Deploying Avaya Aura® Communication Manager in Virtualized Environment

Release 8.0.x
Issue 11
April 2022

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 mediums which may include product information, 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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 Inc.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® Communication Manager virtual application in the Avaya Aura® Virtualized Environment. 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 and Kernel-based Virtual Machine (KVM) 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.

Change history

Issue	Date	Summary of changes
11	April 2022	Updated the “Setting up the network time protocol” section.
10	October 2019	Updated the “Supported footprints of Communication Manager on KVM” section.
9	September 2019	“Accessing the port matrix document” section is added.
8	August 2019	Following sections are updated: • Network port considerations • BIOS • VMware networking best practices
7	April 2019	Updated the section “Supported footprints of Communication Manager on VMware”.
6	February 2019	Added the section Deploying the application OVA using vSphere Web Client by accessing the host directly on page 22 for deploying OVA in ACP 130.

Table continues…

Issue	Date	Summary of changes
5	December 2018	For Release 8.0.1, updated the following sections: • Applying the Communication Manager patch using SMI on page 47 • Software details of Communication Manager on page 19 • Planning checklist for VMware on page 13 • Planning checklist for Kernel-based Virtual Machine(KVM) on page 14
4	September 2018	Default login information is updated in the following section: • Configuring the Communication Manager instance on page 68
3	August 2018	“Supported footprints of Communication Manager on VMware” section is updated.
2	August 2018	CPU speed in the “Supported footprints of Communication Manager on KVM” section is updated.
1	July 2018	Initial 8.0 version.

Chapter 2: Architecture Overview

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® and Kernel-based Virtual Machine (KVM).

Avaya Aura® on Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure with SELinux implementation.
- Open source software that can be customized as per the changing business requirements of the customers.

Virtualized Environment components

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.
VMware	
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Table continues…

Virtualized component	Description
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available in vSphere 6.5. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
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.
KVM	
KVM hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Deployment guidelines

- Deploy maximum number of virtualized environment 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.

Important:

The values for performance, occupancy, and usage might vary. The blade server might run at 5% occupancy, but a virtual machine might run at 50% occupancy. Note that a virtual machine behaves differently when the CPU usage is higher.

Chapter 3: Planning and preconfiguration for deploying Communication Manager

Planning Checklist

Planning checklist for VMware®

Ensure that the customer completes the following before deploying the Communication Manager Open Virtualization Application (OVA):

#	Task	Description	✔
1	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 15.	
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 14.	
5	Download the latest Communication Manager patch. For example: 00.0.441.0-XXXXX.tar.	See Applying the Communication Manager patch. on page 47	

Important:

If you are a new customer planning for fresh deployment of Communication Manager Release 8.0.1, then you can select Communication Manager Release 8.0 OVA file with 2.2 GHz CPU speed or 2.6 GHz CPU speed and then run the Communication Manager Release 8.0.1 patch.

If you are an existing customer with older CPU speed, and you want to upgrade to Communication Manager Release 8.0.1 with a newer CPU speed, then you must use Communication Manager Release 8.0 OVA with newer CPU speed and then run the Communication Manager Release 8.0.1 patch.

Planning checklist for Kernel-based Virtual Machine(KVM)

Ensure that you complete the following before deploying the Communication Manager on KVM:

No.	Task	Link/Notes	✔
1.	Download the required software.	See “Configuration tools and utilities” and “Release details of Communication Manager KVM OVA”	
2.	Purchase and obtain the required licenses.	—	
3.	Register for PLDS and activate license entitlements.	See “Downloading software from PLDS”	
4.	Prepare the site.	See “Supported hardware” and “Site preparation checklist”	

Important:

If you are a new customer planning for fresh deployment of Communication Manager Release 8.0.1, then you can select Communication Manager Release 8.0 OVA file with 2.2 GHz CPU speed or 2.6 GHz CPU speed and then run the Communication Manager Release 8.0.1 patch.

If you are an existing customer with older CPU speed, and you want to upgrade to Communication Manager Release 8.0.1 with a newer CPU speed, then you must use Communication Manager Release 8.0 OVA with newer CPU speed and then run the Communication Manager Release 8.0.1 patch.

Downloading software from PLDS

When you place an order for an Avaya 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 http://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. Enter http://plds.avaya.com in your Web browser 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 on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. 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.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

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 http://www.vmware.com/resources/guides.html.

Supported hardware

To deploy the Avaya Aura® application KVM OVA on a customer-provided server, the server must be on the Red Hat supported server list for Red Hat Enterprise Linux 7.2 or 7.3.

Configuration tools and utilities

To deploy and configure the Communication Manager KVM OVA, you need the following tools and utilities:

- Communication Manager KVM OVA, see “Release version of Communication Manager OVAs.”
- A browser for accessing Communication Manager
- PuTTY, PuTTYgen, and WinSCP
- MobaXterm

Supported browsers

The Avaya Aura® applications support the following web browsers:

- Internet Explorer 11
- Mozilla Firefox 59, 60, and 61

Correcting the CPU resources

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: 3* the CPU speed noted under the host's **Summary** tab
   - Simplex: 1* 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.

VMware software requirements

The following VMware software versions are supported:

- VMware vSphere ESXi 6.0
- VMware vSphere ESXi 6.5
- VMware vSphere ESXi 6.7
- VMware vCenter Server 6.0
- VMware vCenter Server 6.5
- VMware vCenter Server 6.7

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

Software requirements

You can deploy the Communication Manager OVA using ESXi, VMware vSphere. You cannot deploy the Communication Manager OVA using VMware vSphere versions 4.1, 5.0, 5.1 or 5.5.

With VMware vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration.

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 web site at https://support.avaya.com/.

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

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

Supported footprints of Communication Manager on VMware

Footprint (Max users)	vCPU	CPU Reservation (MHz)	Memory (MB)	Hard disk (GB)	Minimum CPU Speed (MHz)	Extra NICs
CM Main Max users 1000	2	3900	3584	64	1950	0
CM Survivable Max users 1000	1	1950	3584	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

Supported footprints of Communication Manager on KVM

Product name	Footprint (Max users)	Minimum CPU Speed (MHz)	Number of vCPUs	CPU Reservation (MHz)	RAM (MB)	Hard Disk (GB)	NICs
Communication Manager Simplex	41000	2200	2	4340	4608	64	2
Communication Manager Duplex	30000	2200	3	6510	5120	64	3
Communication Manager Hi Duplex	41000	2600	3	7650	5120	64	3

Note:

NICs must be in bridge mode.

Supported tools for deploying the KVM OVA

- Virt Manager GUI
- virsh command line interface
- OpenStack
- Nutanix
- Red Hat Virtualization Manager

Software details of Communication Manager

The following table lists the software details of all the supported platform for the application. You can download the softwares from the Avaya PLDS website at http://plds.avaya.com/.

