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

Release 10.2.x
Issue 10
March 2026

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

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

- Customer-provided hardware
- Infrastructure as a Service environment

This document is intended for people who deploy and configure Communication Manager *ISO image* at a customer site.

The *Software-Only* offer is for customers who want to deploy the Avaya Aura® applications on their own standard Linux operating system. Avaya Aura® applications support third party applications only on the *Software-Only* deployments.

Note:

A virtualized environment is required for the software-only deployment.

Changes to platform support

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

Discontinued Platforms:

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

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

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

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

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

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

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

Prerequisites

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

Knowledge

- Linux® Operating System
- Avaya Aura® Communication Manager
- Infrastructure as a Service
- Virtualized environment

Skills

To administer the Linux server and Avaya Aura® applications.

Tools

For information about tools and utilities, see Configuration tools and utilities on page 22.

System capacities for applications

For information about the system capacities, such as, number of users, gateways, and endpoints, see the product specific documentation on the Avaya Support website at http://support.avaya.com.

Change History

Issue	Date	Summary of changes
10	March 2026	Added the section: Changes to platform support on page 7
9	February 2026	Updated the following section: • Deploying Communication Manager Software-only ISO using the OS console on page 41
8	August 2026	Upfated the following section: • Unsupported features of Avaya Aura application on Infrastructure as a Service on page 17
7	April 2025	Updated the following sections for R10.2.1.1: • Viewing the license status on page 79 • License Status field descriptions on page 81
6	February 2025	Updated the following sections: • Configuring load balancer on Microsoft Azure on page 71. • Connection types for Infrastructure as a Service on page 15.
5	January 2025	Update the following sections for Release 10.2.1: • Appendix C: List of required RPMs on RHEL 8.4 on page 107 • Appendix D: List of required RPMs on RHEL 8.10 on page 121 • Supported footprints of Communication Manager ISO on Infrastructure as a Service on page 23
4	December 2024	Added the following chapters and sections for Release 10.2.1: • Appendix D: List of required RPMs on RHEL 8.10 on page 121 • Appendix G: Creating RHEL virtual machine on Nutanix - Uploading the RHEL ISO to Nutanix server on page 133 - Installing RHEL on the Nutanix server on page 134 Updated the following sections for Release 10.2.1: • Third-party software requirements on page 20 • Supported Red Hat Enterprise Linux operating system versions for Software-only Environment on page 21 • Site preparation checklist on page 25 • Creating RHEL instance on Microsoft Azure on page 31 • Adding a software-only platform on page 45 • Supported platforms on page 12 • Disk partitioning on page 40

Table continues…

Issue	Date	Summary of changes
3	May 2024	Updated the following sections: • Software-only environment overview • Avaya Aura® Software-Only environment RPMs • Creating RHEL instance on Amazon Web Services • Creating RHEL instance on Microsoft Azure • Creating RHEL instance on Google Cloud Platform • Appendix C: List of required RPMs
2	April 2024	Updated the following sections: • Supported footprints of Communication Manager Software-only ISO image for on-premise • Supported footprints of Communication Manager ISO on Infrastructure as a Service • Deploying Communication Manager Software-only ISO using the OS console
1	December 2023	Release 10.2.x

Chapter 2: Overview

Software-only environment overview

In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Customers and/or Service Providers must procure a server or virtual machine that meets the recommended hardware requirements and the appropriate version of Red Hat Enterprise Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

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

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

For information about RPM updates for the Red Hat Enterprise Linux operating system and required changes to operating system files on Software only installation, see *Avaya Aura® Software Only White paper* on the Avaya Support website.

With Release 10.1 and later, there are no separate Kernel Service Packs (KSP), and Linux Security Update (LSU).

Supported platforms

You can deploy the Avaya Aura® application software-only *ISO image* on the following:

- On-premise platforms:
  - VMware
  - Kernel-based Virtual Machine (KVM)
  - Hyper-V
  - Nutanix 6.5 and later
- Cloud platforms:
  - Amazon Web Services
  - Google Cloud Platform
  - Microsoft Azure
  - IBM Cloud for VMware Solutions

    Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

    For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Linux users and system file changes

The Communication Manager software-only installer creates Linux users and groups, and removes other users and groups. The installer removes other users and groups to avoid conflicts with Linux users and groups ID in the customer provided operating system. For more information, see Users and groups on page 94.

Communication Manager software-only installer makes modification to system configuration files. For the list of files that are modified, see System configuration file changes on page 96.

Infrastructure as a Service environment overview

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services

  Note:

  With Release 10.1.x and later, Avaya Aura® will no longer have the Amazon Web Services OVA. Deployment on Amazon Web Services is supported through the software only offer.
- Microsoft Azure

- Google Cloud Platform
- IBM Cloud for VMware Solutions

  For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

The Infrastructure as a Service environment supports the following offers:

Offer	Supported environments
ISO	Simplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions Duplex • Amazon Web Services • Microsoft Azure • Google Cloud Platform • IBM Cloud for VMware Solutions

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.
- Allows you to stay current with latest security updates provided by the service provider.

