# Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment

Release 10.2.x
Issue 8
March 2026

# Notices

© 2026 Avaya LLC. All Rights Reserved.

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.

© 2019-2026, Avaya LLC
All Rights Reserved.

**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** ..... 8
Purpose ..... 8
Changes to platform support ..... 8
Prerequisites ..... 9
Change history ..... 9
**Chapter 2: Virtualized Environment overview** ..... 12
Virtualized Environment components for VMware ..... 12
Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) ..... 13
**Chapter 3: Planning and configuration** ..... 14
Planning checklist for VMware® ..... 14
Planning checklist for ASP R6.0.x (KVM on RHEL 8.10) ..... 15
Supported footprints of Session Manager on VMware ..... 16
Supported footprints of Branch Session Manager on VMware ..... 18
Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) ..... 19
Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) ..... 20
Customer configuration data for Session Manager ..... 20
Installing the license file ..... 22
SAL Gateway ..... 22
Software details of Session Manager and Branch Session Manager ..... 22
VMware software requirements ..... 23
Supported hardware for VMware ..... 23
Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) ..... 23
Supported ESXi version ..... 23
Supported ASP R6.0.x (KVM on RHEL 8.10) version ..... 24
Software requirements ..... 25
Downloading software from PLDS ..... 26
Latest software updates and patch information ..... 27
Conditions for VM hosts ..... 27
Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host ..... 28
Adding an Avaya Solutions Platform 130 Release 5.1 host ..... 30
Adding an Avaya Solutions Platform S8300 Release host ..... 32
**Chapter 4: Deploying Session Manager and Branch Session Manager on VMware®** ..... 34
Session Manager deployment checklist ..... 34
Branch Session Manager Deployment checklist ..... 35
Configuring the system for Session Manager and Branch Session Manager deployment ..... 35
Methods for deploying the Session Manager and Branch Session Manager OVA ..... 36
Deploying the Session Manager OVA on vCenter using vSphere Client (HTML5) ..... 37
Deploying the application OVA by accessing the ESXi host directly ..... 38

Deploying the Session Manager and Branch Session Manager OVA using Solution Deployment Manager ... 40
Application Deployment field descriptions ... 42
Configuring the virtual machine automatic startup settings on VMware ... 48
Configuring the virtual machine automatic startup settings using vSphere ... 49
Configuring Session Manager ... 49
Survivable Remote Server ... 50
patchSM command ... 50
Installing software patches ... 51
Installing a Session Manager or Branch Session Manager patch with the snapshot option ... 51
**Chapter 5: Deploying Session Manager and Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)** ... 53
Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit ... 53
Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit ... 61
Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script ... 70
Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script ... 77
Updating the CPU resources for KVM Cockpit ... 83
**Chapter 6: Configuring edge Branch Session Manager** ... 85
Install certificates for edge Branch Session Manager ... 85
Installing the root CA certificate in the trust store of the tunnel ... 85
Installing identity certificates for configuring mutual authentication for the tunnel ... 86
Installing third-party identity certificates ... 86
edgeSetup command ... 87
Application Delivery Controller ... 88
Configuring the edge Branch Session Manager server in graphical-user interface mode through CLI ... 89
Configuring the edge Branch Session Manager system in text mode through CLI ... 90
Configuring the edge Branch Session Manager server through CLI ... 91
**Chapter 7: Post-installation verification** ... 92
Post-installation checklist ... 92
Running maintenance tests ... 92
Verifying data replication ... 93
Troubleshooting Data Replication ... 93
Verifying the connections ... 93
Generating a test alarm ... 94
**Chapter 8: Maintenance and administration procedures** ... 96
Managing snapshots through Session Manager CLI ... 96
vmsnapshot command ... 96
Configuring the authentication file with ESXi detail ... 97
Creating a snapshot through CLI ... 97
Viewing list of snapshots through CLI ... 98
Reverting a snapshot through CLI ... 98
Removing a snapshot through CLI ... 99

Managing snapshot through vSphere Client ..... 99
Creating a snapshot ..... 99
Deleting a snapshot for VMware ..... 100
Restoring a snapshot for VMware ..... 100
Restarting an application from Solution Deployment Manager ..... 101
Session Manager Backup and Restore ..... 101
Using CLI to backup and restore Session Manager ..... 102
Verifying Active Call Count ..... 103
Troubleshooting a Session Manager virtual machine that does not power on ..... 103
Reconfiguring hardware resources for flexible footprint ..... 104
Viewing the Security Module status ..... 105
Troubleshooting Security Module Sanity failure ..... 105
Viewing the Session Manager entity link connection status ..... 106
Viewing the SIP Monitoring Status Summary page ..... 106
Enhanced Access Security Gateway ..... 107
Checking EASG status ..... 107
Enabling and disabling EASG using CLI ..... 107
Enabling and disabling EASG through System Manager ..... 108
EASGManage ..... 108
Loading and managing site certificate ..... 109
General Maintenance ..... 110
Adding Session Manager or Branch Session Manager as SIP entity ..... 110
Accepting new service ..... 111
Denying new service ..... 112
**Chapter 9: Resources** ..... 113
Session Manager documentation ..... 113
Finding documents on the Avaya Support website ..... 114
Training ..... 115
Viewing Avaya Mentor videos ..... 115
Support ..... 116
Using the Avaya InSite Knowledge Base ..... 116
**Appendix A: Upgrading RHEL** ..... 117
Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines ..... 117
**Appendix B: Best Practices for VMware performance and features** ..... 119
BIOS ..... 119
Intel Virtualization Technology ..... 119
Dell PowerEdge Server ..... 120
Timekeeping ..... 120
VMware Tools ..... 121
VMware networking best practices ..... 122
Separating Session Manager management and Security Module traffic ..... 126
Storage ..... 127
Thin vs. thick deployments ..... 127

Best Practices for VMware features ..... 128
VMware High Availability ..... 128
VMware vMotion ..... 128
VMware snapshots ..... 129
VMware features supported by Avaya Aura® ..... 130
**Appendix C: PCN and PSN notifications** ..... 133
PCN and PSN notifications ..... 133
Viewing PCNs and PSNs ..... 133
Signing up for PCNs and PSNs ..... 134

# Chapter 1: Introduction

## Purpose

This document provides procedures for deploying:

- Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager application on VMware® in a customer-provided Virtualized Environment, Avaya Solutions Platform 130 (Dell PowerEdge R640) in a Avaya-Supplied VMware ESXi 7.0, or Avaya Solutions Platform S8300 in a Avaya-Supplied VMware ESXi 7.0. It includes installation, configuration, installation verification, troubleshooting, and basic maintenance checklists and procedures.
- Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager application on Kernel-Based Virtual Machine (KVM) Avaya Solution Platform 130 (Dell Power Edge R640, R660xs) in the Avaya-Supplied KVM on Red Hat Enterprise Linux (RHEL) R8.10 or Avaya Solution Platform S8300 in the Avaya-supplied KVM on RHEL R8.10.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying System Manager at a customer site. For example, implementation engineers, field technicians, business partners, solution providers, and customers.

This document does not include optional or customized aspects of a configuration.

## 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 Session Manager or Branch Session Manager, ensure that you have the following knowledge, skills, and tools.

### Knowledge

- For Avaya Solutions Platform 130: Avaya Solutions Platform 130 (Dell PowerEdge R640) installation and set up
- For Avaya Solutions Platform S8300: Avaya Solutions Platform S8300 installation and set up
- For VMware: VMware® vSphere™ virtualized environment
- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager

### Skills

To administer:

- VMware® vSphere™ virtualized environment
- Avaya Solutions Platform 130 (Dell PowerEdge R640)
- Avaya Solutions Platform S8300

### Tools

VMware tools in case of deployment in VMWare environment.

# Change history

| Issue | Date | Summary of changes |
|---|---|---|
| 8 | March 2026 | Added the section:<br>Changes to platform support on page 8 |
| 7 | March 2026 | Updated the following sections:<br>• Purpose on page 8<br>• Virtualized Environment overview on page 12<br>• Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 24<br>• Software requirements on page 25<br>• Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit on page 61 |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 6 | April 2025 | Updated the following sections:<br>• Supported ESXi version on page 23<br>• Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 70<br>• Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 77 |
| 5 | December 2024 | Added the following sections:<br>• Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 70<br>• Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 77 |
| 4 | December 2024 | Added the following sections for R10.2.1:<br>• Planning checklist for ASP R6.0.x (KVM on RHEL 8.10) on page 15<br>• Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) on page 23<br>• Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 24<br>• Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) on page 13<br>• Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 19<br>• Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 20<br>• Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit on page 53<br>• Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit on page 61<br>• Updating the CPU resources for KVM Cockpit on page 83<br>• Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines on page 117<br>Updated the following sections for R10.2.1:<br>• Purpose<br>• Virtualized Environment overview<br>• Virtualized Environment components<br>• Software requirements |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 3 | April 2024 | Updated the sections: Supported footprints of Session Manager on VMware on page 16<br>Supported footprints of Branch Session Manager on VMware on page 18 |
| 2 | March 2024 | Updated the section:VMware features supported by Avaya Aura on page 130. |
| 1 | December 2023 | 10.2 document release. |

# Chapter 2: Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.2.x applications in one of the following Virtualized Environments:

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with a preinstalled ESXi 7.0 Standard VMware License.
- Avaya Solutions Platform S8300 with a preinstalled ESXi 7.0 Foundation License for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- VMware in a customer-provided Virtualized Environment.

**Note:**

For more information about deploying applications, see the product-specific Software-Only and Infrastructure as a Service guide.

## Virtualized Environment components for VMware

| Virtualized component | Description |
|---|---|
| Open Virtualization Appliance (OVA) | The virtualized OS and application packaged in a single file that is used to deploy a virtual machine. |
| Customer-provided VMware or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) or Avaya Solutions Platform S8300 | |
| ESXi | The physical machine running the ESXi Hypervisor software. |
| ESXi Hypervisor | A platform that runs multiple operating systems on a host computer at the same time. |

*Table continues…*

| Virtualized component | Description |
|---|---|
| ESXi Embedded Host Client | The ESXi Embedded Host Client is a native HTML and JavaScript application and is served directly from the ESXi host. |
| vSphere Client (HTML5) | Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. |
| vCenter Server | vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.<br>This is not applicable for Avaya Solutions Platform 130 or Avaya Solutions Platform S8300. |

# Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10)

| Virtualized component | Description |
|---|---|
| Avaya Solutions Platform 130 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 (Avaya-Supplied KVM on RHEL R8.10) | |
| KVM Cockpit | Cockpit is a system administration tool that provides a user interface for monitoring and administering servers through a web browser. Cockpit administrators can create and manage KVM-based virtual machines on the host system |

# Chapter 3: Planning and configuration

## Planning checklist for VMware®

Complete the following actions before deploying Session Manager.

| # | Action | Links/Notes | ✔ |
|---|---|---|---|
| 1 | Assess and verify the resource requirements with the customer.<br>The key factors are:<br>• CPU utilization<br>• Memory usage<br>• Storage requirements<br>• Network utilization<br>• Supported capacity | See Supported footprints of Session Manager on VMware on page 16. | |
| 2 | Enter the required information in the Customer Configuration Data worksheet. | See Customer configuration data on page 20. | |
| 3 | Verify the customer has the required hardware at the customer site. | See Supported hardware for VMware on page 23. | |
| 4 | Download the required software. | See Downloading software from PLDS on page 26. | |
| 5 | Licenses:<br>1. Obtain the License Activation Code (LAC).<br>2. Install the license file. | See Installing a license file on page 22. | |
| 6 | Verify you have the necessary resources for the SAL Gateway. | See SAL Gateway on page 22. | |
| 7 | Register for PLDS and activate license entitlements. | Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/. | |

# Planning checklist for ASP R6.0.x (KVM on RHEL 8.10)

Ensure that the customer completes the following before deploying the Session Manager Open Virtualization Application (OVA) on Avaya-supplied Avaya Solutions Platform 130.

| # | Action | Links/Notes | ✔ |
|---|---|---|---|
| 1 | Assess and verify the resource requirements with the customer.<br>The key factors are:<br>• CPU utilization<br>• Memory usage<br>• Storage requirements<br>• Network utilization<br>• Supported capacity | See Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 19. | |
| 2 | Enter the required information in the Customer Configuration Data worksheet. | See Customer configuration data on page 20. | |
| 3 | Verify the customer has the required hardware at the customer site. | See Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) on page 23. | |
| 3 | Download the required software. | See Downloading software from PLDS on page 26. | |
| 4 | Licenses:<br>1. Obtain the License Activation Code (LAC).<br>2. Install the license file. | See Installing a license file on page 22. | |
| 5 | Verify you have the necessary resources for the SAL Gateway. | See SAL Gateway on page 22. | |
| 6 | Register for PLDS and activate license entitlements. | Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/. | |

**Note:**

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

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

# Supported footprints of Session Manager on VMware

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

**Note:**

The capacities listed here are only for Session Manager. For information about capacity limits for AADS, see the AADS documentation.

**Note:**

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

| Session Manager Device Footprints | Up to 2K Devices | 2K to 4.5K Devices | 4.5K to 7K Devices | 7K to 10K Devices | 10K to 23.3K Devices | 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 | 5132MiB | 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 VMware OVA (GiB)[3] | 100 | 100 | 135 | 135 | 210 | 210 |
| HDD for Software-Only ISO (GiB)[4] | 100 | 100 | 135 | 135 | 210 | 210 |

*Table continues…*

| Session Manager Device Footprints | Up to 2K Devices | 2K to 4.5K Devices | 4.5K to 7K Devices | 7K to 10K Devices | 10K to 23.3K Devices | 23.3K to 66.7K Devices |
|---|---|---|---|---|---|---|
| Notes:<br>1. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints.<br>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.<br>3. HDD for VMware OVA: When deployed with SDM. Other deployment methods require that disk size be resized manually.<br>4. You can deploy Session Manager software-only *ISO image* on VMware, KVM, Hyper-V, Amazon Web Services, Google Cloud Platform, and Microsoft Azure platforms. | | | | | | |

Session Manager instances are intended to operate as redundant, homogeneous servers to provide high reliability if a Session Manager failure or a network component failure occurs. Each Session Manager should have similar system resources and a balanced number of devices.

Session Manager instances must be similarly sized in both processing power and available memory to accommodate distributions of devices during failover. Small and large footprints are not intended to be mixed in a solution. However, closely sized footprints, such as one size with the next size down in the table above, can be mixed temporarily as capacities increase. You must ensure that the number of devices failing over to a smaller footprint does not exceed the device capacities of that footprint.

You can implement a system that consists of a mixture of Session Manager instances hosted on VMware platforms as well as Session Manager instances hosted on the existing non-VMware platforms. You must configure the VMware-based Session Manager to be similar to the non-VMware-based Session Manager across the enterprise. Similar configurations ensure the best use of system resources and handling failover scenarios. Be careful when configuring the system where a large non-VMware Session Manager can failover to Session Manager running in VMware environment. You must ensure that the target Session Manager can handle the total capacities.

Avaya Aura® deployment supports a geo-redundant Session Manager configuration of up to 28 Session Manager instances that are interconnected and aware of each other. Configurations that exceed this limit are not expected to have problems, but these configurations are not guaranteed to be supported.

The following table summarizes the number of soft clients supported per Session Manager when the soft clients are using Avaya Aura® Device Services.

| Session Manager profile | Total SIP devices | Number of Workplace devices | Previous Workplace devices |
|---|---|---|---|
| Profile 1 | 2,000 | 1,200 | 750 |
| Profile 2 | 4,500 | 2,700 | 1350 |
| Profile 3 | 7,000 | 4,200 | 2100 |
| Profile 4 | 10,000 | 6,000 | 3000 |

*Table continues…*

| Session Manager profile | Total SIP devices | Number of Workplace devices | Previous Workplace devices |
|---|---|---|---|
| Profile 5 | 23,300 | 13,900 | 5240 |
| Profile 6 | 66,700 | 13,900 | - |

# 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[1] | 2200 | 4400 |
| Memory Reservation[1] | 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 |

**Note:**

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

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

# Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

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

**Note:**

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

| 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 23.5K Devices (R2 footprint) | 23.5K to 72K Devices |
|---|---|---|---|---|---|---|
| CPU Minimum | 2200 MHz | | | | | |
| vCPUs | 3 | 5 | 8 | 12 | 20 | 53 |
| CPU MHz Reservation[1] | 3300 | 5500 | 8800 | 13200 | 22000 | 58300 |
| Memory Reservation[1] | 5132 MiB | 7828 MiB | 10552 MiB | 13368 MiB | 24370 MiB | 74064 MiB |
| SIP Devices[2] (Normal/Failure)[3] | 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 VMware OVA (GiB) | 100 | 100 | 135 | 135 | 210 | 210 |

**Note:**

1. Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.
2. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints.
3. 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.

# Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

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

**Note:**

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

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[1] | 2200 | 4400 |
| Memory Reservation[1] | 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 |

**Note:**

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

# Customer configuration data for Session Manager

The following table identifies the required customer configuration information for deployment and configuration. An asterisk (*) indicates a required field.

| Configuration Data | Field | Example value for the System | ✔ |
|---|---|---|---|
| **Network Settings** | Short hostname* | example-sm-1 | |
| | Network domain* | Mycompany.com | |
| | IPv4 address* | | |
| | Netmask* | | |

*Table continues…*

| Configuration Data | Field | Example value for the System | ✔ |
|---|---|---|---|
| | Default gateway* | | |
| | IPv6 address | | |
| | IPv6 prefix | | |
| | IPv6 gateway | | |
| **System Time Settings** | Local time zone* | | |
| | NTP server(s)<br>Comma-separated list, up to 3 servers | Timeserver.ex.com,TS1.ex2.com | |
| **DNS Settings** | DNS server(s)<br>Comma-separated list, up to 3 servers | 123.4.56.789,142.67.2.123 | |
| | Search Domain List<br>Comma-separated list | avaya.com | |
| **System Manager Settings** | Primary System Manager IP address* | | |
| | Enrollment password*<br>**Note:**<br>Verify the enrollment password is active. | | |
| **Login Settings** | Login Name* | | |
| | Password* | | |
| **Survivable Remote**<br>**Note:**<br>This configuration data is only for Branch Session Manager. | • **LSP IPv4**<br>• **LSP IPv6**<br>**Note:**<br>This field takes either of the two values. | | |
| EASG status | EASG | Enable or Disable | |
| Data Encryption | Data Encryption | Enable or Disable | |
| Edge Topology BSM<br>**Note:**<br>This configuration data is only for Branch Session Manager. | Edge Topology BSM | Enable or Disable | |

# 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.

# SAL Gateway

You require a Secure Access Link (SAL) Gateway for remote access and alarming.

Through SAL, support personnel or tools can gain remote access to managed devices to troubleshoot and debug problems.

A SAL Gateway:

1. Receives alarms from Avaya products in the customer network.
2. Reformats the alarms.
3. Forwards the alarms to the Avaya support center or a customer-managed Network Management System.

For more information about SAL Gateway and its deployment, see the Secure Access Link documentation on the Avaya Support website at https://support.avaya.com.