Table 1: Communication Manager build details

Release	Bundle offer type	Installer files
8.0	OVA	• **AVP and VMware Simplex:** `CM-Simplex-08.0.0.0.822-e67-1.ova` • **AVP and VMware Duplex:** `CM-Duplex-08.0.0.0.822-e67-1.ova` • **KVM Simplex:** `CMKVM-Simplex-08.0.0.0.822-e67-1.ova` • **KVM Duplex:** `CMKVM-Duplex-08.0.0.0.822-e67-1.ova` • **AWS Simplex:** `CMAWS-Simplex-08.0.0.0.822-e67-1.ova` • **AWS Duplex:** `CMAWS-Duplex-08.0.0.0.822-e67-1.ova`
8.0	ISO	**Simplex or Duplex:** `CM-08.0.0.0.822-e67-0.iso`
8.0.1	Patch file	**Simplex or Duplex:** `8.0.1.0.0.25031.tar`
8.0.1	Solution Deployment Manager Client	`Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip` contains the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe` file.

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.

For server separation support on Amazon Web Services, the duplex servers must be in the same availability zone (AZ) to ensure that both the servers are in the same subnet.

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.

Site preparation checklist

Use the following checklist to know the set up required to deploy the KVM OVA.

No.	Task	Description	Notes	✔
1	Install the KVM hypervisor.			
2	Install the MobaXterm and Xming softwares on your laptop.	To remotely access the KVM hypervisor, the Virt Manager GUI, and virsh command line interface or PuTTY.		

Extracting KVM OVA

Procedure

1. Create a folder on the KVM host and copy the KVM OVA in the created folder or you can copy the KVM OVA in the /var/lib/libvirt/images directory.
2. Type the command **`tar -xvf`** *`<application_KVM.ova>`*.

   The system extracts the files from the application KVM OVA.

Unsupported feature

- Solution Deployment Manager deployments

Chapter 4: Deploying Communication Manager on VMware

Deploying the application OVA using vSphere Web Client by accessing the host directly

About this task

Use this procedure for deploying application OVA on ACP 130. This same procedure is applicable for ESXi 6.5 u2 onwards.

Before you begin

- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.

Procedure

1. On the Web browser, type the host URL: `https://<Host FQDN or IP Address>/ui`.
2. Enter login and password.
3. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.
4. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
5. Click **Next**.
6. 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.
7. Click **Next**.
8. On the Select storage page, select a datastore, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I Agree**.
10. Click **Next**.

11. 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. Uncheck **Power on automatically**.
12. Click **Next**.
13. On the Additional settings page, click **Next**.
14. On the Ready to complete page, review the settings, and click **Finish**.

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

    Note:

    Ensure that the virtual machine is powered down to edit the settings.
16. To ensure that the virtual machine automatically starts after a hypervisor reboot, click VM radio option, and click **Actions** > **Autostart** > **Enable**.

    Note:

    If you do not enable autostart you must manually start the virtual machine after the hypervisor reboot.
17. To start the virtual machine, if application is not already powered on perform one of the following steps:
    - Click VM radio option, and click **Actions** > **Power** > **Power On**.
    - 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 application.
18. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the application configuration parameters.

Deploying on vCenter using the vSphere Web client

About this task

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

Before you begin

- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.

Procedure

1. On the web browser, type the following URL: `https://<vCenter FQDN or IP Address>/vsphere-client/`.
2. To log in to vCenter Server, do the following:
   a. In **User name**, type the user name of vCenter Server.
   b. In **Password**, type the password of vCenter Server.
3. Right-click the ESXi host and select **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.
4. 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.
5. Click **Next**.
6. On the Select name and location page, do the following:
   a. In **Name**, type a name for the virtual machine.
   b. In **Browse**, select a datacenter.
7. Click **Next**.
8. On the Select a resource page, select a host, and click **Next**.
9. On the Review details page, verify the OVA details, and click **Next**.
10. To accept the End User License Agreement, on the Accept license agreements page, click **Accept**.
11. Click **Next**.
12. Select the application profile in the **Deployment Configuration** section.
13. On the Select storage page, in **Select virtual disk format**, click **Thick provision lazy zeroed**.
14. Click **Next**.

15. On the Select networks page, select the destination network for each source network.
16. Click **Next**.
17. 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 25.
18. Click **Next**.
19. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
20. 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.
21. Click the **Console** tab and verify that the system startup is successful.

Properties field descriptions

Note:

If you specify an invalid value for a field. the system does not assign the value for the field. Until you assign the valid values for the field, you cannot power on the virtual machine.

Name	Description
CM IPv4 Address	Specifies the IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	Specifies the subnet mask of the Communication Manager virtual machine.

Table continues…

Name	Description
CM IPv4 Gateway	Specifies the IP address of the default gateway. **Note:** The default gateway should be configured for the Public network.
CM IPv6 Address	Specifies the IPv6 address of the Communication Manager virtual machine.
CM IPv6 Gateway	Specifies the IPv6 address of the default gateway. **Note:** The default gateway should be configured for the Public network.
CM IPv6 Network Prefix	Specifies the IPv6 network prefix of the Communication Manager virtual machine.
EASG Enabled	Enables the Enhanced Access Security Gateway (EASG) feature.
Out of Band Management IPv4 Address	Specifies the IP Address for Out-of-Band Management. This is an optional field. 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	Specifies the netmask for Out-of-Band Management. This is an optional field. If you do not want to configure Out-of-Band Management, leave the value of this field as zeros.
CM Hostname	Specifies the host name or an FQDN of Communication Manager. **Note:** The host name is regardless of the interface that is used to access. The Public interface is the default interface.
NTP Server(s)	Specifies the IP Address of the Network Time Protocol (NTP) server for the Communication Manager virtual machine. This is an optional field. You can add up to three NTP servers.
DNS Server(s)	Specifies the IP Address of the Domain Name System (DNS) server for the Communication Manager virtual machine. This is an optional field. You can add up to three DNS servers.
Search Domain List	This is an optional field.
WebLM Server IPv4 Address	Specifies the IP address of WebLM Server .

Table continues…

Name	Description
CM Privileged Administrator User Login	Specifies the login name for the Communication Manager privileged administrator.
CM Privileged Administrator User Password	Specifies the password for the Communication Manager privileged administrator. The value range is from 8 to 255 characters.

Deployment of cloned and copied OVAs

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 on the virtual machine. At this time, Avaya only supports the deployment of new OVAs.

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. The system automatically assigns the Duplex OVAs first NIC and second NIC to the one network. 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 2

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 27

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*.