You can connect the following applications to the Avaya Aura® IaaS instances from the customer premises:

- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway and G450 Branch Gateway

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

Avaya Communication Manager Security Service Packs (SSP) can be incompatible or fail to install on a customer controlled operating system.

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

Related links

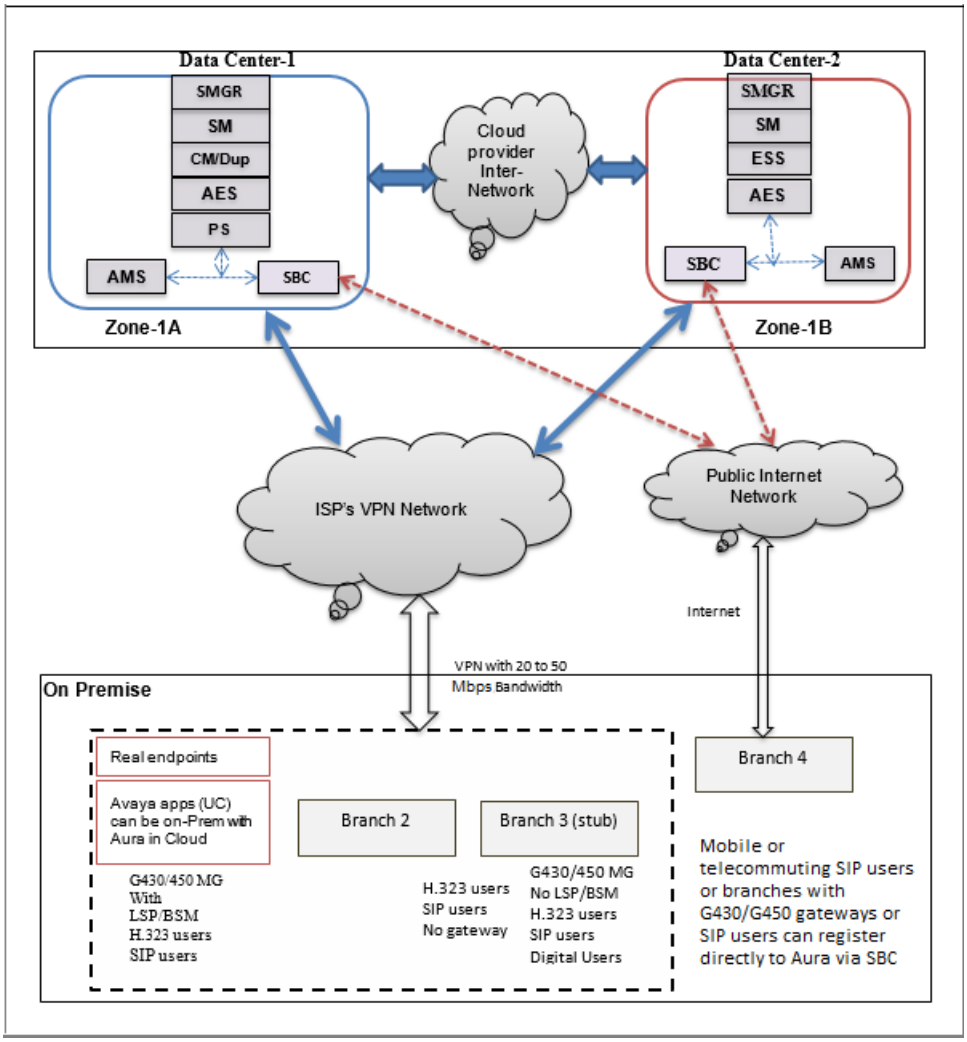
Topology on page 14
Connection types for Infrastructure as a Service on page 15
Networking considerations on page 16
Unsupported features of Avaya Aura application on Infrastructure as a Service on page 17

Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.

Important:

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.



Related links

Infrastructure as a Service environment overview on page 12

Connection types for Infrastructure as a Service

Amazon Web Services

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

Connection type	Resource
VPN connection	For more information, go to AWS documentation and search for “VPN connections”.
Direct connection	For more information, see AWS documentation section and search for “Direct connection”.

Microsoft Azure

You can connect applications in a hybrid network on the Virtual Networks (VNet) in the following ways:

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

Google Cloud Platform

You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

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

Related links

Infrastructure as a Service environment overview on page 12

Networking considerations

When you deploy an Avaya application at main location or at a branch location on Infrastructure as a Service, ensure that you follow the networking requirements, such as, the WAN network topology, bandwidth and latency of the Avaya applications. You must adhere to the Avaya network recommendations and Infrastructure as a Service networking rules.

Infrastructure as a Service has some limitations for establishing public internet VPNs and direct connections.

For more information about Amazon VPC Limits, refer to the Amazon Web Services documentation and search for relevant term.

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

Important:

Avaya recommends the use of direct connection in combination of a private WAN connection with Service Level Agreement that measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between Infrastructure as a Service and customer premises.

Related links

Infrastructure as a Service environment overview on page 12

Unsupported features of Avaya Aura® application on Infrastructure as a Service

The following features are unsupported on the Software-Only Environment.

For more information on Out of Band Management (OOBM) feature support matrix for Avaya Aura® components, refer to section Out of Band Management Support Matrix for Avaya Aura Components on page 17.

