Deploying Avaya Aura® Communication Manager in Virtualized Environment

Release 10.2.x
Issue 7
April 2025

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying:

- Avaya Aura® Communication 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.
- Avaya Aura® Communication Manager application on Kernel-Based Virtual Machine (KVM) Avaya Solution Platform 130 (Dell Power Edge R640, R660) 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.

This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying Avaya Aura® Communication Manager on a VMware® vSphere™ virtualization environment at a customer site.

The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers themselves. This document does not include optional or customized aspects of a configuration.

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Change History

Issue	Date	Summary of changes
7	April 2025	Updated the following sections for R10.2.1.1: • Viewing the license status on page 107 • License Status field descriptions on page 109 • Supported ESXi version on page 15
6	April 2025	Updated the following sections: • Reducing CPU reservations on the duplex Communication Manager server on page 37 • Correcting the CPU resources for VMware on page 38
5	March 2025	Updated the Deploying Communication Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 64 section.
4	December 2024	Added the Deploying Communication Manager on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 64 section.
3	December 2024	Added the following sections for Release 10.2.1: • Planning checklist for ASP R6.0.x (KVM on RHEL 8.10) on page 13 • Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) on page 14 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 16 • Supported footprints of Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10) on page 20 • Deploying Communication Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit on page 43 • Deploying Communication Manager LSP on ASP R6.0.x (S8300 only) using KVM Cockpit on page 54 • Updating the CPU resources for KVM Cockpit on page 75 Updated the following sections for Release 10.2.1: • Purpose on page 7 • Virtualized Environment overview on page 10 • Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) on page 11 • Updating the CPU resources for KVM Cockpit on page 75
2	March 2024	Updated the following sections: • VMware features supported by Avaya Aura on page 135 • Supported footprints of Communication Manager OVA on VMware on page 18

Table continues…

Issue	Date	Summary of changes
1	December 2023	Release 10.2

Chapter 2: Architecture Overview

Virtualized Environment overview

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

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with 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, R660) is a single host server with 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 customer-provided Virtualized Environment.

Note:

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

Related links

Supported ESXi version on page 15

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.

Table continues…

Virtualized component	Description
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
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. 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

Deployment guidelines

- Deploy maximum number of virtualized environments on the same host.
- Deploy the virtualized environment on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as Avaya Aura® applications, from other virtual machines.
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not oversubscribe resources. Oversubscribing affects performance.
- Monitor the server, host, and virtualized environment performance.

Chapter 3: Planning and preconfiguration for deploying Communication Manager

Planning checklist for VMware®

Ensure that the customer completes the following before deploying the Communication Manager Open Virtualization Application (OVA) on Customer-provided VMware or Avaya-supplied Avaya Solutions Platform 130.

#	Task	Description	✔
1	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 14.	
2	Plan the staging and verification activities and assign the resources.		
3	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4	Download the required Communication Manager OVA.	See Downloading software from PLDS on page 13.	
5	Download the latest Communication Manager patch. For example: 00.0.441.0-XXXXX.tar.	See Patch Installation or Patch Updates on page 42	

For information about VMware features supported by Avaya Aura®, see VMware features supported by Avaya Aura on page 135

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

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

#	Task	Description	✔
1	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 14.	
2	Plan the staging and verification activities and assign the resources.		
3	Download the required Avaya Aura® OVA.	See Downloading software from PLDS on page 13.	
4	Download the latest Communication Manager patch (Service Pack or Feature Pack).	See Patch Installation or Patch Updates on page 42	

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.

Downloading software from PLDS

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

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

Note:

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

Procedure

1. On your web browser, type https://plds.avaya.com to access the Avaya PLDS website.
2. Enter your login ID and password.

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

   Note:

   The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

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

Supported 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 browsers

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

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

Note:

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

Related links

Accessing Communication Manager System Management Interface on page 106

Supported ESXi version

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

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

Note:

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

Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).

- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

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

Supported 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	Y	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 R660 or Dell R640. The Dell R660 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 R660 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, R660) is a single host server with 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, R660, 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 R660 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, R660, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0): S8300E
- 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, R660) is a single host server with 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® Communication Manager*

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.

Supported footprints of Communication Manager OVA on VMware

Note:

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

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

The following table describes the resource requirements to support different profiles for Communication Manager on Customer-provided VMware and Avaya-supplied Avaya Solutions Platform 130:

Footprint (Max users)	vCPU	CPU Reservation (MHz)	Memory (MiB)	Hard disk (GiB)	Minimum CPU Speed (MHz)	Extra NICs
CM Main Max users 1000	2	3900	3584	64	1950	0
CM Survivable Max users 1000	1	1950	4096	64	1950	0
CM Simplex1 Max users 2400	2	4340	4096	64	2170	0
CM Simplex2 Max users 41000 (Can be used as Main or Survivable)	2	4340	4608	64	2170	0
CM Duplex Max users 30000 (CM Duplex–Main or Survivable–up to 30,000 users)	3	6510	5120	64	2170	1
CM High Duplex Max users 41000 (For Hi-Duplex Servers for Main or survivable)	3	7650	5120	64	2550	1

Note:

The following deployment options are for future use:

- CM Standard Duplex Array Max Users 300000
- CM High Duplex Array Max Users 300000
- CM Simplex Array Max users 300000

If you select any of these options during deployment, it results in an unsupported configuration, and you must redeploy Communication Manager with a supported profile.

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.

Supported footprints of Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10)

Note:

- Avaya Aura® Communication Manager supports ASP R6.0.x (KVM on RHEL 8.10) hosts with Hyperthreading enabled at the BIOS level.
- Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

The following table describes the resource requirements to support different profiles for Communication Manager on Avaya-supplied Avaya Solutions Platform 130 Release 6.0:

Footprint (Max users)	vCPU	CPU Reservation (MHz)	Memory (MiB)	Hard disk (GiB)	Minimum CPU Speed (MHz)	Extra NICs
CM Main Max users 1000	2	3900	3584	64	1950	0
CM Survivable Max users 1000	1	1950	4096	64	1950	0
CM Simplex1 Max users 2400	2	4340	4096	64	2170	0
CM Simplex2 Max users 41000 (Can be used as Main or Survivable)	2	4340	4608	64	2170	0
CM Duplex Max users 30000 (CM Duplex–Main or Survivable–up to 30,000 users)	3	6510	5120	64	2170	1
CM High Duplex Max users 41000 (For Hi-Duplex Servers for Main or survivable)	3	7650	5120	64	2550	1

Note:

The following deployment options are for future use:

- CM Standard Duplex Array Max Users 300000
- CM High Duplex Array Max Users 300000
- CM Simplex Array Max users 300000

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

If you select any of these options during deployment, it results in an unsupported configuration, and you must redeploy Communication Manager with a supported profile.

Software details of Communication Manager

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

Communication Manager server separation

In earlier releases, Communication Manager duplex configurations required a cable for connecting two Communication Manager instances with dedicated Communication Manager server hardware. From Communication Manager 7.1 and later, you can physically separate the Communication Manager duplex instances.

Following are the minimum requirements for software duplex connectivity that must be met between the two Communication Manager instances:

- Total capacity must be 1 Gbps or more.
- Round-trip packet loss must be 0.1% or less.
- Round trip delay must be 60 ms when Application Enablement Services is not configured and 30 ms when Application Enablement Services is configured.
- The duplication ports of both servers must be on the same LAN/IP subnet.
- Duplication link encryption must be disabled for the busy-hour call rates that results in greater than 40% CPU occupancy.
- CPU occupancy on the active server must be less than 65% to allow memory refresh from the active to standby server.

Cloned and copied OVAs are not supported

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA. At this time, Avaya only supports the deployment of new OVAs.

Chapter 4: Deploying Communication Manager on VMware

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.

Note:

Enabling of encryption is not supported when deploying Communication Manager on ESXi host directly.

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.

       For more information about supported footprints, see “Supported footprints of Communication Manager on VMware”.
    d. Clear **Power on automatically**.
11. Click **Next**.
12. On the Additional settings page, click **Next**.

    Note:

    Entering IP or Naming data under Additional settings will not carry forward to the virtual machine. This information must be entered manually later in the implementation process.
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.

      Expand the Memory setting for Communication Manager deployed as an LSP, and set the value of the **Reservation** parameter to None.

      Note:
    - 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.

    Log in as craft/craft01, then input the application configuration parameters explained in the “Configuration” chapter.

Deploying the OVA on vCenter by using vSphere Client (HTML5)

About this task

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

Before you begin

- Access vCenter Server by using vSphere Client.

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.
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.
    - The system displays an additional Properties window to configure the Communication Manager parameters. For more information about configuring Communication Manager parameters, see Properties field descriptions on page 28.
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.
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. When the system starts for the first time, configure the parameters for the application.

20. Click the **Console** tab and verify that the system startup is successful.

Deploying the Communication Manager OVA file by using Solution Deployment Manager

About this task

Use this procedure to deploy Communication Manager by using Solution Deployment Manager.

Before you begin

- 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.
- Remove the existing Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the Solution Deployment Manager by using the FQDN only. 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 Location <location name> section, click **New**.

   Solution Deployment 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 Communication Manager 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 Configuration Parameters section, complete the fields.

    For more information, see Application Deployment field descriptions on page 30.
12. In the Network Parameters section:

    For the ESXi host or Avaya Solutions Platform 130, select the required port groups.
13. For Duplex configuration, on the **Network Parameters** tab, perform one of the following:
    - For Avaya Solutions Platform, in the Select a Network Mapping for Additional VM Network Interfaces section, select the required values in **Duplication Link**.
    - For VMware, in the Select a Network Mapping for VM Network Interfaces section, select the required values in the **Duplication Link** field.
14. Click **Deploy**.
15. 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.
16. To view details, click the **Status Details** link.

Result

When you deploy the Communication Manager duplex pair through Solution Deployment Manager Application Management, Solution Deployment Manager creates the Active Communication

Manager and Standby Communication Manager element entries using the IP Address or FQDN of the respective Communication Manager on the System Manager **Services** > **Inventory** > **Manage Elements** page. To perform the Communication Manager synchronization and other operations, you must edit the Active Communication Manager server entry as following:

1. On the Manage Elements page, select the current Active Communication Manager element entry and click **Edit**.
2. On the Edit Communication Manager page, in **Alternate IP Address**, type the current Standby Communication Manager server IP Address or FQDN.
3. To administer Communication Manager on System Manager, select the **Add to Communication Manager** check box.
4. To enable the Notify Sync feature, select the **Enable Notifications** check box.

Properties field descriptions

Note:

Assign a valid value for each field. If you assign an invalid value for a field, you cannot power on the virtual machine.

Name	Description
CM IPv4 Address	Enter the IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	Enter the subnet mask of the Communication Manager virtual machine.
CM IPv4 Gateway	Enter the IP address of the default gateway. **Note:** Configure the default gateway for the Public network.
CM IPv6 Address	Enter the IPv6 address of the Communication Manager virtual machine.
CM IPv6 Gateway	Enter the IPv6 address of the default gateway. **Note:** Configure the default gateway for the Public network.
CM IPv6 Network Prefix	Enter the IPv6 network prefix of the Communication Manager virtual machine.
EASG Enabled	Enables the Enhanced Access Security Gateway (EASG) feature.

Table continues…

Name	Description
Out of Band Management IPv4 Address	Enter the IP Address for Out-of-Band Management. This field is optional. If you do not want to configure Out-of-Band Management, leave the value of this field as zeros.
Out of Band Management IPv4 Netmask	Enter the netmask for Out-of-Band Management. This field is optional. If you do not want to configure Out-of-Band Management, leave the value of this field as zeros.
CM Hostname	Enter the hostname or an FQDN of Communication Manager. **Note:** Regardless of the interface used to access, the hostname remains the same. The Public interface is the default.
NTP Server(s)	Enter the IP Address of the Network Time Protocol (NTP) server for the Communication Manager virtual machine. This field is optional. You can add up to three NTP servers. The application supports only the NTP server. It does not support the NTP pool.
DNS Server(s)	Enter the IP Address of the Domain Name System (DNS) server for the Communication Manager virtual machine. This field is optional. You can add up to three DNS servers.
Search Domain List	This field is optional.
WebLM Server IPv4 Address	Enter the IP address of the reachable WebLM Server.
CM Privileged Administrator User Login	Enter the login name for the Communication Manager privileged administrator.
CM Privileged Administrator User Password	Enter the password for the Communication Manager privileged administrator. The value range is from 8 to 255 characters.

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. 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.

Table continues…

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. 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`. 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.
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>` The field is available only when you click **Browse**. **Note:** 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. 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**. Selects the OVA or ISO file of the application that you want to deploy.
Flexi Footprint	The footprint size supported for the selected application. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.

Communication Manager Configuration Parameters

Name	Description
CM IPv4 Address	The IPv4 address of the Communication Manager virtual machine.
CM IPv4 Netmask	The IPv4 network mask of the Communication Manager virtual machine.

Table continues…

Name	Description
CM IPv4 Gateway	The IPv4 default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine. The field is optional.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine. The field is optional.
CM IPv6 Gateway	The IPv6 gateway of the Communication Manager virtual machine. The field is optional.
Out of Band Management IPv4 Address	The IPv4 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv4 Netmask	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Server(s)	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). You can type up to three NTP servers. The application supports only the NTP server. It does not support the NTP pool.
DNS Server(s)	The DNS IP address of the Communication Manager virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IPv4 address of the reachable WebLM server. The field is mandatory.

Table continues…

Name	Description
EASG User Access	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends that you enable EASG. You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.
Confirm Password	The password required to be confirmed. The field is mandatory.

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. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • 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. • In case the administrator forgets to add the passphrase at deployment time, then the boot will proceed with a blank passphrase. The administrator has to just press enter to proceed, because the passphrase is blank. The administrator will be prompted to set the passphrase, only after the Release 8.1.2 and later patch is installed and the system is rebooted. • **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. • **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. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. 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. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

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. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**. 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. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
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**.

Cloned and copied OVAs are not supported

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA. At this time, Avaya only supports the deployment of new OVAs.

Duplication link configuration for duplex OVA deployment

To deploy the Duplex OVA, install the Duplex OVA on two different hosts. Ensure that the hosts reside on two different clusters. Similar to the Simplex OVA, the Duplex OVA has one network interface configured in the OVA. An example host configuration for the Duplex OVA can be setup to include two virtual machine network connection type vSwitches, For example,

- *VM Network* to use with the Communication Manager NIC 0 administration/call_processing traffic – connected to say vmnic 0
- *CM_duplication_link* to use with the Communication Manager NIC 1 duplication link traffic – connected to say vmnic 1

Before you start the virtual machine, you must change the Communication Manager virtual machine settings to configure the second NIC. For information about changing the virtual machine settings, see *Changing the virtual machine settings*.

Related links

Changing the virtual machine settings on page 37

Changing the virtual machine settings

About this task

To configure the second NIC, you must change the virtual machine settings.

Procedure

1. In the vSphere client, select the host ESXi server.
2. Right-click the OVA and select **Edit Settings**.

   The system displays the Virtual Machine Properties window.
3. In the **Hardware** tab, select the Network adapter 1 to assign to the *VM Network* under *Network Connection*.
4. Select the Network adapter 2 and then select the *CM_duplication_link* network name from the **Network label** drop-down list under *Network Connection*.

Related links

Duplication link configuration for duplex OVA deployment on page 36

Reducing CPU reservations on the duplex Communication Manager server

Procedure

1. In the vSphere client, select the host ESXi server.
2. Deploy the Communication Manager OVA.
3. Reduce reservations before the virtual machine starts booting.
   a. Right-click the Communication Manager virtual machine and select **Edit Settings**.
   b. On the **Settings** window, select the **Resources** tab.
   c. In the left pane, under **Settings**, select **CPU**.
   d. In the right pane, adjust the MHz values in the **Reservation** line.
   e. Change the value from **7650** to **7200** MHz.
   f. Click **OK** to exit the window.
4. Boot the Communication Manager virtual machine.

   Note:

   The default deployment reserves the CPU resources based on CPU speed as mentioned in the table on page 20. However, the number of CPUs may increase to match the CPU speed. The VM might not power on due to a higher number of CPUs.

To correct the CPU resources, see Correcting the CPU resources for VMware on page 38.

Note:

Modifying the CPU reservation below the recommended CPU speed lowers the performance.

Correcting the CPU resources for VMware

Procedure

1. In the vSphere client, select the host ESXi server.
2. Select and right-click the virtual machine.
3. Click **Edit Settings**.

   The system displays the Virtual Machine Properties window.
4. Click the **Resources** tab to display the virtual machine resources, such as CPU, Memory, Disk, Advanced CPU, and Advanced Memory.
5. In the *Resource Allocation* section, adjust the CPU reservation and click **OK**.
6. Check the CPU requirements in the **Summary** tab of the virtual machine.
   - Duplex: 3x the CPU speed noted under the host's **Summary** tab
   - Simplex: 1x or 2x the CPU speed noted under the host's **Summary** tab

   Sometimes adjusting the CPU reservations might not correct the problem for starting the virtual machine. To start the virtual machine adjust the CPU speed more. Also, you can follow the same procedure to adjust the other virtual machine resources.

   Important:

   Do not change any other resource settings, for example, removing resources completely. Modifying these allocated resources can have a direct impact on the performance and capacity of the Communication Manager virtual machine. Virtual machine must meet the resource size requirements so that Communication Manager can run at full capacity. Removing or greatly downsizing resource reservations can put this requirement at risk. You are responsible for making any modifications to the resource reservation settings.

   Warning:

   If a virtual machine problem occurs, Avaya Global Support Services (GSS) might not be able to assist in fully resolving a problem. Avaya GSS can help you to reset the values to the optimized values before starting to investigate the problem.

Support for Enhanced Access Security Gateway

Communication Manager supports Enhanced Access Security Gateway (EASG). EASG is a certificate based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provides support and troubleshooting.