# 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/.

# VMware software requirements

The Avaya Aura® Virtualized Environment supports the following VMware software versions:

- VMware vSphere ESXi 7.0
- VMware vSphere ESXi 8.0
- VMware vCenter Server 7.0
- VMware vCenter Server 8.0

To view compatibility with other solution releases, see *VMware Product Interoperability Matrices* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

# Supported hardware for VMware

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

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

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

# Supported ESXi version

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

| ESXi version | Avaya Aura® Release | | | | |
|---|---|---|---|---|---|
| | 7.1.x | 8.0.x | 8.1.x | 10.1.x | 10.2.x |
| ESXi 5.0 | N | N | N | N | N |
| ESXi 5.1 | N | N | N | N | N |
| ESXi 5.5 | Y | N | N | N | N |
| ESXi 6.0 | Y | Y | Y | N | N |
| ESXi 6.5 | Y | Y | Y | N | N |
| ESXi 6.7 | N | Y | Y | Y | N |

*Table continues…*

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

**Note:**

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

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

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

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

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

| Avaya Solutions Platform (KVM on RHEL 8.10) | Avaya Aura® Release | | |
|---|---|---|---|
| | 8.1.x | 10.1.x | 10.2.x |
| KVM Release 8.10 | Y | Not supported for Session Manager | Y |

**Note:**

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

# Software requirements

Avaya Aura® supports the following software versions:

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

**Note:**

Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.

- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 7.0 or 8.0
  - VMware® vCenter Server 7.0 or 8.0

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

**Note:**

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

  For more information about upgrading from RHEL 8.4 to RHEL 8.10, see *Upgrading Avaya Aura® Session Manager*

# 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.

# Latest software updates and patch information

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

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

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

# Conditions for VM hosts

All virtual machines running on the host must be on the same subnet mask.

If Out of Band Management is configured in a virtual environment deployment, you need two subnet masks, one for each of the following:

- Public or signaling traffic and all virtual machines public traffic.
- Management and all virtual machine management ports.

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

### About this task

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

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

**Note:**

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

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

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

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

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

**Note:**

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

### Before you begin

Add a location.

### Procedure

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

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

   b. In **Platform Type**, select **AVP/ESXi**.
   c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.
5. Click **Save**.
6. In the Certificate dialog box, click **Accept Certificate**.

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

   In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.
7. To view the discovered application details, such as name and version, do the following to establish trust between the application and System Manager:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

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

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

   **Important:**

   To change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure it is available.

8. On the **Platforms** tab, select the required platform and click **Refresh Host**.

### Next steps

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

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

# Adding an Avaya Solutions Platform 130 Release 5.1 host

### About this task

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

### Before you begin

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

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

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

### Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

- For SDM client, on the **SDM Client** web console, click **Application Management**.

2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

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

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

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

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

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

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

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

### Next steps

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

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

# Adding an Avaya Solutions Platform S8300 Release host

## About this task

This procedure is required for both preloaded or prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to add an Avaya Solutions Platform S8300 Release 5.1.x host. You can associate an Avaya Solutions Platform S8300 Release 5.1.x and later host with an existing location.

## Before you begin

- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1.x is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and add the Avaya Solutions Platform S8300 Release 5.1.x host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface".
- If you are connected to the Avaya Solutions Platform S8300 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- Add Avaya Solutions Platform S8300 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform S8300 host.

## Procedure

1. To add an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform S8300 deployment, you can also provide the root username.

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

5. Click **Save**.

   The Avaya Solutions Platform S8300 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, perform the following:

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

   System Manager generates the certificate and adds the Avaya Solutions Platform S8300 host.

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

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

## Next steps

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

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

# Chapter 4: Deploying Session Manager and Branch Session Manager on VMware®

## Session Manager deployment checklist

Session Manager footprints are configured as part of the OVA. Both VMware and Solution Deployment Manager display these footprints to the user during deployment.

**Important:**

You cannot administer a core Session Manager OVA as a Branch Session Manager (remote survivable server). Deploy the Session Manager OVA as a core Session Manager only.

| # | Action | Reference | ✔ |
|---|---|---|---|
| 1 | Verify System Manager and Session Manager are configured. | Configuring the system for SM/BSM deployment on page 35. | |
| 2 | Download the following from PLDS:<br>• Session Manager OVA file<br>• Session Manager patch file | Downloading software from PLDS on page 26. | |
| 3 | Deploy the Session Manager OVA. | Methods for deploying the Session Manager OVA on page 36. | |
| 4 | Configure the Session Manager virtual machine to start automatically after a power failure. | Configuring the virtual machine automatic startup settings on page 48. | |
| 5 | Start the Session Manager server. | | |
| 6 | Configure Session Manager. | Configuring Session Manager on page 49. | |
| 7 | Apply the latest Session Manager Release 10.2.x patch if required. | Installing software patches on page 51. | |
| 8 | Configure the alarming. | | |
| 9 | Verify the deployment. | Post-installation checklist on page 92. | |

# Branch Session Manager Deployment checklist

Branch Session Manager footprints are configured as part of the OVA. Both VMware and Solution Deployment Manager display these footprints to the user during deployment.

| # | Action | Reference | ✔ |
|---|---|---|---|
| 1 | Verify System Manager and Branch Session Manager are configured.<br>**Note:**<br>Also verify that Communication Manager Survivable Remote Server (SRS), formerly known as Local Survivable Processor (LSP), is configured for Branch Session Manager. | Verifying configuration for deployment on page 35. | |
| 2 | Download the Branch Session Manager OVA from PLDS. | Downloading software from PLDS on page 26. | |
| 3 | Deploy the Branch Session Manager OVA. | Methods for deploying the Branch Session Manager OVA on page 36. | |
| 4 | Configure the Branch Session Manager virtual machine to start automatically after a power failure. | Configuring the virtual machine automatic startup settings on page 48. | |
| 5 | Start the Branch Session Manager server. | | |
| 6 | Configure Branch Session Manager. | Configuring Branch Session Manager on page 49. | |
| 7 | Apply the latest Branch Session Manager Release 10.2.x patch, if required. | Installing software patches on page 51. | |
| 8 | Configure the alarming. | | |
| 9 | Verify the deployment. | Post-installation checklist on page 92. | |

# Configuring the system for Session Manager and Branch Session Manager deployment

### Procedure

1. Log in to System Manager associated with Session Manager and Branch Session Manager.
2. Verify System Manager is running the same or later Service Pack level as the Session Manager and Branch Session Manager that you will be installing.

3. Navigate to the **Elements** > **Routing** > **SIP Entities** page and add the Session Manager and Branch Session Manager as a SIP entity.
4. Navigate to the **Elements** > **Session Manager** > **Session Manager Administration** page and add a Session Manager or Branch Session Manager instance.

   For Session Manager, select **Core Session Manager**.

   For Branch Session Manager, select **Branch Session Manager**.
5. Navigate to the **Services** > **Security** > **Certificates** > **Enrollment Password** page and type an Enrollment Password.

   **Note:**

   Password must be alphanumeric and 6 to 25 characters long. Make note of the password for future reference.
6. Define FQDNs for both System Manager and Session Manager and Branch Session Manager. You can either configure the FQDNs in the referenced DNS servers or add the FQDN of Session Manager and Branch Session Manager to the hosts file of System Manager.

# Methods for deploying the Session Manager and Branch Session Manager OVA

Deploy the Session Manager and Branch Session Manager OVA using one of the following methods:

- Deploying the Session Manager OVA on vCenter using vSphere Client (HTML5) on page 37
- Deploying the application OVA by accessing the ESXi host directly on page 38
- Deploying the Session Manager and Branch Session Manager OVA using Solution Deployment Manager on page 40

**Note:**

- The recommended deployment model is the Solution Deployment Manager (SDM), as it automatically reconfigures disk sizes based on the selected profile. It is necessary to resize the disks manually, if you deploy Session Manager of Profile 3 or larger using a model other than SDM.
- Before you deploy Session Manager and Branch Session Manager ensure the time is correct on the ESXi host.

# Deploying the Session Manager OVA on vCenter using vSphere Client (HTML5)

## About this task

Use this procedure to deploy application on vCenter using the vSphere Client (HTML5).

## Before you begin

- Access vCenter Server by using vSphere client (HTML5).
- Download the Client Integration Plug-in.

## Procedure

1. To access the vCenter Server, do the following:
   a. On the web browser, type the vCenter FQDN or IP Address.
   b. Select vSphere Client (HTML5) and type the vCenter Server credentials.
2. Select the Cluster or ESXi host, right-click, and then click **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.
3. On the **Select template** page, perform one of the following steps:
   - To download the application OVA from a web location, select **URL**, and provide the complete path of the OVA file.
   - To access the application OVA from the local computer, select **Locate file**, click **Browse**, and navigate to the OVA file.
4. Click **Next**.
5. On the Select a name and folder page, do the following:
   a. In **Virtual machine name**, type a name for the virtual machine.
   b. In **Select a location for the virtual machine**, select a location for the virtual machine.
6. Click **Next**.
7. On the Select a compute resource page, select a host, and click **Next**.
8. On the Review details page, verify the OVA details, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I accept all license agreements**.
10. Click **Next**.
11. Select the application profile in the **Deployment Configuration** section. For more information on application profiles, see Supported footprints of Session Manager on VMware on page 16.
12. On the Select storage page, in **Select virtual disk format**, click the required disk format.
13. Click **Next**.

14. On the Select networks page, select the destination network for each source network.
15. Click **Next**.
16. On the **Customize template** page, enter the configuration and network parameters.

    **Note:**

    - If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful.
    - During the startup, the system validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the console of the virtual machine.
17. Click **Next**.
18. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.

    **Note:**

    Check the disk sizes. If the HDD sizes are not appropriate resize the disks manually. For more information about the disk sizes, see *Supported footprints of Session Manager*.
19. To start the Session Manager virtual machine, perform one of the following options:
    - Right-click the virtual machine and click **Power** > **Power On**.
    - On the Inventory menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the application virtual machine.
20. Click the **Console** tab and verify that the system startup is successful.

**Related links**

Reconfiguring hardware resources for flexible footprint on page 104

# Deploying the application OVA by accessing the ESXi host directly

## About this task

Use this procedure to deploy the application OVA on Avaya Solutions Platform 130 and equivalent server.

## Before you begin

When you deploy or upgrade Avaya Aura® applications on Avaya Solutions Platform 130 ensure to:

- Update the Dell R640 BIOS and firmware to the latest release.
- Enable the iDRAC and connect it to an ethernet switch.

**Note:**

After deploying OVA directly from host, you must check that HDD size matches your profile.

## Procedure

1. To access the ESXi host, do the following:
   a. On the web browser, type the ESXi host FQDN or IP address.
   b. In **User name**, type the username of the ESXi host.
   c. In **Password**, type the password of the ESXi host.
   d. Click **Log in**.
2. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.
3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK file page, do the following:
   a. Type a name for the virtual machine.
   b. Click to select files or drag and drop the OVA file from your local computer.
6. Click **Next**.
7. On the Select storage page, select a datastore, and click **Next**.
8. To accept the End User License Agreement on the License agreements page, click **I Agree**.
9. Click **Next**.
10. On the Deployment options page, perform the following:
    a. From **Network mappings**, select the required network.
    b. From **Disk provisioning**, select **Thick provision lazy zeroed**.
    c. From **Deployment type**, select profile.
    d. Clear **Power on automatically**.
11. Click **Next**.
12. On the Additional settings page, click **Next**.
13. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
14. To edit the virtual machine settings, click the VM radio option and perform the following:
    - Click **Actions** > **Edit Settings** to edit the required parameters.

**Note:**

Check the disk sizes. If the HDD sizes are not appropriate resize the disks manually. For more information about the disk sizes, see *Supported footprints of Session Manager*.

- Click **Save** to save the reservation changes.

**Note:**

Ensure that the virtual machine is powered down to edit the settings.

15. To ensure that the virtual machine automatically starts after a hypervisor reboot, click the VM radio option, and click **Actions** > **Autostart** > **Enable**.

**Note:**

If you do not enable autostart, manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.

16. To start the virtual machine, if application is not already powered on, perform one of the following steps:
    - Click the VM radio option and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine and click **Power** > **Power On**.
    - Navigate to **Host** > **Virtual Machines**, select the virtual machine and click **Actions** > **Power** > **Power On**.

    The system starts the application virtual machine. When the system starts for the first time, configure the parameters for the application.
17. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the application configuration parameters.

**Related links**

Reconfiguring hardware resources for flexible footprint on page 104

# Deploying the Session Manager and Branch Session Manager OVA using Solution Deployment Manager

## About this task

Use this procedure to deploy Session Manager or Branch Session Manager by using Solution Deployment Manager.

## Before you begin

To deploy Session Manager or Branch Session Manager by using Solution Deployment Manager, you must have System Manager.

- If System Manager Solution Deployment Manager is not available, install the Solution Deployment Manager client. Always use the latest version of Solution Deployment Manager and Solution Deployment Manager client.

- Add a location.
- Add the ESXi, vCenter, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300 host.

  You can deploy an edge Branch Session Manager only on an Avaya Solutions Platform S8300 that is deployed on an S8300E card.

  **Note:**

  Use the FQDN when you replace the existing Appliance Virtualization Platform with Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the Solution Deployment Manager. Do not add an ASP S8300 Release 5.1 host using the IP address.

## Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ( ).
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Host <host name> section, click **New**.

   System Manager displays the Applications Deployment window.
4. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      Solution Deployment Manager displays the host name in the **Platform FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The Capacity Details section displays the capacity details.
6. Click **Next**.
7. To get the OVA file, select the **OVA** tab, and click one of the following:
   - **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the application OVA file.
   - **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the following message: `Invalid file content. Avaya Certificate not found or invalid`
8. In **Flexi Footprint**, select the footprint size that the application supports.

9. **(Optional)** To install the patch file, click **Service or Feature Pack**, and enter the appropriate parameters.
   - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
   - **S/W Library**, and select the latest service or feature pack from the drop-down list.
   - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

   You can install the patch file now or after completing the Session Manager OVA deployment.

   **Important:**

   If the **Service or Feature Pack** tab is disabled, install the patch file after completing the OVA deployment.
10. Click **Next**.

    In Configuration Parameters and Network Parameters sections, Solution Deployment Manager displays the fields that are specific to the application that you deploy.
11. In the Network Parameters section:

    For the ESXi host or Avaya Solutions Platform 130, select the required port groups.
12. In the Configuration Parameters section, complete the fields.

    For more information, see “Application Deployment field descriptions”.
13. Click **Deploy**.
14. Click **Accept the license terms**.

    In the Platforms for Selected Location <location name> section, Solution Deployment Manager displays the deployment status in the **Current Action Status** column.

    Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.
15. To view details, click the **Status Details** link.

# Application Deployment field descriptions

## Select Location and Platform

| Name | Description |
|---|---|
| **Select Location** | The location name. |
| **Select Platform** | The platform name that you must select. |
| **Platform FQDN** | The platform FQDN. |
| **Data Store** | The data store for the application.<br>The page populates the capacity details in the Capacity Details section. |

### Capacity Details

The system displays the CPU and memory details of the ESXi host. The fields are read-only.

**Note:**

If the host is in a cluster, the system does not display the capacity details of CPU and memory. Ensure that the host resource requirements are met before you deploy the virtual machine.

| Name | Description |
|---|---|
| **Name** | The resource name. |
| **Full Capacity** | The maximum capacity. |
| **Free Capacity** | The available capacity. |
| **Reserved Capacity** | The reserved capacity. |
| **Status** | The configuration status. |

### Provide admin and root Credentials

The system displays the Provide admin and root Credentials section for OS.

| Name | Description |
|---|---|
| **Platform IP** | The platform IP. |
| **Platform FQDN** | The platform FQDN. |
| **Admin User of OS** | The admin username of OS. |
| **Admin Password of OS** | The admin password of OS. |
| **Root User of OS** | The root user of OS. |

### OVA Details

| Name | Description |
|---|---|
| **Application Name** | The name of the application. |
| **ME Deployment** | The option to perform the Midsize Enterprise deployment.<br>The option is available only while deploying Communication Manager simplex OVA. |
| **URL** | The option to specify the URL or absolute path from where you can get the OVA or ISO file. |
| **OVA from software library** | The option to specify the software library where the OVA or ISO file is saved. |
| **Select Software Library** | The default path provided during the installation of the Solution Deployment Manager client. The default path is `C:\Program Files\Avaya\SDMClient\Default_Artifacts`.<br>The field is available only when you click **OVA from software library**. |
| **Browse** | The option to specify the location from where you can get the OVA or ISO file. |

*Table continues…*

| Name | Description |
|---|---|
| **Select OVA** | The URL or absolute path to the OVA or ISO file of the application that you must provide. For example, `C:\Program Files\SDM\<Application OVA_10.2.x.ova>`<br>The field is available only when you click **Browse**.<br>**Note:**<br>System Manager validates any file that you upload during deployment and accepts only the OVA or ISO file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.<br>When you select **OVA from software library**, you can select the OVA or ISO file of the application that you want to deploy. |
| **Submit File** | The field is available only when you click **Browse**.<br>Selects the OVA or ISO file of the application that you want to deploy. |
| **Flexi Footprint** | The footprint size supported for the selected application.<br>**Important:**<br>• Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.<br>• Ensure that the application contains the footprint size values that are supported. |

## Enhanced Access Security Gateway (EASG) - EASG User Access

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

## System Time Settings

| Name | Description |
|---|---|
| **Timezone** | The timezone where the application is located.<br>This field is not applicable for software-only deployment. |

*Table continues…*

| Name | Description |
|---|---|
| **NTP Server(s)** | The IP address or FQDN of the NTP server.<br>Separate the IP addresses with commas (,). You can provide up to four IP Addresses.<br>This field is not applicable for software-only deployment.<br>The application supports only the NTP server. It does not support the NTP pool. |

## DNS Settings

| Name | Description |
|---|---|
| **DNS Server(s)** | The DNS IP address of the virtual machine.<br>Separate the IP addresses with commas (,). You can provide up to three IP Addresses. |
| **Search Domain List** | The search list of domain names. For example, mydomain.com.<br>Separate the search list names with commas (,). |

## System Manager Setting

| Name | Description |
|---|---|
| **Primary System Manager IP** | The IP Address of the primary System Manager server. |
| **Enrollment Password** | The enrollment password. |
| **Confirm Password** | The enrollment password to re-enter. |

## Branch Session Manager Settings

| Name | Description |
|---|---|
| **Edge Topology BSM** | The option to select the edge Branch Session Manager setup.<br>To deploy the edge Branch Session Manager, select this check box. |
| **LSP IP** | The IP Address of the Communication Manager Survivable Remote Server (SRS). |

## Login Settings

| Name | Description |
|---|---|
| **Customer Account User Login** | The customer account username to log in. |
| **Customer Account User Password** | The customer account password to log in. |
| **Confirm Password** | The customer account password to re-enter. |

## Data Encryption

**Note:**

Data Encryption is supported only for Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware Virtualized Environment.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

| Name | Description |
|---|---|
| **Data Encryption** | Enables or disables the data encryption.<br>The options are:<br>• **1**: To enable the data encryption.<br>• **2**: To disable the data encryption.<br>**Important:**<br>• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.<br>• While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.<br>• **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase.<br>• **On vCenter or ESXi:** When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields. |
| **Encryption Pass-Phrase** | This field is applicable when data encryption is enabled.<br>The passphrase for data encryption.<br>When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.<br>When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules. |
| **Re-enter Encryption Pass-Phrase** | The passphrase for data encryption. |

*Table continues…*

| Name | Description |
|---|---|
| **Require Encryption Pass-Phrase at Boot-Time** | If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected.<br>**Important:**<br>You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application.<br>If you lose the data encryption passphrase, the only option is to reinstall the OVA.<br>If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure.<br>You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application. |

## Customer Root Account

**Note:**

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using vSphere Client (HTML5).
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

| Name | Description |
|---|---|
| **Enable Customer Root Account for this Application** | Enables or disables the customer root account for the application.<br>Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**.<br>When you accept the root access statement, the system displays the **Customer Root Password** and **Re-enter Customer Root Password** fields. |
| **Customer Root Password** | The root password for the application |
| **Re-enter Customer Root Password** | The root password for the application |

## Network Parameters

When you deploy the application on VMware, the system displays the Select a Network Mapping for VM Network Interfaces section.

| Name | Description |
|---|---|
| **Public** | The port number that is mapped to public port group.<br>You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional. |
| **Out of Band Management** | The port number that is mapped to the out of band management port group. |

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

# Configuring the virtual machine automatic startup settings on VMware

## About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software does not use the startup selections.

## Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

## Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Manage**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Edit**.