Amazon Web Services

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Network configuration changes, such as, IP Address, Gateway, and FQDN using the SMI. These must match the virtual network configuration and cannot be changed.
- NAT in the IP link is not supported for H.323 Stations on Communication Manager.

Microsoft Azure

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Network configuration changes, such as, IP Address, Gateway, and FQDN. NAT in the IP link is not supported for H.323 Stations on Communication Manager.

Google Cloud Platform

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

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Network configuration changes, such as, IP Address, Gateway, and FQDN. NAT in the IP link is not supported for H.323 Stations on Communication Manager.

Out of Band Management Support Matrix for Avaya Aura® Components

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

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

Related links

Infrastructure as a Service environment overview on page 12

Chapter 3: Planning and preconfiguration

Downloading software from PLDS

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

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

Note:

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

Procedure

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

Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

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

Software details of Communication Manager

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

Latest software updates and patch information

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

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

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

Third-party software requirements

You can deploy the Avaya Aura® application ISO file on a Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 virtual machine by using the operating system command line interface or by using Solution Deployment Manager.

Note:

Ensure that the Communication Manager is the only application running on the virtual machine. Also, you can add third party applications like antivirus, monitoring, and backup to the same virtual machine as long as the application is on the list of approved applications.

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

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

Red Hat Enterprise Linux operating system	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
Linux operating system Release 7.4 with 64-bit			
Linux operating system Release 7.6 with 64-bit	Y		
Linux operating system Release 8.4 with 64-bit		Y	Y
Linux operating system Release 8.10 with 64 bit			Y

Supported browsers

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

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

Note:

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

Related links

Accessing Communication Manager System Management Interface on page 78

Configuration tools and utilities

To deploy Avaya Aura® ISO image and to configure the application, you need the following tools and utilities:

- PuTTY and WinSCP
- Solution Deployment Manager Client

Supported footprints for Software-Only ISO image

Supported footprints of Communication Manager Software-only ISO image for on-premise

These footprint values are applicable for Software-Only deployments on:

- VMware
- KVM
- Hyper-v
- Nutanix 6.5 +

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

Note:

The partitions size can be larger than the values listed in the following table.

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

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

Configuration	Profile (max users)	CPUs	CPU Reservation (MHz)	Minimum CPU Speed (MHz)	Memory (MiB)	Number of Ethernet NICs (OOB optional)	Minimum Disk size (GiB)
Communication Manager Simplex	Large (41000)	2	4340	2170	4608	2 - procr (eth0), OOB (eth1)	64
	Medium (2400)	2	4340	2170	4096	2 - procr (eth0), OOB (eth1)	64
	Small Main (1000)	2	3900	1950	3585	2 - procr (eth0), OOB (eth1)	64
	Small Survivable (1000)	1	1950	1950	4096	2 - procr (eth0), OOB (eth1)	64
Communication Manager Duplex	Duplex High (41000)	3	7650	2550	5120	3 - procr (eth0), dup link (eth1), OOB (eth2)	64
	Duplex Standard (30000)	3	6510	2170	5120	3 - procr (eth0), dup link (eth1), OOB (eth2)	64

Supported footprints of Communication Manager ISO on Infrastructure as a Service

Here are supported footprints of Communication Manager ISO on:

- Amazon Web Services (AWS)
- Microsoft Azure (Azure)
- Google Cloud Platform (GCP)

Note:

Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

For IBM Cloud for VMware Solutions, instance type is not applicable.

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

Note:

The partitions size can be larger than the values listed in the following table.

Footprints		Configuration					
		Communication Manager Simplex				Communication Manager Duplex	
		Large	Medium	Small Main	Small Survivable	Duplex High	Duplex Standard
Profile (max users)		41000	2400	1000	1000	41000	30000
CPUs		2	2	2	1	3	3
Min CPU Speed (MHz)		2170	2170	1950	1950	2550	2170
Memory (MiB)		4608	4096	3585	4096	5120	
Number of Ethernet NICs		1 - procr (eth0)				2 - procr (eth0), dup link (eth1)	
Min Disk size (GiB)	AWS / GCP	64				64	
	Azure	80				80	
Azure ISO instance type		• Standard D4as v4 (4 vCPUs, 16-GiB memory) • Standard B2ms (2 vCPUs, 8-GiB memory)			Standard DS1 v2 (1 vCPU, 3.5-GiB memory)	Standard D4as v4 (4 vCPUs, 16-GiB memory)	
AWS ISO instance type		• m4.large • m5.large • m5a.large • C5.large • C5a.large				• m4.xlarge • m5.xlarge • m5a.xlarge • C5.xlarge • C5a.xlarge	
GCP ISO instance type		• E2-custom-2- 5120 (2 vCPUs, 5-GiB memory) • E2-standard-4 (4 vCPUs, 16-GiB memory)				• E2-custom-4 (4 vCPUs, 16-GB memory) • N2-custom-4 (4 vCPUs, 16-GB memory)	

Note:

In Microsoft Azure, you must provide an additional 16 GiB of disk space as the Communication Manager does not fully utilize the existing `/usr` partition, and the installer also ignores the `/usr` partition.