EASG provides a secure method for Avaya services personnel to access the Communication Manager 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 Health check. EASG must be enabled for Avaya Services to perform the required maintenance tasks.

You can enable or disable EASG through Communication Manager.

EASG only supports Avaya services logins, such as init, inads, and craft.

Discontinuance of ASG and ASG-enabled logins

EASG in Communication Manager 7.1.1 and later replaces Avaya's older ASG feature. In the older ASG, Communication Manager allowed the creation of ASG-enabled user logins through the SMI Administrator Accounts web page. Such logins are no longer supported in Communication Manager 7.1.1 and later. When upgrading to Communication Manager 7.1.1 or later from older releases, Communication Manager does not support ASG-enabled logins.

For more information about EASG, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Enabling or disabling EASG through the CLI interface

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, 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 (http://support.avaya.com/registration) 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.

Procedure

1. Log in to the Communication Manager CLI interface as an administrator.
2. To check the status of EASG, run the following command: `EASGStatus`.
3. To enable EASG (Recommended), run the following command: `EASGManage --enableEASG`.

4. To disable EASG, run the following command: `EASGManage --disableEASG`.

Enabling or disabling EASG through the SMI interface

About this task

By enabling Avaya Services Logins you are granting Avaya access to your system. This setting is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com for Avaya remote connectivity. See the Avaya support site support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Services Logins you are denying Avaya access to your 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.

Procedure

1. Log on to the Communication Manager SMI interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the **Security** section, click **Server Access**.
4. In the **Avaya Services Access via EASG** field, select:
   - **Enable** to enable EASG.
   - **Disable** to disable EASG.
5. Click **Submit**.

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Communication Manager CLI interface.
2. Run the following command: `EASGProductCert --certInfo`.

EASG product certificate expiration

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

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

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge or response.

Managing site certificates

Before you begin

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

Procedure

1. Log in to the CLI interface as an administrator.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate, run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates currently installed on the system.

Patch Installation or Patch Updates

You can apply the Communication Manager patch using any of the following:

- Solution Deployment Manager
- Communication Manager SMI
- Communication Manager CLI

For more information about applying the Communication Manager patch or installing the Communication Manager Security Service Pack (SSP), see the *Upgrading Avaya Aura® Communication Manager* document.

Chapter 5: Deploying Communication Manager on ASP R6.0.x (KVM on RHEL 8.10)

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

About this task

Communication Manager Simplex requires two network interfaces and Communication Manager Duplex requires three network interfaces.

Communication Manager provides a KVM OVA that contains two `qcow2` files:

- system.qcow2
- Var_Disk.qcow2

Note:

- Disk encryption is currently *not* supported.
- 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 Communication 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`
- The **chown** command now allows **custadm** to write into the `staging` directory with **sudo**. The permissions should look as follows:

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

```
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo ls -ld /var/lib/libvirt/staging
ls: cannot access '/var/lib/libvirt/staging': No such file or directory
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo mkdir /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo chown custadm:wheel /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 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@cmdvitkvm1 libvirt]$
```

- Copy the Communication Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using the winscp tool and **custadm** credentials.
- Ensure you are logged into the CLI. If not, login to the ASP R6.0.x CLI with **custadm** credentials.
- Ensure that the network bridge is configured during the KVM deployment.

  Make sure that you create the required brdges during KVM deployment:

  For example, Management VM Netowrk, OOBM Network.

  Duplex Communication Manager requires Duplication network. For more information, see Creating Duplication Network on ASP R6.0.x (KVM on RHEL 8.10) using direct attachment on page 73.

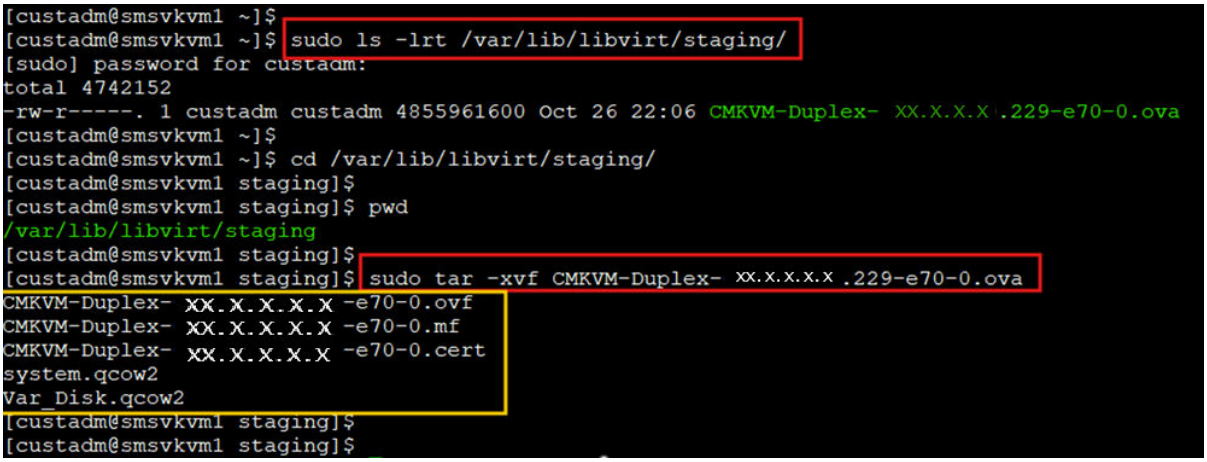
Note:

All the following commands *must* be prefaced with **sudo**:

- Run the following command to verify the Communication 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 CMKVM-Duplex-010.2.0.0.229-e70-0.ova**

  KVM OVA file extracts the following files:
  - CMKVM-Duplex-010.2.0.0.229-e70-0.ovf

- CMKVM-Duplex-010.2.0.0.229-e70-0.mf
- CMKVM-Duplex-010.2.0.0.229-e70-0.cert
- system.qcow2
- Var_Disk.qcow2



The extracted qcow2 images are in thin provision format. The qcow2 images MUST be converted to thick provision. 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:

- CM10.2[unique identifier]-system.qcow2
- CM10.2[unique identifier]-Var_Disk.qcow2

The examples in this document will use the following:

- CM10.2-system.qcow2
- CM10.2-Var_Disk.qcow2

Go to `/var/lib/libvirt/staging` folder, and run the following command to convert `system.qcow2` (thin) to `CM10.2-system.qcow2` (thick) image:

- **`sudo qemu-img convert -O qcow2 -o preallocation=full system.qcow2 CM10.2-system.qcow2`**

Go to `/var/lib/libvirt/staging` folder, and run the following command to convert `Var_Disk.qcow2` (thin) to `CM10.2Var_Disk.qcow2` (thick):

- **`sudo qemu-img convert -O qcow2 -o preallocation=full Var_Disk.qcow2 CM10.2-Var_Disk.qcow2`**

```
[custadm@smsvkvm1 ~]$
[custadm@smsvkvm1 ~]$ cd /var/lib/libvirt/staging/
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ pwd
/var/lib/libvirt/staging
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo ls -lrt
total 9484304
-rw-r--r--. 1   12359 users        7492 Aug 29 13:20 CMKVM-Duplex- XX.X.X.X.X -e70-0.cert
-rw-r--r--. 1   12359 users       58999 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X.X -e70-0.ovf
-rw-r--r--. 1   12359 users         284 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X.X -e70-0.mf
-rw-r--r--. 1   12359 users  3268083712 Sep  3 17:27 system.qcow2
-rw-r--r--. 1   12359 users  1587806208 Sep  3 17:28 Var_Disk.qcow2
-rw-r-----. 1 custadm custadm 4855961600 Oct 26 22:06 CMKVM-Duplex-XX.X.X.X.X-e70-0.ova
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo qemu-img convert -O qcow2 -o preallocation=full system.qcow2 CM XX.X-system.qcow2
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo qemu-img convert -O qcow2 -o preallocation=full Var_Disk.qcow2 CM XX.X-Var_Disk.qcow2
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$
```

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

- sudo qemu-img info CM10.2-system.qcow2

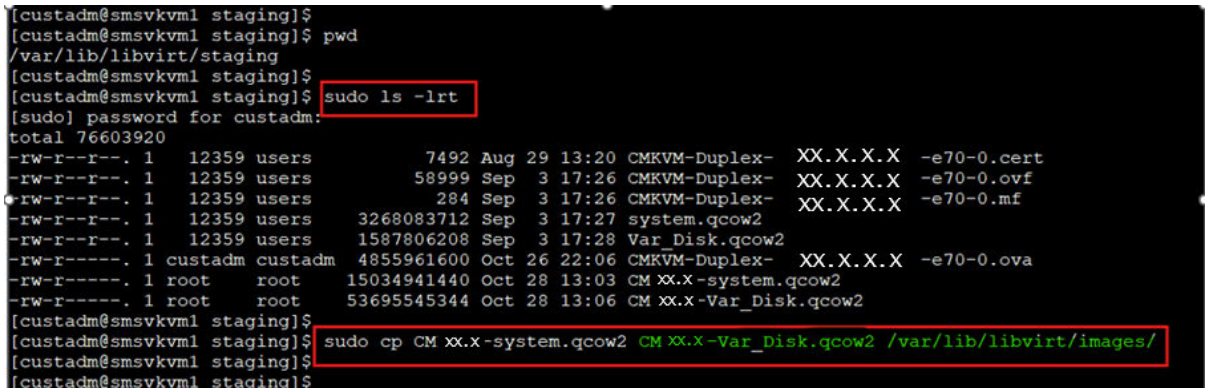
  Disk size must display as 14 GB
- sudo qemu-img info CM10.2-Var_Disk.qcow2

  Disk size must display as 50 GB

```
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo ls -lrt
total 76603920
-rw-r--r--. 1   12359 users          7492 Aug 29 13:20 CMKVM-Duplex- XX.X.X.X.X -e70-0.cert
-rw-r--r--. 1   12359 users         58999 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X.X -e70-0.ovf
-rw-r--r--. 1   12359 users           284 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X.X -e70-0.mf
-rw-r--r--. 1   12359 users    3268083712 Sep  3 17:27 system.qcow2
-rw-r--r--. 1   12359 users    1587806208 Sep  3 17:28 Var_Disk.qcow2
-rw-r-----. 1 custadm custadm  4855961600 Oct 26 22:06 CMKVM-Duplex- XX.X.X.X.X -e70-0.ova
-rw-r-----. 1 root    root    15034941440 Oct 28 13:03 CM XX.X -system.qcow2
-rw-r-----. 1 root    root    53695545344 Oct 28 13:06 CM XX.X -Var_Disk.qcow2
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo qemu-img info CM XX.X -system.qcow2
image: CM XX.X -system.qcow2
file format: qcow2
virtual size: 14 GiB (15032385536 bytes)
disk size: 14 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@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo qemu-img info CM XX.X -Var_Disk.qcow2
image: CM XX.X -Var_Disk.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@smsvkvm1 staging]$
```

Go to `/var/lib/libvirt/staging` folder and run the following command to copy the `CM10.2-system.qcow2` and `CM10.2-Var_Disk.qcow2` to the `/var/lib/libvirt/images` directory:

- **sudo cp CM10.2-system.qcow2 CM10.2-Var_Disk.qcow2 /var/lib/libvirt/images**



Go to `/var/lib/libvirt/images` directory and run the following command to verify the qcow2 images are present:

- sudo ls –lrt

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 CM10.2-system.qcow2

  sudo chown qemu:qemu CM10.2-Var_Disk.qcow2

  sudo chmod 640 CM10.2-system.qcow2

  sudo chmod 640 CM10.2-Var_Disk.qcow2

```
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ pwd
/var/lib/libvirt/images
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo ls -lrt
total 67119616
-rw-r-----. 1 root root 15034941440 Oct 28 14:18 CM xx.x -system.qcow2
-rw-r-----. 1 root root 53695545344 Oct 28 14:21 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chown qemu:qemu CM xx.x -system.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chown qemu:qemu CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chmod 640 CM xx.x -system.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chmod 640 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo ls -lrt
total 67119616
-rw-r-----. 1 qemu qemu 15034941440 Oct 28 14:18 CM xx.x -system.qcow2
-rw-r-----. 1 qemu qemu 53695545344 Oct 28 14:21 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 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.

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.

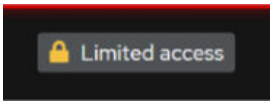


Figure 1: Limited access button

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`**.

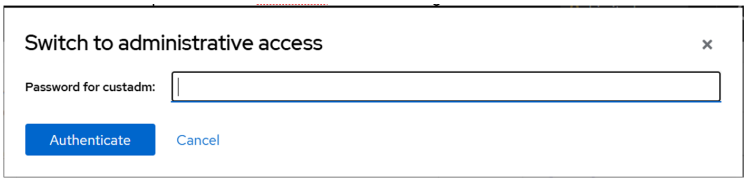


Figure 2: Switch to administrative access

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

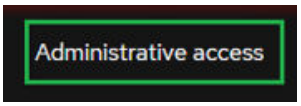


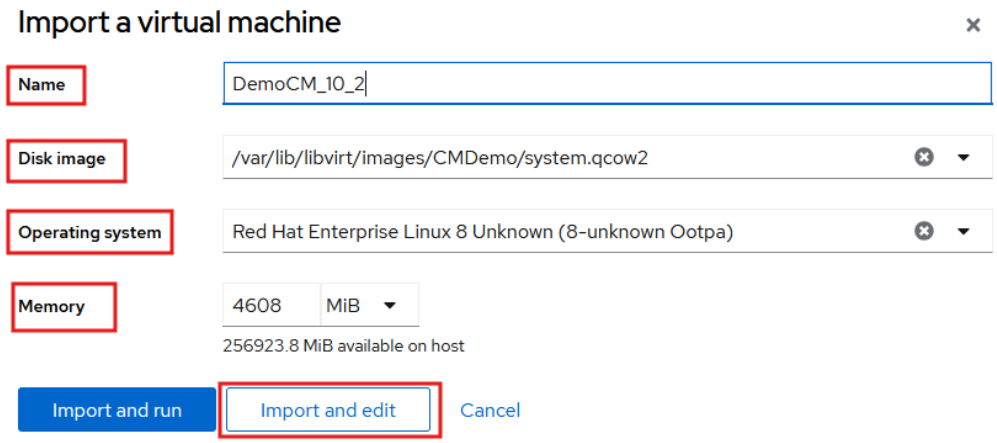
Figure 3: Administrative access button

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 Communication Manager virtual machine.
   b. In the **Disk Image** field, select the `CM10.2-system.qcow2` image of the Communication Manager on the KVM Cockpit host under `/var/lib/libvirt/images/` directory.
   c. In the **Operating System** field, select **RHEL 8 Unknown** 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 Communication Manager OVA 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 `cm10.2-system.qcow2` disk image size is correctly displayed in the **Capacity** field.

Note:

Communication Manager requires a total of 64 GB hard disk. In which, 14 GB is used for `CM10.2-system.qcow2` and 50 GB is used for `CM10.2-Var_Disk.qcow2`.

By default, **virtio** is selected under the **Bus** field, and this needs to be modified.

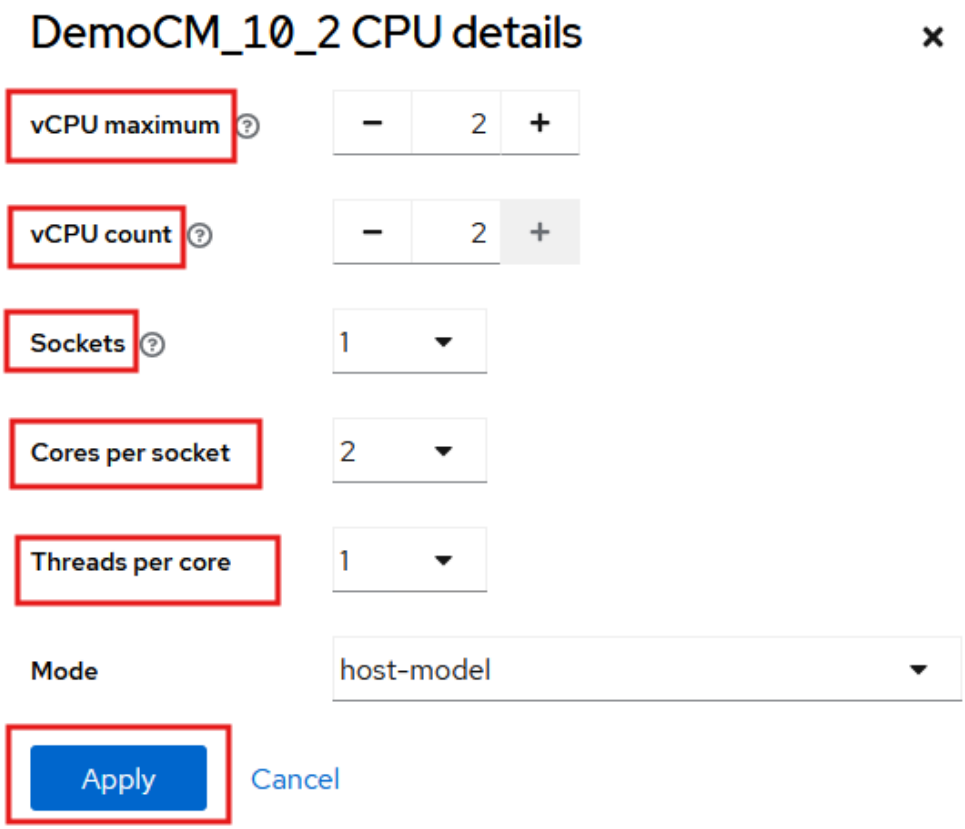
6. Under the Disks section, click **Edit**.
7. In the Edit <attributes name> window, do the following:
   a. in the **Bus** field, select **scsi**.
   b. In the **Cache** field, select **directsync**.
   c. click **Save**.

      In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.
8. Click **Add disk** to add `CM10.2-Var_Disk.qcow2` disk image, and do the following:
   a. In the **Source** field, select **Custom path**.
   b. In the **Custom path** field, select `CM10.2-Var_Disk.qcow2` image on the KVM host location path `/var/lib/libvirt/images`
   c. In the **Device** field, select **Disk image file**.
   d. Expand the **Show additional options** field.
   e. In the **Cache** field, select **directsync**.
   f. In the **Bus** field, select **SCSI** bus type.
   g. Click **Add**.

   In the Disks section, verify that the two disk images are assigned correctly. The newly added disk must have the 50 GiB assigned under the **Capacity** and **Used** fields, **scsi** assigned under the **Bus** field, and **directsync** under the **Cache** field.
9. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
10. In the Overview section, in the **CPU** field, click **edit**.

    CPU Details window opens.
11. 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 Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10) on page 20.



12. In the **Mode** field, keep the default **host-model** as is. Do Not change it.
13. Click **Apply**.
14. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.

Note:

- Simplex Communication Manager requires two NICs:
  - NIC1 is for the Public IP address
  - NIC2 is for the Out of Band Management (OOBM)
- Duplex Communication Manager requires three NICs. Ensure that NIC1 and NIC2 must be in two different networks.
  - NIC1 is for the Public IP address
  - NIC2 is for the Duplication Network
  - NIC3 is for the Out of Band Management (OOBM)

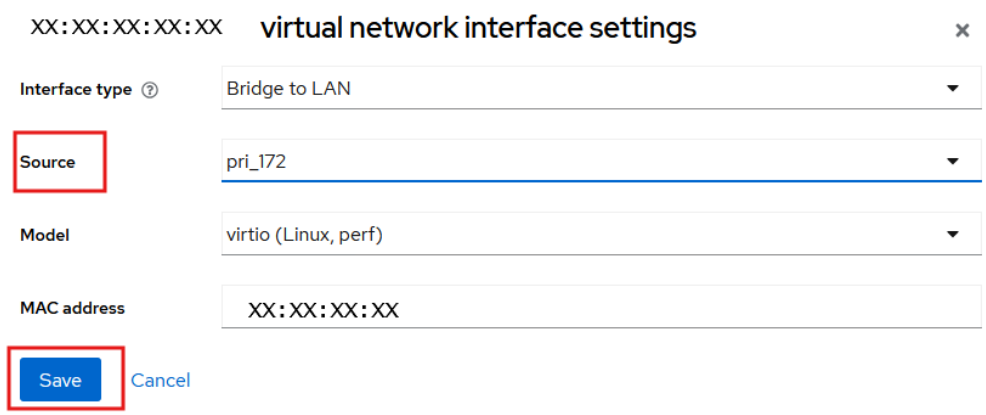
Ensure that two network interfaces are added for Communication Manager Simplex and three network interfaces are added for Communication Manager Duplex.

For Duplex Communication Manager, add Duplication Network and OOBM Network.

Note:

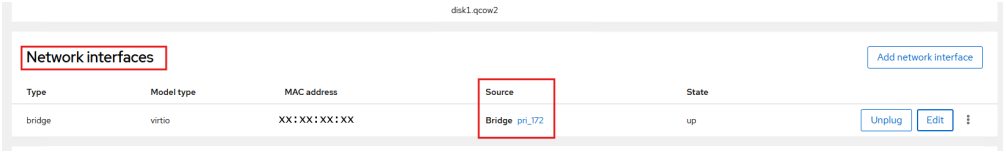
For Duplication Network, value in the **Interface type** must be **Direct attachment**.

For Simplex Communication Manager, add OOBM Network.



15. To configure the duplication network interface, or OOBM network interface, or both, 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.

       For Duplex Communication Manager configuration, select the required source for eth1 and duplicated ethernet interface.

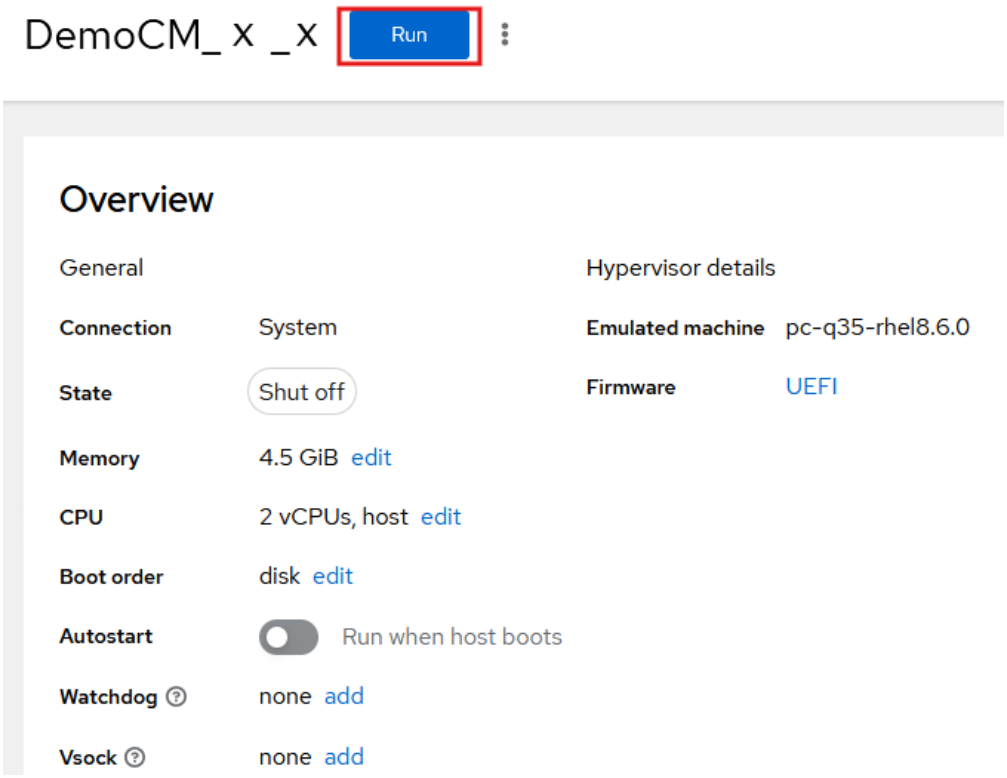


16. Click **Add**.

    For Duplex Communication Manager, ensure that three NICs are added. The three NICs must appear in the Network interfaces window.

    For Simplex Communication Manager, ensure that two NICs are added. Two NICs must appear in the Network interfaces window.

17. On the virtual machine, click **Run** to start the Communication Manager virtual machine.



Next steps

On first boot of the Communication Manager virtual machine, login to the virtual console using the `craft`/`craft01` and provide the configuration and networking parameters.

Follow the Configuration steps described in the “Configuring the Communication Manager” chapter. These steps are the same regardless of the underlying hypervisor. For more information, see Configuration and administration checklist on page 89

Application of Communication Manager Feature Packs, Service Packs, SSPs, Patches should then be performed. Note that these will need to be done using the Communication Manager CLI or Communication Manager SMI.

Existing instructions for installation of these artifacts using the CLI and UI are applicable. Note that the “snapshot” functionality present in ASP R5.1.x and earlier is replaced with an equivalent feature, titled Virtual Machine Backup. For more information about installing Service Packs or SSPs, and Virtual Machine Backup (clone), see the *Upgrading Avaya Aura® Communication Manager*

Deploying Communication Manager LSP on ASP R6.0.x (S8300 only) using KVM Cockpit

About this task

Communication Manager Simplex requires two network interfaces

Communication Manager provides a KVM OVA that contains two `qcow2` files:

- system.qcow2
- Var_Disk.qcow2

Note:

- Disk encryption is currently *not* supported for Communication Manager LSP
- 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.

Before you begin

- Download the Communication 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`

  The **`chown`** command now allows **`custadm`** to write into the `staging` directory with **`sudo`**. The permissions should look as follows:

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

```
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo ls -ld /var/lib/libvirt/staging
ls: cannot access '/var/lib/libvirt/staging': No such file or directory
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo mkdir /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo chown custadm:wheel /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 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@cmdvitkvm1 libvirt]$
```

- Copy the Communication Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using the winscp tool and **`custadm`** credentials.
- If not still in the CLI, login again to the ASP R6.0.x CLI with **`custadm`** credentials.
- Ensure that the network bridge is configured during the KVM deployment.

Note:

All the following commands *must* be prefaced with "**`sudo`**":

- Run the following command to verify the Communication 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 CMKVM-Simplex-010.2.0.0.229-e70-0.ova`**

  KVM OVA file extracts the following files:

  - CMKVM-Simplex-010.2.0.0.229-e70-0.ovf
  - CMKVM-Simplex-010.2.0.0.229-e70-0.mf
  - CMKVM-Simplex-010.2.0.0.229-e70-0.cert
  - system.qcow2
  - Var_Disk.qcow2

```
[custadm@cmdvitkvml ~]$
[custadm@cmdvitkvml ~]$ cd /var/lib/libvirt/staging/
[custadm@cmdvitkvml staging]$
[custadm@cmdvitkvml staging]$ pwd
/var/lib/libvirt/staging
[custadm@cmdvitkvml staging]$
[custadm@cmdvitkvml staging]$ sudo ls -lrt
[sudo] password for custadm:
total 2900800
-rw-r-----. 1 custadm custadm 2970419200 Nov 29 11:59 CMKVM-Simplex-X.X.X.X.890-e67-3E.ova
[custadm@cmdvitkvml staging]$
[custadm@cmdvitkvml staging]$ sudo tar -xvf CMKVM-Simplex-X.X.X.X.890-e67-3E.ova
CMKVM-Simplex-X.X.X.X.890-e67-3E.ovf
CMKVM-Simplex-X.X.X.X.890-e67-3E.mf
CMKVM-Simplex-X.X.X.X.890-e67-3E.cert
install_vm.py
ovf.py
system.qcow2
Var_Disk.qcow2
[custadm@cmdvitkvml staging]$
[custadm@cmdvitkvml staging]$
```

The extracted qcow2 images are in thin provision format. The qcow2 images MUST be converted to thick provision. 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:

- CM10.2[unique identifier]-system.qcow2
- CM10.2[unique identifier]-Var_Disk.qcow2

The examples in this document will use the following:

- CM10.2-system.qcow2
- CM10.2-Var_Disk.qcow2

Go to `/var/lib/libvirt/staging` folder, and run the following command to convert `system.qcow2` (thin) to `CM10.2-system.qcow2` (thick) image:

- **`sudo qemu-img convert -O qcow2 -o preallocation=full system.qcow2 CM10.2-system.qcow2`**

Go to `/var/lib/libvirt/staging` folder, and run the following command to convert `Var_Disk.qcow2` (thin) to `CM10.2Var_Disk.qcow2` (thick):

- **`sudo qemu-img convert -O qcow2 -o preallocation=full Var_Disk.qcow2 CM10.2-Var_Disk.qcow2`**

```
[custadm@smsvkvml ~]$
[custadm@smsvkvml ~]$ cd /var/lib/libvirt/staging/
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$ pwd
/var/lib/libvirt/staging
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$ sudo ls -lrt
total 9484304
-rw-r--r--. 1   12359 users        7492 Aug 29 13:20 CMKVM-Duplex-XX.X.X.X.X-e70-0.cert
-rw-r--r--. 1   12359 users       58999 Sep  3 17:26 CMKVM-Duplex-XX.X.X.X.X-e70-0.ovf
-rw-r--r--. 1   12359 users         284 Sep  3 17:26 CMKVM-Duplex-XX.X.X.X.X-e70-0.mf
-rw-r--r--. 1   12359 users  3268083712 Sep  3 17:27 system.qcow2
-rw-r--r--. 1   12359 users  1587806208 Sep  3 17:28 Var_Disk.qcow2
-rw-r-----. 1 custadm custadm 4855961600 Oct 26 22:06 CMKVM-Duplex-XX.X.X.X.X-e70-0.ova
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$ sudo qemu-img convert -O qcow2 -o preallocation=full system.qcow2 CMXX.X-system.qcow2
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$ sudo qemu-img convert -O qcow2 -o preallocation=full Var_Disk.qcow2 CMXX.X-Var_Disk.qcow2
[custadm@smsvkvml staging]$
[custadm@smsvkvml staging]$
```

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

- sudo qemu-img info CM10.2-system.qcow2

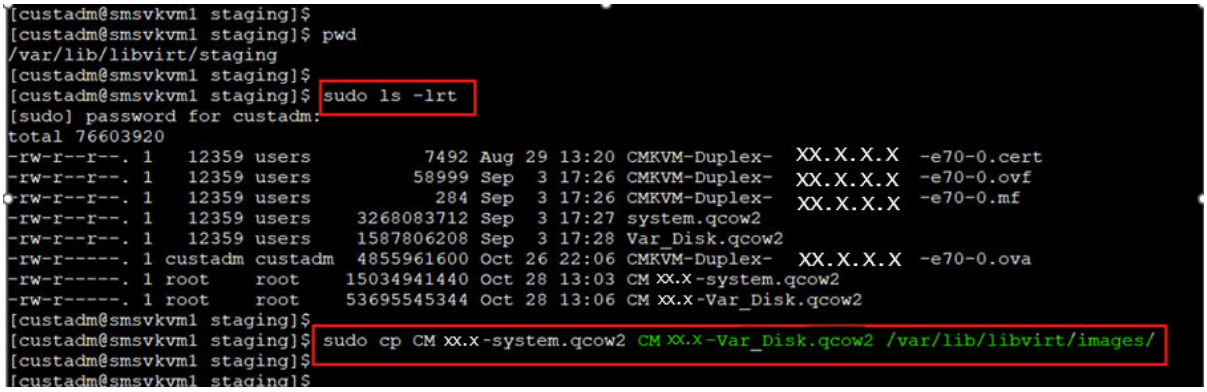
  Disk size must display as 14 GB

- sudo qemu-img info CM10.2-Var_Disk.qcow2

  Disk size must display as 50 GB

Go to `/var/lib/libvirt/staging` folder and run the following command to copy the `CM10.2-system.qcow2` and `CM10.2-Var_Disk.qcow2` to the `/var/lib/libvirt/images` directory:

- **sudo cp CM10.2-system.qcow2 CM10.2-Var_Disk.qcow2 /var/lib/libvirt/images**



Go to `/var/lib/libvirt/images` directory and run the following command to verify the qcow2 images are present:

- sudo ls –lrt

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 CM10.2-system.qcow2

  sudo chown qemu:qemu CM10.2-Var_Disk.qcow2

  sudo chmod 640 CM10.2-system.qcow2

  sudo chmod 640 CM10.2-Var_Disk.qcow2

```
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ pwd
/var/lib/libvirt/images
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo ls -lrt
total 67119616
-rw-r-----. 1 root root 15034941440 Oct 28 14:18 CM xx.x -system.qcow2
-rw-r-----. 1 root root 53695545344 Oct 28 14:21 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chown qemu:qemu CM xx.x -system.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chown qemu:qemu CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chmod 640 CM xx.x -system.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo chmod 640 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ sudo ls -lrt
total 67119616
-rw-r-----. 1 qemu qemu 15034941440 Oct 28 14:18 CM xx.x -system.qcow2
-rw-r-----. 1 qemu qemu 53695545344 Oct 28 14:21 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 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 *CM*