   The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

# Configuring the virtual machine automatic startup settings using vSphere

### About this task

Use this procedure to configure the virtual machine automatic startup settings using vSphere.

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software overlooks the startup selections.

### Before you begin

- Get appropriate permissions from the system administrator to configure the automatic startup settings.
- Ensure **Autostart** is enabled for the virtual machine.

### Procedure

1. On your web browser, type the host IP address to access the VMware Host Client.
2. On the Welcome page, click **Open the VMware Host Client**.
3. Type your **Username** and **Password**, and click **Log in**.
4. On the VMware ESXI home page, in the navigation pane under **Navigator**, click **Virtual Machines**.

   The web client displays a list of available virtual machines in the left panel.
5. Click a virtual machine, and then click the **Actions** tab.
6. Hover on the **Autostart** option, and click **Increase priority**.
7. Click **Save** and wait until the virtual machine finishes the configuration procedure.

# Configuring Session Manager

### About this task

Use this procedure only if you have deployed Session Manager OVA using vSphere Web Client connected directly to the VMware host and Session Manager is not yet configured.

If you deployed the Session Manager OVA using vCenter or the Solution Deployment Manager, skip this procedure and continue to the post-deployment activities.

You are prompted for setup information during the first boot.

### Procedure

1. Verify that System Manager is configured and operational.

2. Right-click the Session Manager virtual machine and select **Open Console**.
3. Configure Session Manager:
   a. At each prompt, enter the appropriate information from the Customer Configuration Data worksheet.
   b. Verify your settings.
   c. Enter the enrollment password.

      The system starts the configuration process. The process takes approximately 15 minutes to complete.

# Survivable Remote Server

In a survivable remote environment, each IP endpoint and each H.248 media gateway is manually configured with a list of call controllers during initialization. If for any reason, the communication between an H.248 media gateway and its primary controller stops, the H.248 media gateways and the IP endpoints register with a call controller on its list. If the Survivable Remote Server (SRS), formerly known as Local Survivable Processor (LSP), is in the list of call controllers, the H.248 media gateway and the IP endpoint registers with the SRS. The H.248 media gateway registers with the SRS first before the IP telephone registers with the SRS.

The Processor Ethernet (PE) interface on the SRS is used for:

- Connectivity to three adjuncts: Call Detail Recording (CDR), Application Enablement Services (AE Services), and Call Management System (CMS)
- H.323 and H.248 registration

For more information about Local Survivable Processor and deployment see, *Avaya Aura® Communication ManagerSurvivability Options* and *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

# patchSM command

From Release 10.2, the **patchSM** command is enhanced to take the snapshot while installing the Session Manager or Branch Session Manager patch in a virtualized environment.

**Note:**

The **patchSM** command is not available in a Software-Only environment.

## Syntax

```
patchSM [-i <patch>] [-s <patch>] [-v <patch>] [-r <patch ID>] [-c <patch ID>] [-d]
[--snapshot]
```

| | |
|---|---|
| **-i <patch>** | Installs the provided patch file. This is the default option if you just provide a patch file. |
| **-s <patch>** | Displays the patch status information.<br>The -s option with the patch file displays information about the latest installed patch.<br>The -s option without providing the patch file displays information about all currently installed patches. |
| **-v <patch>** | Verifies that the patch can be installed on current version of Session Manager. |
| **-r <patch ID>** | Removes the patch that matches with the provided patch ID. |
| **-c <patch ID>** | Moves the patch from the pending state to installed by removing the associated snapshot. |
| **-d, --debug** | Turn on debug logging |
| **--snapshot** | Creates a snapshot before applying the patch. |

# Installing software patches

### About this task

Use the procedure to install the software patches for Session Manager.

### Procedure

1. Log in to Session Manager and copy the 10.2.*.bin file.
2. On the Session Manager Dashboard page, change the **Service State** of the Session Manager server to **Deny New Service**.
3. To upgrade to Release 10.2.x, run the following command:

   **`patchSM Session_Manager_10.2.*.bin`**
4. Verify the patch installation and version using the command: **`swversion`**
5. After Session Manager upgrades successfully, on the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Accept New Service**.

# Installing a Session Manager or Branch Session Manager patch with the snapshot option

### About this task

From Release 10.2, use this procedure to install the software patches of Session Manager or Branch Session Manager with the snapshot option.

### Procedure

1. Log in to Session Manager command-line interface and copy the 10.2 bin file.
2. On the Session Manager Dashboard page, change the **Service State** of the Session Manager server to **Deny New Service**.
3. Type the command **`patchSM -i Session_Manager_10.2.0.0.xxxxxx.bin --snapshot`**

   Session Manager displays the following message:

   ```
   The system will be rebooted after the patch is applied.

   Do you wish to continue (y/n)?
   ```
4. At the prompt, type `y`.
5. In **ESXi host address**, type the IP address of the ESXi host.
6. In **ESXi username**, type the user name of the ESXi host.
7. In **ESXi password**, type the password of the ESXi host.

   Session Manager displays the following message:

   ```
   Snapshot complete

   Stopping Session Manager before installing patch.
   ```

   Session Manager applies the patch.
8. To commit the Session Manager patch, type the command: `patchSM -c 10.2.0.0`

   Perform this step when Session Manager is stable.

   Session Manager commits the patch and removes the snapshot.
9. Check the patch installation and version using the command: **`swversion`**
10. After Session Manager upgrades successfully, on the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Accept New Service**.

# Chapter 5: Deploying Session Manager and Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

## Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit

### About this task

Session Manager requires two network interfaces.

Session Manager provides OVA that contains SM.qcow2 file.

**Note:**

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

### Before you begin

Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.

Deployment of applications *MUST* be performed one at a time and artifacts cleaned up/removed prior to deploying then next application.

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

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the SM KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **`custadm`** credentials.
- Run the command **`sudo ls -ld /var/lib/libvirt/images`** to check to see the staging folder `/var/lib/libvirt/staging`.

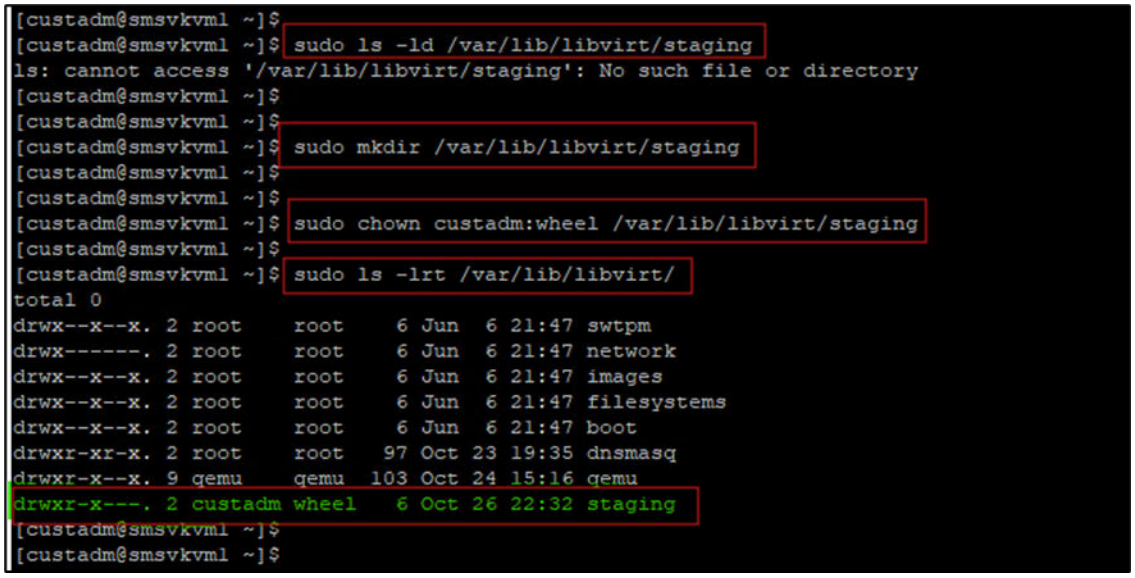
  Verify if there is sufficient space in the staging folder to copy the KVM image. Ensure to remove the older images from the staging folder.

  If the staging folder does not exist, create it using the following commands:
- `sudo mkdir /var/lib/libvirt/staging`

  `sudo chown custadm:wheel /var/lib/libvirt/staging`

- Verify file permissions. The `sudo chown custadm:wheel /var/lib/libvirt/staging` command allows the **`custadm`** to write into this directory with sudo. The permissions appear as seen below:

  `drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging`




- Copy the Session Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **`custadm`** credentials.
- If not still in the CLI, login again to the ASP R6.0.x CLI with **`custadm`** credentials.

**Important:**

Preface the following commands with **`sudo`**.

- Run the following command to verify the Session Manager KVM image available in the staging folder: **`sudo ls -lr /var/lib/libvirt/staging`**
- Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: **`Sudo tar -xvf SM-x.x.x.x.x-kvm-0x.ova`**

  KVM OVA file extracts the following files:

  - SM.ovf
  - SM.mf
  - SM.qcow2

SM has different profiles but one image. The disk size may need to be resized based on the SM profile that will be deployed:

- P1 & P2 will have the same disk size 100GB not required to resize
- P3 & P4 requires 135 GB, required to resize the disk from 100GB to 135 GB with following command `sudo qemu-img resize SM.qcow2 +35G`
- P5 & P6 requires 210 GB, required to resize the disk from 100GB to 210 GB with following command `sudo qemu-img resize SM.qcow2 +110G`

  The extracted qcow2 images are in thin provision format. The qcow2 images *MUST* be converted to thick provision. Ensure you are in the `/var/lib/libvirt/staging` directory before the next steps. When running the commands to convert to thick provision, a unique identifier can be added to the new qcow2 image. Avaya recommends to use VM name as a unique identifier. For example:

  ```
  SMx.x[unique identifier]-system.qcow2
  ```

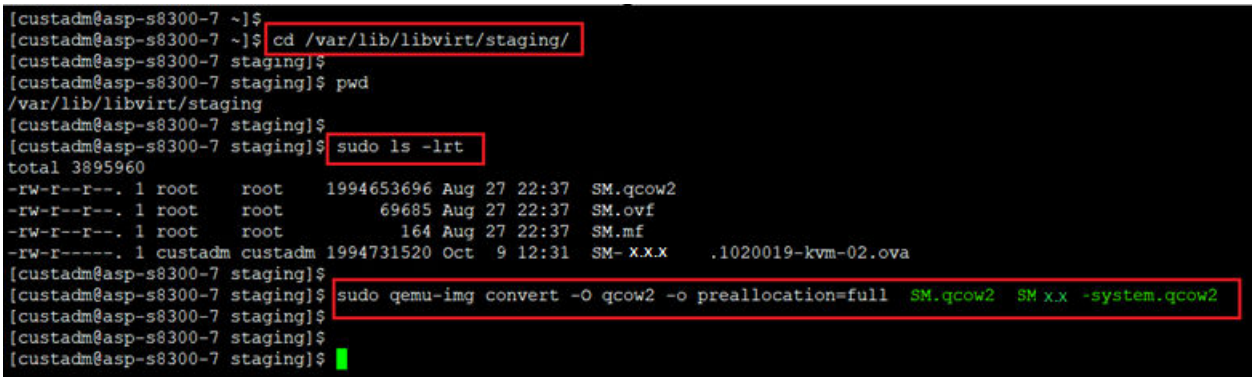
  The examples in this document will simply use the following:

  ```
  SMx.x-system.qcow2
  ```

- Convert SM.qcow2 (thin) to SMx.x-system.qcow2 (thick)

  ```
  sudo qemu-img convert -O qcow2 -o preallocation=full SM.qcow2
  ```

  ```
  SMx.x-system.qcow2
  ```



To verify that the conversion is successful and to verify the disk size, run the command **sudo qemu-img info SMx.x-system.qcow2**.

Disk size is displayed based on the profile.

- P1, P2 = 100GB
- P3, P4 = 135GB
- P5, P6 = 210GB

```
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 56333020
-rw-r--r--. 1 root    root     1994653696 Aug 27 22:37  SM.qcow2
-rw-r--r--. 1 root    root          69685 Aug 27 22:37  SM.ovf
-rw-r--r--. 1 root    root            164 Aug 27 22:37  SM.mf
-rw-r-----. 1 custadm custadm  1994731520 Oct  9 12:31  SM-X.X.0.0.1020019-kvm-02.ova
-rw-r-----. 1 root    root    53695545344 Oct 30 17:51  SM10.2-system.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo qemu-img info SM X.X-system.qcow2
image: SM X.X-system.qcow2
file format: qcow2
virtual size: 50 GiB (53687091200 bytes)
disk size: 50 GiB
cluster_size: 65536
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
    extended l2: false
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

Copy the SMx.x-system.qcow2, to the `/var/lib/libvirt/images` directory. Ensure you are in the `/var/lib/libvirt/staging` directory before performing these steps.

- `sudo cp SMx.x-system.qcow2 /var/lib/libvirt/images`

```
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ pwd
/var/lib/libvirt/staging
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 56333020
-rw-r--r--. 1 root    root     1994653696 Aug 27 22:37  SM.qcow2
-rw-r--r--. 1 root    root          69685 Aug 27 22:37  SM.ovf
-rw-r--r--. 1 root    root            164 Aug 27 22:37  SM.mf
-rw-r-----. 1 custadm custadm  1994731520 Oct  9 12:31  SM-X.X .0.0.1020019-kvm-02.ova
-rw-r-----. 1 root    root    53695545344 Oct 30 17:51  SM X.X system.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo cp  SM X.X system.qcow2 /var/lib/libvirt/images/
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

- Verify the images are present in the `/var/lib/libvirt/images` directory

- **cd /var/lib/libvirt/images**
- **sudo ls -lrt**

```
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ cd /var/lib/libvirt/images/
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ pwd
/var/lib/libvirt/images
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo ls -lrt
total 52437056
-rw-r-----. 1 root root 53695545344 Oct 30 18:28  SM X.X -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$
```

From the `/var/lib/libvirt/images` directory, run the following command to change the owner and permissions to 640 on the files:

- **sudo chown qemu:qemu SMx.x-system.qcow2**
- **sudo chmod 640 SMx.x-system.qcow2**

```
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ cd /var/lib/libvirt/images/
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ pwd
/var/lib/libvirt/images
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo ls -lrt
total 52437056
-rw-r-----. 1 root root 53695545344 Oct 30 18:28  SM X.X -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$
```

Go to `/var/lib/libvirt/staging` directory and remove all the extracted images and converted images from the staging directory to ensure that there is sufficient space for future deployments of KVM images. Do NOT remove files from the *images* directory.

- **cd /var/lib/libvirt/staging**

  **sudo ls -lr**

  **sudo rm *SM***

## Procedure

1. Log in to the KVM Cockpit web console as **custadm** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

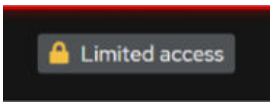



**Figure 1: Limited access button**

**Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

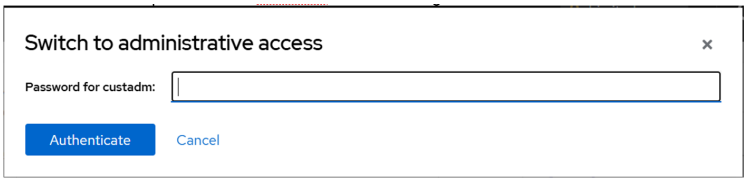



**Figure 2: Switch to administrative access**

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

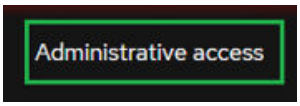



**Figure 3: Administrative access button**

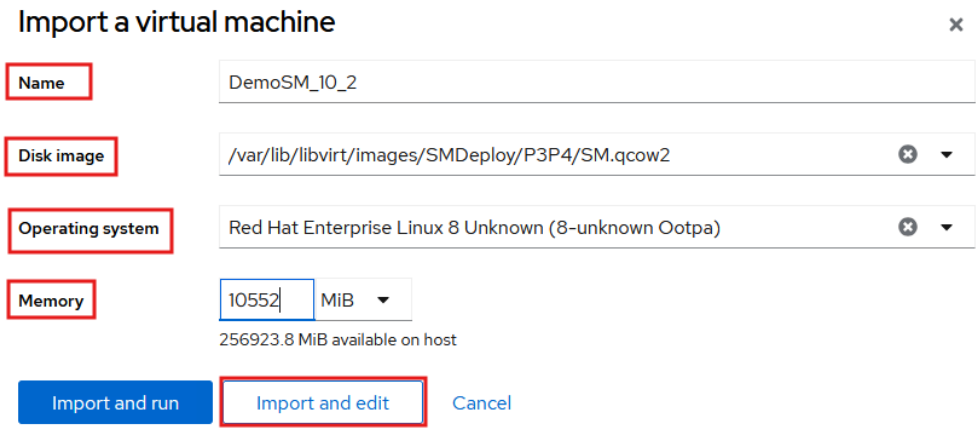
4. Navigate to **System** > **Virtual Machines** > **Import VM**.
5. In the Import a virtual machine window, do the following:
   a. In the **Name** field, enter a name for the Session Manager virtual machine.
   b. In the **Disk Image** field, select the `SMx.x- system.qcow2` image of the Session Manager on the KVM Cockpit host under `/var/lib/libvirt/images/` directory.
   c. In the **Operating System** field, select **RHEL 8** version.
   d. In the **Memory** field, select the required memory in MiB format.

      **Note:**

      Based on the required footprint, enter a value in the **Memory** field.

      For more information on footprints, see Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 19

e. Click **Import and edit**.




Virtual Machine details page appears.

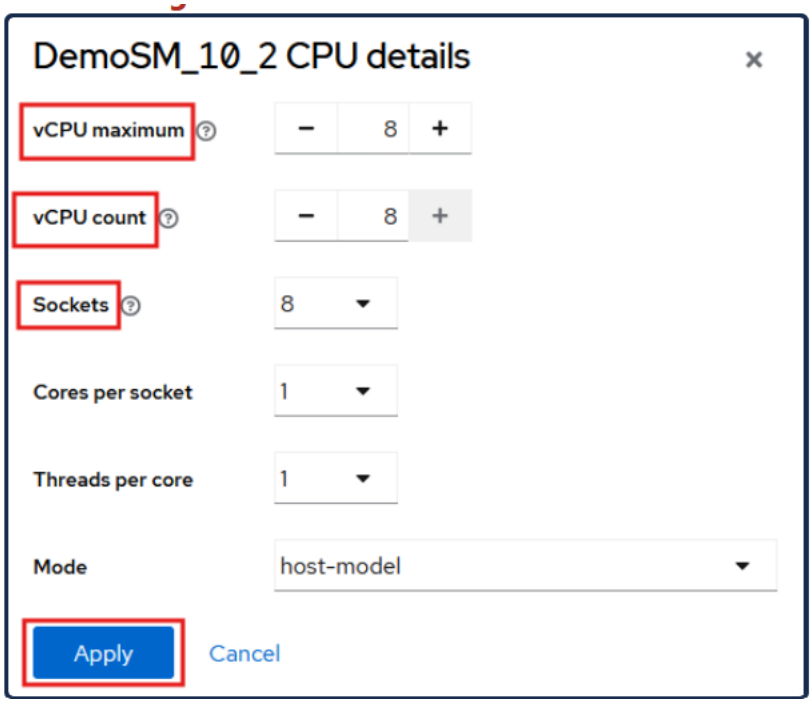
Under the Disks section, verify the `SMx.x.x- system.qcow2` image disk image size is correctly displayed in the **Capacity** field. By default, **virtio** is selected under the **Bus** field, and this needs to be modified.