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

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

Preconfiguration in Software-Only

Planning checklist

Before creating a virtual machine and installing the operating system, you must perform the following:

No.	Task	Description/Notes	✔
1	Download and install the virtualization software and the operating system. **Note:** The operating system needs to be configured to meet the application's requirement.	Ensure that the virtual environment with required operating system is installed and is available for software-only deployment.	
2	Download the ISO.	**Note:** For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at https://support.avaya.com/.	
3	Install the required third-party software.		
4	Purchase and obtain the required licenses.	Downloading software from PLDS on page 19	
5	Register for PLDS and activate license entitlements.	Downloading software from PLDS on page 19	
6	Prepare the site.	Site preparation checklist on page 25	

Site preparation checklist

Use the following checklist to know the set up required to deploy the application ISO file in the software-only environment:

No.	Task	Description	✔
1	Create a virtual machine on the supported virtualized environment.	See the corresponding virtualized environment documentation.	
2	Subscribe to Red Hat network.		
3	Install the Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 with **Minimal Install** for the Software-Only deployment.	See Red Hat documentation.	
4	Configure Yum.	See Configuring Yum on RHEL on page 38	

Preconfiguration in Infrastructure as a Service

Preconfiguration for deploying ISO on Amazon Web Services

Checklist for deploying ISO on Amazon Web Services

Ensure that you complete the following before deploying Avaya Aura® Communication Manager ISO on Amazon Web Services.

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 19.	
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Ensure that you have the required resources.	See Disk partitioning on page 40	

Table continues…

No.	Task	Link/Notes	✔
5	Create an RHEL instance.	See Creating RHEL instance on Amazon Web Services on page 27	
6	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services on page 30	
7	Configure Yum.	See Configuring Yum on RHEL on page 38	

Creating RHEL instance on Amazon Web Services

About this task

Use this procedure to create RHEL virtual machine on Amazon Web Services.

Note:

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

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Also, note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Amazon Web Services documentation.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Compute** > **EC2**.

   The system displays the EC2 Management Console page.
3. Click **Launch an Instance**.
4. Under **Name and tags**, for Name, enter a descriptive name for your instance.

   Note:

   Remember the name entered for the tag. The name entered for the tag is used to identify the RHEL instance after the instance is created.
5. Under **Application and OS Images (Amazon Machine Image)**, search for the supported RHEL version in **Community AMIs**, and click **Select**.

   For the supported RHEL version, see “Third party software requirements” section.
6. Under **Instance type**, select the instance type according to your required footprints.

   For more information, see “Supported footprints of Communication Manager ISO on Amazon Web Services”.

Note:

Do the following configuration on Amazon Web Services platform only.

- For Simplex Communication Manager, do the following:
  a. In the **Network** field, click a VPC network.
  b. In the **Subnet** field, select the appropriate subnet.
  c. In the **Network Interfaces** section, assign an IP address.

     This IP address must be in the subnet.
- For Duplex Communication Manager, do the following:
  a. In the **Network** field, click a VPC network.
  b. In the **Subnet** field, select the appropriate subnet.
  c. Select the **Add instance to placement group** check box.

     Note:

     If you have an existing placement group, select **Add to existing placement group** option and select the placement group which you already created.

     To add a new placement group, do the following:

     a. Select **Add to a new placement group** option.
     b. In the **Name** field, enter the name of the placement group.
     c. Under **Placement Strategy**, choose the **Spread** option.
     d. Click **Create group** button.

     Note:

     Duplex deployment of Communication Manager for shared placement group is available for both ISO and OVA deployment types.

     If there is an existing system with a dedicated host and you want to have a shared placement group instance, follow the given steps to retain all the existing users and configurations:

     - Create a backup of the existing Communication Manager. For more information on creating a backup, see “Creating a backup” in *Upgrading Avaya Aura® Communication Manager*.
     - Delete all the existing duplex Communication Manager instances from your system.
     - Deploy Communication Manager and create a new Communication Manager instance in the Shared Placement group with the same IP. For more information about shared placement, please refer to chapter 5 “Deploying” in this guide.

- Restore the full backup created of the existing Communication Manager. For more information on restoring a backup, see “Restoring backup” in *Upgrading Avaya Aura® Communication Manager*.
- Generate a CSR certificate signed with CA and install it in the Communication Manager. For more information on generating a CSR, see “Generating a CSR” in *Administering Avaya Aura® Communication Manager*.

d. In the **IAM role** field, add role with policy **AmazonEC2FullAccess**.

Note:

Communication Manager only uses the capabilities of **AssignPrivateIpAddress** and **UnassignPrivateIpAddress** for the EC2 instances. The customer may want to create a more restrictive IAM policy than what is provided by the EC2FullAccess policy for these EC2 instances.

e. In the **Network Interfaces** section, for DuplexCM1, do the following:

a. In the **Primary IP** field of eth0, assign an IP address in the subnet.

b. In the **Secondary IP addresses** field of eth0, assign an IP address in the subnet.

Note:

The secondary IP address is the alias/floating IP address that moves from one server to another during the interchange.

c. Add an additional network interface eth1, and assign an IP address in a different network than the Secondary IP address.

f. In the **Network Interfaces** section, for DuplexCM2, do the following:

a. In the **Primary IP** field of eth0, assign an IP address in the subnet.

b. Add an additional network interface eth1, and assign an IP address in a different network than the Secondary IP address.