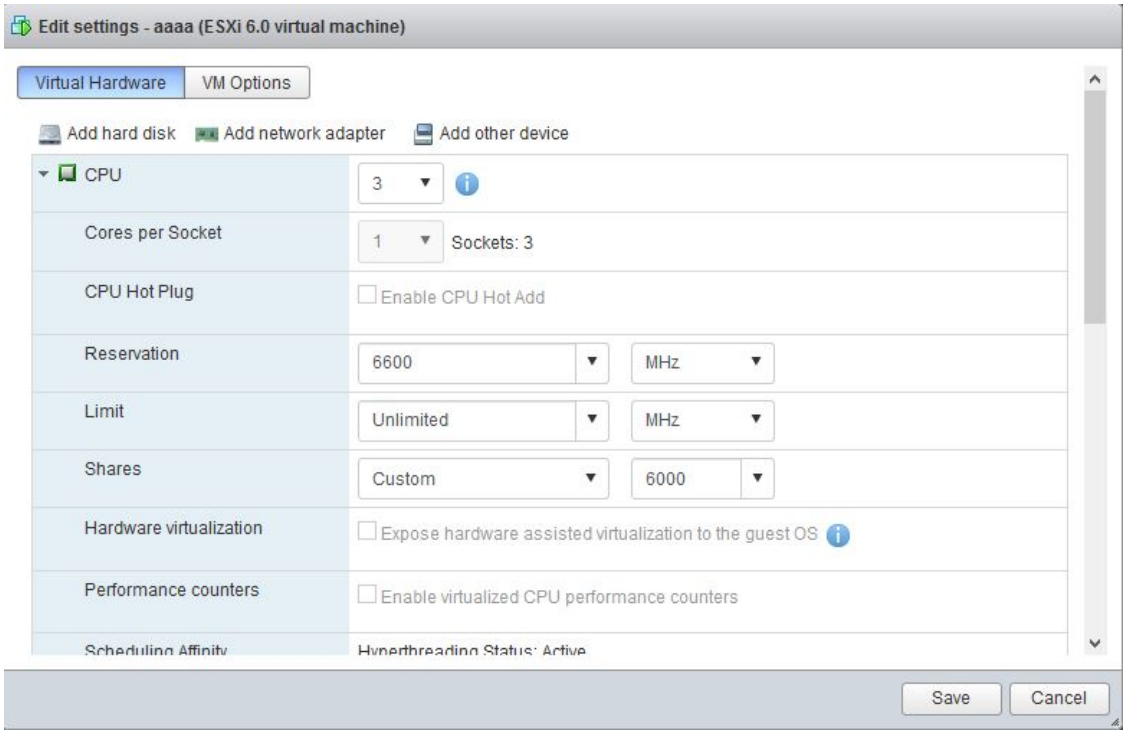
Related links

Duplex OVA deployment on page 27

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.

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 Healthcheck. 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 (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/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 that 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 that are 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 that are currently installed on the system.

Chapter 5: Deploying Communication Manager on KVM

Deploying KVM OVA by using Virt Manager

Before you begin

- Access the KVM host remotely.
- Install virt-manager on KVM host.

Procedure

1. Connect to KVM host using an SSH session.
2. On the SSH terminal, run the command: `virt-manager`.
3. On the Virtual Machine Manager window, click **File** > **New Virtual Machine**, and select **Import existing disk image**.
4. On the Create a new virtual machine Step 1 of 4 window, select **Import existing disk image**.
5. Click **Forward**.
6. On the Create a new virtual machine Step 2 of 4 window, perform the following:
   a. In **Provide the existing storage path**, add the path where the file is located or click **Browse**, and select the `qcow2` image of application on the KVM host.
   b. In **OS type**, select **Linux**.
   c. In **Version**, select **Red Hat Linux Enterprise 7.2** or **Red Hat Linux Enterprise 7.3**.
   d. Click **Forward**.
7. On the Create a new virtual machine Step 3 of 4 window, perform the following:
   a. In **Memory (RAM)**, enter the required memory.

      Refer to the “Supported footprints of Communication Manager on KVM” section.
   b. In **CPU**, enter the number of CPUs for the virtual machine based on the application profile.

      Refer to the “Supported footprints of Communication Manager on KVM” section.

Note:

Select the appropriate CPU and memory configuration for Simplex and Duplex.

c. Click **Forward**.

8. On the Create a new virtual machine Step 4 of 4 window, perform the following:
   a. In **Name**, type the name of the virtual machine.
   b. Select the **Customize Configuration before Install** check box.
   c. Check **Network selection** and verify the required network interface.

      This configuration is for eth0.

   d. For public network, select NIC and set the **Service model** to **Hypervisor Default**.
   e. Click **Finish**.
9. In the left navigation pane, click **Disk 1**. In the **Advanced options** section, perform the following:
   a. In **Disk bus**, select **IDE**.
   b. In **Storage format**, type `qcow2`.
   c. Click **Apply**.
10. For Duplex configuration, in the left navigation pane, click **Add Hardware**. In the **Advanced options** section, perform the following:
    a. Select **Network**.
    b. From **Network source**, select the required source for eth1 for duplication configuration. Use this option if you are deploying CM Duplex only.
    c. Click **Apply**.
11. For Out of Band Management configuration, in the left navigation pane, click **Add Hardware**. In the **Advanced options** section, perform the following:
    a. Select **Network**.
    b. From **Network source**, select the required source for eth2 for Out of Band Management.
    c. Click **Apply**.
12. In the left navigation pane, click **Display Spice** and perform the following:
    a. In the **Type** field, select **VNC Server**.
    b. In the **Keymap** field, select **EN-US**.
    c. Click **Apply**.
13. In the left navigation pane, click **Boot Options** and perform the following:
    a. In **Boot device order**, click **IDE Disk 1**.

b. Click **Apply**.

14. Click **Begin Installation**.

    The system creates a new virtual machine.

Next steps

On first boot of the virtual machine, provide the configuration and networking parameters.

Deploying Communication Manager KVM from CLI by using virsh

Before you begin

- Access the KVM host remotely.
- Keep the OVA file ready.

Procedure

On the KVM host CLI, perform the following:

a. Navigate to the Communication Manager KVM OVA directory.

b. Run the Communication Manager installation utility by using the following script: `sh CMKVM_installerScript.sh`.

c. For Duplex configuration, when the system prompts, select the required profile.

d. In **VM name**, type a name of the virtual machine.

e. In **Drive storage location**, type storage location of the virtual machine.

f. In **Public network**, select the public network.

g. For Duplex configuration, in **Duplication Link network**, select the available network.

h. In **Out of Band Management network**, select the available network.

i. To continue, type `Y`.

   The system displays the message: `Deploying image`.

Next steps

On first boot of the virtual machine, provide the configuration and networking parameters.

Deploying application by using OpenStack

Connecting to OpenStack Dashboard

Before you begin

- Create an OpenStack account.
- Acquire adequate permission to upload and deploy the KVM ova.

Procedure

1. In your web browser, type the OpenStack URL.

   For example, http://<openstack.xyz.com>/horizon.
2. In **Domain**, type the domain name.
3. In **User Name**, type the user name.
4. In **Password**, type the password.
5. Click **Connect**.

   The system displays the Instance Overview - OpenStack Dashboard page.

Uploading the qcow2 image

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Images**.
3. On the Images page, click **Create Image**.

   The system displays the Create An Image dialog box.
4. In **Name**, type the name of the image.
5. In **Description**, type the description of the image.
6. In **Image Source**, click **Image Location** or **Image File**, and perform one of the following:
   - In **Image Location**, type the exact URL of the qcow2 image.
   - In **Image File**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
7. In **Format**, click **QCOW2 - QEMU Emulator**.
8. Click **Create Image**.

   The system displays the created image on the Images page.

9. Click the image and click **Update Metadata**.
    a. In the **Custom** field, select **hw_disk_bus**.
    b. Click **+**.
    c. In the **hw_disk_bus** field, type `IDE`.
    d. Click **Save**.