6. Under the Disks section, click **Edit**.
7. In the Edit <attributes name> window, do the following:
   a. in the **Bus** field, select **scsi**.
   b. In the **Cache** field, select **directsync**.
   c. click **Save**.

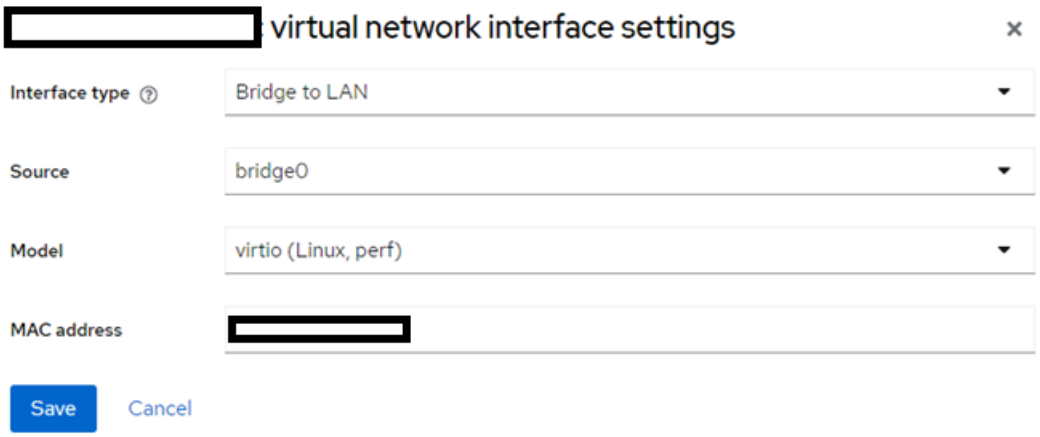
   In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.
8. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
9. In the Overview section, in the **CPU** field, click **edit**.

   CPU Details window opens.
10. In the CPU details window, based on the required footprint, enter a value in the **vCPU Maximum** and **vCPU Count** fields.

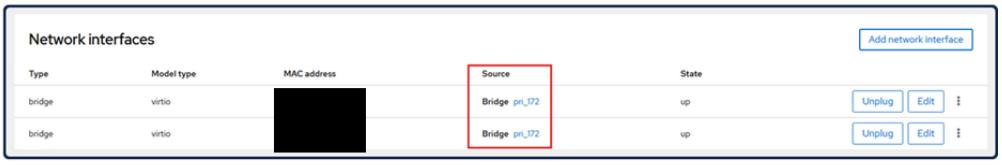
    For more information on footprints, see Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 19.



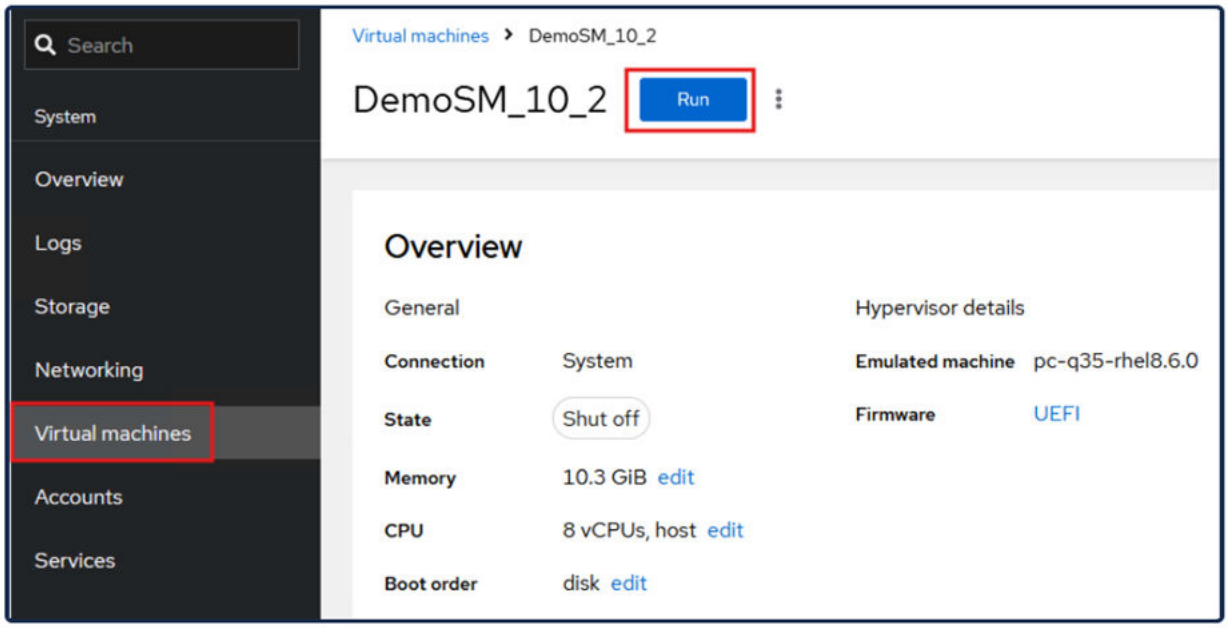

11. Select the default **host-model** mode.
12. Click **Apply**.
13. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.
    Session Manager requires two NICs
    - NIC1 is for the Management IP
    - NIC2 is for the Asset IP



14. To add more network interfaces, under the Network interfaces section, click **Add network interface** and do the following:
    a. In the **Interface type** field, select **Bridge to LAN**.
    b. From the **Source** field, select the required network bridge.
    c. Click **Add**.




15. On the virtual machine, click **Run** to start the Session Manager virtual machine.




### Next steps

On first boot of the Session Manager configure the virtual machine, network properties and follow the Session Manager deployment guide.

# Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit

### About this task

Branch Session Manager requires two network interfaces.

Branch Session Manager has 2 different profiles, Profile 1 supports/recommended to deploy on S8300E card and Profile 2 supports/recommended to deploy on Dell R640 and R660xs Servers.

Branch Session Manager provides OVA that contains bsm.qcow2 file.

**Note:**

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

### Before you begin

Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.

Deployment of applications *MUST* be performed one at a time and artifacts cleaned up/removed prior to deploying then next application.

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

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

- Download the BSM KVM image from PLDS to your computer.
- Log in to the ASP R6.0.x CLI with **`custadm`** credentials.
- Ensure that the staging folder exists: `/var/lib/libvirt/staging`.

  ```
  sudo ls -ld /var/lib/libvirt/images
  ```

  Ensure to remove the older images from the staging folder.

  Ensure sufficient space is available in the staging folder to copy the KVM image.

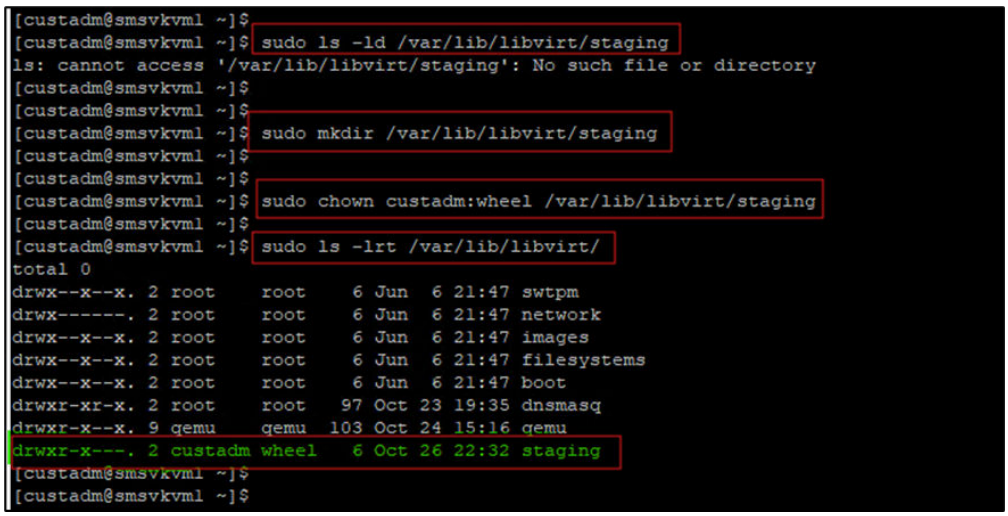
  If the staging folder does not exist, create it using the following commands:

- `sudo mkdir /var/lib/libvirt/staging`

  ```
  sudo chown custadm:wheel /var/lib/libvirt/staging
  ```

- Verify file permissions. The above `sudo chown custadm:wheel /var/lib/libvirt/staging`command enables the **`custadm`** to write into this directory with sudo. The permissions must appear as seen below:

  ```
  drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
  ```




- Copy the Branch Session Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **`custadm`** credentials.
- If not still in the CLI, login again to the ASP R6.0.x CLI with **`custadm`** credentials.

**Important:**

Preface the following commands with **`sudo`**.

- Run the following command to verify the Branch Session Manager KVM image available in the staging folder: **`sudo ls -lr /var/lib/libvirt/staging`**
- Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: **`Sudo tar -xvf SM-x.x.x.x.x-kvm-0x.ova`**

  The command extracts the following files:

  - BSM.ovf
  - BSM.mf
  - BSM.qcow2

```
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ sudo ls -lrt /var/lib/libvirt/staging/
[sudo] password for custadm:
total 1947980
-rw-r-----. 1 custadm custadm 1994731520 Oct  9 12:31 BSM- x.x.x    .1020019-kvm-02.ova
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ cd /var/lib/libvirt/staging/
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ pwd
/var/lib/libvirt/staging
[custadm@asp-s8300-7 staging]$ sudo tar -xvf BSM- x.x.x    .1020019-kvm-02.ova
BSM.ovf
BSM.mf
BSM.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

- The extracted qcow2 images are in thin provision format. The qcow2 images *must* be converted to thick provision. Ensure you are in the `/var/lib/libvirt/staging` directory before the next steps. When running the commands to convert to thick provision, a unique identifier can be added to the new qcow2 image. Avaya recommends to use VM name as a unique identifier. For example:

  `BSMx.x[unique identifier]-system.qcow2`

  The examples in this document will simply use the following:

  `BSMx.x-system.qcow2`

- Convert BSM.qcow2 (thin) to BSMx.x-system.qcow2 (thick)

  `sudo qemu-img convert -O qcow2 -o preallocation=full BSM.qcow2`

  `BSMx.x-system.qcow2`

```
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ cd /var/lib/libvirt/staging/
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ pwd
/var/lib/libvirt/staging
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 3895960
-rw-r--r--. 1 root    root    1994653696 Aug 27 22:37 BSM.qcow2
-rw-r--r--. 1 root    root         69685 Aug 27 22:37 BSM.ovf
-rw-r--r--. 1 root    root           164 Aug 27 22:37 BSM.mf
-rw-r-----. 1 custadm custadm 1994731520 Oct  9 12:31 BSM- x.x.x    .1020019-kvm-02.ova
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo qemu-img convert -O qcow2 -o preallocation=full BSM.qcow2 BSM x.x. -system.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

To verify that the conversion is successful and to verify the disk size, run the following commands:

- sudo qemu-img info BSMx.x-system.qcow2

  Disk size must be displayed based on the profile. 50GB

Copy BSMx.x-system.qcow2, to the `/var/lib/libvirt/images` directory. Ensure you are in the `/var/lib/libvirt/staging` directory before performing these steps.

- `sudo cp BSMx.x-system.qcow2 /var/lib/libvirt/images`

```
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ pwd
/var/lib/libvirt/staging
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 56333020
-rw-r--r--. 1 root    root     1994653696 Aug 27 22:37 BSM.qcow2
-rw-r--r--. 1 root    root          69685 Aug 27 22:37 BSM.ovf
-rw-r--r--. 1 root    root            164 Aug 27 22:37 BSM.mf
-rw-r-----. 1 custadm custadm  1994731520 Oct  9 12:31 BSM-X.X.X.X.1020019-kvm-02.ova
-rw-r-----. 1 root    root    53695545344 Oct 30 17:51 BSM X.X-system.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo cp BSM X.X-system.qcow2 /var/lib/libvirt/images/
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

- Verify the images are present in the `/var/lib/libvirt/images` directory.
- cd /var/lib/libvirt/images
- sudo ls -lrt

```
[custadm@asp-s8300-7 ~]$
[custadm@asp-s8300-7 ~]$ cd /var/lib/libvirt/images/
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ pwd
/var/lib/libvirt/images
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo ls -lrt
total 52437056
-rw-r-----. 1 root root 53695545344 Oct 30 18:28 BSM X.X -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$
```

From the `/var/lib/libvirt/images` directory, run the following commands to change the owner and permissions to 640 on the files:

- sudo chown qemu:qemu BSMx.x-system.qcow2

  sudo chmod 640 BSMx.x-system.qcow2

```
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ pwd
/var/lib/libvirt/images
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo ls -lrt
total 52437056
-rw-r-----. 1 root root 53695545344 Oct 30 18:28 BSM x.x  -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo chown qemu:qemu BSM x.x  -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo chmod 640 BSM x.x  -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ sudo ls -lrt
total 52437056
-rw-r-----. 1 qemu qemu 53695545344 Oct 30 18:28 BSM x.x -system.qcow2
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$
```

Go to /var/lib/libvirt/staging directory and remove all the extracted images and converted images. This is important to ensure that there is sufficient space for future deployments of KVM images. Do NOT remove files from the *images* directory.

- cd /var/lib/libvirt/staging

  sudo ls -lr

  sudo rm *BSM*