7. Under **Key pair (login)**, select an existing key pair or create a new key pair dialog box using the following options:
   - **Choose an existing key pair**.
   - **Create a new key pair**.
8. If you select the **Choose an existing key pair** option, from the **Select a key pair** drop-down list, and select a key pair.
9. If you select the **Create a new key pair** option, perform the following:
   a. In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
   b. Click **Create key pair**. The key pair will automatically download to the system after clicking on **Create key pair**.

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

Note:

You will not be able to download the file again.

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

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

11. Click **Configure storage**.

    Ensure that the hard disk size must be minimum 64 GiB. For more information, see Disk partitioning on page 40.

    The partitions size can be larger than the value specified.

12. Review the details of each configuration in the **Summary** panel.
13. Click **Launch Instances**.

    The system creates the RHEL instance.

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

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

Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Amazon Web Services

Create a ppk file

Procedure

1. Open WinSCP.
2. From the advance section, choose the authentication and browse to the .ppk file, and click login.
3. Enter the login credentials.
4. Upload the .iso to the virtual machine instance by using the IP address of the virtual machine.

Preconfiguration for deploying ISO on Microsoft Azure

Checklist for deploying ISO on Microsoft Azure

Ensure that you complete the following before deploying Avaya Aura® Communication Manager ISO on Microsoft Azure.

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 19.	
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Ensure that you have the required resources.	See Disk partitioning on page 40	
5	Create an RHEL instance.	See Creating RHEL instance on Microsoft Azure on page 31	
6	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure on page 34	
7	Configure Yum.	See Configuring Yum on RHEL on page 38	

Creating RHEL instance on Microsoft Azure

Before you begin

Create an account on Microsoft Azure.

Do the following in Microsoft Azure environment:

- Create a resource group.

  You must provide the same resource group while creating any resource in Microsoft Azure.
- Create a storage account.

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

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

    For more information, see Microsoft Azure documentation and search for relevant terms.
  - Create a Network Security group and ensure that the ports are open as per the port matrix guide of respective product.
  - Optionally, create an availability set. A pair of VM under availability set shares different hardware and power resources.
  - While deploying Duplex Communication Manager, it would be good to have both the Communication Managers in different Hardware Server.
  - Create a customized RHEL virtual machine in your environment and convert it into vhd image.

    For more information about disk partitions and size, see Disk partitioning on page 40.

    For more information about creating virtual machines and uploading them to Azure, see Microsoft Azure documentation.
  - Upload the RHEL customized instance to Microsoft Azure and use the same to create a new instance.

    While creating a virtual machine for Communication Manager, select appropriate size according to the Communication Managers footprint and HA configuration. See *Avaya Aura® Communication Manager Hardware Description and Reference* guide and refer to the Microsoft Azure website to select appropriate size.
  - If you want to deploy Communication Manager Duplex, then your virtual machine must have two different interfaces. At the time of launching the virtual machine, you must assign an interface from the subnet created for main network. Once your virtual machine is launched, stop the virtual machine and attach interface from the subnet created for duplication link.

Important:

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

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

Please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Microsoft Azure documentation.

Procedure

1. Log on to the Azure portal.
2. In the search box, type virtual machine, and click **Virtual machines**.
3. On the Virtual machines page, click on the **+ Create** link and select **+ Virtual machine**.

   The system displays the Create a virtual machine page.
4. In the **Basics** tab, do the following:
   a. In **Project details**, select the **Resource group**.
   b. In **Instance details**, provide the **Virtual machine name** and select the **Region**.
   c. In **Image**, select **Red Hat Enterprise Linux 8.4 or Red Hat Enterprise Linux 8.10** from the images list.
   d. In **Size**, select the required details.

      Select appropriate size according to the Communication Manager footprint and HA configuration

      See *Avaya Aura® Communication Manager Hardware Description and Reference* guide, and also refer to the Microsoft Azure website to select appropriate size.
   e. From **Administrator account**, in **Authentication type**, select **Password**, and enter the required credentials.

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

      Caution:

      Do not use temporary disk for application configuration. It might lead to loss of data.
   b. In **Data disks for 'undefined'**, click **Create and attach a new disk**.
   c. On Create a new disk page, click **Change size** and select **55 GiB** from the list.
   d. Click **OK**.

      A new disk of size 55 GiB is created.
   e. Click **Next: Networking**.
6. In the **Networking** tab, from **Network interface** select the required **Virtual network**, **Subnet**, and **Public inbound ports**.

Select other fields on that page, if required.

7. In the **Management**, **Advanced**, and **Tags** tabs, fill the details, if required.
8. In the **Review + create** tab, review the details and click **Create**.

   The deployment begins. Wait till the deployment is complete.

Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure

Before you begin

Create RHEL virtual machine instance on Microsoft Azure.

Procedure

1. Open WinSCP session with your RHEL machine on Microsoft Azure by using the user ID and password that you provided at the time of creating the virtual machine.
2. From the advance section, choose the authentication and browse to the .ppk file, and click **login**.
3. Enter the login credentials.
4. Upload the .iso file to the virtual machine instance.