Flavors

Flavors are footprints of an application. The administrator must create flavors for each application.

For information about the footprints, see the profiles and footprints information for the application.

Creating a security group

About this task

Security groups are sets of IP filter rules. Each user must create security groups to specify the network settings for the application.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Access & Security**.
3. On the Access & Security page, click **Create Security Group**.

   The system displays the Create Security Group dialog box.
4. In **Name**, type the name of the security group.
5. In **Description**, type the description of the security group.
6. Click **Create Security Group**.

   The system displays the created security group on the Access & Security page.

Next steps

Add rules to security group.

Adding rules to a security group

Before you begin

Create a security group.

For information about the application-specific ports and protocols, see the port matrix document at http://support.avaya.com/security.

Procedure

1. On the Access & Security page, click **Manage Rules** that is corresponding to the created security group.
2. On the Access & Security / Manage Security Group Rules page, click **Add Rule**.

   The system displays the Add Rule dialog box.
3. In **Rule**, click a rule

   The system displays the fields that are associated with the selected rule.
4. Enter the appropriate values in the fields.
5. Click **Add**.

   The system displays the created rule on the Access & Security / Manage Security Group Rules page.

Deploying application by using OpenStack

Before you begin

- Create flavors.
- Create a security group.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Instances**.
3. On the Instance page, click **Launch Instance**.

   The system displays the Launch Instance dialog box.
4. In **Details**, perform the following:
   a. In **Instance Name**, type a name of the instance.
   b. In **Availability zone**, select the availability zone of the instance.
   c. Click **Next**.
5. In **Source**, perform the following:
   a. In the **Available** section, select a check box corresponding to an instance image.

      The system displays the selected image in the **Allocated** section.
   b. Click **Next**.
6. In **Flavors**, perform the following:
   a. In the **Available** section, select a check box corresponding to a flavor name.

      The system displays the selected flavor in the **Allocated** section.

b. Click **Next**.

7. In **Networks**, perform the following:
   a. In the **Available** section, select a check box corresponding to a network name.

      The system displays the selected network in the **Allocated** section. Also assign Network for Duplication.

      For duplex deployments, you must attach two interfaces from the same network to a single machine, and then configure. For more information on configuring Communication Manager for duplex deployments, see “Configuring Duplex Communication Manager”. Also, assign two IP addresses of the same network on one instance.

   b. Click **Next**.
8. In **Network Ports**, leave the default settings, and click **Next**.
9. In **Security Groups**, perform the following:
   a. In the **Available** section, select a check box corresponding to a security group name.

      The system displays the selected security group in the **Allocated** section.

   b. Click **Next**.
10. In **Key Pair**, leave the default settings, and click **Next**.
11. In **Configuration**, leave the default settings, and click **Next**.
12. In **Metadata**, leave the default settings.
13. Click **Launch Instance**.

    The system displays the created instance on the Instances page. The **Status** column displays: `Spawning`. When the system creates the application instance, the **Status** column displays: `Active`.

    The system displays the static IP Address of the application in the **IP Address** column.

Next steps

Configure the application instance. Use the static IP Address to configure the application instance.

Configuring application instance

Procedure

1. On the Instances page, in the **INSTANCE NAME** column, click the application instance name.
2. On the Instances / <Instance Name> page, click **Console**.
3. On the Instance Console page, go to console, and follow the prompt to configure the application instance.

Configuring Duplex Communication Manager

About this task

Perform the following steps after deploying Duplex Communication Manager using Openstack to make the alias IP address reachable.

Procedure

1. Get the network port ID associated with Duplex Communication Manager, CM1 and CM2.
2. Log in to the Openstack controller.
3. Run the following commands:
   - `source openrc`

     All login-related information need to be updated in this file, so that the following two commands run successfully. Else, login-related information must be part of following port-update commands.

     Provide the following two commands for Alias IP Address.
   - `neutron port-update <port-id-cm1>--allowed_address_pairs list=true type=dict ip_address=<alias-ip-address>`

     For example, `neutron port-update 1a523c2f-a6b4-4ee1-9ace-b877a60a131e --allowed_address_pairs list=true type=dict ip_address=192.168.121.16`
   - `neutron port-update <port-id-cm2>--allowed_address_pairs list=true type=dict ip_address=<alias-ip-address>`

     For example, `neutron port-update ae0cc604-a040-4f31-83e7-d24f110f9ff1 --allowed_address_pairs list=true type=dict ip_address=192.168.121.16`

Deploying application by using Nutanix

Logging on to the Nutanix Web console

Procedure

1. To log on to the Nutanix Web console, in your web browser, type the PRISM URL.

   For example, http://<PRISM_IPAddress>/.
2. In **username**, type the user name.

3. In **password**, type the password.
4. Press **Enter**.

   The system displays the Home page.

Transferring the files by using the WinSCP utility

About this task

Use the following procedure to transfer the files from a remote system to a Nutanix container by using the WinSCP utility.

Procedure

1. Use WinSCP or a similar file transfer utility to connect to the Nutanix container.
2. In **File protocol**, click **SCP**.
3. Enter the credentials to gain access to SCP.
4. Click **Login**.
5. Click **OK** or **Continue** as necessary in the warning dialog boxes.
6. In the WinSCP destination machine pane, browse to `/home/<Container_Name>` as the destination location for the file transfer.
7. Click and drag the `qcow2` image from the WinSCP source window to `/home/<Container_Name>` in the WinSCP destination window.
8. Click the WinSCP **Copy** button to transfer the file.
9. When the copy completes, close the WinSCP window (**x** icon) and click **OK**.

Uploading the qcow2 image

Procedure

1. Log on to the Nutanix Web console.
2. Click **Settings icon ( )** > **Image Configuration**.

   The system displays the Image Configuration dialog box.
3. Click **+ Upload Image**.

   The system displays the Create Image dialog box.
4. In **NAME**, type the name of the image.
5. In **ANNOTATION**, type the description of the image.
6. In **IMAGE TYPE**, click **DISK**.

7. In **STORAGE CONTAINER**, click the storage container of the image.
8. In **IMAGE SOURCE**, perform one of the following:
   - Select **From URL**, type the exact URL of the qcow2 image. For example: `nfs://<127.0.0.1>/<Storage Container Name>/<Image Name>`
   - Select **Upload a file**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
9. Click **Save**.

   The system displays the created image on Image Configuration.

Creating the virtual machine by using Nutanix

Before you begin

- Upload the `qcow2` image.
- Configure the network.

Procedure

1. Log on to the Nutanix Web console.
2. Click **Home** > **VM**.
3. Click **+ Create VM**.

   The system displays the Create VM dialog box.
4. In the General Configuration section, perform the following:
   a. In **NAME**, type the name of the virtual machine.
   b. In **DESCRIPTION**, type the description of the virtual machine.
5. In the Compute Details section, perform the following:
   a. In **VCPU(S)**, type the number of virtual CPUs required for the virtual machine.
   b. In **NUMBER OF CORES PER VCPU**, type the number of core virtual CPUs required for the virtual machine.
   c. In **Memory**, type the memory required for the virtual machine.