```
[custadm@asp-s8300-7 images]$
[custadm@asp-s8300-7 images]$ cd /var/lib/libvirt/staging/
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 56333020
-rw-r--r--. 1 root    root     1994653696 Aug 27 22:37 BSM.qcow2
-rw-r--r--. 1 root    root          69685 Aug 27 22:37 BSM.ovf
-rw-r--r--. 1 root    root            164 Aug 27 22:37 BSM.mf
-rw-r-----. 1 custadm custadm  1994731520 Oct  9 12:31 BSM- x.x.x.x  .1020019-kvm-02.ova
-rw-r-----. 1 root    root    53695545344 Oct 30 17:51 BSM x.x -system.qcow2
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo rm *BSM*
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$ sudo ls -lrt
total 0
[custadm@asp-s8300-7 staging]$
[custadm@asp-s8300-7 staging]$
```

## Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

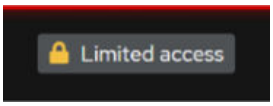



**Figure 4: Limited access button**

**Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

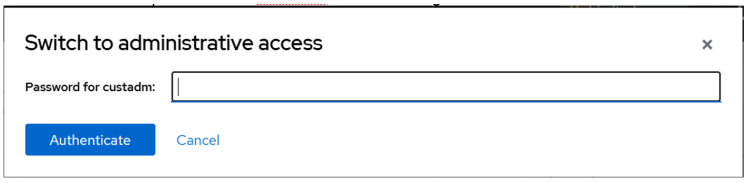



**Figure 5: Switch to administrative access**

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

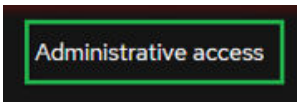



**Figure 6: Administrative access button**

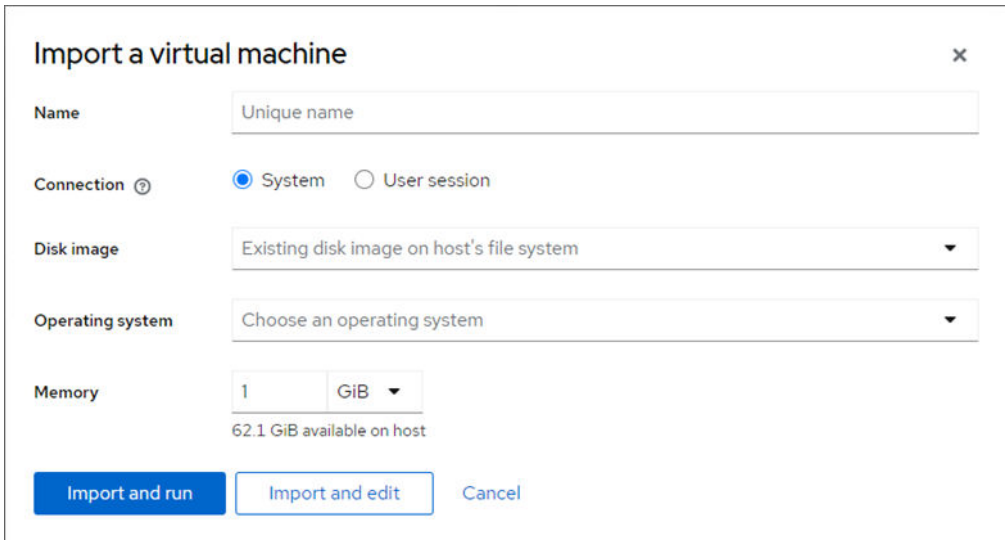
4. Navigate to **System** > **Virtual Machines** > **Import VM**.
5. In the Import a virtual machine window, do the following:
   a. In the **Name** field, enter a name for the Session Manager virtual machine.
   b. In the **Disk Image** field, select the `BSMx.x- system.qcow2` image of the Session Manager on the KVM Cockpit host under `/var/lib/libvirt/images/` directory.
   c. In the **Operating System** field, select **RHEL 8** version.
   d. In the **Memory** field, select the required memory in MiB format.

      **Note:**

      Based on the required footprint, enter a value in the **Memory** field.

      For more information on footprints, see Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 20.

e. Click **Import and edit**.

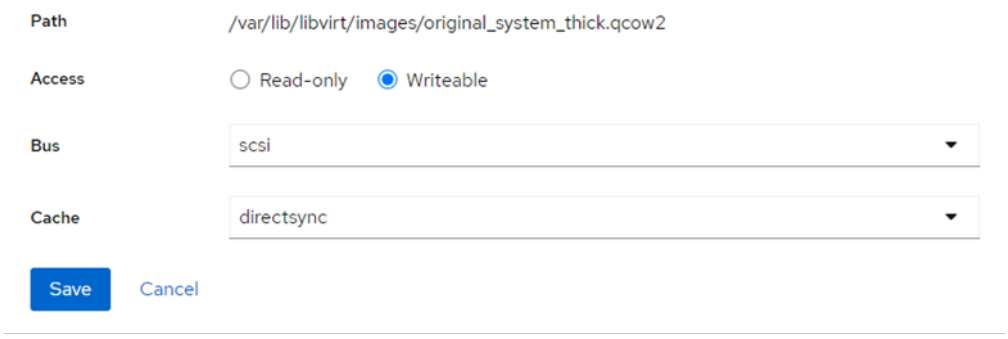



Virtual Machine details page appears.

Under the Disks section, verify the `BSMx.x- system.qcow2` image disk image size is correctly displayed in the **Capacity** field. By default, **virtio** is selected under the **Bus** field, and this needs to be modified.

6. Under the Disks section, click **Edit**.
7. In the Edit <attributes name> window, do the following:
   a. in the **Bus** field, select **scsi**.
   b. In the **Cache** field, select **directsync**.
   c. click **Save**.

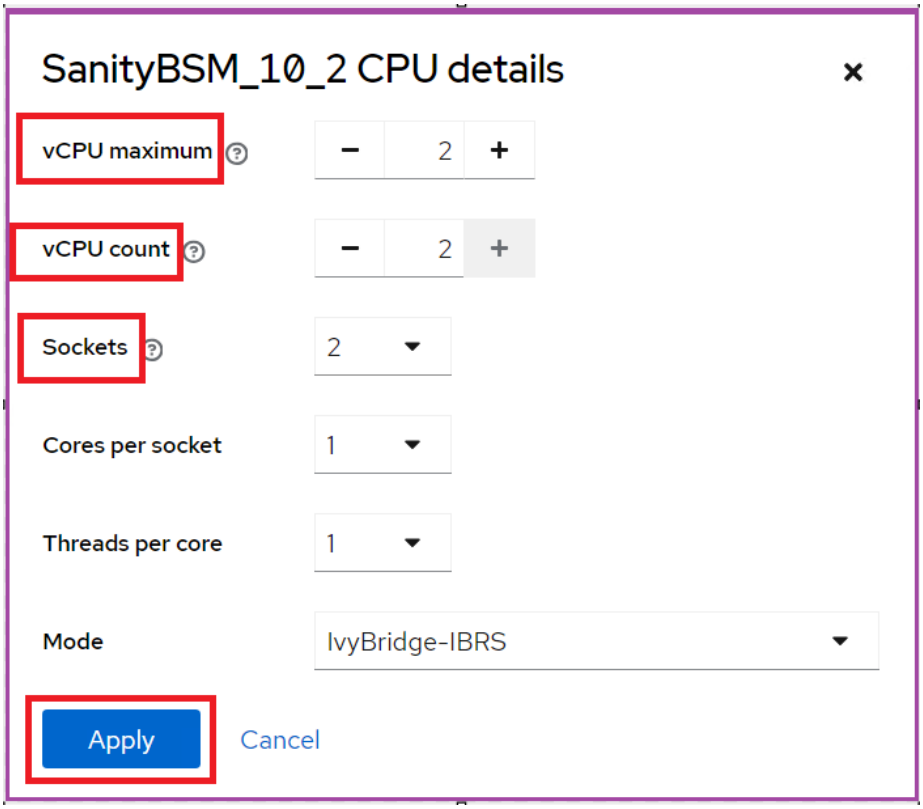
   In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.




8. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
9. In the Overview section, in the **CPU** field, click **edit**.

   CPU Details window opens.

10. In the CPU details window, based on the required footprint, enter a value in the **vCPU Maximum** and **vCPU Count** fields.




For more information on footprints, see Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 20.

11. Select the default **IvyBridge-IBRS** mode. Do not change this value.
12. Click **Apply**.
13. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.

    Session Manager requires two NICs

    - NIC1 is for the Management IP
    - NIC2 is for the Asset IP

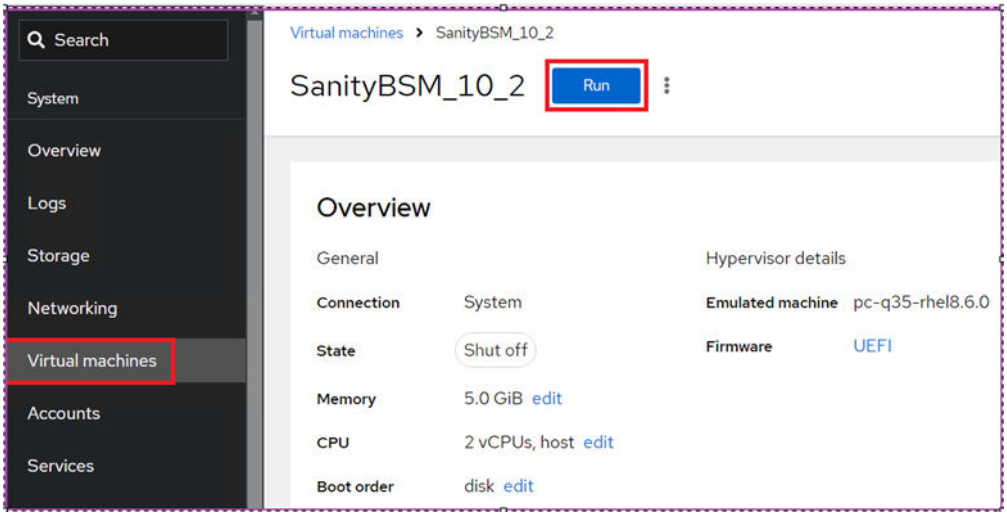
14. To add more network interfaces, under the Network interfaces section, click **Add network interface** and do the following:

    a. In the **Interface type** field, select **Bridge to LAN**.

    b. From the **Source** field, select the required network bridge.

c. Click **Add**.

15. On the virtual machine, click **Run** to start the Session Manager virtual machine.




### Next steps

On first boot of the Session Manager configure the virtual machine, network properties and follow the Session Manager deployment guide.

# Deploying Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script

### About this task

Session Manager provides a KVM OVA that contains SM.qcow2 file.

**Note:**

- Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.
- Deployment of applications *MUST* be performed one at a time and delete the artifacts prior to deploying the next application.

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

## Before you begin

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

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the Session Manager KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **custadm** credentials.
- Ensure that the staging folder exist:

  **sudo ls -ld /var/lib/libvirt/staging**
- Ensure to remove the older images from the staging folder.
- Ensure sufficient space is available in the staging folder to copy the KVM image.
- If the staging folder does not exist, create it using the following commands:

  **sudo mkdir /var/lib/libvirt/staging**

  **sudo chown custadm:wheel /var/lib/libvirt/staging**

  **sudo ls -lrt /var/lib/libvirt/**
- Verify file permissions. The chown command now allows **custadm** to write into the staging directory with **sudo**. For example, the permissions should look as follows:

```
drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
```

```
[custadm@      kvm1 libvirt]$
[custadm@      kvm1 libvirt]$ sudo ls -ld /var/lib/libvirt/staging
ls: cannot access '/var/lib/libvirt/staging': No such file or directory
[custadm@      kvm1 libvirt]$
[custadm@      kvm1 libvirt]$ sudo mkdir /var/lib/libvirt/staging
[custadm@      kvm1 libvirt]$
[custadm@      kvm1 libvirt]$ sudo chown custadm:wheel /var/lib/libvirt/staging
[custadm@      kvm1 libvirt]$
[custadm@      kvm1 libvirt]$ sudo ls -lrt /var/lib/libvirt/
total 8
drwx--x--x.  2 root    root     6 Jun  6 21:47 swtpm
drwx------.  2 root    root     6 Jun  6 21:47 network
drwx--x--x.  2 root    root     6 Jun  6 21:47 filesystems
drwx--x--x.  2 root    root     6 Jun  6 21:47 boot
drwxr-xr-x.  2 root    root    97 Oct 29 11:26 dnsmasq
drwxr-x--x. 13 qemu    qemu  4096 Oct 29 17:40 qemu
drwx--x--x.  2 root    root  4096 Oct 30 14:42 images
drwxr-x---.  2 custadm wheel    6 Oct 30 14:43 staging
[custadm@      kvm1 libvirt]$
```

- Copy the Session Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **custadm** credentials.
- Run the following command to verify the Session Manager KVM image is available in the staging folder:

  **sudo ls -lr /var/lib/libvirt/staging**.

## Procedure

1. Log in to the ASP R6.0.x CLI as a **custadm** user and verify the ASP version using the following command: **swversion**
2. Go to the staging folder;

   **sudo cd /var/lib/libvirt/staging**
3. Do the following:

| ASP is on R6.0.0.0 | ASP is on R6.0.0.1 |
|---|---|
| a. Run the following command to extract the OVA file: **sudo tar -xvf SM-*.ova**<br><br>KVM OVA extracts the following files:<br>• SM.ovf<br>• SM.mf<br>• SM.cert<br>• install_vm.py<br>• ovf.py<br>• SM.qcow2<br>b. Run the following script to deploy Session Manager:<br><br>**sudo python3 install_vm.py** | Run the following script to deploy Session Manager: **installVM SMKVM-*.ova**<br><br>ASP completes the auto-verification to ensure the following files are available:<br><br>SM.ovf<br>SM.mf<br>SM.cert<br>install_vm.py<br>ovf.py<br>SM.qcow2<br>SM.cert: OK<br>Verified OK<br>SM.ovf: OK<br>install_vm.py: OK<br>ovf.py: OK<br>SM.qcow2: OK |

4. Press **ENTER** to read the **EULA**.
5. Press **Y** to accept the **EULA**.
6. Enter a name for the Session Manager virtual machine. For example, SMonKVM.
7. Select the required Session Manager profile.

   For more information, see Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 19.
8. Select the Public and OOBM network interfaces.

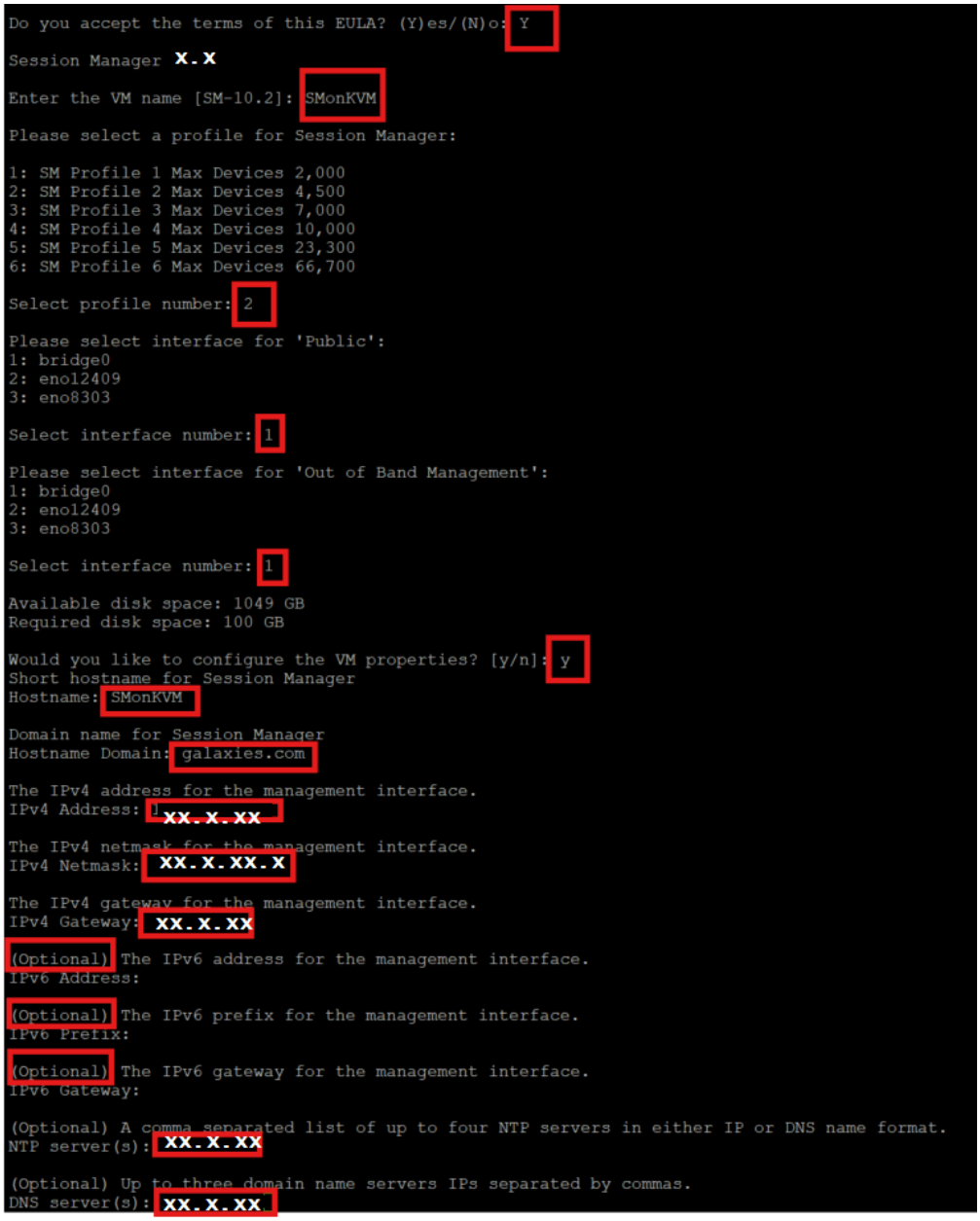
   ASP 6.0.x CLI displays the currently available network interface bridges and select the required bridge for Session Manager.

   ASP 6.0.x CLI displays the currently available disk space and the required disk space to deploy Session Manager.
9. To configure the VM properties, enter **Y** in the **Would you like to configure the VM properties? [y/n]:** field, and continue providing the property details:
   a. In the **Hostname** field, enter a short host name for Session Manager.
   b. In the **Host Domain** field, enter the domain name for Session Manager.
   c. Enter **IPv4 address**. For example, x.x.x.x

d. Enter **IPv4 Netmask**. For example, m.m.m.m
e. Enter **IPv4 Gateway**. For example, g.g.g.g
f. **(Optional)** For **IPv6 address**, enter the valid IPv6 address.
g. **(Optional)** For **IPv6 Network Prefix**, enter the valid IPv6 network prefix.
h. **(Optional)** For **IPv6 Network Gateway**, enter the valid IPv6 network gateway.
i. The **NTP servers**, enter a valid NTP server address in IP or DNS name format.

   You can type up to four NTP servers separated by a comma.
j. The **DNS servers**, enter a valid DNS server IP address.

   You can type up to three DNS servers separated by a comma.
k. The **Search Domain List**, enter a search list of domain names.




10. In the **IP Address of Primary System Manager** field, enter the IP address of the reachable System Manager server.
11. In the **Trust Management Enrollment Password** field, enter the IP address of the password and confirm the Trust Management Enrollment Password.
12. In the **Command line customer account user login** field, enter the customer account user login.
13. In the **Customer account user password** field, enter the password and confirm the Customer account user password.
14. Enable or disable Data Encryption.

By enabling Data Encryption, your Communication Product's Operational data, Configuration data, along with all of the Log Files will be encrypted. You will be prompted to enter a pass-phrase that will be used to create/access an encryption key. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, contact the Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

Enter 1 to Enable Encryption or enter 2 to Disable Encryption.

a. In the **Data Encryption Active** field, if `1` is entered, do the following

   - In the **Enter Encryption Passphrase** field, enter the passphrase.
   - In the **Confirm Enter Encryption Passphrase** field, reenter the passphrase.
   - In the **Require Encryption Passphrase at Boot-Time: (yes/no)**, enter the required value.

   If **1** is entered, you must enter the encryption passphrase whenever the Session Manager reboots.

   If **2** is entered, there is no need to enter the encryption passphrase whenever the Session Manager reboots.

   **Important:**

   *Note* the data encryption passphrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA.

b. In the **Data Encryption Active** field, if `2` is entered, no action is required.

15. Enable or disable Enhanced Avaya Security Gateway (EASG).

    **Important:**

    Avaya recommends to enable **EASG**.

    **Note:**

    Enable: (Recommended)

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

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

    Disable:

By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

- Enter `1` to enable EASG.
- Enter `2` to disable EASG.

16. In the **`Do you want to set a root password?(yes/no)`** field, enter the required value.
17. In the **`Power on VM automatically after deploy?: [y/n]`** field, enter one of the following:
    - **`y`**: Indicates Session Manager virtual machine is automatically powered-on after deployment.
    - **`n`**: Indicates user has to manually power on the Session Manager virtual machine on KVM cockpit.
18. In the **`Proceed?[y/n]`** field, enter one of the following:
    - **`y`**: Session Manager deployment begins.
    - **`n`**: Session Manager deployment cancels.

    **Note:**

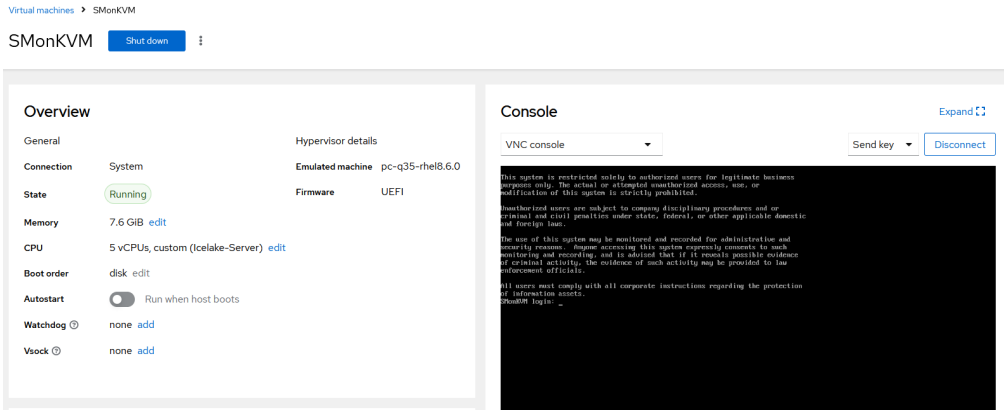
    After the Session Manager virtual machine is successfully deployed, ASP R6.0.x displays the following message: `Domain creation completed`.
19. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
20. If Web console is in **Limited access** mode, click on **Turn on administrative access** button.

    **Note:**

    VMs are not visible when in **Limited access** mode.
21. For administration actions, on the top-right of the window, click on the **Limited access** or **Turn on administrative access** button.
22. Navigate to **System** > **Virtual Machines**.

    The Session Manager is deployed.

23. Click on **VM Name** and login from Console.




# Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script

## About this task

Branch Session Manager provides a KVM OVA that contains BSM.qcow2 file.

**Note:**

- Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.
- Deployment of applications *MUST* be performed one at a time and delete the artifacts prior to deploying the next application.

  Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

## Before you begin

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

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the Branch Session Manager KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **`custadm`** credentials.
- Ensure that the staging folder exist:

  **`sudo ls -ld /var/lib/libvirt/staging`**
- Ensure to remove the older images from the staging folder.
- Ensure sufficient space is available in the staging folder to copy the KVM image.
- If the staging folder does not exist, create it using the following commands:

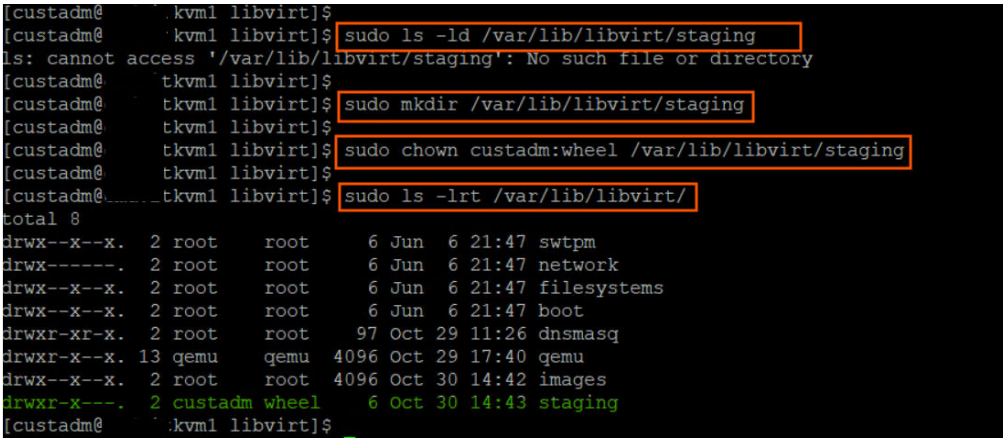
  **`sudo mkdir /var/lib/libvirt/staging`**

**sudo chown custadm:wheel /var/lib/libvirt/staging**

**sudo ls -lrt /var/lib/libvirt/**

- Verify file permissions. The chown command now allows **custadm** to write into the staging directory with **sudo**. For example, the permissions should look as follows:

```
drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
```




- Copy the Branch Session Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **custadm** credentials.
- Run the following command to verify the Branch Session Manager KVM image is available in the staging folder:

  **sudo ls -lr /var/lib/libvirt/staging**.

## Procedure

1. Log in to the ASP R6.0.x CLI as a **custadm** user and verify the ASP version using the following command: **swversion**
2. Go to the staging folder;

   **sudo cd /var/lib/libvirt/staging**
3. Do the following:

| ASP is on R6.0.0.0 | ASP is on R6.0.0.1 |
|---|---|

*Table continues…*

| | |
|---|---|
| a. Run the following command to extract the OVA file: **`sudo tar -xvf BSM-*.ova`**<br>KVM OVA extracts the following files:<br>• BSM.ovf<br>• BSM.mf<br>• BSM.cert<br>• install_vm.py<br>• ovf.py<br>• BSM.qcow2<br>b. Run the following script to deploy Branch Session Manager:<br>**`sudo python3 install_vm.py`** | Run the following script to deploy Branch Session Manager: **`installVM BSMKVM-*.ova`**<br>ASP completes the auto-verification to ensure the following files are available:<br>`BSM.ovf`<br>`BSM.mf`<br>`BSM.cert`<br>`install_vm.py`<br>`ovf.py`<br>`BSM.qcow2`<br>`BSM.cert: OK`<br>`Verified OK`<br>`BSM.ovf: OK`<br>`install_vm.py: OK`<br>`ovf.py: OK`<br>`BSM.qcow2: OK` |

4. Press **`ENTER`** to read the **`EULA`**.
5. Press **`Y`** to accept the **`EULA`**.
6. Enter a name for the Branch Session Manager virtual machine. For example, `SanityBSM`.
7. Select the required Branch Session Manager profile.

   For more information, see Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 20.
8. Select the Public and OOBM network interfaces.

   ASP 6.0.x CLI displays the currently available network interface bridges and select the required bridge for Branch Session Manager.

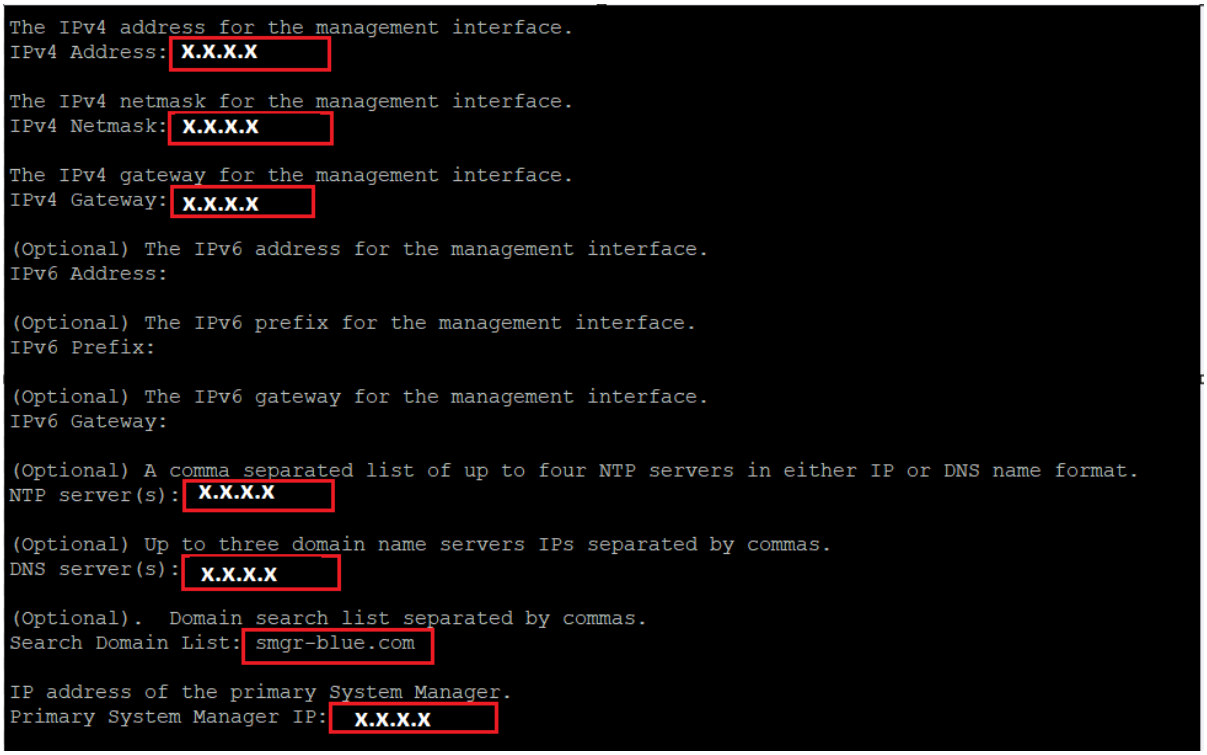
   ASP 6.0.x CLI displays the currently available disk space and the required disk space to deploy Branch Session Manager.
9. To configure the VM properties, enter **`Y`** in the **Would you like to configure the VM properties? [y/n]:** field, and continue providing the property details:
   a. In the **Hostname** field, enter a short host name for Branch Session Manager.
   b. Enter **IPv4 address**. For example, x.x.x.x
   c. Enter **IPv4 Netmask**. For example, m.m.m.m
   d. Enter **IPv4 Gateway**. For example, g.g.g.g
   e. **(Optional)** The **IPv6 address** for management interface, enter the valid IPv6 address.
   f. **(Optional)** The **IPv6 Network Prefix** for management interface, enter the valid IPv6 network prefix.
   g. **(Optional)** The **IPv6 Network Gateway** for management interface, enter the valid IPv6 network gateway.
   h. The **NTP servers**, enter a valid NTP server address in IP or DNS name format.

      You can type up to four NTP servers separated by a comma.

i. The **DNS servers**, enter a valid DNS server IP address.

You can type up to three DNS servers separated by a comma.

j. The **Search Domain List**, enter a search list of domain names.




10. In the **IP Address of Primary System Manager** field, enter the IP address of the reachable System Manager server.
11. Select the **Edge Topology BSM** as required. This indicates BSM configuration.
12. In the **LSP IP** field, enter the IPv4 or IPv6 LSP address.
13. In the **Command line customer account user login** field, enter the customer account user login.
14. In the **Customer account user password** field, enter the password and confirm the Customer account user password.
15. Enable or disable Data Encryption.

    By enabling Data Encryption, your Communication Product's Operational data, Configuration data, along with all of the Log Files will be encrypted. You will be prompted to enter a pass-phrase that will be used to create/access an encryption key. Secondly, you will be asked to configure the option for local key storage.

    It is important to note that the encryption of the disk may have a performance impact. For further information, contact the Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

Enter 1 to Enable Encryption or enter 2 to Disable Encryption.

a. In the **Data Encryption Active** field, if `1` is entered, do the following

- In the **Enter Encryption Passphrase** field, enter the passphrase.
- In the **Confirm Enter Encryption Passphrase** field, reenter the passphrase.
- In the **Require Encryption Passphrase at Boot-Time: (yes/no)**, enter the required value.

If **1** is entered, you must enter the encryption passphrase whenever the Branch Session Manager reboots.

If **2** is entered, there is no need to enter the encryption passphrase whenever the Branch Session Manager reboots.

**Important:**

*Note* the data encryption passphrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA.

b. In the **Data Encryption Active** field, if `2` is entered, no action is required.

16. Enable or disable Enhanced Avaya Security Gateway (EASG).

**Important:**

Avaya recommends to enable **EASG**.

**Note:**

Enable: (Recommended)

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

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

Disable:

By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

- Enter `1` to enable EASG.
- Enter `2` to disable EASG.

17. In the **`Do you want to set a root password?(yes/no)`** field, enter the required value.

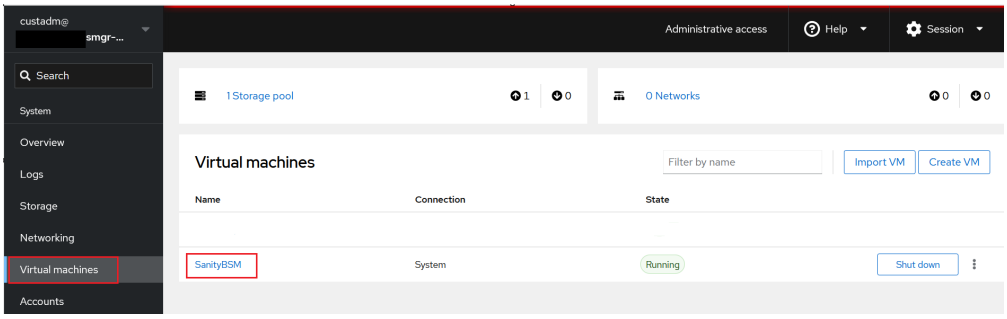
18. In the **`Power on VM automatically after deploy?: [y/n]`** field, enter one of the following:
    - **`y`**: Indicates Branch Session Manager virtual machine is automatically powered-on after deployment.
    - **`n`**: Indicates user has to manually power on the Branch Session Manager virtual machine on KVM cockpit.
19. In the **`Proceed?[y/n]`** field, enter one of the following:
    - **`y`**: Branch Session Manager deployment begins.
    - **`n`**: Branch Session Manager deployment cancels.

    **Note:**

    After the Branch Session Manager virtual machine is successfully deployed, ASP R6.0.x displays the following message: `Domain creation completed`.
20. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
21. If Web console is in **Limited access** mode, click on **Turn on administrative access** button.

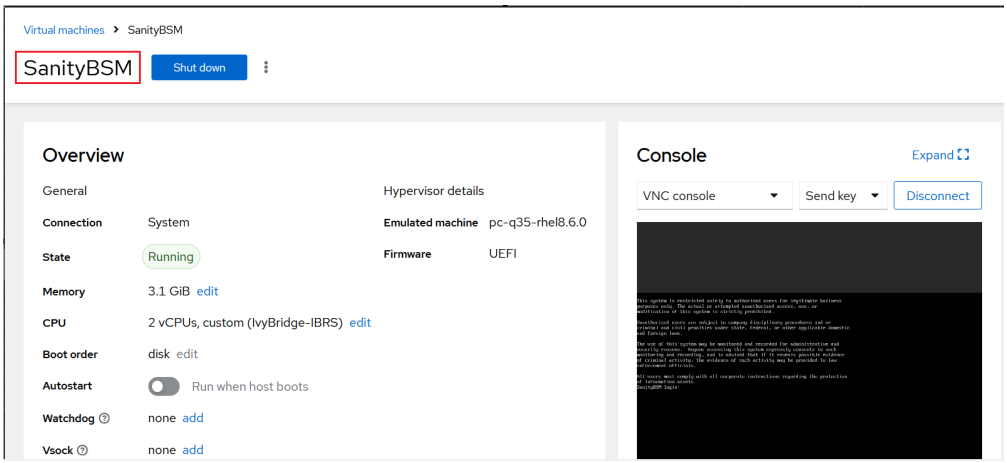
    **Note:**

    Virtual Machines are not visible when in **Limited access** mode.
22. For administration actions, on the top-right of the window, click on the **Limited access** or **Turn on administrative access** button.
23. Navigate to **System** > **Virtual Machines**.




The Branch Session Manager is deployed.

24. Click on **VM Name** and login from Console.




# Updating the CPU resources for KVM Cockpit

## Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

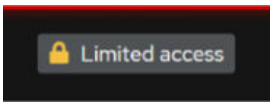



**Figure 7: Limited access button**

**Note:**

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.

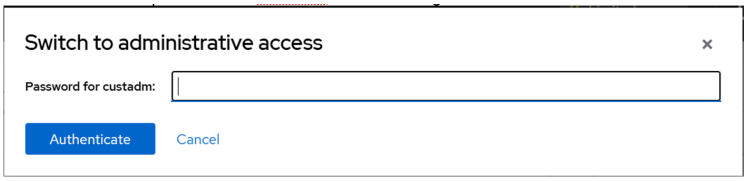



**Figure 8: Switch to administrative access**

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

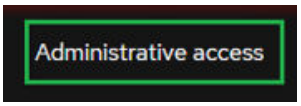



**Figure 9: Administrative access button**

4. Navigate to **System** > **Virtual Machines**.
5. If the virtual machine is running, right-click on the virtual machine to update and select **Shut Down**.
6. Right-click on the virtual machine and choose **Open/Edit**, and go to Overivew section.

   KVM Cockpit displays the CPU details window.
7. Update the CPU reservation details such as vCPU maximum, vCPU count, Sockets, Core per socket, and Threads per core.
8. Click **Apply**.
9. Click **Run** to start the virtual machine.

# Chapter 6: Configuring edge Branch Session Manager

## Install certificates for edge Branch Session Manager

Unlike enterprise Session Manager or Branch Session Manager, a TLS connection is required before running the initTM command for an edge Branch Session Manager. The initTM command initializes the Avaya Aura® Session Manager Trust Management.

The edge Branch Session Manager is connected to the System Manager at the core through an Application Delivery Controller (ADC) or a reverse proxy.

By default, Entrust certificates are installed for the tunnel as part of the edge Branch Session Manager deployment. A tunnel is an outbound connection from the branch to the core and does not contain any inbound connection. The tunnel supports bidirectional traffic between System Manager at the core and the edge Branch Session Manager to support all management functions, including database replication.

However, if the ADC or reverse proxy uses a certificate authority (CA) other than the Entrust CA to connect to the edge Branch Session Manager, you must install the root CA certificates for the tunnel before configuring the edge Branch Session Manager.

Use certTool to install the certificates for the tunnel.

## Installing the root CA certificate in the trust store of the tunnel

### Procedure

1. Download the CA certificate chain in a PEM format from the certificate authority that issued the certificate for the ADC or reverse proxy.
2. Copy the .pem file on the edge Branch Session Manager server.
3. At the command prompt of the edge Branch Session Manager server, run the following command to import the .pem file:

   ```
   certTool -i <rootca>.pem -t -s tunnel
   ```

4. Type `yes` when the following message is displayed:

   ```
   Trust this certificate? [no]:
   ```

# Installing identity certificates for configuring mutual authentication for the tunnel

## About this task

Use this procedure if you want to configure mutual authentication for the tunnel.

## Procedure

1. Obtain and download the PKCS#12 certificate for the Branch Session Manager and copy it on the edge Branch Session Manager server.
2. At the command prompt of the edge Branch Session Manager server, run the following command to import the PKCS#12 file:

   ```
   certTool -i tunnel.p12 -s tunnel
   ```

3. When prompted, type the password of the PKCS#12 file.

## Next steps

If the file contains the root CA certificate, the root CA certificate is automatically installed in the trust store of the tunnel. Otherwise, manually install the root CA certificate in the trust store of the tunnel.

### Related links

Installing the root CA certificate in the trust store of the tunnel on page 85

# Installing third-party identity certificates

## About this task

If the identity certificates of the ADC or reverse proxy are signed by a third-party CA, download the identity certificates in a PKCS#12 format from the third-party CA.

If the CN and SAN are configured correctly in the certificates, you can use a single PKCS#12 file. Otherwise, two PKCS#12 files are required, one for the management applications and one for SIP/PPM.

## Procedure

1. Download the identity certificates from the third-party CA in a PKCS#12 format and copy it on the edge Branch Session Manager server.
2. If you use separate PKCS#12 files for the management applications and SIP/PPM, do the following at the command prompt of the edge Branch Session Manager server:
   a. Run the following command to import the PKCS#12 file for the management applications:

      ```
      certTool -i bsm-eth0.p12 -s eth0
      ```

   b. Run the following command to import the PKCS#12 file for SIP/PPM:

      ```
      certTool -i bsm-eth1.p12 -s eth1
      ```

3. If you use a single PKCS#12 file for the management applications and SIP/PPM, at the command prompt of the edge Branch Session Manager server, run the following command to import the PKCS#12 file:

   ```
   certTool -i bsm.p12 -s all
   ```

### Next steps

If the PKCS#12 file contains the root CA certificate, the root CA certificate is automatically installed in the trust store. Otherwise, manually install the root CA certificate in the trust store.

**Related links**

Installing the root CA certificate in the trust store of the tunnel on page 85

# edgeSetup command

With Release 10.2, use the **edgeSetup** command to configure an edge Branch Session Manager server.

You can run the **edgeSetup** command in the following modes:

- **Graphical:** This is the default mode to configure the edge Branch Session Manager server. You can provide the configuration details in a graphical user interface.
- **Text:** This provides a text-based mode interface to configure the edge Branch Session Manager server.
- **Command-line interface:** This provides a set of parameters to configure the edge Branch Session Manager server.

### Syntax

```
edgeSetup
```

Displays a graphical user interface to configure the edge Branch Session Manager server.

### Syntax

```
edgeSetup [-t]
```

Displays a text-based mode to configure the edge Branch Session Manager server.

### Syntax

