Net-SSLeay | perl-open | perl-Package-Generator | perl-Params-Check |
| perl-Params-Util | perl-parent | perl-PathTools | perl-perlfaq |
| perl-PerlIO-via-QuotedPrint | perl-Perl-OSType | perl-Pod-Checker | perl-Pod-Escapes |
| perl-Pod-Html | perl-podlators | perl-Pod-Parser | perl-Pod-Perldoc |
| perl-Pod-Simple | perl-Pod-Usage | perl-Scalar-List-Utils | perl-SelfLoader |
| perl-Socket | perl-Software-License | perl-srpm-macros | perl-Storable |
| perl-Sub-Exporter | perl-Sub-Install | perl-Sys-Syslog | perl-Term-ANSIColor |
| perl-Term-Cap | perl-TermReadKey | perl-Test | perl-Test-Harness |

*Table continues…*

| | | | |
|---|---|---|---|
| perl-Test-Simple | perl-Text-Balanced | perl-Text-Diff | perl-Text-Glob |
| perl-Text-ParseWords | perl-Text-Tabs+Wrap | perl-Text-Template | perl-Thread-Queue |
| perl-threads | perl-threads-shared | perl-Time-HiRes | perl-Time-Local |
| perl-Time-Piece | perl-Unicode-Collate | perl-Unicode-Normalize | perl-URI |
| perl-utils | perl-version | 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 |
| postgresql13 | postgresql13-libs | postgresql13-server | procps-ng |
| protobuf-c | psmisc | publicsuffix-list-dafsa | python36 |
| python3-audit | python3-augeas | python3-bind | python3-cffi |
| python3-chardet | python3-cryptography | python3-dateutil | python3-dbus |
| python3-dialog | python3-dnf | python3-dnf-plugins-core | python3-gpg |
| python3-hawkey | python3-html5lib | python3-idna | python3-libcomps |
| python3-libdnf | python3-libs | python3-libselinux | python3-libsemanage |
| python3-lxml | python3-netifaces | python3-pip | python3-pip-wheel |
| python3-ply | python3-policycoreutils | python3-psutil | python3-psycopg2 |
| python3-pwquality | python3-pycparser | python3-pyparsing | python3-pysocks |
| python3-pyyaml | python3-requests | python3-rpm | python3-rpm-macros |
| python3-setools | python3-setuptools | python3-setuptools-wheel | python3-six |
| python3-systemd | python3-termcolor | python3-unbound | python3-urllib3 |
| python3-webencodings | python-rpm-macros | python-srpm-macros | |

## Q

| |
|---|
| qt5-srpm-macros |

## R

| | | | |
|---|---|---|---|
| rdma-core | readline | redhat-release | redhat-release-eula |
| redhat-rpm-config | rng-tools | rpm | rpm-build-libs |
| rpm-libs | rpm-plugin-selinux | rpm-plugin-systemd-inhibit | rsyslog |
| rsyslog-gnutls | rust-srpm-macros | | |

### S

| | | | |
|---|---|---|---|
| sed | selinux-policy | selinux-policy-targeted | setools-console |
| setup | shadow-utils | shared-mime-info | shim-x64 |
| slang | snfw | spiritAgentrpm | sqlite |
| sqlite-libs | sssd-client | sudo | sysstat |
| systemd | systemd-libs | systemd-pam | systemd-udev |
| systemtap-sdt-devel | | | |

### T

| | | | |
|---|---|---|---|
| tar | timedatex | tmux | tpm2-tools |
| tpm2-tss | traceroute | trousers | trousers-lib |
| ttmkfdir | tzdata | tzdata-java | |

### U

| | | | |
|---|---|---|---|
| udisks2 | unbound-libs | unzip | util-linux |
| uuid | | | |

### V

| | | | |
|---|---|---|---|
| vim-common | vim-filesystem | vim-minimal | virt-what |
| volume_key-libs | wget | | |