      The value must be in GiB.

   You must select the CPU and Memory according to the application footprint profile.
6. In the Disk section, perform the following:
   a. Click **+ Add New Disk**.

      The system displays the Add Disk dialog box.
   b. In **TYPE**, click **DISK**.

c. In **OPERATION**, click **Clone from Image Service**.

d. In **IMAGE**, click the application image.

e. In **BUS TYPE**, click **IDE**.

f. Click **Add**.

The system displays the added disk in the **Disk** section.

7. In the Disk section, select a boot device.
8. In the Network Adopters (NIC) section, perform the following:

a. Click **Add New NIC**.

The system displays the Create NIC dialog box.

b. In **VLAN NAME**, click the appropriate NIC.

The system displays **VLAN ID**, **VLAN UUID**, and **NETWORK ADDRESS / PREFIX** for the selected NIC.

c. Click **Add**.

The system displays the added NIC in the Network Adopters (NIC) section.

You must select the number of NIC according to the application footprint profile.

If you are configuring Out of Band Management, select one more NIC.

For Duplex configuration, select one more NIC.

9. In the VM Host Affinity section, perform the following:

a. Click **Set Affinity**.

The system displays the Set VM Host Affinity dialog box.

b. Select one or more host to deploy the virtual machine.

c. Click **Save**.

The system displays the added hosts in the VM Host Affinity section.

10. Click **Save**.

The system displays the message: `Received operation to create VM <name of the VM>`.

After the operation is successful, the system displays the created virtual machine on the VM page.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Power On**.

   The system starts the virtual machine.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

Configuring the virtual machine

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Launch Console**.
5. Follow the prompt to configure the virtual machine.

Deploying application by using Red Hat Virtualization Manager

Logging on to the Red Hat Virtualization Manager Web console

Procedure

1. In your web browser, type the Red Hat Virtualization Manager URL.

   For example, https://<RedHatVirtualizationManager_IPAddress>/ovirt-engine/.

2. Click **Admin Portal**.

   The system displays the Red Hat Virtualization Manager Log In page.
3. In **Username**, type the user name.
4. In **Password**, type the password.
5. In **Profile**, click the appropriate profile.
6. Click **Log In**.

   The system displays the Red Hat Virtualization Manager Web Administration page.

Uploading the disk

Before you begin

You must import the `ovirt-engine` certificate into your browser by accessing the `http://<engine_url>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA` link to get the certificate. Establish the trust for the new Certificate Authority (CA) with the website.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Disks** tab, click **Upload** > **Start**.

   The system displays the Upload Image dialog box.
4. Click **Browse**.
5. In the Choose File to Upload dialog box, select the qcow2 disk image from your local system, and click **Open**.
6. In **Size(GB)**, type the size of the disk.
7. In **Alias**, type the name of the disk.
8. In **Description**, type the description of the disk.
9. In **Data Center**, click the data center to store the disk.
10. In **Storage Domain**, click the storage domain of the disk.
11. In **Disk Profile**, click disk profile.
12. In **Use Host**, click the host of the disk.
13. Click **OK**.

    The system displays the uploaded image on the **Disks** tab. Once the disk image is successfully uploaded, the **Status** column displays `OK`.

Creating the virtual machine by using Red Hat Virtualization Manager

Before you begin

- Upload the `qcow2` disk image.
- Configure the network according to the product requirements.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Virtual Machines** tab, click **New VM**.

   The system displays the New Virtual Machine dialog box.
4. In **Operating System**, click **Linux**.
5. In **Instance Type**, click an instance type.

   You must select the instance type according to the application footprint profile.
6. In **Optimized for**, click **Server**.
7. In **Name**, type the name of the virtual machine.
8. In **Description**, type the description of the virtual machine.
9. In the Instance Images section, perform the following:
   a. Click **Attach**.

      The system displays the Attach Virtual Disks dialog box.
   b. In **Interface**, click **IDE**.
   c. Click **OK**.

      The system displays the added disk in the Instance Images section.
10. In **nic1**, click a vNIC profile.

    If you are configuring Out of Band Management, select one more NIC.

    For Duplex configuration, select one more vNIC for duplication.
11. Click **Show Advanced options**.
12. Click **System**.
13. Configure the memory size and CPU according to the product requirements.

    For more information, see “Supported footprints of Communication Manager on KVM”.
14. Click **OK**.

    After the operation is successful, the system displays the created virtual machine on the **Virtual Machines** tab.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

Right-click the virtual machine and click **Run**.

When the system starts the virtual machine, the system displays a green upward arrow key ( ) corresponding to the virtual machine name.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

Configuring the virtual machine

Before you begin

- Start the virtual machine.
- Install the `virt-viewer` installer to access console.

Procedure

1. Right-click the virtual machine and click **Console**.
2. Follow the prompt to configure the virtual machine.

Applying the Communication Manager patch using SMI

Before you begin

You must deploy the Communication Manager Release 8.0 OVA file.

About this task

Use the Communication Manager System Management Interface (SMI) to apply the Communication Manager patch.

Procedure

1. Log in to Communication Manager System Management Interface using a service account.

2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous** > **Download Files**.

   The system displays the Download Files page.
4. Select the **File(s) to download from the machine I'm using to connect to the server** option, click **Choose File** to browse the file from your local machine, and click **Download**.
5. In the left navigation pane, click **Server Upgrades** > **Manage Updates**.

   The system displays the Manage Updates page.
6. Select the update ID and click **Unpack**.

   The status of the selected file changes to unpacked.
7. Select the update ID and click **Activate**.

   The status of the patch file changes to activated.

   Note:

   - If you are installing the Kernel Service Pack click **Commit** after clicking **Activate**.
   - Activating Communication Manager Service Packs impacts service. You can schedule this activity in a maintenance window.
   - If you are installing Communication Manager Release 8.0.1, first install Communication Manager Release 8.0, and then apply patch.

Chapter 6: 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 49	
2	Configure the Communication Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 50	
3	Set up network configuration.	Administering network parameters on page 50	
4	Apply the latest Communication Manager patch.	Applying the Communication Manager patch on page 47	
5	Set the date and time.	Setting the date and time on page 51	
6	Configure the time zone.	Setting the time zone on page 52	
7	Set up the network time protocol.	Setting up the network time protocol on page 52	
8	Direct Communication Manager to the WebLM server.	Configuring WebLM Server on page 54	
9	Create an suser account.	Adding an administrator account login on page 53	

Starting the Communication Manager virtual machine

Procedure

In the vSphere Web client, select the host server, 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 log in.

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 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 **Configure**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Properties**.

   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 `craft`.
2. On first attempt log in as `craft`, 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 as *craft* 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.
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 alphabetic characters.
   - Can have numbers.
   - Can have an underscore (_).
   - 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**.

Applying the Communication Manager patch using SMI

Before you begin

You must deploy the Communication Manager Release 8.0 OVA file.

About this task

Use the Communication Manager System Management Interface (SMI) to apply the Communication Manager patch.