  sudo rm system.qcow2 Var_disk.qcow2

```
[custadm@smsvkvm1 images]$
[custadm@smsvkvm1 images]$ cd /var/lib/libvirt/staging/
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo ls -lrt
total 76603920
-rw-r--r--. 1   12359 users          7492 Aug 29 13:20 CMKVM-Duplex- XX.X.X.X -e70-0.cert
-rw-r--r--. 1   12359 users         58999 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X -e70-0.ovf
-rw-r--r--. 1   12359 users           284 Sep  3 17:26 CMKVM-Duplex- XX.X.X.X -e70-0.mf
-rw-r--r--. 1   12359 users    3268083712 Sep  3 17:27 system.qcow2
-rw-r--r--. 1   12359 users    1587806208 Sep  3 17:28 Var_Disk.qcow2
-rw-r-----. 1 custadm custadm  4855961600 Oct 26 22:06 CMKVM-Duplex- XX.X.X.X -e70-0.ova
-rw-r-----. 1 root    root    15034941440 Oct 28 13:03 CM xx.x -system.qcow2
-rw-r-----. 1 root    root    53695545344 Oct 28 13:06 CM xx.x -Var_Disk.qcow2
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo rm *CM*
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo rm system.qcow2 Var_Disk.qcow2
[custadm@smsvkvm1 staging]$
[custadm@smsvkvm1 staging]$ sudo ls -lrt
total 0
[custadm@smsvkvm1 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.

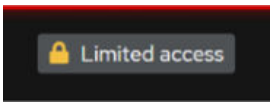


Figure 4: Limited access button

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**.

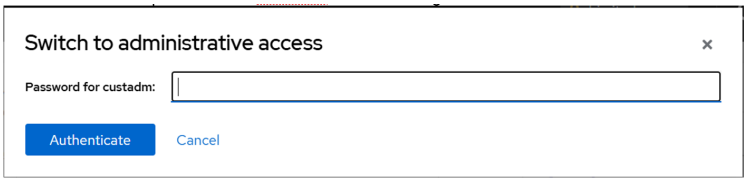


Figure 5: Switch to administrative access

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

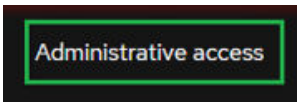


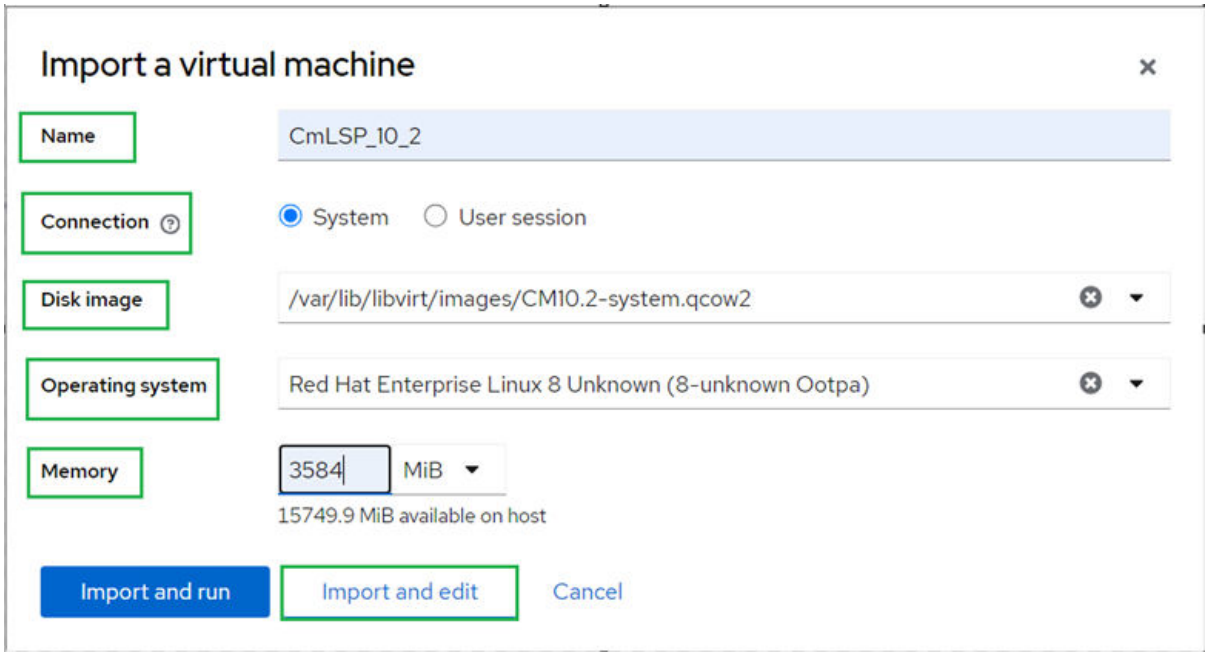
Figure 6: Administrative access button

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 Communication Manager virtual machine.
   b. In the **Disk Image** field, select the `CM10.2Simplex-system.qcow2` image of the Communication Manager on the KVM Cockpit host under `/var/lib/libvirt/images/` directory.
   c. In the **Operating System** field, select **RHEL 8 Unknown** 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 Communication Manager OVA 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 `cm10.2Simplex-system.qcow2` disk image size is correctly displayed in the **Capacity** field.

Note:

Communication Manager requires a total of 64 GB hard disk. In which, 14 GB is used for `CM10.2-system.qcow2` and 50 GB is used for `CM10.2-Var_Disk.qcow2`.

By default, **virtio** is selected under the **Bus** field.

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. Click **Add disk** to add `CM10.2-Var_Disk.qcow2` disk image, and do the following:
   a. In the **Source** field, select **Custom path**.
   b. In the **Custom path** field, select `CM10.2Simplex-Var_Disk.qcow2` image on the KVM host location path `/var/lib/libvirt/images`
   c. In the **Device** field, select **Disk image file**.

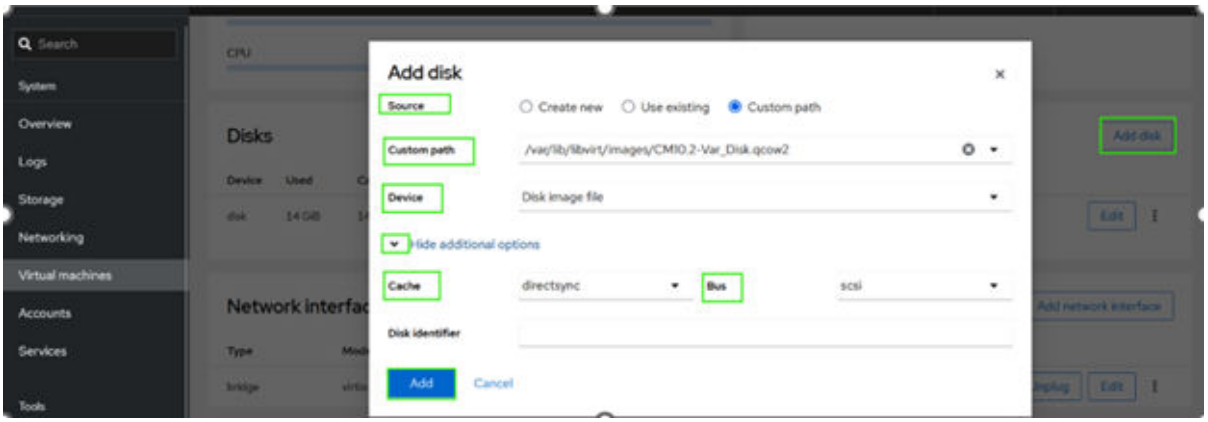
d. Expand the **Show additional options** field.

e. In the **Cache** field, select **directsync**.

f. In the **Bus** field, select **SCSI** bus type.

g. Click **Add**.

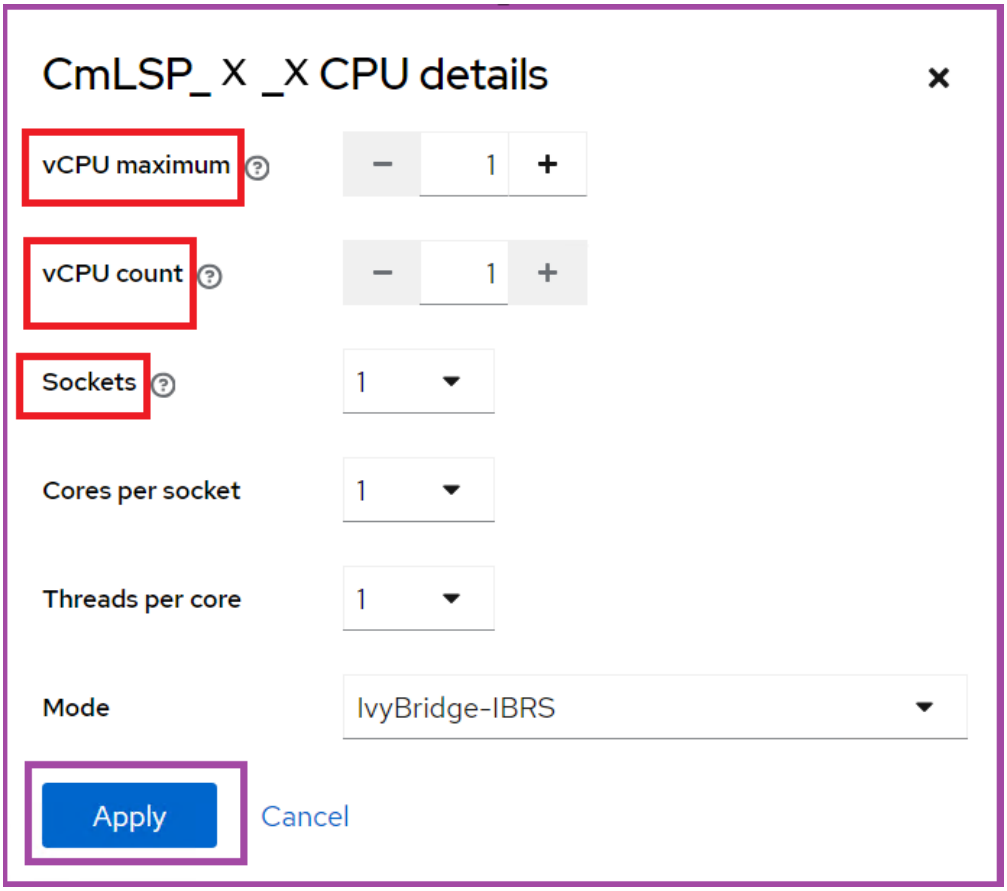
In the Disks section, verify that the two disk images are assigned correctly. The newly added disk must have the 50 GiB assigned under the **Capacity** and **Used** fields, **scsi** assigned under the **Bus** field, and **directsync** under the **Cache** field.



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

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

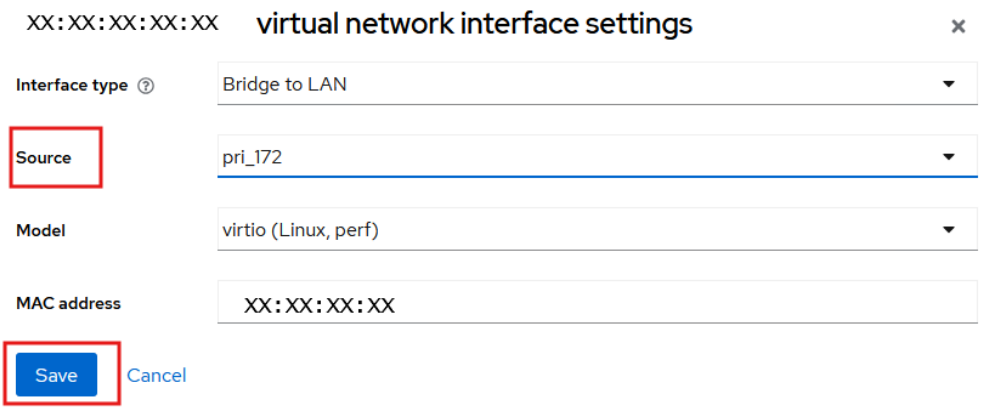
    For more information on footprints, see Supported footprints of Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10) on page 20.
12. In the **Mode** field, keep the default **IvyBridge-IBRS** as is. Do Not change it.
13. Click **Apply**.



14. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.

Note:

- Simplex Communication Manager requires two NICs:
  - NIC1 is for the Public IP address
  - NIC2 is for the Out of Band Management (OOBM)

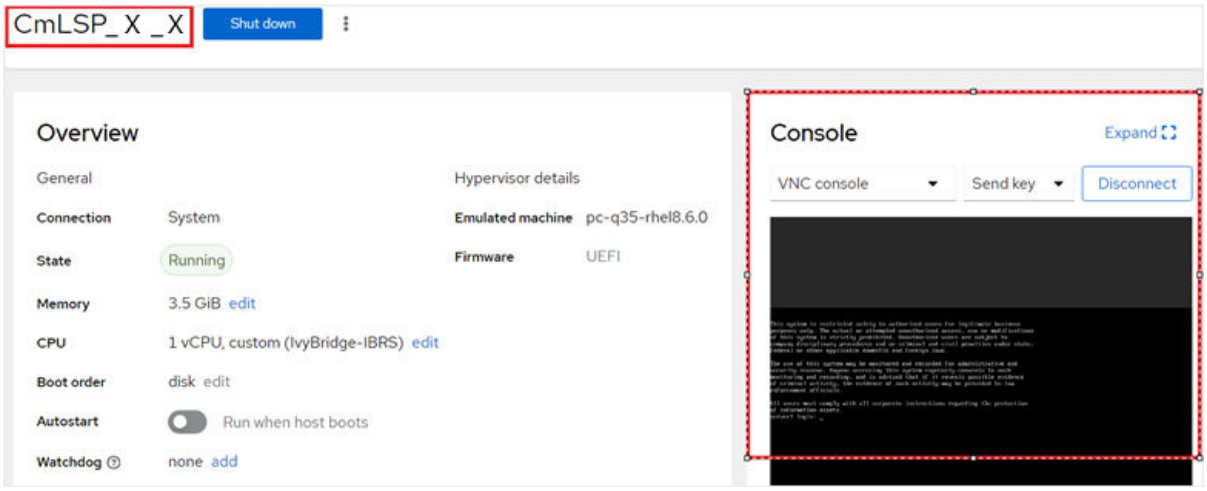


Ensure that two network interfaces are added for Communication Manager Simplex.

For Simplex Communication Manager, add OOBM Network.

15. To configure the duplication network interface, or OOBM network interface, or both, 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.
16. Click **Add**.

    For Simplex Communication Manager, ensure that two NICs are added. Two NICs must appear in the Network interfaces window.
17. On the virtual machine, click **Run** to start the Communication Manager virtual machine.



Next steps

On first boot of the Communication Manager virtual machine, login to the virtual console using the `craft`/`craft01` and provide the configuration and networking parameters.

Follow the Configuration steps described in the Communication Manager 10.2 deployment guide for standard Communication Manager configuration. These steps are the same regardless of the underlying hypervisor.

Application of Communication Manager Feature Packs, Service Packs, SSPs, Patches should then be performed. Note that these will need to be done using the Communication Manager CLI or Communication Manager SMI. SDM and SDM Client cannot currently be used with the new *KVM on RHEL 8.10* hypervisor.

Existing instructions for installation of these artifacts using the CLI and UI are applicable. Note that the “snapshot” functionality present in ASP R5.1.x and earlier is replaced with an equivalent feature, titled Virtual Machine Backup. For more information about installing Service Packs or SSPs, see the *Upgrading Avaya Aura® Communication Manager*

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

About this task

Communication Manager provides a KVM OVA that contains two `qcow2` files:

- system.qcow2
- Var_Disk.qcow2

Note:

- Disk encryption is possible using the script-based deployment.
- 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 Communication 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`**
- 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@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo ls -ld /var/lib/libvirt/staging
ls: cannot access '/var/lib/libvirt/staging': No such file or directory
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo mkdir /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 libvirt]$ sudo chown custadm:wheel /var/lib/libvirt/staging
[custadm@cmdvitkvm1 libvirt]$
[custadm@cmdvitkvm1 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@cmdvitkvm1 libvirt]$
```

- Copy the Communication Manager KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **custadm** credentials.
- Ensure you are logged into the ASP R6.0.x CLI. If not, login to the ASP R6.0.x CLI with **custadm** credentials.
- Run the following command to verify the Communication Manager KVM image is available in the staging folder:

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

```
[custadm@cmdvitkvm1 ~]$
[custadm@cmdvitkvm1 ~]$ sudo ls -lrt /var/lib/libvirt/staging/
[sudo] password for custadm:
total 2900752
-rw-r-----. 1 custadm custadm 2970368000 Oct 21 11:12 CMKVM-Simplex-xx.x.0.0.890-e67-3E.ova
[custadm@cmdvitkvm1 ~]$
[custadm@cmdvitkvm1 ~]$
```

- Ensure that the required network bridges are configured during the KVM deployment. For example, Management VM Network, OOBM Network. Duplex Communication Manager requires Duplication network (Direct attachment). For more information, see Creating Duplication Network on ASP R6.0.x (KVM on RHEL 8.10) using direct attachment on page 73.

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:
• For simplex, run: **sudo tar -xvf CMKVM-Simplex-*.ova**
KVM OVA extracts the following files:
- CMKVM-Simplex-*.ovf
- CMKVM-Simplex-*.mf
- CMKVM-Simplex-*.cert
- install_vm.py
- ovf.py
- system.qcow2
- Var_Disk.qcow2
• For duplex, run: **sudo tar -xvf CMKVM-Duplex-*.ova**
KVM OVA extracts the following files:
- CMKVM-Duplex-*.ovf
- CMKVM-Duplex-*.mf
- CMKVM-Duplex-*.cert
- install_vm.py
- ovf.py
- system.qcow2
- Var_Disk.qcow2
b. Run the following script to deploy Communication Manager:
sudo python3 install_vm.py
	Run the following script to deploy Communication Manager: **installVM CMKVM-*.ova**
	ASP completes the auto-verification to ensure the following files are available:
	`CM-Duplex-*-KVM-1.ovf`
	`CM-Duplex-*-KVM-1.mf`
	`CM-Duplex-*-KVM-1.cert`
	`install_vm.py`
	`ovf.py`
	`system.qcow2`
	`Var_Disk.qcow2`
	`CM-Duplex-*-KVM-1.cert: OK`
	`Verified OK`
	`CM-Duplex-*-KVM-1.ovf: OK`
	`install_vm.py: OK`
	`ovf.py: OK`
	`system.qcow2: OK`
	`Var_Disk.qcow2: OK`

4. Press **ENTER** to read the **EULA**.
5. Press **Y** to accept the **EULA**.
6. Enter a name for the Communication Manager virtual machine. For example, `CM_Main`.
7. Select the required Communication Manager profile from the following table:

Communication Manager Simplex	Communication Manager Duplex
CM Array Max users 300000	CM High Duplex Array Max Users 300000
CM Main Max users 1000	CM High Duplex Max Users 41000
CM Main Max users 2400	CM Standard Duplex Array Max Users 300000

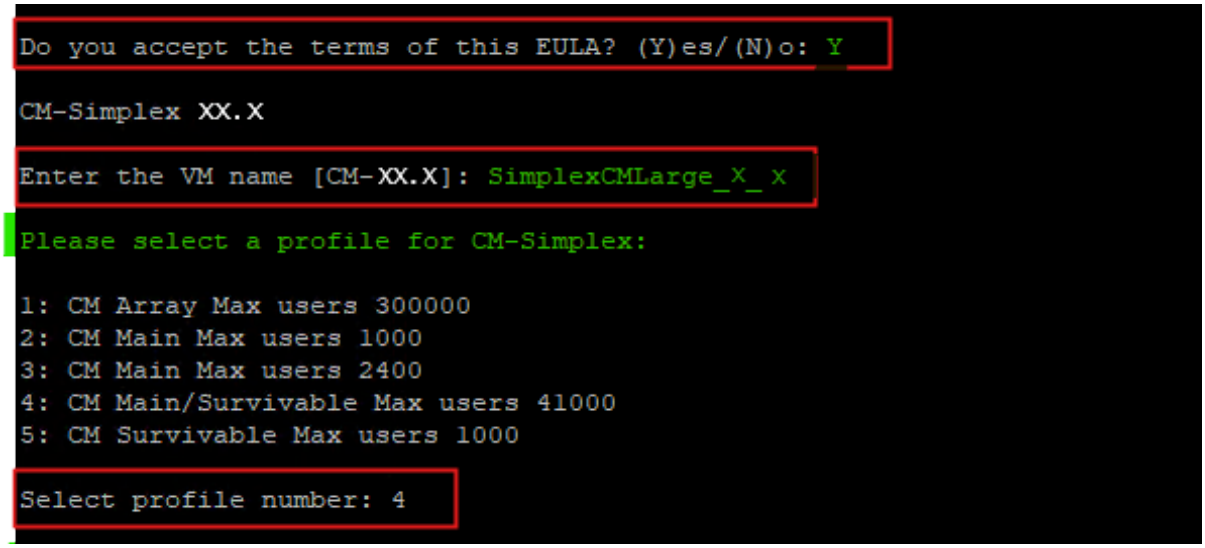
Table continues…

Communication Manager Simplex	Communication Manager Duplex
CM Main/Survivable Max users 41000	CM Standard Duplex Max users 30000
CM Survivable Max users 1000	

The following deployment options are for future use:

- CM Standard Duplex Array Max Users 300000
- CM High Duplex Array Max Users 300000
- CM Simplex Array Max users 300000

For more information, see Supported footprints of Communication Manager OVA 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 Communication Manager.