```
edgeSetup [-h] [--adc <FQDN>] [--port <PORT>] [--primary_fqdn <FQDN>] [--secondary_fqdn
<FQDN>] [--vfqdn <FQDN>] [STDIN PASSWORD]
```

| | |
|---|---|
| **-h, --help** | Displays the help for the command and also displays the required and optional parameters. |
| **--adc <FQDN>** | The ADC FQDN. |
| **--port <PORT>** | The ADC port.<br>The default port is 443. |

| | |
|---|---|
| **[--primary_fqdn <FQDN>]** | FQDN of the primary System Manager server. |
| **[--secondary_fqdn <FQDN>]** | FQDN of the secondary System Manager server.<br>If edge Branch Session Manager is part of the System Manager Geographic Redundancy system, provide the secondary System Manager server details. |
| **[--vfqdn <FQDN>]** | Virtual FQDN of System Manager.<br>STDIN PASSWORD |
| **[STDIN PASSWORD]** | This is the enrollment password.<br>You can provide the password in one of the following ways:<br>• Using the **echo** command:<br>For example:<br>`echo <enrollpassword> \| edgeSetup --port 443 --adc <adc.avaya.com> --primary_fqdn <prim.avaya.com> --vfqdn <vfqdn.avaya.com>`<br>• Using a password file:<br>For example:<br>`edgeSetup --adc <adc.avaya.com> --port 443 --primary_fqdn <prim.avaya.com> --vfqdn <vfqdn.avaya.com> <enrollpasswordfile>`<br>You can save the enrollment password in a text file. |

# Application Delivery Controller

Application Delivery Controller (ADC) is a network device or a set of services that helps optimize the performance, availability, and security of applications by managing and distributing incoming network traffic to multiple servers or resources that host those applications. ADCs can be physical appliances, virtual instances, or software solutions. ADCs are usually integrated with or used in conjunction with load balancers. These devices are commonly deployed in data centers, cloud environments, and content delivery networks to enhance the performance, security, and reliability of applications and services delivered to end-users.

# Configuring the edge Branch Session Manager server in graphical-user interface mode through CLI

### Before you begin

- Deploy and configure System Manager.
- Deploy the edge Branch Session Manager server.

### Procedure

1. Log in to the edge Branch Session Manager command-line interface.
2. Type the following command:

   **`edgeSetup`**

   Edge Branch Session Manager displays the Edge Configuration window.
3. In **ADC FQDN**, type the FQDN of the application delivery controller.
4. In **ADC Port**, type the port of the application delivery controller.

   The default port is 443.
5. In **Primary System Manager FQDN**, type the FQDN of the primary System Manager server.
6. In **Secondary System Manager FQDN**, type the FQDN of the secondary System Manager server.

   If edge Branch Session Manager is part of the System Manager Geographic Redundancy system, provide the secondary System Manager server details.
7. In **Virtual FQDN**, type the virtual FQDN of the System Manager server.
8. In **Enrollment Password**, type the enrollment password.

   Enrollment password must match with the value on the **Security** > **Certificates** > **Enrollment Password** page.
9. In **Enrollment Password (again)**, retype the enrollment password.
10. Click **OK**.

    Edge Branch Session Manager applies the changes and starts the trust management with System Manager.

# Configuring the edge Branch Session Manager system in text mode through CLI

### Before you begin

- Deploy and configure System Manager.
- Deploy the edge Branch Session Manager server.

### Procedure

1. Log in to the edge Branch Session Manager command-line interface.
2. Type the following command:

   **edgeSetup -t**

   Edge Branch Session Manager displays the Edge Configuration page.
3. In **ADC FQDN**, type the FQDN of the application delivery controller.
4. In **ADC Port**, type the port of the application delivery controller.

   The default port is 443.
5. In **Primary System Manager FQDN**, type the FQDN of the primary System Manager server.
6. At the **Is this part of a Geo-Redundant system** prompt, type one of the following:
   - `y` if edge Branch Session Manager is part of the System Manager Geographic Redundancy system.

     When you type `y`, edge Branch Session Manager displays the **Secondary System Manager FQDN** field.
   - `n` if edge Branch Session Manager is not part of the System Manager Geographic Redundancy system.
7. In **Secondary System Manager FQDN**, type the FQDN of the secondary System Manager server for the System Manager Geographic Redundancy system.
8. In **Virtual FQDN**, type the virtual FQDN of the System Manager server.
9. In **Enrollment Password**, type the enrollment password.

   Enrollment password must match with the value on the **Security** > **Certificates** > **Enrollment Password** page.
10. In **Enrollment Password (again)**, retype the enrollment password and press `Enter`.

    Edge Branch Session Manager applies the changes and starts the trust management with System Manager.

# Configuring the edge Branch Session Manager server through CLI

### Before you begin

- Deploy and configure System Manager.
- Deploy the edge Branch Session Manager server.

### Procedure

1. Log in to the edge Branch Session Manager command-line interface.
2. Type the following command:

   **edgeSetup** --adc <FQDN> --port <PORT> --primary_fqdn <FQDN> --secondary_fqdn <FQDN> --vfqdn <FQDN> <passwordfile>

   For example:

   **edgeSetup** --adc <test.adc.com> --port 443 --primary_fqdn <test.primfqdn.com> --secondary_fqdn <test.seconfqdn.com> --vfqdn <test.fqdn.com> < enrollpasswordfile>

   You can save the enrollment password in a text file.

   If edge Branch Session Manager server is part of the System Manager Geographic Redundancy system, provide the secondary System Manager server details.

   Enrollment password must match with the value on the **Security** > **Certificates** > **Enrollment Password** page.

   Edge Branch Session Manager applies the changes and starts the trust management with System Manager.

### Next steps

After the edge Branch Session Manager setup is complete, delete the enrollment password file.

# Chapter 7: Post-installation verification

## Post-installation checklist

Perform the following steps to verify the Session Manager OVA deployment.

| # | Action | Link | ✔ |
|---|---|---|---|
| 1 | Run the maintenance tests on the deployed Session Manager. | See Running Session Manager maintenance tests on page 92. | |
| 2 | Verify data replication. | See Verifying data replication on page 93. | |
| 3 | Verify the connections of the deployed Session Manager. | See Verifying the connections on page 93. | |
| 4 | Generate a test alarm. | See Generating a test alarm on page 94. | |

## 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.

# Verifying the connections

### About this task

Verify the connections of the deployed Session Manager.

Verify the connections of the deployed Session Manager and Branch 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**.

# 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

## Managing snapshots through Session Manager CLI

### vmsnapshot command

From Release 10.2, use the **vmsnapshot** command to create, remove, revert, and list the snapshot of Session Manager and Branch Session Manager deployed in a virtualized environment.

Verify with the system administrator that the required Virtual machine state privileges are available on the virtual machine.

**Note:**

The **vmsnapshot** command is not available in a Software-Only environment.

#### Syntax

```
vmsnapshot [-h] [-d] [--host] [-u] [-p] [-a] [-y][create] [remove] [revert] [list --current]
```

| | |
|---|---|
| **-h, --help** | Displays help for the command and also the required and optional parameters. |
| **-d, --debug** | Displays the log information. |
| **--host** | Displays the ESXi IP or FQDN. |
| **-u, --user** | Displays the ESXi username. |
| **-p, --passwd** | Displays the ESXi password.<br>**Note:**<br>You can also provide the password through a file without exposing it to the command-line. You can use the following command:<br>`vmsnapshot --host <ESXi host IP Address> -u root list <full path of the file containing the password>` |

| | |
|---|---|
| | For example: `vmsnapshot --host 12.12.15.14 -u root list </tmp/passwd` |
| **-a, --auth** | Use ESXi host, ESXi user, and ESXi password from encrypted file. |
| **-y, --assumeYes** | Silent operation, assume "yes" for any prompts. |
| **create <Name of the new snapshot>** | Creates a new snapshot. |
| **remove <Name of the snapshot to remove>** | Removes the given snapshot. |
| **revert <Name of the snapshot to revert>** | Reverts the virtual machine to the given snapshot. |
| **list, list --current** | • **list:** Displays all the snapshot.<br>• **list --current:** Displays the latest snapshot. |

# Configuring the authentication file with ESXi detail

## Procedure

1. Log in to the Session Manager command-line interface.
2. Type the following command:

   **`sudo /opt/Avaya/vm-tools/bin/authfile.py`**
3. In **ESXi host address**, type the ESXi host address.
4. In **ESXi username**, type the ESXi user name.
5. In **ESXi password**, type the ESXi password.

   Session Manager saves the ESXi details and displays the following message:

   ```
   Auth file saved at /opt/avaya/vm-tools/conf/auth.yaml
   ```

# Creating a snapshot through CLI

## Before you begin

Configure the authentication file with ESXi details, see “Configuring the authentication file with ESXi detail”.

When you configure the authentication file with ESXi detail, Session Manager does not prompt you to provide ESXi details each time you run the **`vmsnapshot`** command.

## Procedure

1. Log in to the Session Manager command-line interface.

2. Type the following command:

   **vmsnapshot create <Name of the new snapshot>**

   For example, **vmsnapshot create testsnapshot1**

   **Important:**

   Snapshots occupy the system resources and degrade the performance of the virtual application. Therefore, delete the snapshot after the required Session Manager operation is complete.

   Session Manager creates the snapshot.

# Viewing list of snapshots through CLI

## Procedure

1. Log in to the Session Manager command-line interface.
2. Do one of the following:
   - To list all the snapshots of the virtual machine, type **vmsnapshot list**.
   - To list the latest snapshot of the virtual machine, type **vmsnapshot list --current**.

   Session Manager displays the name, description, and timestamp of the snapshot.

   For example,

   ```
   Name: <testsnapshot1>; Description: automated snapshot; CreateTime:
   2023-05-31 19:32:08.676835+00:00
   ```

# Reverting a snapshot through CLI

## Procedure

1. Log in to the Session Manager command-line interface.
2. Type the following command:

   **vmsnapshot revert <Name of the snapshot to revert>**

   For example, **vmsnapshot revert testsnapshot1**

   Session Manager displays the following message:

   ```
   Current state of the virtual machine will be lost unless it is
   saved in a snapshot. Revert to snapshot '<testsnapshot1>' (y/n)?
   ```

3. At the prompt, type `y`.

   Session Manager reverts the snapshot and displays the following message:

   ```
   Reverting to snapshot <testsnapshot1>

   WARN: connection will drop!
   ```

## Removing a snapshot through CLI

### Procedure

1. Log in to the Session Manager command-line interface.
2. Type the following command:

   **vmsnapshot remove <Name of the snapshot to remove>**

   For example, **vmsnapshot remove testsnapshot1**

   Session Manager displays the following message:

   ```
   This will permanently remove snapshot '<testsnapshot1>' from this
   virtual machine. Do you want to continue (y/n)?
   ```

3. At the prompt, type `y`.

   Session Manager removes the snapshot and displays the following message:

   ```
   Snapshot: <testsnapshot1> successfully removed
   ```

# Managing snapshot through vSphere Client

## Creating a snapshot

**Caution:**

Do not perform any activity on the virtual application until the snapshot backup is complete. Snapshot operations can adversely affect service.

**Warning:**

Snapshots can cause performance issues with Session Manager. It is recommended to use snapshots for short periods of time.

### Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Create snapshot** is available on the virtual machine.

**Note:**

Differences exist between the vSphere Web Client versions. You might need to modify the following steps accordingly.

### Procedure

1. To select a virtual machine using the vSphere Web Client:
   a. Search for a virtual machine and select it from the search results list.

b. Stop the application that is running on the virtual machine or make the application out-of-service.
c. Right-click the virtual machine and select **Snapshot** > **Take Snapshot**.

2. In the **Name** field, enter a name for the snapshot.
3. In the **Description** field, enter a description for the snapshot.
4. Disable **Snapshot the virtual machine's memory**.
5. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
6. Click **OK**.

   The system displays `Completed` when the snapshot backup is complete.

# Deleting a snapshot for VMware

**Note:**

Differences exist between the vSphere Web Client versions. Modify the steps accordingly.

### Before you begin

Verify the required privilege **Virtual machine.State.Remove snapshot** is available on the virtual machine.

### Procedure

1. To open the **Snapshot Manager** using the vSphere Web Client:
   a. Search for a virtual machine.
   b. Select the virtual machine from the search results list.
   c. Right-click the virtual machine and select **Snapshot** > **Snapshot Manager**.
2. In the **Snapshot Manager**, click a snapshot that you want to delete.
3. Select **Delete from Disk**.
4. When the Snapshot Manager displays a dialog box for confirmation, click **Yes**.
5. Click **Close** to close the Snapshot Manager.

# Restoring a snapshot for VMware

Use this procedure to return the memory, settings, and state of the virtual machines to the state when you took the snapshot. The power and data states of the virtual machines return to the state when you took the parent snapshot.

**Important:**

Do not perform any activity on the virtual application until the snapshot restoration is complete.

### Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Revert to snapshot** is available on the virtual machine.

**Note:**

Differences exist between the vSphere Web Client versions. You might need to modify the steps accordingly.

### Procedure

1. Click **Inventory** > **Virtual Machine**.
2. Right-click the virtual machine name on which you want to restore the snapshot, and click **Snapshot**.
3. Open **Snapshot Manager**.
4. Select the snapshot version that you want to restore.
5. Click **Go to**.
6. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task.

   Wait until the system displays the `Completed` message

# Restarting an application from Solution Deployment Manager

### Before you begin

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

### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.
4. Click **Restart**.

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

# 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.

# 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.

# Troubleshooting a Session Manager virtual machine that does not power on

The system displays appropriate messages for CPU or memory resource limitations. The Session Manager might be deployed on a host that does not have the necessary resources allocated for power up. A power up failure indicates the newly deployed OVA must be resized or resources are being oversubscribed. The recommendation is to *not* oversubscribe resources.

Default CPU and memory reservations are built into the Session Manager OVA. The reservations are set to match the desired configuration and based on the footprint. If the system does not have sufficient resources to support a given footprint of Session Manager, select one of the following:

- A smaller footprint — You can support less number of devices, when you select a smaller footprint.
- A footprint with larger capacity.

# Reconfiguring hardware resources for flexible footprint

## About this task

Reconfigure the CPU, RAM or Hard Disk resources for the Session Manager virtual machine. The procedure is for the setup in virtualized environment.

## Procedure

1. Connect to the vCenter server or ESXi host using the VMware vSphere web client.
2. Log in as an administrator
3. Power off the virtual machine:
   a. In the vSphere client inventory, right-click the required virtual machine and then select **Shut Down Guest OS**.
   b. Click **Yes** in the **Shutdown Confirmation** dialog box.
4. Right-click the virtual machine name and select **Edit Settings**.
5. Navigate to the **Virtual Hardware** tab.
6. Under the **CPU** section, select the appropriate numbers of CPU to match the desired Session Manager profile.
7. Verify the **Reservation** is set correctly. The **Reservation** value must be at least half of the stated minimum MHz requirement because Session Manager capacities assume hyperthreading is active.
8. If you want to limit the Session Manager CPU use:
   a. Clear the **unlimited** check box.
   b. Verify the **Limit** slide is set to the full value of the stated minimum MHz requirement.
9. Change the **Number of sockets** according to the limit requirement.
10. Under the **Memory** section change the RAM size to the appropriate limit and verify the **Reservation** is set correctly.
11. If you want to limit the Session Manager memory use, clear the **unlimited** check box and verify the **Limit** slide is set to the same value as the **Reservation**.
12. To change the **Hard Disk** size, do the following:
    a. Delete all virtual machine snapshots.
    b. Expand the **Hard Disk** section under the **Virtual Hardware** tab.
    c. Select the desired unit size as GiB and enter the new value for the **Hard Disk** size.

    **Important:**

    Perform this step with caution because updating the disk size cannot be undone. Make sure you use the recommended units and disk size values as per the Session Manager profiles. Otherwise, you might need to delete the virtual machine and deploy a new OVA.

13. Click **OK** and wait until the virtual machine finishes the reconfiguration procedure.
14. Right-click the virtual machine and select **Power On** to start the virtual machine.

**Related links**

#unique_83

# 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.

# 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
```

# General Maintenance

## 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**.

# 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 |

**Related links**

Finding documents on the Avaya Support website on page 114

# Finding documents on the Avaya Support website

## Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

**Related links**

Session Manager documentation on page 113

# 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: Upgrading RHEL

## Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines

### About this task

You can upgrade RHEL 8.4 to RHEL 8.10 using the following **av-upgrade-os** command. The **av-upgrade-os** command is available when Session Manager R10.2.1 is installed.

### Before you begin

1. Install Session Manager R10.2.1.

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

2. Verify that **av-upgrade-os** command is available.

   To verify if the **av-upgrade-os** command is available, run the following command: **which av-upgrade-os**

3. Verify the current version of RHEL on which Session Manager is running.

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

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

4. Download Session Manager RHEL 8.10 Operating System bundle on Session Manager R10.2.1 virtual machine.

### Procedure

1. Login to Session Manager CLI.
2. To upgrade from RHEL 8.4 to RHEL 8.10, run the following command: **av-upgrade-os <SM RHEL OS Bundle>**

   For example, run **av-upgrade-os AV-SM10.2-RHEL8.10-OSUpdate-001.tar.bz2**

3. After successful upgrade to RHEL 8.10, the Session Manager virtual machine reboots.
4. Log in to Session Manager CLI.
5. To verify that RHEL 8.10 is upgraded successfully, run any of the following commands:

   - **cat /etc/redhat-release**

- **av-version**

# Appendix B: Best Practices for VMware performance and features

The following sections describe the best practices for VMware performance and features.

## BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper, “Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs” at https://www.vmware.com/.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers

### Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

**Note:**

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

### Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

## Dell PowerEdge Server

The following are the BIOS recommendations for Dell PowerEdge Servers supported by Avaya SBC:

When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- In Processor Settings, set:
  - **Turbo Mode** to **enable**.
  - **C States** to **disabled**.

# Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the

network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the **`chronyc sources -v`** command from a command window. The results from this command:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **chronyd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

# VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration

- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

**Important:**

*Do not* upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

# VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

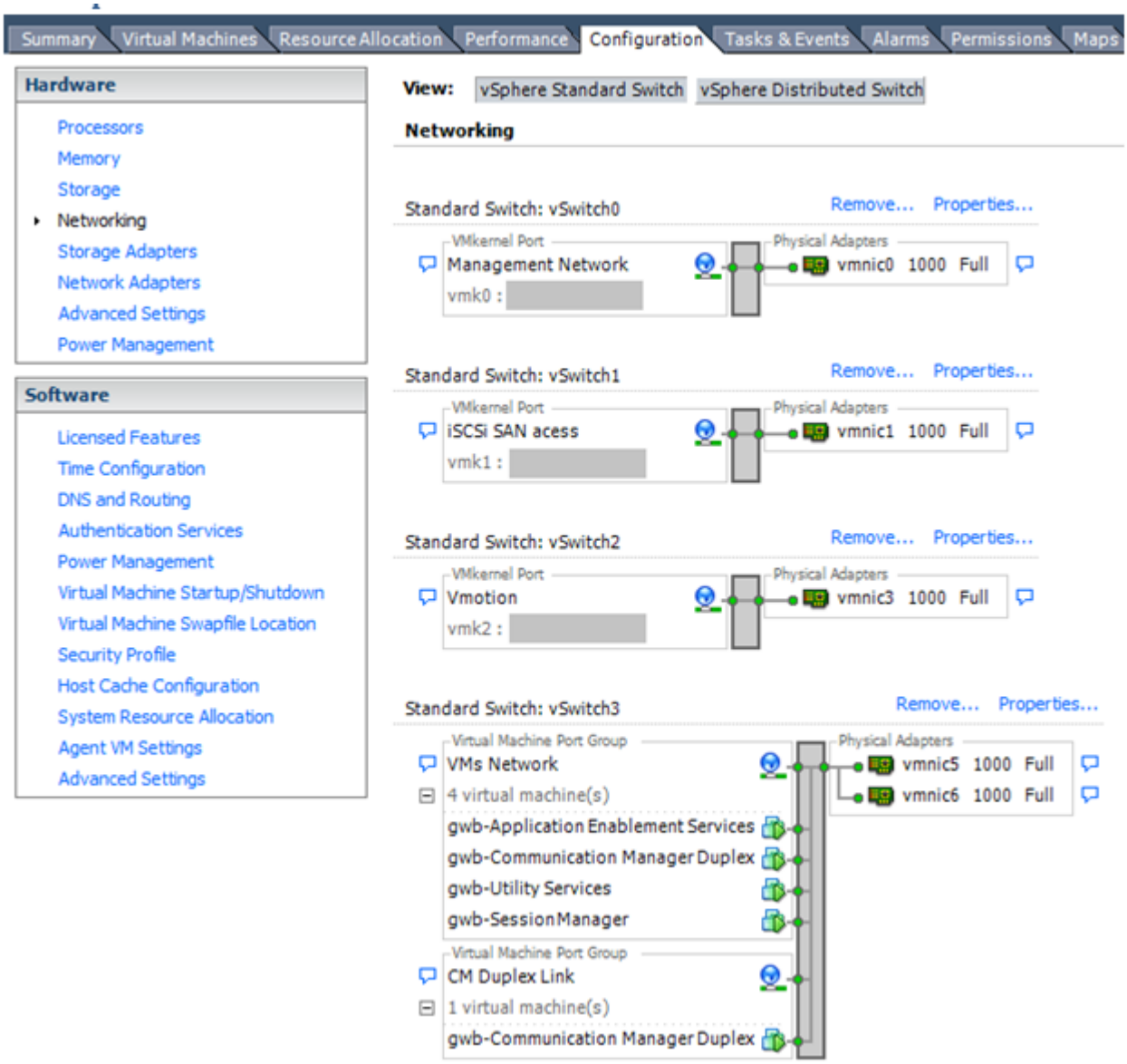
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