Preconfiguration for deploying ISO on Google Cloud Platform

Checklist for deploying ISO on Google Cloud Platform

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

No.	Task	Link/Notes	✔
1	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
2	Download the required software.	See Downloading software from PLDS on page 19.	

Table continues…

No.	Task	Link/Notes	✔
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	
4	Create a PPK file.	See Creating a PPK file on page 35	
5	Ensure that you have the required resources.	See Disk partitioning on page 40	
6	Create an RHEL instance.	See Creating RHEL instance on Google Cloud Platform on page 35	
7	Copy the ISO to the RHEL instance.	See Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform on page 37	
8	Configure Yum.	See Configuring Yum on RHEL on page 38	

Creating a PPK file

Procedure

1. Open puttygen file, and click **Load**.
2. Under the **Parameters** section, select SSH-2 RSA.
3. Under **Actions** section, click **Generate**.

   You will be instructed to move the mouse cursor around within the PuTTY Key Generator window as a randomizer to generate the private key.
4. Enter a value in the **Key passphrase** and enter the same value in the **Confirm passphrase** field to protect the private key.
5. Click **Save private key**, and save the file to your local computer.
6. The box under **Public key for pasting into OpenSSH authorized_keys file:** contains the public key.
7. Copy the public key.
8. Open a text editor and paste the public key into the text editor and save the file.

Creating RHEL instance on Google Cloud Platform

Before you begin

- Create an account on the Google Cloud Platform

- Create a ppk file.

Important:

Installing only the required RPMs to the system for security and stability. Do not install a complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

Please note that the steps provided in this section are for reference. For the most up-to-date information, see the Google Cloud Platform documentation.

Procedure

1. Log on to the Google Cloud Platform.
2. Go to **Compute Engine** > **VM Instances**.
3. On the VM Instances page, click **CREATE INSTANCE**
4. On the **Create an instance** page, update the following fields:
   a. In **Name**, enter your product name.

      For example, cm-simplex-10.1.
   b. In **Region**, select the required region.
   c. In **Zone**, select the required zone.
   d. Under **Machine configuration**, in **Series**, select **E2**.
5. Under the **Boot disk** section, click **Change** and do the following:
   a. Select the appropriate RHEL image. For the supported RHEL version, see the “Third party software requirements” section.
   b. In **Size (GiB)**, enter the required disk size and click **Select**.
6. Do the following configuration on Google Cloud Platform:
   - For Simplex Communication Manager, do the following:
     a. Navigate to **Advanced Options** > **Networking** > **Networking interfaces**.
     b. In the **Network** field, select the VPC1 network.
     c. In the **Subnetwork** field, select the required subnet.
     d. In the **Primary Internal IP** field, select Ephemeral Custom.
     e. In the **Custom ephemeral IP address** field, enter an IP address that is within the range of your subnet as mentioned in 6.c on page 36.
     f. In the **External IP** field, select None.

- For Duplex Communication Manager, do the following:
    a. Navigate to **Advanced Options** > **Networking** > **Networking interfaces**.
    b. In the **Network** field, select the VPC1 network which shall be used for management and signaling.
    c. In the **Subnetwork** field, select the required subnet.
    d. In the **Primary Internal IP** field, select Ephemeral Custom.
    e. In the **Custom ephemeral IP address** field, enter an IP address that is within the range of your subnet as mentioned in 6.c on page 37.
    f. In the **External IP** field, select None.
    g. Click **Done**.
    h. In the **Network** field, select the VPC2 network which shall be used for duplex link.
    i. In the **Subnetwork** field, select the required subnet.
    j. In the **Primary Internal IP** field, select Ephemeral Custom.
    k. In the **Custom ephemeral IP address** field, enter an IP address that is within the range of your subnet as mentioned in 6.i on page 37.
    l. In the **External IP** field, select None.

7. Click **Done**.
8. Click **Security**.
9. Click **Create**.

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

Next steps

Uploading the ISO to the RHEL virtual machine instance.

Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Google Cloud Platform.

Reuse the PPK file that was created earlier.

Procedure

1. Open WinSCP and enter the login credentials.
2. Click **Advanced**, and select **Advanced**.
3. In the left pane of the Advanced Site Settings window, click **Authentication**.

4. In the right pane, click the browse icon under the **Private key file** field and browse to the .ppk file.
5. Click **OK**, and click **Login**.
6. Upload the .iso to the virtual machine instance.

Configuring Yum on RHEL

Before you begin

- Converting the *.pem file to the *.ppk format.
- Configuring PuTTY for an SSH session.
- Find the SSH user name of the instance you deployed.

For more information, see “Appendix”.

Procedure

1. Log on to the RHEL virtual machine using SSH.

   Use the SSH user name to log on.
2. Switch to root user by using the following command: `sudo su`
3. Check if the BaseOS and AppStream repos are enabled.