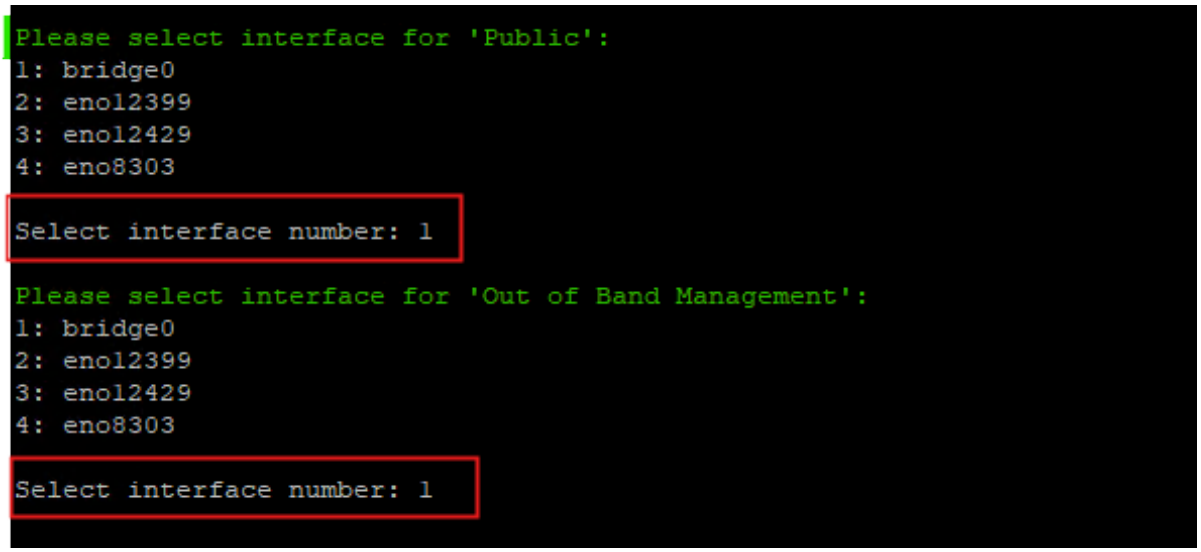
   Note:

   - Simplex Communication Manager requires two NICs.
     - NIC1 is for the Public IP address
     - NIC2 is for the Out of Band Management (OOBM)
   - Duplex Communication Manager requires three NICs. Ensure that NIC1 and NIC2 must be in two different networks.
     - NIC1 is for the Public IP address
     - NIC2 is for the Duplication Network
     - NIC3 is for the Out of Band Management (OOBM)

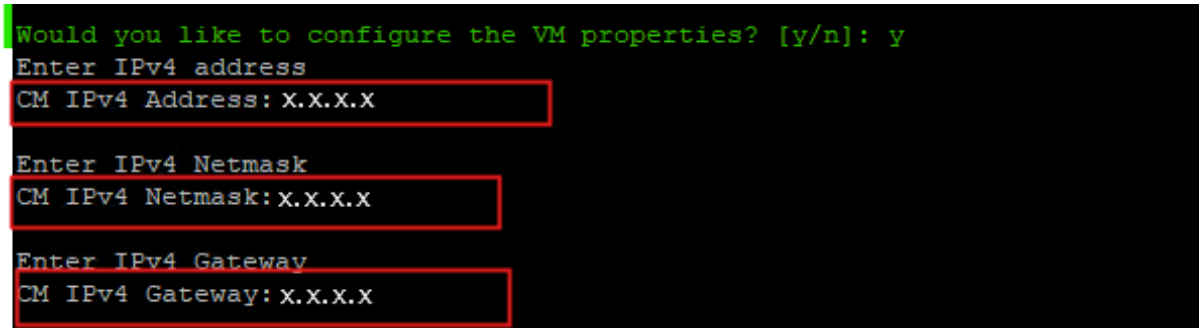
For Duplex Communication Manager , Duplication Link interface is Mandatory, and MUST use the Direct Attachment (interface name). For example, **eno***

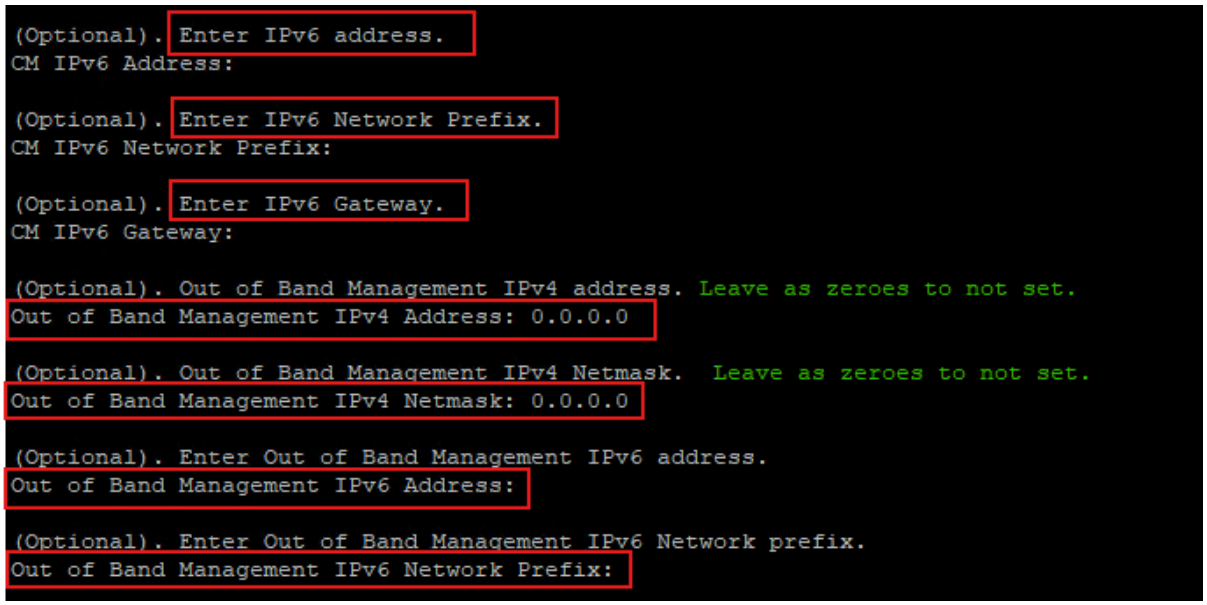
Ensure that two network interfaces are added for Communication Manager Simplex and three network interfaces are added for Communication Manager Duplex.

ASP 6.0.x CLI displays the currently available disk space and the required disk space to deploy Communication 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. Enter **IPv4 address**. For example, x.x.x.x
   b. Enter **IPv4 Netmask**. For example, m.m.m.m
   c. Enter **IPv4 Gateway**. For example, g.g.g.g
   d. **(Optional)** For **IPv6 address**, enter the valid IPv6 address.
   e. **(Optional)** For **IPv6 Network Prefix**, enter the valid IPv6 network prefix.
   f. **(Optional)** For **IPv6 Network Gateway**, enter the valid IPv6 network gateway.
   g. For **Out of Band Management IPv4 address**, if you don't want to use OOBM, enter 0.0.0.0 or enter the valid IPv4 address.
   h. For **Out of Band Management IPv4 Netmask**, if you don't want to use OOBM, enter 0.0.0.0 or enter the valid IPv4 Netmask.
   i. **(Optional)** For **Out of Band Management IPv6 address**, enter the valid OOBM IPv6 address.
   j. **(Optional)** For **Out of Band Management IPv6 Network prefix,** enter the valid OOBM IPv6 network prefix.





10. In the **CM Hostname** field, enter a valid host name or a FQDN.

    If a FQDN is entered, FQDN also administers the local domain name. Valid characters are, a - z, A - Z, 0 - 9, and hyphen (-).

11. In the **NTP Server(s)** field, enter a valid NTP address or a hostname.

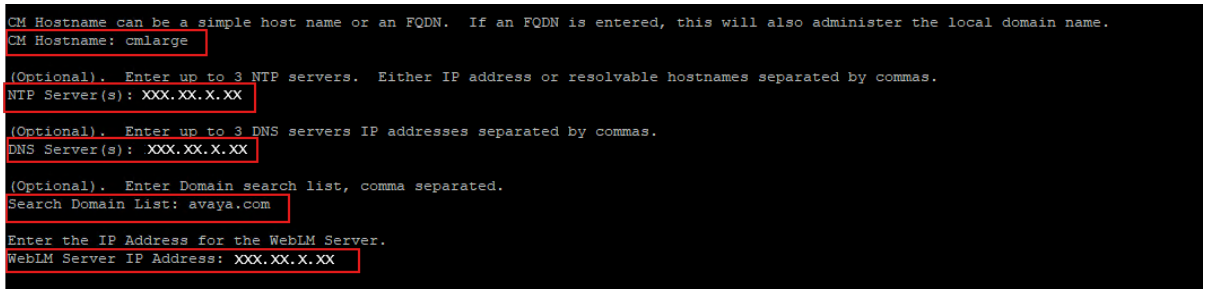
    You can type up to three NTP servers seperated by a comma.

12. In the **DNS Server(s)** field, enter a valid DNS server IP address.

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

13. In the **Search Domain List** field, enter a search list of domain names. For example,*mydomain.com*

14. In the **WebLM Server IP Address** field, enter the IP address of the reachable WebLM server.



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. To create CM Privileged Administrator User Login, do the following:

    - In the **CM Privileged Administrator User Login**, enter a privileged user name for the administrator.

      This is the login name for the Communication Manager privileged administrator.
    - In the **CM Privileged Administrator User Password** field, enter a password for the Communication Manager privileged administrator.
    - In the **Confirm CM Privileged Administrator User Password** field, reenter the password for the Communication Manager privileged administrator.

17. 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 Communication Manager reboots.

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

   Important:

   You *MUST* remember 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.

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

    Note:

    Once the Communication Manager virtual machine is successfully deployed, ASP R6.0.x displays the following message: `Domain creation completed`. Otherwise, repeat step 3 on page 65 onwards.

21. Log in to the KVM Cockpit web console as **custadm** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
22. If Web console is in **Limited access** mode, click on **Turn on administrative access** button.

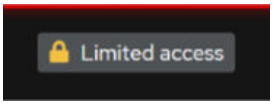


Figure 7: Limited access button

Note:

VMs are not visible when in **Limited access** mode.

23. For administration actions, on the top-right of the window, click on the **Limited access** or **Turn on administrative access** button.

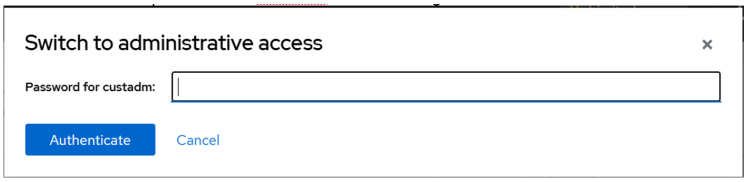


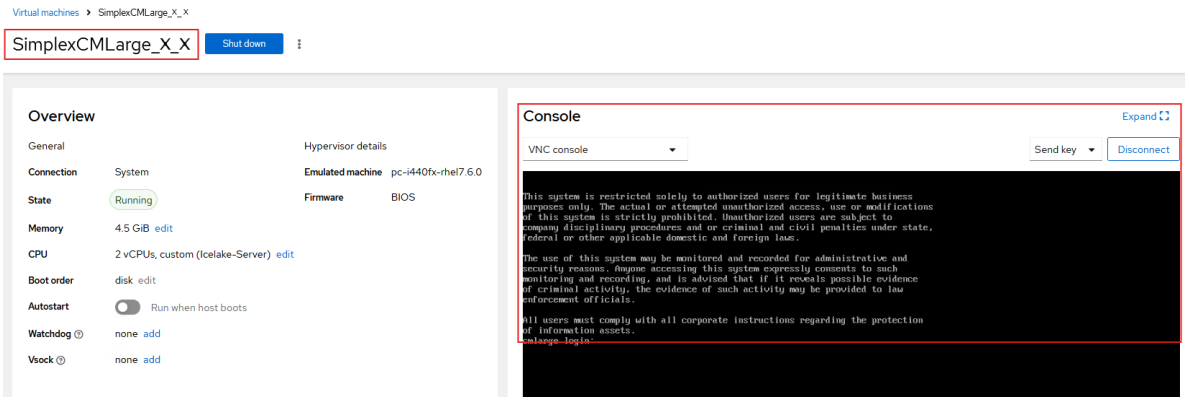
Figure 8: Switch to administrative access

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

    Verify that the Communication Manager virtual machine is deployed.
25. Click on the Communication Manager virtual machine.
26. If the **Power on VM automatically after deploy?: [y/n]** field is set to **n**, then click **Run** to power on the virtual machine.

    If the **Power on VM automatically after deploy?: [y/n]** field is set to **y**, Communication Manager virtual machine starts automatically.
27. Click on **VM Name** and login from Console.
28. Login to Communication Manager virtual machine console using privilege user credentials created in step 16 on page 70.

    During the first login, change the privilege user password.



29. **(Optional)** In the Overview section, enable **AutoStart** to automatically start the virtual machine whenever the host reboots.

Creating Duplication Network on ASP R6.0.x (KVM on RHEL 8.10) using direct attachment

About this task

You must connect two servers ethernet port with each other to enable duplication network.

Following is an example of a duplication network where ethernet ports are connected between two servers:

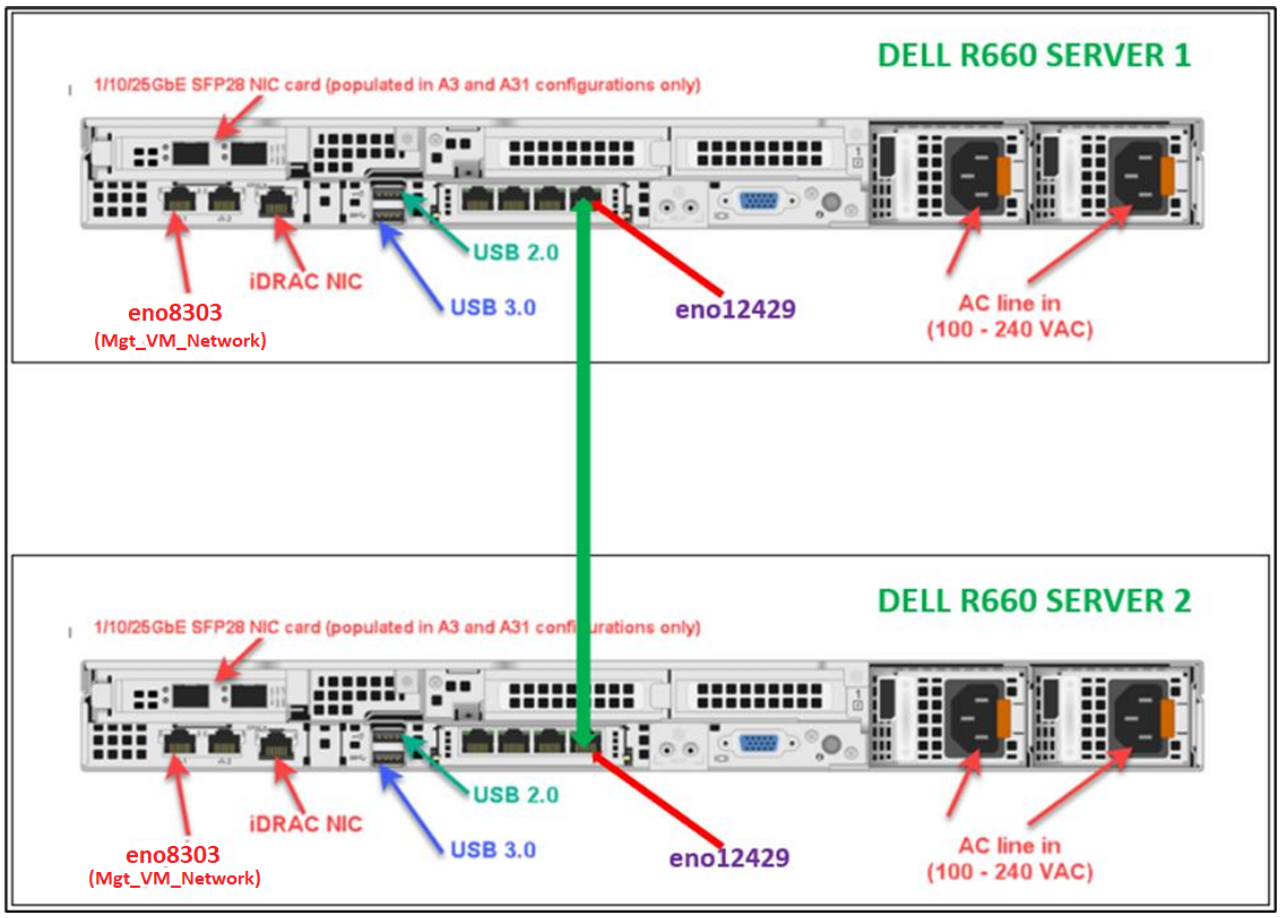


Figure 9: Duplication network

Procedure

1. Login 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 top-right of the window, click **Limited access** button.

   The button changes to **Administrative access**.