Procedure

1. Log in to Communication Manager System Management Interface using a service account.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous** > **Download Files**.

   The system displays the Download Files page.

4. Select the **File(s) to download from the machine I'm using to connect to the server** option, click **Choose File** to browse the file from your local machine, and click **Download**.
5. In the left navigation pane, click **Server Upgrades** > **Manage Updates**.

   The system displays the Manage Updates page.

6. Select the update ID and click **Unpack**.

   The status of the selected file changes to unpacked.

7. Select the update ID and click **Activate**.

   The status of the patch file changes to activated.

   Note:

   - If you are installing the Kernel Service Pack click **Commit** after clicking **Activate**.
   - Activating Communication Manager Service Packs impacts service. You can schedule this activity in a maintenance window.

- If you are installing Communication Manager Release 8.0.1, first install Communication Manager Release 8.0, and then apply patch.

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

The main virtual machine, survivable remote virtual machines, and survivable core virtual machines use a specific port across a customer network for registration and translation distribution. Use the **`firewall`** command with *suser* level access, to change the firewall settings from the command line.

Note:

Use ports 80 and 443 to gain access to System Management Interface. Use port 5022 for a secured System Access Terminal (SAT).

For more information about port utilization, see “Accessing the port matrix document” section.

Use the information in the following table to determine the ports that must be open in the customer network in a survivable core virtual machine environment.

Port	Used by	Description
20	ftp data	-
21	ftp	-
22	ssh/sftp	-
68	DHCP	-
514	Communication Manager 1.3 to download the translations.	-
1719 (UDP port)	The survivable core virtual machine to register to the main virtual machine.	This a survivable core virtual machine registers with the main virtual machine using port 1719. For more information about survivable core virtual machine registration, see *Avaya Aura® Communication Manager Survivability Options*, 03-603633.
1024 and later	Processor Ethernet	TCP outgoing
1956	Command server - IPSI	-
5000 to 9999	Processor Ethernet	TCP incoming
5010	IPSI/Virtual machine control channel	-
5011	IPSI/Server IPSI version channel	-
5012	IPSI/Virtual machine serial number channel	-

Table continues…

Port	Used by	Description
21874 (TCP port)	The main virtual machine that downloads translations to the survivable core virtual machine.	The main virtual machine uses port 21874 to download translations to the survivable core virtual machine and the survivable remote virtual machines.

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 OVA template installation.
- Duplication parameters: Use to configure the duplication settings if you installed the Duplex Main or the Survivable Core OVA or both.

Related links

Server role configuration on page 58
Configuring Server Role on page 59
Server Role field descriptions on page 60

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 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 Appliance Virtualization Platform. 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 Appliance Virtualization Platform.

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 58

Configuring Server Role

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**.

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

   System ID and Module ID must be set to default value of 1.

   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 58

Server Role field descriptions

Server Settings field descriptions

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.
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 field descriptions

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.

Table continues…

Name	Description
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 field descriptions

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 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 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 58

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. For more information on configuring load balancer, see *Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment*.

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 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 left 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. 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 duplication method. The choices are: • **This is a duplicated server using software-based duplication**: Software-based duplication provides memory synchronization between an active and a standby virtual machine by 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 by using AES 128 encryption.
Hostname	The host name of the other virtual machine.
Server ID	The unique virtual machine ID of the other virtual machine, which must be an integer from 1 through 256.
Corporate LAN/PE IP	• **IPv4**: The IP address of the Corporate LAN or Processor Ethernet interface for the other virtual machine. • **IPv6**: The IPv6-compliant IP address of the Corporate LAN or Processor Ethernet interface for the other virtual machine.
Duplication IP	• **IPv4**: The IP address of the duplication interface of the other virtual machine. You can assign the IP addresses according to the network configuration. • **IPv6**: The IPv6-compliant IP address of the duplication interface of the other virtual machine. You can assign the IP addresses according to the network configuration.

Table continues…

Name	Description
PE Interchange Priority	A relative priority as compared to IPSIs in configurations that use both Processor Ethernet and IPSIs. Select one of the following priority levels: • **HIGH:** Favors the virtual machine with the best PE state of health (SOH) when PE SOH is different between virtual machines. • **EQUAL:** Counts the Processor Ethernet interface as an IPSI and favors the virtual machine with the best connectivity count. • **LOW:** Favors the virtual machine with the best IPSI connectivity when IPSI SOH is different between virtual machines. • **IGNORE:** Does not includes the Processor Ethernet in virtual machine interchange decisions.
IP address for PE Health Check	• **IPv4**: The IP 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**: 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. The system displays a dialog box with three buttons: **Restart Now**, **Restart Later**, and **Cancel**. **Note:** Click **Restart Now** only after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Table continues…

Name	Description
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.

Configuring the Communication Manager using KVM

Configuring the Communication Manager instance

Procedure

1. Log in with the user name as `configuser` and password as `configuser01`.
2. In **Do you accept the terms of this EULA? (Y)es/(N)o**, scroll to the end and then type `y`.
3. Log in with the user name as `craft` and password as `craft01`.
4. For deployments using Virt Manager, virsh, Nutanix, or Red Hat Virtualization Manager when the system prompts to configure the Communication Manager IP address, assign an IP address.

   The system will not prompt for deployments using Openstack as the IP address has already been assigned.
5. When the system prompts to create a customer privileged administrator account, enter the login details to create an account.

   You must create the Communication Manager privileged administrator account credentials. The craft credentials will not work to log in to the Communication Manager System Management Interface for further configuration.
6. In **Enable Avaya Services EASG Access**, type:
   - `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 affect Avaya's ability to provide support for the product. Unless the customer can manage the product, do not disable Avaya Services Logins.

7. After the configuration is complete, log in to the Communication Manager System Management Interface with the Communication Manager privileged administrator credentials.
8. For Openstack, configure network parameters.

Chapter 7: Post-installation verification of Communication Manager

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 and IPSIs.

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.

   SMI supports Internet Explorer 11 and Mozilla Firefox 45.0 and later.

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 `http://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 `http://media-server1.mycompany.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 user name.

   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.

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, and supported end date.

   The 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

License Status field descriptions

Name	Description
CommunicaMgr License Mode	Specifies the license status. • 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. • 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`.

Table continues…

Name	Description
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.
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/SAL Product Registration Request form.

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 backup of a system in a translation file, and restore the files on another system.

Procedure

1. Log in to the Communication Manager CLI as a root user.
2. If the system translations are prepared offsite, install the prepared translations, and reset Communication Manager using the command **`reset system 4`** or **`drestart 1 4`**.
3. If translations are not prepared offsite:
   a. Type **`save translation`** and press `Enter` to save the translations to the hard disk drive.
   b. Type **`reset system 4`** or **`drestart 1 4`** and press `Enter`.
4. Enter minimal translations to verify connectivity to the port networks or media gateway.
5. After you enter the translations, type **`save translation`**, and press `Enter` to save the translations to the hard disk drive.