**Disclaimer**: The images in this section represent older ESXi versions and may vary for the latest ESXi versions.

## Networking Avaya applications on VMware ESXi – Example 1




This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

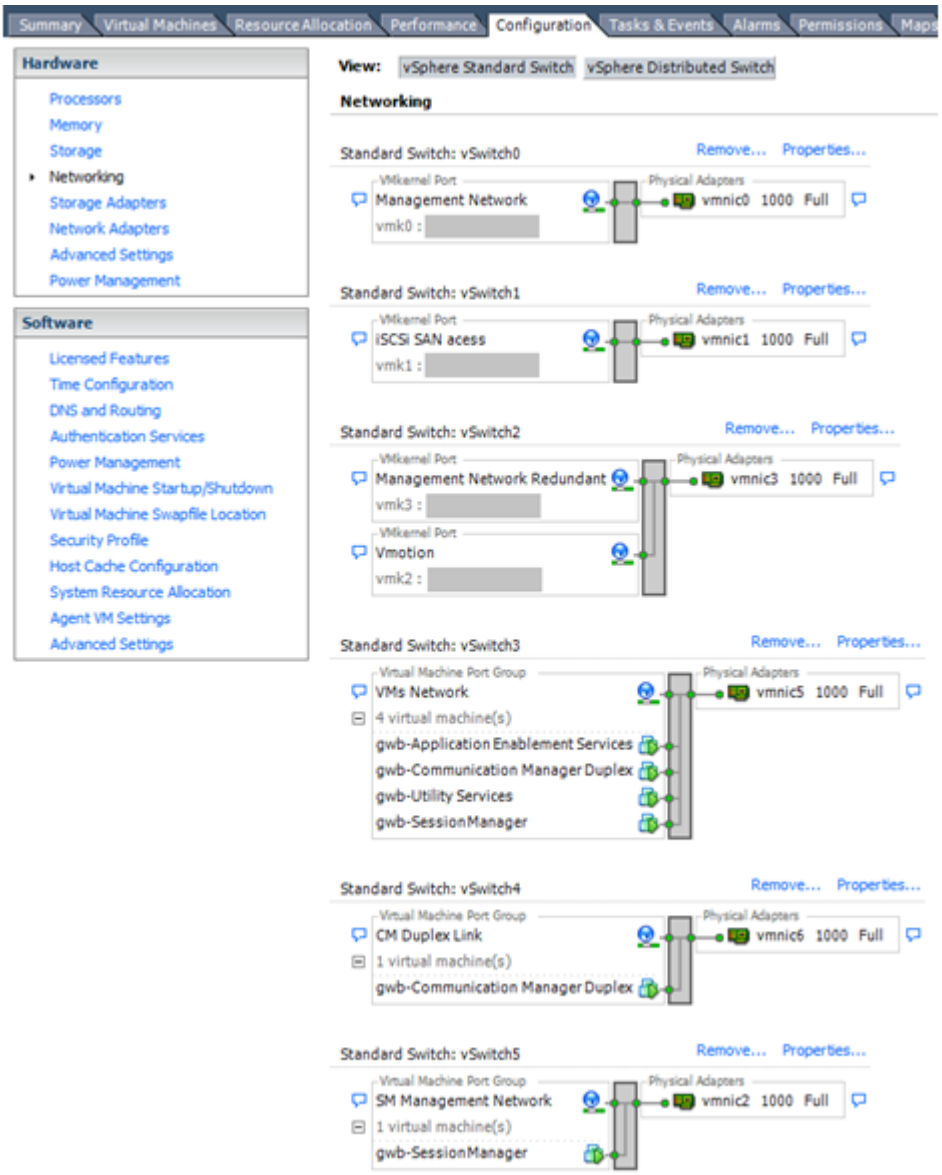
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The

Communication Manager software duplication link must meet specific network requirements. For more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:

- The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
- The round-trip delay must be 8 ms or less.
- The round-trip packet loss must be 0.1% or less.
- Both servers' duplication ports must be on the same IP subnet.
- You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
- The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.

- Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

## Networking Avaya applications on VMware ESXi – Example 2




This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.

- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

### References

| Title | Link |
|---|---|
| Product Support Notice PSN003556u | Go to https://support.avaya.com and search for PSN003556u. |
| VMware vSphere 8.0 Documentation | Go to Broadcom website (formerly known as VMware) and search for *VMware vSphere 8.0 Documentation*. |
| VMware vSphere 7.0 Documentation | Go to Broadcom website (formerly known as VMware) and search for *VMware vSphere 7.0 Documentation*. |

## Separating Session Manager management and Security Module traffic

### About this task

As a best practice, Session Manager management and Security Module related traffic should be separate. There are many ways in which to separate Session Manager including VLANs, VMware port groups, and VMware virtual switches connected to different physical network interface cards.

Using a VLAN to separate management and Security Module related traffic must be done from a customer's switch, as VLAN configuration cannot be accomplished from a virtual machine or Hypervisor level. The result is a Session Manager virtual machine with all of its NICs connected to the same vSwitch.

If the defaults are selected during deployment, management and Security Module traffic are placed on the same vSwitch. As a best practice, separate Session Manager management and Security Module traffic using the following procedure.

### Procedure

1. Create a vSwitch for dedicated Session Manager Security Module traffic.
2. From the vSphere client inventory view, right-click the Session Manager virtual machine and select **Edit Settings**.
3. The **Hardware** tab is selected by default. Select the proper Network adapter from the hardware list on the left-side.
4. On the right side, under the **Network label** list, select a separate vSwitch for this NIC.
5. Click **OK** to complete configuration.

# Storage

There is no stipulation on the underlying storage vendor type and storage technology used. Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

# Thin vs. thick deployments

VMware ESXi uses a thick virtual disk by default when it creates a virtual disk file.. The thick disk preallocates the entire amount of space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are preallocated for that virtual disk.

In contrast, a thin virtual disk does not preallocate disk space. Blocks in the VMDK file are not allocated and backed up by physical storage until they are written on the disk during the normal course of operation. A read instruction to an unallocated block returns zeroes, but the block is not backed by physical storage until it is written on the disk. Consider the following details when implementing thin-provisioned disk in your VMware environment:

- Thin-provisioned disks can grow to the full size as specified at the time of virtual disk creation, but they cannot shrink. Once you allocate the blocks, you cannot deallocate them.
- Thin-provisioned disks run the risk of overallocating storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the formatting process may cause the thin-provisioned disk to grow to full size. For example, if you present a thin-provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the format tool in Microsoft Windows writes information to all sectors on the disk, which in turn inflates the thin-provisioned disk to full size.

Thin-provisioned disks can overallocate storage. If the storage is overallocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin-provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not consumed to its full capacity. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin-provisioned disks are a viable option.

# Best Practices for VMware features

## VMware High Availability

VMware High Availability (HA) provides automatic detection of hardware failures, server failures, and operating system failures. In the event of a physical server failure, VMware HA automatically restarts the affected virtual machine on other production servers that have spare capacity. In the event of an operating system failure, VMware HA restarts the affected virtual machine on the same server.

VMware HA ensures that capacity is available to restart all virtual machines that are affected by a service failure. HA continuously monitors capacity utilization and reserves spare capacity to restart virtual machines.

VMware HA helps users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions along with suggested remediation steps.

For more information, see the VMware website at https://www.vmware.com/pdf/ha_datasheet.pdf.

**Note:**

- All virtual machines and their configuration files must be on shared storage, e.g. Fibre Channel SAN, iSCSI SAN, or SAN iSCI NAS.
- The console network must have redundant network paths to have reliable failure detection for HA clusters. VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses virtual machine priority to decide order of restart.
- VMware HA only works across a LAN. VMware HA does not work across a WAN.

## VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.

- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

## VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

**Caution:**

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

  If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.

- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the Take Snapshot window, clear the **Include virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

**Note:**

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

### Related resources

| Title | Link |
|---|---|
| Best practices for virtual machine snapshots in the VMware environment | Best Practices for virtual machine snapshots in the VMware environment |
| Understanding virtual machine snapshots in VMware ESXi and ESX | Understanding virtual machine snapshots in VMware ESXi and ESX |
| Working with snapshots | Working with snapshots |
| Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots | Send alarms when virtual machines are running from snapshots |

# VMware features supported by Avaya Aura®

This section does not cover Avaya Solutions Platform (ASP) 130 and ASP S83000. Avaya does not support advanced VMware features on its ASP 130 and ASP S8300 hardware. It supports the basic VMware features as listed in the following table. For more information about support and limitations on ASP 130 and ASP S8300, see https://download.avaya.com/css/public/documents/101062774.

**Note:**

For more information about Avaya Aura® Media Server, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

The following table lists the VMware features supported on customer-provided Virtualized Environment for various Avaya Aura® Release10.2 components.

| Product or feature | Communication Manager | Session Manager | System Manager | Application Enablement Services | Avaya SBC | Avaya Aura® Device Services |
|---|---|---|---|---|---|---|
| ESXi 7.0 | Yes | Yes | Yes | Yes | Yes | Yes |
| ESXi 8.0 | Yes | Yes | Yes | Yes | Yes | Yes |
| vCenter<br>See foot note[1] | Yes | Yes | Yes | Yes | Yes | Yes |
| vSphere WebClient (HTML5) | Yes | Yes | Yes | Yes | Yes | Yes |
| VMFS 6 | Yes | Yes | Yes | Yes | Yes | Yes |
| VMware vMotion<br>See foot note[2] | Yes | Yes | Yes | Yes | Yes | Yes |
| Storage vMotion | Yes | Yes | Yes | Yes | Yes | Yes |
| VMware Snapshot<br>See foot note[3] | Yes | Yes | Yes | Yes | Yes | Yes |
| VMware Live Snapshot | Not supported | Not supported | Not supported | Not supported | Not supported | No |
| VMware High Availability | Yes | Yes | Yes | Yes | Yes | Yes |
| Proactive High Availability | Best effort basis support (Not tested) | Best effort basis support (Not tested) | Best effort basis support (Not tested) | Best effort basis support (Not tested) | Best effort basis support (Not tested) | Best effort basis support (Not tested) |
| Storage DRS | Yes | Yes | Yes | Yes | Yes | Yes |
| Hyperthreading | Yes | Yes | Yes | Yes | Yes | Yes |
| Hyperthreading ratio for Virtual CPUs and Physical CPU | 2:1 | 2:1 | 2:1 | 2:1 | 2:1 | 2:1 |

*Table continues…*

1 Limited to deployment, managing VMs, basic monitoring, and making VMs part of a vCenter cluster.
2 Ensure that vMotion occurs when an Avaya Aura® application virtual machine is in maintenance mode.
3 Snapshots should be used when patching the products. As per the backup mechanism provided in the product-specific documentation, you should perform daily backups instead of using snapshots of the products. Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

| Product or feature | Communication Manager | Session Manager | System Manager | Application Enablement Services | Avaya SBC | Avaya Aura® Device Services |
|---|---|---|---|---|---|---|
| VMware DRS (Compute and Memory)<br>See foot note[4] | Yes | Yes | Yes | Yes<br>See foot note[5] | Yes | Yes |
| Secure boot for virtual machine | Yes | Yes | Yes | Yes | Yes | Yes |
| Content Library | Yes | Yes | Yes | Yes | Yes | Yes |
| VMware Fault Tolerance (FT) | Not supported | Not supported | Not supported | Yes<br>See foot note[6] | Not supported | Yes |
| vSphere Standard Switch | Yes | Yes | Yes | Yes | Yes | Yes |
| vSphere Distributed Switch | Yes | Yes | Yes | Yes | Yes | Yes |
| Hot Pluggable Virtual Hardware | Not supported | Not supported | Not supported | Not supported | Not supported | Not supported |
| Reservation Required<br>see foot note[7] | Yes | Yes | Yes | Yes | Yes | Yes |
| vSAN support<br>See foot note[8] | Yes | Yes | Yes | Yes | Yes | Yes |
| Thin Provisioning | Not supported | Not supported | Not supported | Not supported | Not supported | Not supported |

[4] With two conservative modes - Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

[5] DRS supports In-cluster migration - Applicable for Avaya SBC for Enterprise.

[6] For more information about the Fault Tolerance for Application Enablement Services, see *Avaya Aura Application Enablement (AE) Services 7.x, 8.x, and 10.x High Availability (HA) White Paper.*

[7] Avaya Aura® does not support reservationless deployments on ASP 130. Avaya recommends always making reservations when choosing a reservationless deployment. It is crucial to strictly adhere to the guidelines outlined in the Application Notes. For more information on reservationless deployment, see the *"Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware"* at https://support.avaya.com .

[8] If you are using vSAN, use Thick Provisioning. Even though VMware supports vSAN with Thin Provisioning, Avaya Aura® does not support it.

# Appendix C: PCN and PSN notifications

## PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

## Viewing PCNs and PSNs

### About this task

To view PCNs and PSNs, perform the following steps:

### Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.
2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

# Signing up for PCNs and PSNs

### About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

### Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

# Index


## A

accepting new service ..... 111
Active Call Count
    verifying ..... 103
ADC ..... 88
adding
    Appliance Virtualization Platform host ..... 28
    AVP host ..... 28
    ESXi host ..... 28
    Session Manager as SIP Entity ..... 110
adding ESXi host ..... 28
alarm test ..... 94
Appliance Virtualization Platform
    conditions ..... 27
application
    restart ..... 101
Application Delivery Controller
    overview ..... 88
Application Deployment
    Session Manager field descriptions ..... 42
automatic restart ..... 49
    virtual machine ..... 48
automatic restart configuration ..... 49
Avaya Aura® application
    ESXi version ..... 23
    KVM version ..... 24
Avaya InSite Knowledge Base ..... 116
Avaya Solutions Platform 130 Release 5.1 host
    adding ..... 30
Avaya support website ..... 116

## B

backup
    backup Session Manager ..... 102
    restore ..... 102
    restore Session Manager ..... 102
best practices
    performance and features ..... 119
    VMware networking ..... 122
BIOS ..... 119
BIOS settings
    for Dell servers ..... 120
Branch Session Manager ..... 22

## C

certificate installation
    edge Branch Session Manager ..... 85
change service state
    deny new service ..... 112
changes to platform support ..... 8
Checking EASG status ..... 107
checklist
    deployment procedures ..... 34, 35
    planning procedures ..... 14
    post-installation procedures ..... 92
checklist for KVM
    planning procedures ..... 15
command
    edgeSetup ..... 87
configuration data worksheet
    customer ..... 20
configure
    authentication file with ESXi detail ..... 97
configuring
    edge Branch Session Manager Setup in graphical-user interface ..... 89
    edge Branch Session Manager Setup in text mode ..... 90
    edge Branch Session Manager Setup through CLI ..... 91
    Session Manager ..... 49
    virtual machine automatic restart ..... 48, 49
connections
    verifying ..... 93
creating
    snapshot ..... 97
creating a snapshot ..... 99
customer configuration data ..... 20

## D

data replication ..... 93
    verifying ..... 93
deleting a snapshot ..... 100
deny new service ..... 112
deploy
    Session Manager ..... 40
deploying Branch Session Manager on vCenter using the vSphere client (HTML5) ..... 37
deploying BSM
    OVA using KVM Cockpit ..... 61
deploying Session Manager on vCenter using the vSphere client (HTML5) ..... 37
deploying SM
    OVA using KVM Cockpit ..... 53
deployingBSM on ASP using Script ..... 77
deployingSM on ASP using Script ..... 70
deployment
    thick ..... 127
    thin ..... 127
deployment configuration verification ..... 35
deployment procedures
    checklist ..... 34, 35
disabling EASG ..... 107
document changes ..... 9

documentation
Session Manager ..... 113
downloading software
using PLDS ..... 26

## E

EASG ..... 107
disabling ..... 107
enabling ..... 107
EASGManage ..... 108
Editing
CPU resources for KVM ..... 83
enabling
EASG ..... 108
enabling EASG ..... 107
Enhanced Access Security Gateway ..... 107
Entity Link Connection Status ..... 106
ESXi ..... 130
ESXi host
adding ..... 28
ESXi version
Avaya Aura® application ..... 23

## F

features best practices ..... 119
flexible footprint
reconfiguring hardware resources ..... 104

## G

generate an alarm ..... 94

## H

hardware resources
reconfiguring for flexible footprint ..... 104
host
adding ..... 32

## I

installing
certificates for mutual authentication ..... 86
license file ..... 22
root CA certificate ..... 85
third-party identity certificates ..... 86
installing Session Manager or Branch Session Manager
software patches ..... 51
installing software patches ..... 51
Intel Virtualization Technology ..... 119

## K

KB
KB *(continued)*
Support site ..... 116
knowledge required ..... 9
KVM component
virtualized environment ..... 13
KVM version
Avaya Aura® application ..... 24

## L

latest software patches ..... 27
license file
installing ..... 22
Loading and managing site certificate ..... 109
Local Survivable Processor ..... 50

## M

multiple vSwitches ..... 126

## N

new service
changing state to accept ..... 111
NTP time source ..... 120

## O

OOBM
conditions ..... 27
OVA file
deploy ..... 38

## P

patch information ..... 27
patchSM
commit ..... 50
install ..... 50
remove ..... 50
snapshot ..... 50
status ..... 50
verify ..... 50
PCN ..... 27
PCN notification ..... 133
performance best practices ..... 119
planning procedures
checklist ..... 14
checklist for KVM ..... 15
PLDS
downloading software ..... 26
post-installation
checklist ..... 92
PSN ..... 27
PSN notification ..... 133

## R


release notes for latest software patches ..... 27
removing
    snapshot ..... 99
resources
    server ..... 23
restart
    application ..... 101
restart application from SDM ..... 101
restoring a snapshot ..... 100
reverting
    snapshot ..... 98


## S


SAL Gateway ..... 22
Security Module sanity failure
    troubleshooting ..... 105
Session Manager ..... 22
    configuring ..... 49
    deploy ..... 40
    does not power up ..... 103
Session Manager as SIP Entity
    adding ..... 110
Session Manager field descriptions
    Application Deployment ..... 42
signing up
    PCNs and PSNs ..... 134
SIP Entity ..... 110
SIP Entity Monitoring Status Summary ..... 106
SIP monitoring ..... 106
skills required ..... 9
snapshot ..... 51
    creating ..... 99
    deleting ..... 100
    restoring ..... 100
snapshots ..... 129
software details ..... 22
software patches ..... 27, 51
software requirements ..... 25
Solution Deployment Manager
    restart application ..... 101
storage ..... 127
support ..... 116
supported hardware and resources ..... 23
supported versions
    VMware ..... 23


## T


thick deployment ..... 127
thin deployment ..... 127
timekeeping ..... 120
tools required ..... 9
troubleshooting ..... 93
    power on problem ..... 103
troubleshooting *(continued)*
    Security Module sanity failure Alarms ..... 105


## U


upradingRHEL 8.4 to RHEL 8.10 ..... 117


## V


verify alarm configuration ..... 94
verifying
    Active Call Count ..... 103
    connections ..... 93
    data replication ..... 93
videos ..... 115
viewing
    Entity Link Connection Status ..... 106
    PCNs ..... 133
    PSNs ..... 133
    Security Module status ..... 105
    snapshot list ..... 98
virtual machine
    automatic restart ..... 49
    automatic restart configuration ..... 48
virtualized environment ..... 12
vMotion ..... 128
vmsnapshot
    create ..... 96
    list ..... 96
    remove ..... 96
    revert ..... 96
VMware ..... 130
VMware components
    virtualized environment ..... 12
VMware High Availability ..... 128
VMware networking
    best practices ..... 122
VMware software
    supported ..... 23
VMware software requirements ..... 25
VMware Tools ..... 121
VMware_Features ..... 130
vSphere ..... 130
VT support ..... 119