### W

| | | | |
|---|---|---|---|
| which | wireshark-cli | | |

### X

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

### Y

| | | | |
|---|---|---|---|
| yum | yum-utils | | |

### Z

| | | | |
|---|---|---|---|
| zip | zlib | | |

# Appendix C: Avaya root certificate

You must copy the following text into a text file and use it.

```
-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgIBADANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wMzA4MjIxMTI1MzZa
Fw0zMzA4MTQxMTI1MzZaMF4xCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTEeMBwGA1UEAxMVQXZheWEg
UHJvZHVjdCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+EpellesygWvwACRNRh/6FbkPYDGrf5jpqIzgd3KG1w7gvvQ/ID953REm2DS7DEI
4y7l+zY0MLtNv+I3rASpdxufsFwkHa5zR1FjpkiaP7XhMKXNpSY7No78rko9uiGt
xCx9VdW20kcP4IiEN23jQWfKjGFzkZItCl/aOf2+peh8bSS2MIprGx4rnCMZN1dU
Nnw8nJFGu7IxRlGDA2XqJ7BWBn/pvPMLdaVU60oI1/4IT9lHPUCaRVAC56jJdtxq
F9sNW0ZsBy05/vtopUiStfq8aMtMWCqGkSwjWB2VDWhWj6HTuGk27YsTsFIREJuT
i7rXYBQqRJN0o15aERM6BwIDAQABo4IBmzCCAZcwHQYDVR0OBBYEFMKatvFzIYIm
bROw/v5R9l6b3DV7MIGGBgNVHSMEfzB9gBTCmrbxcyGCJm0TsP7+UfZem9w1e6Fi
pGAwXjELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xGjAYBgNVBAsT
EUF2YXlhIFByb2R1Y3QgUEtJMR4wHAYDVQQDExVBdmF5YSBQcm9kdWN0IFJvb3Qg
Q0GCAQAwDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwgdEGA1UdIASByTCBxjCB
wwYLYIZIAYb8CwcBAQEwgbMwKgYIKwYBBQUHAgEWHmh0dHBzOi8vd3d3LmF2YXlh
LmNvbS9wa2kvQ1BTOzCBhAYIKwYBBQUHAgIweDAXFhBBdmF5YSBQcm9kdWN0IENB
MAMCAQEaXUF2YXlhIEluYy4gTGltaXRlZCBMaWFiaWxpdHkgUEtJIENBLiAgUGxl
YXNlIHZpc2l0IGh0dHA6Ly93d3cuYXZheWEuY29tL3BraS9DUFMgZm9yIGRldGFp
bHMuOzANBgkqhkiG9w0BAQUFAAOCAQEAQYNqOpJSkAn6tZOAbp7IW2RMFQO2rwNe
UFdyWywqWKdoCNv/+9dAkHXp8wSEwRGPuXRJLuSZloRlK7OnT4GBH+YaFMarHpUr
rChkrmcR9smgN1WvSjvTk1HiFXEyurvpRarLRem3spDdN6Cyu/fhroJJEHc0j97O
U2HTNgz0papOAFxYN497y3teENVmRBGNKoUo6NxayOCjv55JBxegvd6bOtabRv1L
OCNK8yeomL5ri9jiTLUgEEZIn3aFXetuKxTjhQqbxcpy16t70SQctIzLXqdp9ZZu
xz27CykJXlmexi5qREs+MLV0jrduRE50nTHMhkHKZBX7yKIgEb9GwQ==
-----END CERTIFICATE-----
```

# Appendix D: Creating RHEL virtual machine on Nutanix

## Uploading the RHEL ISO to Nutanix server

### About this task

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

**Note:**

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

### Procedure

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

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

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

### Next steps

Installing RHEL on Nutanix 6.5 and later.

# Installing RHEL on the Nutanix server

### Before you begin

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

### Procedure

1. Navigate to **Home** > **VM**.
2. In the **VM** page, click **Create VM**.
3. In the **Create VM** window under **General Configurations**, enter appropriate values in the **Name**, **Description**, and **Timezone** fields.
4. In the **vCPUs** field under **Compute Details**, enter the number of CPUs required for the application.

   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.

   Session Manager requires additional disks. For more information, see <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.

    • Session Manager requires two NICs
      - NIC1 is for the Management IP
      - NIC2 is for the Asset IP
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 46.
    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

## F



## G



## I



## K



## L



## N



## O



## P



## R



## S

## T



## U



## V



## W