Chapter 8: 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
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware and Kernel-based Virtual Machine (KVM).	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Virtual Appliance	Describes the implementation instructions while deploying Communication Manager on Appliance Virtualization Platform.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment	Describes the implementation instructions while deploying Communication Manager on Amazon Web Services, Microsoft Azure, Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only Environment	Describes the implementation instructions while deploying Communication Manager on a software-only environment.	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 are requested by specific customers 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. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.

4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com/.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

Navigate to the **My Content** > **Watch list** menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

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

Course code	Course title
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura® Release 8.0
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.0
21450V	Administering Avaya Aura® Communication Manager Release 8.0

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` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

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 http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.
   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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 84.

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 VMware Knowledge Base, which includes the 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 the RedHat crash utility, see White paper: RedHat Crash Utility.

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 1: VMware cluster configuration with four ESXi hosts on page 86, 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 1: VMware cluster configuration with four ESXi hosts on page 86:

- Host 1 (CMVM_01) is ACT with a duplication link communicating over VMnic3 through the network switch.
- Host 4 (CMVM_02) is STB with a duplication link communicating over VMnic3 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 VMnic3.
- Host 1 is booting so no communication over VMnic3.

- Host 3 (CMVM_01) and Host 4 (CMVM_02) link up and communicate across the network switch over each VMnic3.

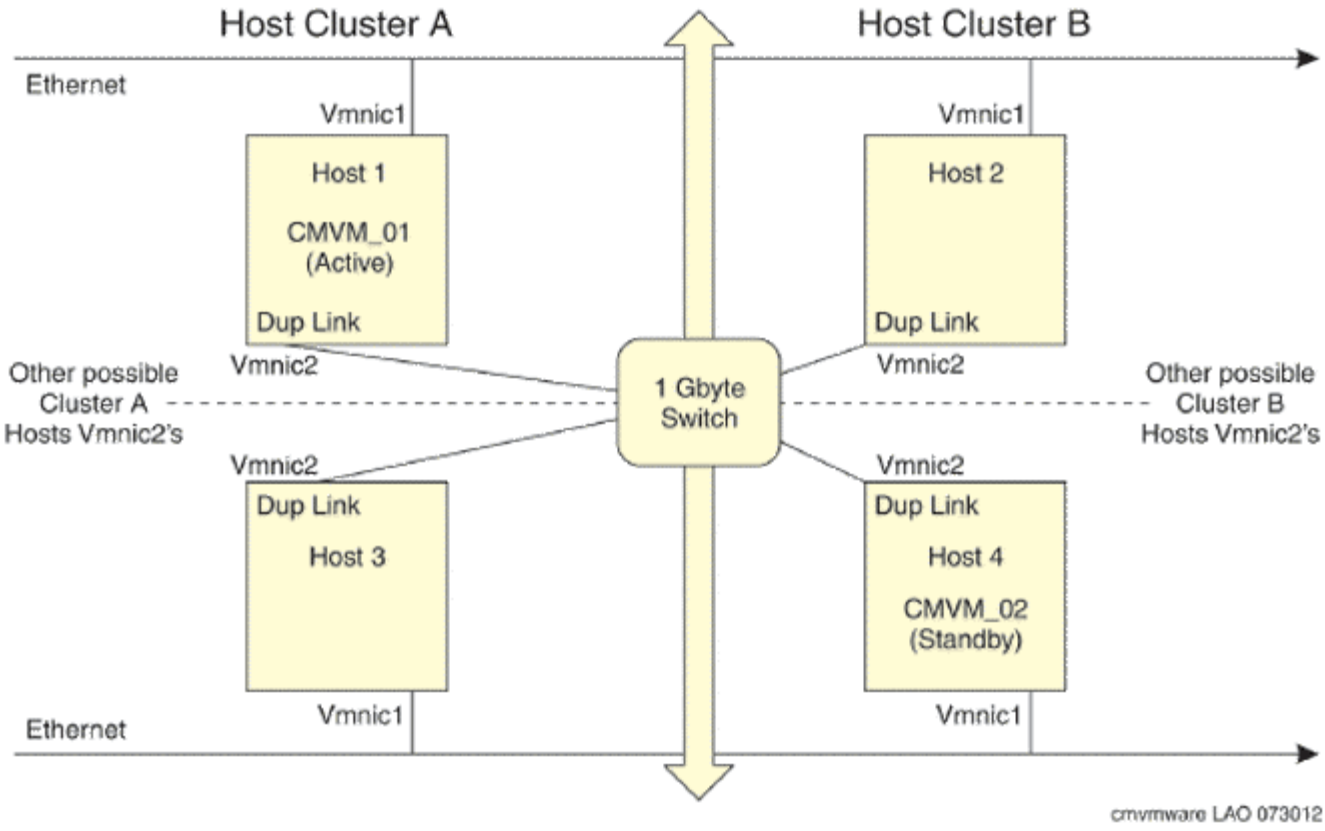


Figure 1: VMware cluster configuration with four ESXi hosts

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: Best Practices

VMware best practices for performance

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

Related links

[VMware networking best practices](#) on page 88
[Thin vs. thick deployments](#) on page 93
[Storage](#) on page 94

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
- HP ProLiant 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 and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

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

Dell PowerEdge Server

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

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

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

VMware networking best practices

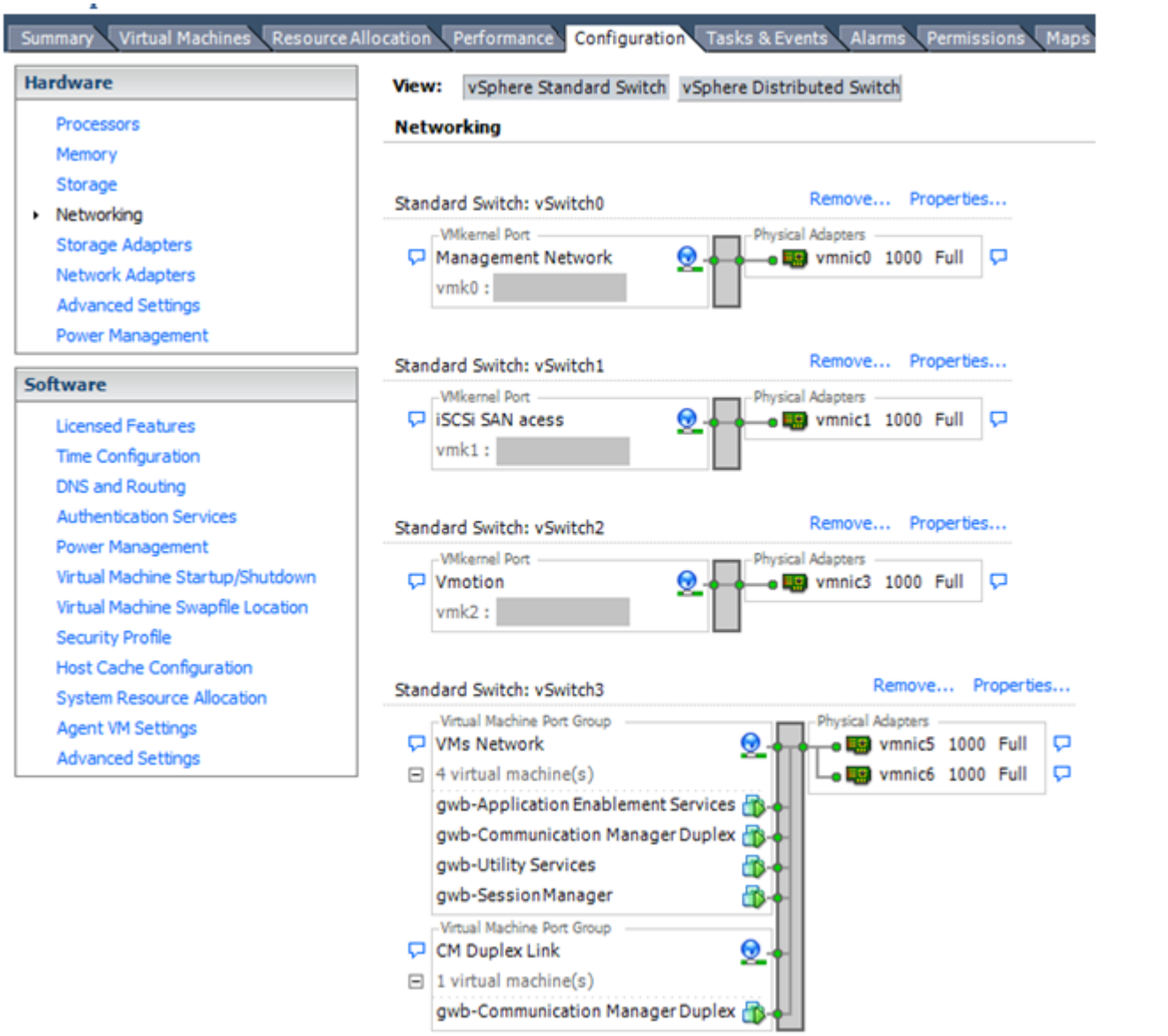
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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).