   Warning:

   Administrative access is equivalent to root access. Be careful when you change the settings!
3. Go to **System** > **Networking** > **Interfaces** and click on a name of the interface.
4. In the **Interfaces** window, configure duplication IPv4 address to use for Communication Manager Duplex configuration.

   The **Network interface** window appears.
5. On top right corner of the **Network interface** window, enable the toggle button.

6. In the **Network interface** window, ensure that the interface status and IPv4 address appears.
7. In the **Interfaces** window, ensure that the interface is assigned with the configured duplication IPv4 address.
8. To add another server, repeat 1 on page 74 to 7 on page 75.

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.

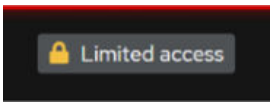


Figure 10: Limited access button

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`**.

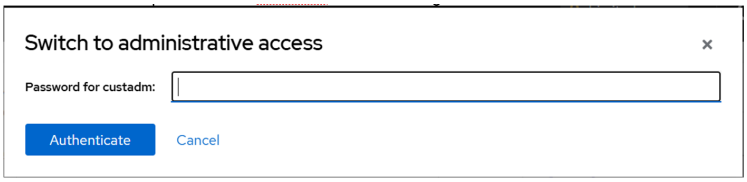


Figure 11: Switch to administrative access

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

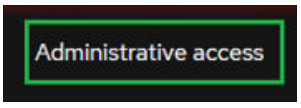


Figure 12: Administrative access button

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.

Configuring the Communication Manager LSP Memory

About this task

Use this procedure to configure CM Memory for the CM LSP.

Before you begin

- Deploy the CM LSP with the correct memory and CPU configuration. For more information, see Deploying Communication Manager LSP on ASP R6.0.x (S8300 only) using KVM Cockpit on page 54.
- Configure the network details.
- Check the CM Memory Config by running the **`swversion`** command. If it does not show Small Survivable then follow the procedure below.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Server Role**.
4. The Communication Manager System Management Interface displays the Server Role page.
5. From the **Server Settings** list, select `a local survivable processor (LSP) of non CM Cluster`.
6. Enter the following fields under **Configure Survivable Data**:
   a. If the Main CM is Simplex, the Registration address and File Synchronization address (Main Server) must be Simplex Main CM IP.
   b. If the Main CM is Duplex, the Registration address must be Alias IP of Duplex CM and enter the File Synchronization address for the **Main Server** (Duplex CM1 IP) and **Duplicate Server**(Duplex CM2 IP).
7. Under **Configure Memory section**, from **This Server's Memory Setting** drop-down list, select `Small Survivable` for CM LSP.
8. Under **Configure Memory section**, from the **Main Server's Memory Setting** drop-down list, select a valid memory option depending on the Main CM.

9. Click **Change**.
10. Click the **Restart CM** button after configuring CM memory.

Result

CM profile configuration displays Small Survivable for CM LSP.

Chapter 6: Managing the ESXi host by using SDM

Adding a location

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
4. Click **Save**.

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

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 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.

Related links

Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 124

Managing vCenter

Creating a role for a user

About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**
      - **Datastore cluster**
      - **Distributed switch**
      - **Folder**
      - **Host profile**
      - **Network**
      - **Resource**
      - **Tasks**
      - **Virtual machine**
      - **vApp**

      Note:

      You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

   b. In All Privileges, expand **Host**, and select the **Configuration** check box.

Note:

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds them to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
      - The FQDN value must match the value of the **SAN** field of the vCenter certificate. The FQDN value is case-sensitive.

   b. In **User Name**, type the username to log in to vCenter.
   c. In **Password**, type the password to log in to vCenter.
   d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

      If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.

e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

PSC must have a valid certificate.

The system enables **PSC IP or FQDN**, and you must provide the IP or FQDN of PSC.

f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.

5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds vCenter.

In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Note:

- System Manager does not support vCenter with Cluster level.
- If there is a large data center with multiple hosts in a vCenter, there can be a delay in discovering all the VMs of those hosts when mapping that vCenter in the Solution Deployment Manager. If you select a smaller number of hosts rather than all hosts, this process can be faster.

Related links

Editing vCenter on page 85
Map vCenter field descriptions on page 86
New vCenter and Edit vCenter field descriptions on page 87

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:

- Select an ESXi host and click the edit icon ( ).
- Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.

7. Click **Commit** to get an updated list of managed and unmanaged hosts.

   If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The options are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.

Table continues…

Button	Description
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.

Button	Description
Add	Displays the New vCenter page where you can add a new ESXi host.
Edit	Displays the Edit vCenter page where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.

Table continues…

Name	Description
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Chapter 7: Configuring the Communication Manager

Configuring the Communication Manager using VMware

Configuration and administration checklist

Use the following checklist to configure the Communication Manager virtual appliance.

#	Action	Link	✔
1	Start the Communication Manager virtual machine.	Starting the Communication Manager virtual machine on page 89	
2	Configure the Communication Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 90	
3	Set up network configuration.	Administering network parameters on page 90	
4	Apply the latest Communication Manager patch.	Patch Installation or Patch Updates on page 42	
5	Set the date and time.	Setting the date and time on page 91	
6	Configure the time zone.	Setting the time zone on page 92	
7	Set up the network time protocol.	Setting up the network time protocol on page 92	
8	Direct Communication Manager to the WebLM server.	Configuring WebLM Server on page 94	
9	Create an suser account.	Adding an administrator account login on page 92	

Starting the Communication Manager virtual machine

Procedure

1. In the vSphere client, select the host server.
2. Right-click the virtual machine, highlight the **Power** and click **Power On**.

   Communication Manager takes some time to start. If Communication Manager does not start, you must wait for Communication Manager to boot before logging in.

Note:

VMware vSphere ESXi 6.0 and 6.5 supports vSphere Client for Windows and vSphere Web Client. However, with VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.

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**.

Administering network parameters

Procedure

1. In the vSphere client, start the Communication Manager virtual machine console and log in as `privileged administrator for Communication Manager`.
2. On first attempt log in as `privileged administrator for Communication Manager`, you must type the following details according to the prompts:
   a. In the **IPv4 IP address** field, type the IP address.
   b. In the **IPv4 subnet mask** field, type the network mask IP address.
   c. In the **IPv4 Default Gateway address** field, type the default gateway IP address.

3. In the **Are these correct** field, verify the IP address details and type `y` to confirm the IP address details.
4. When the system prompts to create a customer privileged administrator account, enter the login details to create an account.
5. In the **Enable Avaya Services EASG Access**, enter:
   - `y` to enable EASG.
   - `n` to disable EASG.

   Note:

   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.

6. To configure the additional network settings, log in to Communication Manager System Management Interface and navigate to **Administration** > **Server (Maintenance)** > **Network Configuration**.

   Note:

   If the system interrupts the initial network prompt or you provide the incorrect data, run the **`/opt/ecs/bin/serverInitialNetworkConfig`** command to retype the data.

Setting the date and time

About this task

To configure time for a virtual machine, first you need to configure the host time, and then sync the time of the virtual machine with the host time.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Time Configuration**.
4. Click **Properties** in the upper-right corner of the screen.
5. In the Time Configuration window, do one of the following:
   - To change the time manually, in the **Date** and **Time** field, set the appropriate date and time.
   - To synchronize the time kept by a host system to a reference NTP server, click **Options** and configure NTP server settings.
6. Click **OK**.
7. To set the Communication Manager virtual machine time, right-click the Communication Manager virtual machine and select **Edit Settings**.

8. In the Options tab, click **VMware Tools**.
9. Select the **Synchronize guest time with host** check box and click **OK**.

Setting the time zone

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Time Zone Configuration**.
4. On the Time Zone Configuration page, select the time zone, and click **Apply**.

Note:

After changing the time zone settings, you must restart the virtual machine to ensure that the system processes use the new time zone.

Setting up the network time protocol

About this task

After the Communication Manager installation is successful, you must configure the time in the Network Time Protocol (NTP). The NTP configuration provides time synchronization of Communication Manager with the NTP server.

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **NTP Configuration**.

   The system displays the Network Time Protocol (NTP) Configuration page.
4. Enable or disable the NTP mode.
5. In NTP Servers, type the primary server, secondary server (Optional), and tertiary server (Optional) details.

   The application supports only the NTP server. It does not support the NTP pool.
6. Click **Apply**.

Adding an administrator account

About this task

When you deploy the Communication Manager OVA using the vSphere client, perform the following procedure after the OVA deployment.

Note:

When you deploy the Communication Manager OVA using vCenter or System Manager Solution Deployment Manager, the system prompts you to specify the login name and password for the Communication Manager privileged administrator account during the deployment.

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Administrator Accounts**.
4. Select **Add Login**.
5. Select the **Privileged Administrator** login for a member of the SUSERS group.

   You can also add the following types of login:

   - **Unprivileged Administrator**: This login is for a member of the USERS group.
   - **SAT Access Only**: This login has access only to the Communication Manager System Administration Terminal (SAT) interface.
   - **Web Access Only**: This login has access only to the server webpage.
   - **CDR Access Only**: This login has access only to the survivable CDR feature.
   - **Business Partner Login (dadmin)**: This login is for primary business partners.
   - **Business Partner Craft Login**: This login is for profile 3 users.
   - **Custom Login**: This login is for administrators with login parameters that you can customize. You can create a new user profile and later add users with this new profile.
6. Click **Submit**.

   The system displays the Administrator Login - Add Login screen.
7. In the **Login name** field, enter the administrator login name.

   The login name:

   - Can have alphanumeric characters.
   - Can have an underscore (_).
   - Cannot have all numberic characters (0 - 9).
   - Cannot have more than 31 characters.
8. In the **Primary group** field, enter **susers** for a privileged login.
9. In the **Additional group (profile)** field, add an access profile.

   The system automatically populates the values in the **Linux shell** and the **Home directory** fields.
10. To set lock parameters for the login, select the **Lock this account** check box.

Note:

If you set the lock parameters, the user cannot log in to the system.

11. In the **SAT Limit** field, enter the limit for the concurrent SAT sessions.

Note:

You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

12. To assign an expiry date to the login, in the **Date on which account is disabled** field, enter the date in the yyyy-mm-dd format.
13. In the **Enter password or key** field, enter the password for the login.
14. In the **Re-enter password or key** field, reenter the same password.
15. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select yes.
16. Click **Submit**.

Configuring the WebLM server

About this task

When you deploy the Communication Manager OVA using the vSphere client, perform the following procedure after the OVA deployment.

Note:

When you deploy the Communication Manager OVA using vCenter or System Manager Solution Deployment Manager, the system prompts you to specify the IP address of WebLM Server during the deployment.

Note:

To perform the administration tasks, you must first install the license file on the Communication Manager virtual machine.

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Licensing**.
3. In the left navigation pane, click **WebLM Configuration**.

   The system displays the WebLM Configuration page.
4. In the **WebLM Server Address** field, type the WebLM server IP address to fetch the license file.

Note:

You can specify the IP address of the WebLM server within System Manager or of the standalone WebLM virtual appliance.

5. Click **Submit**.

IPv6 configuration

Enabling IPv6

About this task

Use this procedure to enable IPv6. For more information about IPv6, see, *Avaya Aura® Communication Manager Feature Description and Implementation*.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. From the **IPv6 is currently** drop-down list, select enabled.
5. Click **Change** to enable the IPv6 fields.

Note:

Restart Communication Manager after enabling IPv6.

Disabling IPv6

About this task

Use this procedure to disable IPv6. For more information about IPv6, see, *Avaya Aura® Communication Manager Feature Description and Implementation*.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. From the **IPv6 is currently** drop-down list, select disabled.
5. Click **Change** to disable the IPv6 fields.

Note:

Restart Communication Manager after disabling IPv6.

Network port considerations

For more information on Port Matrix, see the Avaya Aura® Communication Manager Port Matrix document.

Communication Manager virtual machine configuration

To complete the configuration tasks, use Communication Manager System Management Interface to configure the following:

- Server Role: Indicate the type of virtual machine: main, survivable core, or survivable remote.
- Network configuration: Use to configure the IP-related settings for the virtual machine. On the Network Configuration page, the fields are prepopulated with data generated during the installation.
- Duplication parameters: Use to configure the duplication settings if you installed the Duplex Main or the Survivable Core both.

Related links

Server role configuration on page 96
Configuring Server Role on page 97
Server Role field descriptions on page 98

Server role configuration

A telephony system consists of several virtual machines. Each virtual machine has a certain role, such as main or primary virtual machine, a second redundant virtual machine, Survivable Remote virtual machine, or Survivable Core virtual machine. Use Communication Manager System Management Interface to configure the virtual machine roles, and then configure at least two of the following fields.

- Virtual machine settings
- Survivable data
- Memory

Communication Manager type and virtual machine role

The Communication Manager type determines the virtual machine role.

Note:

- The Communication Manager Simplex and Duplex support Avaya Experience Platform® On-Prem (AXP On-Prem, formerly Avaya Aura® Call Center Elite).
- The Communication Manager Simplex and Duplex do not support Avaya Aura® Communication Manager Messaging.

You can configure the Communication Manager Duplex as one of the following:

- Main server
- Survivable core server

Note:

For a Communication Manager duplicated pair configuration, deploy the Communication Manager duplicated servers either on the VMware platform or on Avaya Solutions Platform 130. However, you can mix and match the deployment of the survivable core server, the survivable remote server, or the main server in a configuration. For example, the main servers can be a CM-duplicated pair on VMware, and the survivable core server can be on Avaya Solutions Platform 130.

You can configure the Communication Manager Simplex as one of the following:

- Main server
- Survivable core server (formerly called Enterprise Survivable Server [ESS])
- Survivable remote server (formerly called Local Survivable Processor [LSP])

Important:

You can deploy the Communication Manager Simplex server and then administer the Communication Manager Simplex as a survivable remote server. However, you cannot administer a core Session Manager as a Branch Session Manager or a remote survivable server. Deploy the Session Manager as a core Session Manager only.

Related links

Communication Manager virtual machine configuration on page 96

Configuring Server Role

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Server Configuration** > **Server Role**.

   The system displays the Server Role page.
4. In the **Server Settings**, **Configure Survivable Data** , and **Configure Memory** sections, enter the required information.

   Note:

   If you are configuring a role for the main virtual machine, the system does not display **Configure Survivable Data**.
5. Click **Change** to apply the virtual machine role configuration.

Related links

Communication Manager virtual machine configuration on page 96

Server Role field descriptions

Server Settings

Name	Description
This Server is	Specifies the role of the server. Select from the following roles: • **a main server:** For a primary virtual machine. • **an enterprise survivable server (ESS):** For a survivable core virtual machine. • **a local survivable server (LSP):** For a survivable remote virtual machine.
SID	Specifies the system ID. This ID must be the same for the main server and each survivable server. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form. System ID must be set to default value of 1.
MID	Specifies the module ID. The main server module ID must be 1 and the ID of the other server must be unique and 2 or more. For a survivable remote server, the MID must match the Cluster ID or MID for that server.

Configure Survivable Data

Name	Description
Registration address at the main server (C-LAN or PE address)	Specifies the IP addresses of the Control LAN (C-LAN) or the Processor Ethernet (PE). You must register the main server to this address.
File Synchronization address at the main cluster (PE address)	Specifies the IP addresses of the NICs of the main server and the second redundant server connected to a LAN to which you also connected the Survivable Remote server or the Survivable Core server. **Note:** If a second server is not in use, keep this field blank. The Survivable Remote or the Survivable Core server must be able to ping these addresses. Avaya recommends use of the enterprise LAN for file synchronization.
File Synchronization address at the alternate main cluster (PE address)	Specifies the IP address of the interface that you can use as an alternate file synchronization interface.

Configure Memory

Name	Description
This Server's Memory Setting	Specifies the servers memory settings of the server. The options are: small, medium, and large.
Main Server's Memory Setting	Specifies the main servers memory settings of the server.

Button	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes.
Restart CM	Updates the system configuration files with the current values on the page. **Note:** Click **Restart CM** only after completing the configuration settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Related links

Communication Manager virtual machine configuration on page 96

Network

Network configuration

Use the Network Configuration page to configure the IP-related settings for the virtual machine.

Note:

Some changes made on the Network Configuration page can affect the settings on other pages under the **Server Configuration** page. Ensure that all the pages under **Server Configuration** have the appropriate configuration information.

Using the Network Configuration page, you can configure or view the settings of the hostname, alias host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

If the configuration setting for a field is blank, you can configure that setting on the Network Configuration page.

Note:

While configuring a survivable server that has ESS and LSP configured, users must ensure that the Server ID must be unique for each survivable server and main server.

The virtual machine uses virtual NICs on virtual switches internal to the hypervisor.

The system uses eth0 in most cases except for duplication traffic. Use eth1 for the duplication IP address. Use eth2 for the Out-of-Band Management interface IP address.

For information about Out-of-Band management, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

The Network Configuration page displays the network interfaces that Communication Manager uses. The setting is eth0 for all Communication Managers except CM_Duplex. For CM_Duplex, the network interfaces are eth0, eth1, and eth2.

To activate the new settings on the virtual machine, you must restart Communication Manager after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

To deploy Duplex Communication Manager using Software-Only offer on Openstack, you must configure Alias IP. For more information on configuring Duplex Communication Manager, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

To deploy Duplex Communication Manager using Software-Only offer on Microsoft Azure, you must configure the load balancer.

Configuring the Communication Manager network

About this task

You must perform the following procedure only if you are deploying the Communication Manager using the vSphere Web client that is directly connected to the ESXi host.

Procedure

1. Log on to Communication Manager System Management Interface, with the Customer Privileged Administrator account user and password created earlier.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. Type the values in the fields.

   For configuring the Communication Manager Duplex Survivable Core OVA, the system displays additional fields. You can use the same values to duplicate the data on the second Communication Manager virtual machine.

   If IPv6 is not enabled, you cannot configure the IPv6 fields.

   For field descriptions, see the *Network Configuration field descriptions* section.
5. Click **Change** to save the network configuration.
6. Click **Restart CM**.

   Note:

   To configure for duplication, restart Communication Manager only after you configure the duplication parameters.

The system takes about 2 minutes to start and stabilize the Communication Manager processes. Depending on your enterprise configuration, the system might require additional time to start the port networks, the gateway, and the telephones.

Network Configuration field descriptions

Name	Description
Host Name	The host name of the virtual machine. You can align the host name with the DNS name of the virtual machine. Do not type underscore (_) in the **Host Name** field.
Alias Host Name	The alias host name for duplicated virtual machines only. When a duplicated virtual machine runs in survivable mode, ensure that the system displays the **Alias Host Name** field.
DNS Domain	The domain name server (DNS) domain of the virtual machine.
Search Domain List	The DNS domain name of the search list. If there are more than one search list names, separate each name with commas.
Primary DNS	The primary DNS IP address.
Secondary DNS	The secondary DNS IP address. This field is optional.
Tertiary DNS	The tertiary DNS IP address. This field is optional.
Server ID	The unique server ID, which is a number between 1 and 256. On a duplicated virtual machine or survivable virtual machine, the number cannot be 1.
IPv6 is currently	Specifies the status of IPv6. The options are: enabled and disabled.
Default Gateway IPv4	The default gateway IP address.
Default Gateway IPv6	The IPv6-compliant IP address of the default gateway.

Table continues…

Name	Description
IP Configuration	The set of parameters to configure an Ethernet port, such as, eth0, eth1, or eth2. The parameters are: • **IPv4 Address** • **Subnet Mask** • **IPv6 Address** • **Prefix** • **Alias IP Address: IPv4 Address** (for duplicated virtual machines only) • **Alias IP Address: IPv6 Address** (for duplicated virtual machines only) **Note:** You can configure as many Ethernet ports as available on the NICs of your virtual machine.
Functional Assignment	Based on the system configuration, the system displays the following options. • Corporate LAN/Processor Ethernet/Control Network • Corporate LAN/Control Network • Duplication Link • Services Port • Out-of-Band Management **Note:** When you select the Out-of-Band Management option, the system displays the **Restrict Management traffic to Out-Of-Band interface is currently** field.
Restrict Management traffic to Out-Of-Band interface is currently	The possible values are: • enabled: restricts the management traffic to Out-Of-Band interface. • disabled: allows the management traffic to Out-Of-Band interface. By default the value of this field is set to disabled.

Button descriptions

Name	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes.
Restart CM	Updates the system configuration files with the current values on the page. **Note:** Click **Restart CM** only after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Duplication parameters configuration

Duplication parameters

The Duplication parameters option is visible and accessible after Duplex deployment. Configuring duplication parameters ensures that the telephony applications run without interruption even when the primary virtual machine is not functional. Communication Manager supports two types of virtual machine duplication: software-based duplication and encrypted software-based duplication.

The duplication type setting must be the same on both the virtual machines. If you are changing the duplication parameters settings, ensure that you make the changes in the following order:

1. Busy out the standby virtual machine, and then change the settings on the standby virtual machine.
2. Change the settings on the active virtual machine. This causes a service outage.
3. Release the standby virtual machine.

Configuring duplication parameters

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Duplication Parameters**.

   The system displays the Duplication Parameters page.
4. In Network Configuration page, type the values in the fields.

   If IPv6 is not enabled, you cannot configure the IPv6 fields.

   For field descriptions, see the *Duplication Parameters field descriptions* section.
5. Add a duplicate server and fill in the required fields, such as host name and IP address.
6. Click **Change**.

7. Click **Restart CM**.

   In the pop-up confirmation page, you click **Restart Now** to restart the virtual machine immediately or click **Restart Later**, to restart the virtual machine later.

Duplication Parameters field descriptions

Name	Description
Select Server Duplication	Specifies the server duplication method. Select one of the following methods: • **This is a duplicated server using software-based duplication**: Software-based duplication provides memory synchronization between an active and a standby virtual machine using a TCP/IP link. • **This is a duplicated server using encrypted software-based duplication**: Encrypted software-based duplication provides memory synchronization between an active and a standby virtual machine using AES 128 encryption.
Hostname	Enter the hostname of the other Communication Manager virtual machine.
Server ID	Enter the unique virtual machine ID of the other Communication Manager virtual machine. The value of this virtual machine must be an integer from 1 through 256.
Corporate LAN/PE IP	• **IPv4**: Enter the IP address of the Processor Ethernet (PE) interface of the other Communication Manager virtual machine. • **IPv6**: Enter the IPv6-compliant IP address of the Processor Ethernet interface of the other Communication Manager virtual machine.
Duplication IP	• **IPv4**: Enter the IP address of the duplication interface of the other Communication Manager virtual machine. You can assign the IP address according to the network configuration. • **IPv6**: Enter the IPv6-compliant IP address of the duplication interface of the other Communication Manager virtual machine. You can assign the IP address according to the network configuration.
PE Interchange Priority	Select one of the following priority levels: • **HIGH:** Favors the virtual machine with the best PE state of health (SOH) when PE SOH varies between virtual machines. • **EQUAL:** Counts the Processor Ethernet interface and favors the virtual machine with the best connectivity count. • **IGNORE:** Does not include the Processor Ethernet in virtual machine interchange decisions.

Table continues…

Name	Description
IP address for PE Health Check	• **IPv4**: Enter the IPv4 address that enables the virtual machine to determine whether the PE interface is working. **Note:** The network gateway router is the default address. However, use the IP address of any other device on the network that responds. • **IPv6**: Enter the IPv6-compliant IP address that enables the virtual machine to determine whether the PE interface is working.

Button descriptions

Name	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes. Restart the Communication Manager virtual machine for the configuration changes to take effect. **Warning:** Multiple restarts can result in a full Communication Manager reboot. Communication Manager displays a dialog box with the following buttons: • **Restart Now**: Restart the Communication Manager virtual machine immediately. • **Restart Later**: Restart the virtual machine later. • **Cancel**
Restart CM	Updates the system configuration files with the current values on the page. **Note:** After configuring the complete settings of the virtual machine, click **Restart Now**. **Warning:** Multiple restarts can result in a full Communication Manager reboot.

Chapter 8: Verifying the Communication Manager post installation

Installation tests

You must perform many post installation administration, verification, and testing tasks to ensure that you have installed and configured the system components as part of the Communication Manager installation.

This section provides a list of tasks for testing the Communication Manager installation, virtual machine, and system component installation and configuration. You cannot perform certain tests until you install and configure the complete solution, including port networks.

Note:

To perform the following tests, you must configure the Communication Manager translation.

You must first perform the following post installation administration and verification tasks:

- Verifying the translations
- Clearing and resolving alarms
- Backing up the files

Verifying the license status

Accessing Communication Manager System Management Interface

About this task

You can gain access to Communication Manager System Management Interface (SMI) remotely through the corporate LAN connection. You must connect the virtual machine to the network.

Procedure

1. Open a compatible web browser.

   For more information the supported browsers, see “Supported browsers” section.

2. In the browser, choose one of the following options depending on the virtual machine configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the Communication Manager virtual machine in the standard dotted-decimal notation, such as `https://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `https://hostname.domain.com`.
3. Press `Enter`.

   Note:

   If the browser does not have a valid security certificate, the system displays a warning with instructions to load the security certificate. If your connection is secure, accept the virtual machine security certificate to access the Logon screen. If you plan to use this computer and browser to access this virtual machine or other Communication Manager virtual machine again, click **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type the username.

   Note:

   If you use an Avaya services login that Enhanced Access Security Gateway (EASG) protects, you must have an EASG tool to generate a response for the challenge that the Logon page generates.
5. Click **Continue**.
6. Type the password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Related links

Supported browsers on page 15

Viewing the license status

About this task

Use this procedure to view the Communication Manager license status.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Licensing**.

3. In the left navigation pane, click **License Status**.

   The License Status page displays the license mode, error information, System ID, Module ID, WebLM server, application version, supported end date, and License Expiry date.

   Prior to R10.2.1.1, the Communication Manager license status can be one of the following:

   - Successfully installed and valid
   - Unlicensed and within the 30-day grace period
   - Unlicensed and the 30-day grace period has expired.

   Note:

   Beginning with R10.2.1.1, if the Communication Manager license is not renewed before expiration, the Communication Manager functions in a 30-day grace period. If the license is not renewed even after the 30-day grace period, the main Communication Manager server blocks call processing, including emergency calls, and system administrations activities.

   Note:

   License expiration alarm generated prior to 90 days and 60 days are applicable only for Main Communication Manager server and not for ESS and LSP.

   Beginning with R10.2.1.1, the Communication Manager license status can be one of the following:

   - Normal mode
   - Normal mode (≤ 90 days of license expiration)

     ```
     The Communication Manager license expires in 90 days.
     Contact Your Service Representative at the earliest to renew the license
     before the expiration date to avoid service disruption and daily late fee
     penalties.
     ```

   - Normal mode (≤ 60 days of license expiration)

     ```
     The Communication Manager license expires in 60 days.
     Contact Your Service Representative at the earliest to renew the license
     before the expiration date.
     Failure to renew will result in the inability to make or receive phone calls
     in 90 days and incur daily late fees starting in 60 days.
     ```

   - License Error

     ```
     System Administration and Call Processing Will Be Blocked in Approximately
     30 days.
     Contact Your Service Representative Immediately.
     ```

   - No License

     ```
     System Administration and Call Processing Is Blocked.
     Contact Your Service Representative Immediately.
     ```

License Status field descriptions

Name	Description
CommunicaMgr License Mode	Specifies the license status. Following are the valid options: • Normal: The Communication Manager license mode is normal, and the system has no license errors. • Error: The Communication Manager license has an error, and the 30-day grace period is active. Error messages are as follows: - License file is missing or corrupted - Local Survivable Processor (LSP) serving as active processor - The license has expired - Feature usage exceeds limits - Software publication date is after the support end date in license file - Platform type/server configuration mismatch - Cluster is disabled in extra large configuration - License server request time-out - Software major release is greater than the major release in license file - Platform type mismatch - 12-party conferences and DCS (basic) cannot be enabled together • No License: The Communication Manager license has an error, and the 30-day grace period has expired. The Communication Manager software is running but blocks normal call processing. The switch administration software remains active so that you can correct license errors. For example, reducing the number of stations.
checking application CommunicaMgr version	Specifies the version of Communication Manager. For example, R016x.00.0.340.0.
WebLM server used for License	Displays the WebLM server URL used for the license. For example, `https://10.18.2.8:52233/WebLM/LicenseServer`.
Module ID	The Communication Manager main virtual machine has a default module ID of 1. You can configure the module ID on the Server Role page. Each survivable virtual machine has a unique module ID of 2 or more. The module ID must be unique for the main virtual machine and all survivable virtual machines.

Table continues…

Name	Description
System ID	Communication Manager has a default system ID of 1. You can configure the system ID on the Server Role page. The system ID is common across the main virtual machine and all survivable virtual machines. Avaya provides the system ID when you submit the Universal Install or SAL Product Registration Request form.
License Expiry Date	Displays when the Communication Manager license expires. For example, Day Mon DD HH:MM:SS YYYY

Verifying the software version

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server** > **Software Version**.
4. Verify that the **CM Reports as:** field shows the correct software load.
5. On the menu bar, click **Log Off**.

Verifying the survivable virtual machine registration

About this task

If you configured a Survivable Core or Survivable Remote virtual machine, verify that the virtual machine is registered with the main virtual machine. This task can take several minutes to complete.

Procedure

1. On the SAT screen, type **`list survivable-processor`**.

   The system displays the Survivable Processor screen.

2. Verify that the **Reg** field is set to **y**.

   This setting indicates that the survivable virtual machine is registered with the main virtual machine.

3. Verify that the **Translations Updated** field shows the last updated time and date.

   This setting indicates that the system has scheduled the translations for the survivable virtual machine.

Verifying the virtual machine mode

About this task

Use this procedure to verify the virtual machine mode, process status, and operations.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server** > **Status Summary**.
4. Verify the **Mode** field.
   - `Active` on an active virtual machine.
   - `StandBy` on a standby virtual machine.
   - `BUSY OUT` on a busy out virtual machine.
   - `NOT READY` on a standby virtual machine that is not ready.
5. To verify the process status, click **Server** > **Process Status**.
6. In the **Frequency** section , select **Display When**.
7. Click **View**.

   The system displays the Process Status Results page.
8. Verify that all operations are:
   - `Down` for dupmanager
   - `UP` all other operations

Entering initial system translations

Before you begin

- Prepare the initial translations offsite and save the translations in the translation file.
- Store the translation file in the `/etc/opt/defty` folder with `xln1` and `xln2` file names.

  Alternatively, you can save the full Communication Manager backup in a translation file and restore the files on another Communication Manager.

Procedure

1. Log in to the Communication Manager CLI.
2. If the Communication Manager translations are prepared offsite, run the **`drestart 1 4`** command to install the prepared translations and reset Communication Manager.

3. If translations are not prepared offsite, do the following:
   a. Type **save_trans** and press Enter to save the translations to the hard disk drive.
   b. Type **drestart 1 4** and press Enter.
4. Enter minimal translations to verify the port networks or media gateway connectivity.
5. After you enter the translations, type **save_trans**, and press Enter to save the translations to the hard disk drive.

Chapter 9: Resources

Communication Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Core Solution Description	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that specific customers request for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

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

Important:

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

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

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

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

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: Communication Manager debugging

Communication Manager processes

Using the *gdb* debugger, you can analyze the Communication Manager processes core files. For example, by segmentation faults that generate core files that are written into the `/var/crash` directory.

Creating Communication Manager virtual machine core images

About this task

Currently, the creation and debugging of Communication Manager virtual machine core images created by the VM kernel is not supported. If you have to create a Communication Manager virtual machine core images to debug, for example, a reproducible problem, use the following steps.

Procedure

1. Install the kexec-tools rpm that provides the functionality to generate core files, for example, on kernel panics. You can install the Virtual Machine kernel dump service from the Virtual Machine kernel dump service documentation Web link. You can follow the CLI instructions for easier navigation. You must note the following points:
   a. The Virtual Machine kernel dump service documentation Web link describes changes to the GRUB tool, which for Communication Manager is lilo, that is `/etc/lilo.conf`. It states to add `crashkernel=128M` on the kernel entry line but actually the string to add is `crashkernel=128M@16M`. Execute the **`lilo`** command and reboot the virtual machine.
   b. Execute the **`service kdump status`** command to ensure that the *kdump rc* script is setup and running.
2. Execute the following to ensure that a virtual machine kernel core can be created

```
echo 1 > /proc/sys/kernel/sysrq
echo c > /proc/sysrq-trigger
```

3. After the Communication Manager virtual machine is rebooted ensure the core image is written to the virtual machine disk space in the `/var/crash/_date_/vmcore` directory. Use the RedHat Crash Utility to debug the core images in the `/var/crash/_date_/vmcore` directory. See VMware generated core images on Communication Manager virtual machine images on page 121.

VMware generated core images on Communication Manager virtual machine images

VMware provides technical assistance for debugging virtual machine issues, for example, VM kernel panics and virtual machines that hang. When you log a service request, you must send the performance snapshots to troubleshoot the issue. You can execute the **`vm-support`** command to collect the virtual machine logs. The **`vm-support`** command also creates a *.tar* file for sending the logs to VMware. The core image can be debugged using the RedHat Crash Utility as described in Collecting performance snapshots using vm-support.

VMware also provides a utility to help you to take an initial look at virtual machine issues, for example, VM kernel panics, a virtual machine with very slow response times, or for a virtual machine that hangs. The utility is called vmss2core. The vmss2core is a command line tool for creating virtual machine core file that you can use with the RedHat crash utility. For the vmss2core command, see Broadcom website (formerly VMware), and search for "vmss2core technical link". The vmss2core tool generates a `vmcore` core file, using the virtual machine's `.vmsn` file from a snapshot, or `.vmss` file from a suspended virtual machine. For more information on RedHat crash utility, search for "White paper:RedHat Crash Utility" on your browser.

Appendix B: Communication Manager Software Duplication

Communication Manager software duplication with VMware high availability

This Appendix shows an illustration of Communication Manager software duplication with four ESXi Hosts configured in two data clusters with VMware high availability (HA).

- In the Figure 13: VMware cluster configuration with four ESXi hosts on page 123, Communication Manager software duplication is established across two VMware Data Clusters. Each cluster is using the VMware HA. Communication Manager active and standby virtual machines are not supported within the same data cluster with VMware HA.
- To establish the connectivity the Software Duplication link must be tied together through a dedicated Ethernet IP private Switch or VLAN, Host to Host (Figure). Hosts 1 and 3 are on Data Cluster A and Hosts 2 and 4 are on Data Cluster B.
- The illustration has two Communication Manager virtual machines, CMVM_01 and CMVM_02 configured as an Active (ACT) and Standby (STB) pair using Communication Manager virtual machine software duplication link.
- CMVM_01 (ACT) Eth2 configuration virtual switch is tied to physical adapter VMnic2 on Host 1 and CMVM_02 (STB) Eth2 configuration virtual switch is tied to physical adapter VMnic2 on Host 4.
- Other virtual machines are not using the VMnic2.