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:

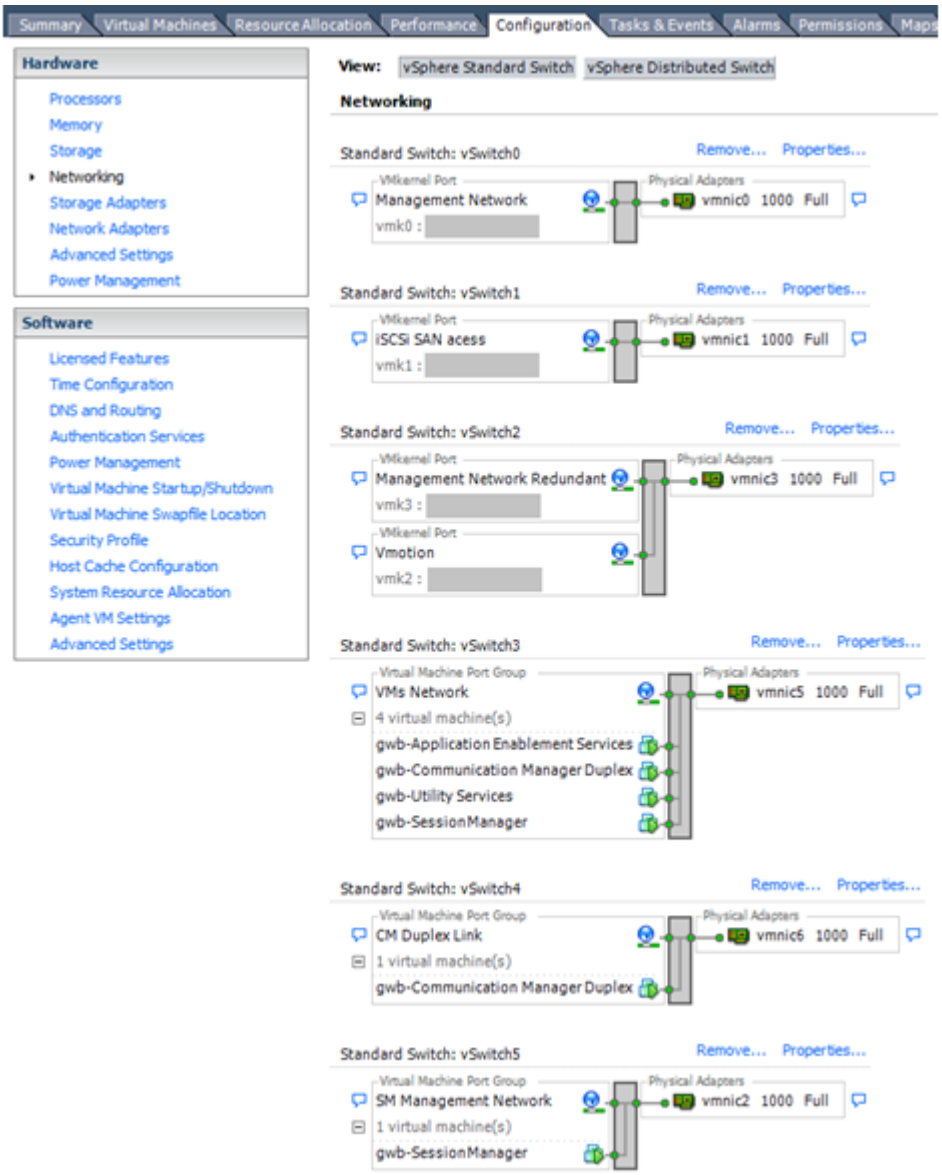
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides 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 http://support.avaya.com and search for PSN003556u.
Performance Best Practices for VMware vSphere® 6.0	Go to https://www.vmware.com/support/pubs/ and search for *Performance Best Practices for VMware vSphere® 6.0*.
VMware vSphere 6.5 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 6.5 Documentation*.
VMware vSphere 6.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 6.0 Documentation*.
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Related links

VMware best practices for performance on page 87

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

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

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate 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 format 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 Microsoft Windows format tool writes information to all sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, 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 completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

Related links

VMware best practices for performance on page 87

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 87

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

See the following resources for more information about snapshots:

Title	Link
Best practices for virtual machine snapshots in the VMware environment	http://kb.vmware.com/kb/1025279
Understanding virtual machine snapshots in VMware ESXi and ESX	http://kb.vmware.com/kb/1015180
Working with snapshots	http://kb.vmware.com/kb/1009402
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	http://kb.vmware.com/kb/1018029
Consolidating snapshots in vSphere 5.x	http://kb.vmware.com/kb/2003638

Related links

VMware best practices for performance on page 87

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 87

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 85.

Related links

VMware best practices for performance on page 87

VMware vMotion

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

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 the vMotion is enabled.
- Ensure that you have identical vSwitches. You must 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 to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Using VMware vMotion with Communication Manager virtual machine moves its current host to a new host and call processing continues with no call failures.

Related links

VMware best practices for performance on page 87

Appendix D: 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) when there is no update, service pack, or release fix, but the business unit or Avaya Services need 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.

   If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, type the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. 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 services packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: E-Notifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Index

E

F

G

I

K

L

M

N

O

P

R

S

T

U

V

W