Example: When Active virtual machine fails

In the Figure 13: VMware cluster configuration with four ESXi hosts on page 123:

- Host 1 (CMVM_01) is ACT with a duplication link communicating over VMnic2 through the network switch.
- Host 4 (CMVM_02) is STB with a duplication link communicating over VMnic2 through the network switch.
- If Host 1 fails, CMVM_02 becomes ACT.
- VMware HA starts CMVM_01 on Host 3.
- Host 3 (CMVM_01) starts communication over VMnic2.
- Host 1 is booting so no communication over VMnic2.

- Host 3 (CMVM_01) and Host 4 (CMVM_02) link up and communicate across the network switch over each VMnic2.

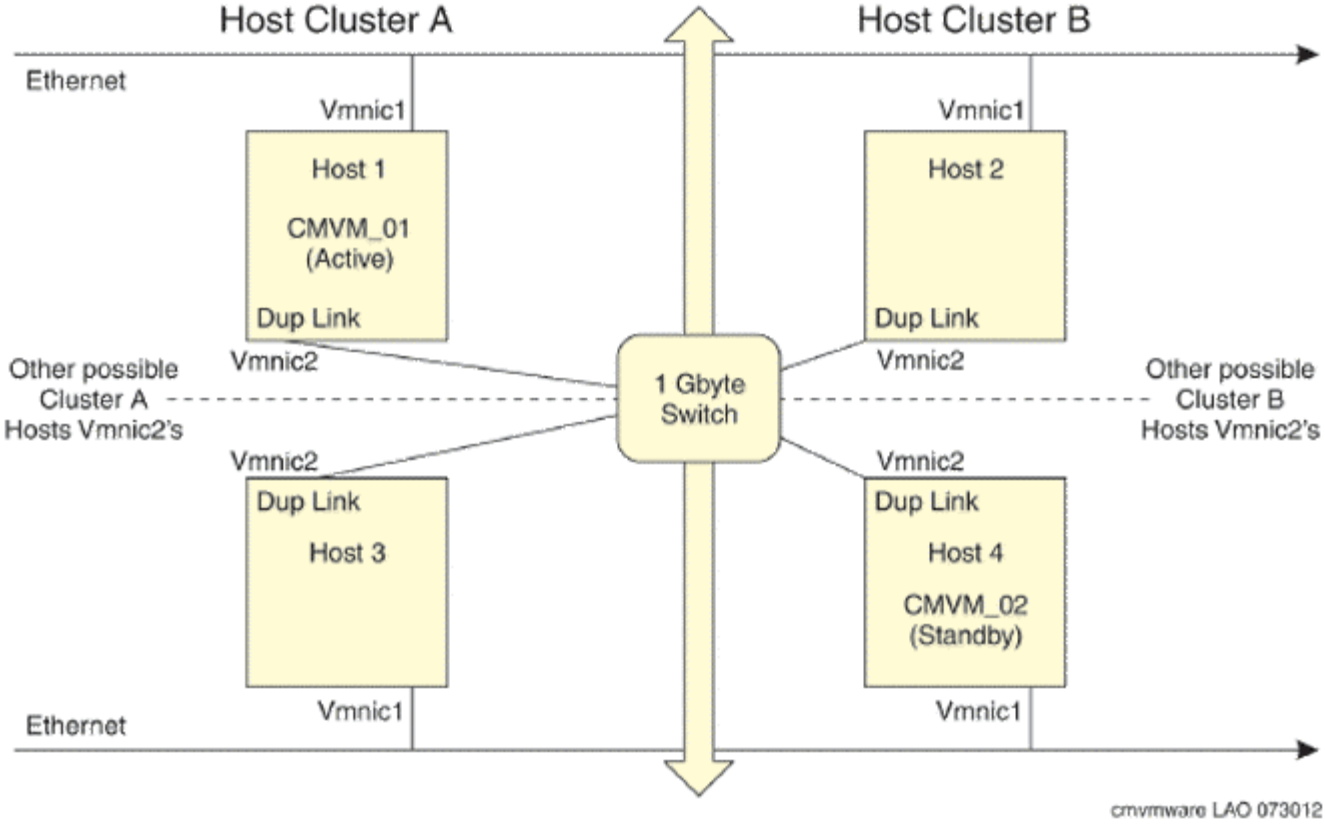


Figure 13: VMware cluster configuration with four ESXi hosts

Software duplication enhancement

You can configure both active and standby servers in the same data cluster. For more information about duplicated server configuration, see *Duplicated Avaya Aura® Communication Manager on VMware* on the Avaya Support website at https://support.avaya.com/.

Appendix C: Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface

About this task

This procedure is required for both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

Before adding an Avaya Solutions Platform S8300 host, to regenerate the Avaya Solutions Platform S8300 self-signed certificate with FQDN, perform the following steps:

For information about adding an Avaya Solutions Platform S8300 host, see Adding an Avaya Solutions Platform S8300 Release host on page 81.

Procedure

1. Log in to the Avaya Solutions Platform S8300 command line interface.
2. To change the FQDN, type the following command:

   ```
   esxcli system hostname set --fqdn=server.abc.com
   ```

   Here, *server.abc.com* is the FQDN of the ESXi host.

   For more information, see Changing the host name on the VMware documentation website.
3. To regenerate the self-signed certificate, do the following:
   a. Enable SSH on the ESXi host, then put the ESXi host into the maintenance mode.
   b. SSH to the ESXi host and use the following commands to take backups of the current certificate file and private key file.

      ```
      cd /etc/vmware/ssl

      mv rui.crt rui.crt.bkp

      mv rui.key rui.key.bkp
      ```

   c. To regenerate a new certificate, type the following command:

      ```
      /sbin/generate-certificates
      ```

Verify that the new certificate file and private key file are generated.

d. To restart the ESXi Server management agent, reboot the host.

The ESXi host generates a new self-signed certificate.

For more information, see Generating new self-signed certificates for the ESXi host.

Appendix D: Best Practices

VMware best practices for performance

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

Considerations

- These best practices are applicable to customer provided server infrastructure environments only.
- These best practices should *not* be used for any Avaya Solutions Platform 100 Series Dell® R640 servers like ASP 110, ASP 130 as these are supplied under OEM relationship and managed differently than commercially available servers from the vendor.
- ASP 100 Series Server configurations are engineered for specific application needs. These servers must *not* be updated with BIOS or firmware updates from the vendor's web site. Use the Avaya provided updates only. Updating directly from the vendor's web site or making changes to the BIOS settings will result in an unsupported configuration.
- For ASP 130, use the Avaya provided ESXi updates only. Updating directly from the Dell or VMware's web sites will result in an unsupported configuration.

Related links

VMware networking best practices on page 127
Thin vs. thick deployments on page 131
Storage on page 132
VMware features supported by Avaya Aura on page 135

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.

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.

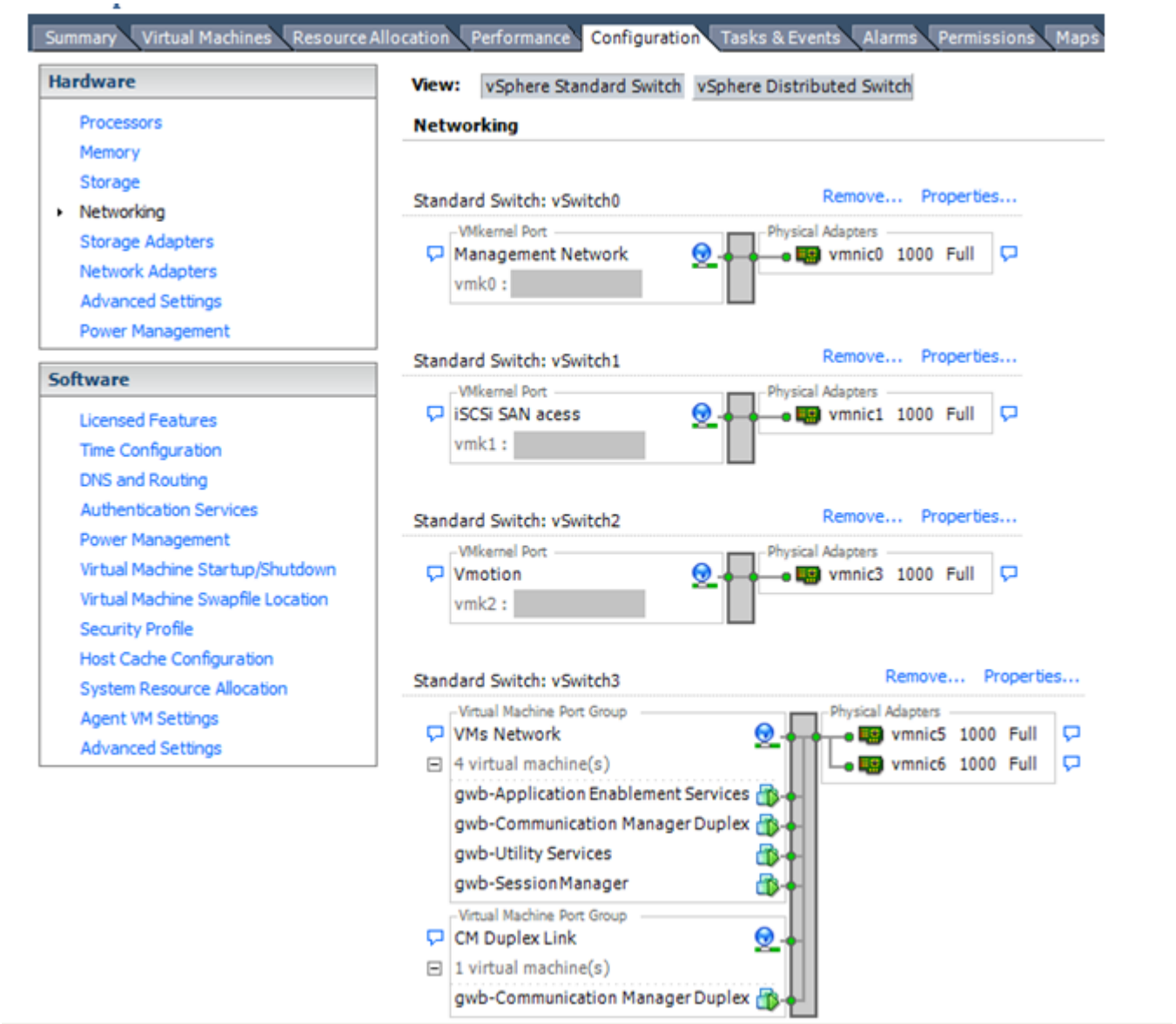
The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- 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.

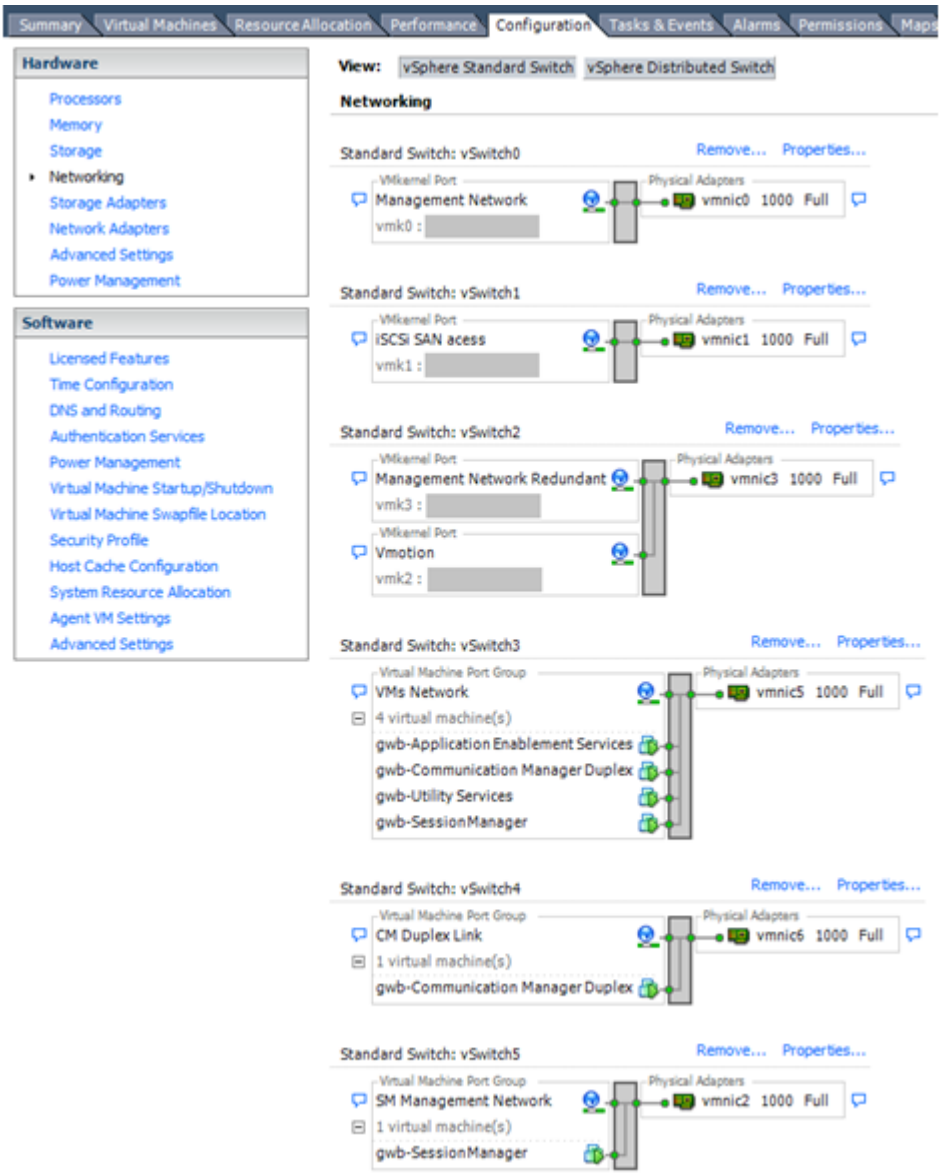
Networking Avaya applications on VMware ESXi – Example 1



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*.

Related links

VMware best practices for performance on page 126

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.

Related links

VMware best practices for performance on page 126

Storage

Fibre Channel SAN arrays and iSCSI SAN arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs and are the preferred storage technology for Communication Manager. 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.

Related links

VMware best practices for performance on page 126

Best Practices for VMware features

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshot is a short-term copy of the running system that you can create before a 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.

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 off of a snapshot*. Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify that 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. When creating a snapshot, perform the following;
  - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the 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 consolidate failure occurs, you 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 in the UI.

If the Duplex OVA is in use, you must take the snapshot on the standby virtual machine when the standby is refreshed. If the snapshot is taken on the active virtual machine under a heavy load there is a possibility an interchange of virtual machine can occur.

Related resources

For more information about Snapshots, see the Broadcom website (formerly known as VMware) and search for following terms:

- Best practices for virtual machine snapshots in the VMware environment
- Understanding virtual machine snapshots in VMware ESXi and ESX
- Working with snapshots
- Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots
- Consolidating snapshots in vSphere 5.x

Related links

VMware best practices for performance on page 126

High availability

Simplex OVA

Communication Manager Simplex Open Virtualization Application (OVA) deployment supports VMware high availability. If the ESXi host fails where the Communication Manager virtual machine is installed, the Communication Manager virtual machine is moved to another ESXi host. The Communication Manager virtual machine powers up, boots, and continues to process the new call processing requests.

Related links

VMware best practices for performance on page 126

Duplex OVA

The VMware (non HA) environment configuration supports an Active (ACT) Communication Manager virtual machine deployed on one stand alone Host with the Standby (STB) Communication Manager virtual machine deployed on a second stand alone Host with the software duplication link (NIC) directly linked together.

Communication Manager software duplication works with VMware HA as long as the Communication Manager Active and Standby virtual machines are in different data clusters.

For example, if an active Communication Manager virtual machine is deployed on a host in one data cluster (A) and standby Communication Manager virtual machine is deployed on a second host in another data cluster (B). The Communication Manager virtual machines are configured on the same sub network. The connectivity requires the software duplication link (NIC) to be tied together through a private network switch or VLAN.

For information about VMware HA in each data cluster, see Communication Manager software duplication with VMware high availability on page 122.

Related links

VMware best practices for performance on page 126

VMware vMotion

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

Before using VMware vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and that the vMotion is enabled.
- Ensure that you have identical vSwitches. Enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

With vMotion, you can:

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

Note:

Ensure that vMotion occurs when the Communication Manager virtual machine is in maintenance mode.

Related links

VMware best practices for performance on page 126

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 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 See foot note[2]	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

[1] Limited to deployment, managing VMs, basic monitoring, and making VMs part of a vCenter cluster.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
Storage vMotion	Yes	Yes	Yes	Yes	Yes	Yes
VMware Snapshot 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
VMware DRS (Compute and Memory) See foot note[4]	Yes	Yes	Yes	Yes 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 See foot note[6]	Not supported	Yes

Table continues…

[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.
[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.*

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
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 see foot note[7]	Yes	Yes	Yes	Yes	Yes	Yes
vSAN support See foot note[8]	Yes	Yes	Yes	Yes	Yes	Yes
Thin Provisioning	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

Related links

VMware best practices for performance on page 126

[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 E: 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

E

F

G

H

I

K

L

M

N

O

P

R

S

T

V

W