   ```
   Repo ID:rhel-8-for-x86_64-baseos-rpms
   Repo Name:Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)
   Repo URL:https://cdn.redhat.com/content/dist/rhel8/$releasever/x86_64/baseos/os
   Enabled: 1
   ```

   and

   ```
   Repo ID:rhel-8-for-x86_64-appstream-rpms
   Repo Name:Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)
   Repo URL:https://cdn.redhat.com/content/dist/rhel8/$releasever/x86_64/appstream/os
   Enabled:1
   ```
4. Enable the CodeReady Builder repository:

   ```
   subscription-manager repos --enable codeready-builder-for-rhel-8-x86_64-rpms
   ```
5. Install the EPEL repository:

   ```
   dnf install: https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-8.noarch.rpm
   ```

Validating the installer ISO file

About this task

Use this procedure to validate the Avaya Aura® application installer ISO, which is signed using Avaya File Signing Authority (AFSA). For a software-only installation, you must validate the ISO manually.

Procedure

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

```
mkdir /mnt/iso
mount -o loop,ro CM*.iso /mnt/iso
```

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

```
openssl verify -CAfile AvayaRootCert.pem /mnt/iso/CM-010.2*.cert
```

This command should return OK.

Note:

To create the file AvayaRootCert.pem, use the file present in the Appendix E of this document.

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

```
openssl x509 -in /mnt/iso/CM-010.2*.cert -pubkey -noout > /tmp/key
```

4. Run the following command to validate manifest files:

```
cd /mnt/iso
sha256sum -c CM-010.2*.mf
```

After you run the command, an output of OK indicates that all the files are correct.

5. Run the following command to verify the signature of the manifest file:

```
openssl dgst -sha256 -verify /tmp/key -signature CM-010*1.sig CM-010*.mf
```

This command should return Verified OK.

Chapter 4: Deloying Communication Manager Software-Only image using Operating System console

Disk partitioning

You can use a single disk or multiple disks for your virtual machine. The total capacity must be at least 64 GiB.

Note:

The partitions size can be larger than the values listed in the following table.

If you are planning to use an antivirus or another approved third-party application, you must add the disk space required by the third-party application to the values in the following table.

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

Note:

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

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

Partition	Size
/	7.7 GiB
/etc/opt/defty	5 GiB
/boot	790 MiB
/boot/efi	540 MiB
/home	5 GiB
/var/log/audit	5 GiB
/tmp	5 GiB
/var	10 GiB

Table continues…

Partition	Size
/var/log	20 GiB
swap	5 GiB

Note:

- Communication Manager does not support a separate partition for `/opt`. In the early boot stages, only the root partition '/' is mounted and the Communication Manager code in `/opt` must be available as a sub-directory of root.
- The installer accepts smaller sizes boot partitions.
- If a partition is not present then, the parent partition must be larger to include the size of the child partition.

  For example, if `/var/log/audit` is not present then, `/var/log` must be 25 GiB. If neither `/var/log/audit` nor `/var/log` are present then, `/var` must be 35 GiB.
- If the virtual machine has partitions not listed in the above table, for example, `/usr` or`/local`, in that case, when determining the disk size, you must add the size of those partitions in addition to the 64 GiB that the Communication Manager requires.
- When you configure partitions sizes manually in the Red Had installer, use GiB and MiB units for binary with base 1024.

Deploying Communication Manager Software-only ISO using the OS console

About this task

Use this procedure to deploy Communication Manager ISO image in a Software-only environment.

Note:

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

Before you begin

- Create an operating system instance.
- Ensure that you have the required hard disk space on the RHEL machine. For more information, see the “Disk partitioning” section.
- Ensure that the RHEL instance should be able to communicate with a public RHEL repo or your private repo for the latest RPM updates.
- Ensure that the Linux installation uses 'eth <x> names for the network interfaces.

- The virtual machines must support at least 2 network interfaces for duplex configurations. On Azure 'accelerated networking' interfaces should not be enabled.
- SSH to the RHEL virtual machine and create a root password.
- Download the Avaya Aura® application ISO file to the virtual machine.

Procedure

1. Switch to root user by using the following command: `sudo su`
2. Create the iso directory under the mnt folder.

   For example, `mkdir /mnt/iso`.
3. Run the following command to mount the ISO file:

   ```
   mount -o loop,ro CM-010.2.0.0.*.iso /mnt/iso
   ```

   Running this command extracts all the files from the Avaya Aura® ISO zip folder.
4. Run the following command to navigate to the iso file:

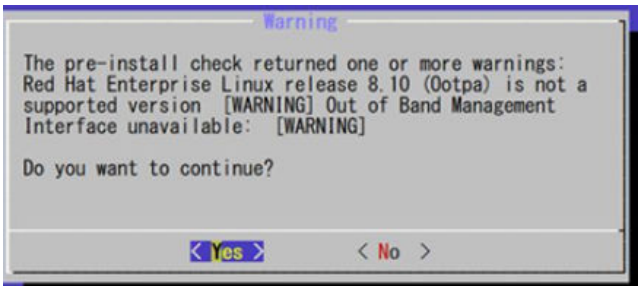
   ```
   cd /mnt/iso
   ```
5. To enable php 7.4 and nginx 1.20, run the following commands:
   a. `yum module reset -q -y php`
   b. `yum module enable -y php:7.4`
   c. `yum module reset -q -y nginx`
   d. `yum module enable -y nginx:1.20`
   e. `yum update -y php`
   f. `yum update -y nginx-filesystem*`
6. Run the following command to install the dependent RPMs:

   ```
   yum install --setopt=install_weak_deps=false -y /mnt/iso/avaya-cm-
   setup-010.2.*.noarch.rpm
   ```

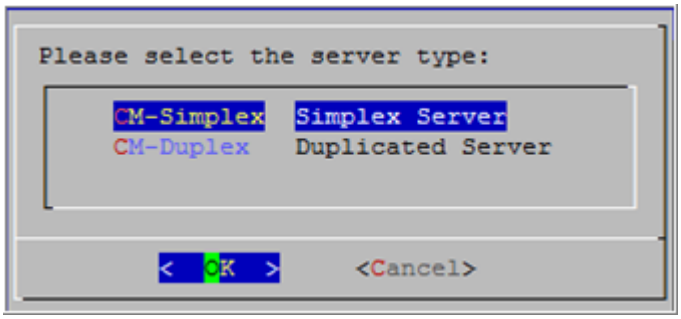
   A message appears that the RPMs installation is complete. To check the RHEL version, run the following command: `cat /etc/redhat-release`.
7. Run the `./install-cm` file to start the installation.

   Note:

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



8. Select the required server type as **Simplex Server** and click **OK**.



9. Select the required number of users and click **OK**.

   For more information on supported footprints, see Supported footprints information for respective environments.

10. If the Out of Band Management interface is not needed and missing, accept the Out of Band Management prompt and click **Yes**.
11. Press any key to read the EULA.
12. Read the software license terms and enter `y` to accept the agreement.
13. Read the system configuration details and click **Accept**.
14. Enter the following Avaya Aura® application details as prompts appear and click **OK**:
    - IPv4 address

      Note:

      IP addresses should be left as is since the IP addresses must match with that configured on the Cloud virtual networks. Also, IPv6 addresses are not supported in cloud virtual networks. Leave the IPv6 fields blank.

    - IPv4 netmask
    - IPv4 gateway
    - IPv6 address (Optional)
    - IPv6 network prefix (Optional)
    - IPv6 gateway (Optional)

- Hostname
- NTP servers IP address or hostnames (Optional)
- DNS servers IP address (Optional)
- Domain search list (Optional)
- WebLM server IP address on which the Avaya Aura® application license is installed, and it *MUST* be reachable.
- Privileged Administrator login user ID
- Password for the administrator login user

15. In the Enhanced Access Security Gateway (EASG) screen, click **Enable** or **Disable**.
16. Verify the Avaya Aura® application details that you have entered and click **Next**.
17. In the Warning screen, click **OK** to complete the installation and reboot the computer.

    CLI displays the status of the Avaya Aura® application installation and the server reboot.

    Note:

    If you want to restore Communication Manager data during backup and restore, disable **`waagent`** by using the `sudo systemctl stop waagent` command.

Duplex deployment

To deploy a Duplex Communication Manager, install using the same Duplex profile on two different hosts. Ensure that the hosts resides on two different clusters. The Duplex Communication Manager configuration requires an extra Ethernet port for duplication link. Therefore, the virtual machine should have at least two network connection type vSwitches. The first Ethernet port is used for all administration or call processing traffic and the second Ethernet port is used for the duplication link traffic.

Before you start the virtual machine, you must change the Communication Manager settings to configure the second NIC.

Note:

For the Communication Manager Duplex:

- If you are using a 2600 MHz (2.6 GHZ) processor, the Communication Manager supports 41000 endpoints.
- If you are using a 2200 MHz (2.2 GHZ) processor, the Communication Manager supports 30000 endpoints.

Chapter 5: Deploying Communication Manager ISO using Solution Deployment Manager

Adding a location

About this task

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

Procedure

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

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

Adding a software-only platform

About this task

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

Before you begin

Add a location.

Procedure

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

   For a software-only deployment, the username must have the permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

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

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

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

Deploying Communication Manager ISO using Solution Deployment Manager

About this task

Use this procedure to deploy the Avaya Aura® Communication Manager ISO.

Note:

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

Before you begin

- Create a Linux RHEL 8.4 or RHEL 8.10 instance.

- Ensure that the RHEL instance should be able to communicate with a public RHEL repo or your private repo for latest RPM updates.
- Ensure that the Linux installation uses 'eth <x> names for the network interfaces. The virtual machines must support at least 2 network interfaces for duplex configurations. On Azure 'accelerated networking' interfaces should not be enabled.
- SSH to the RHEL instance and create a root password.

  For example, you can set the password using the following command: **`passwd <root>`**
- Download the Avaya Aura® Communication Manager ISO file to the RHEL instance.
- Add an Operating System admin user and set a password on RHEL instance.

  For example, you can add a user using the following commands: **`adduser <username>`**, **`passwd <username>`**
- Add a location.
- Add a platform

Procedure

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

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

      The system displays the IP Address and FQDN of the platform in the **Platform IP** and **Platform FQDN** fields.
6. In the Provide admin and root Credentials section, do the following:
   a. In **Admin User of OS**, type the admin user name.
   b. In **Admin Password of OS**, type the admin user password.
   c. In **Root User of OS**, type the root user name.
   d. In **Root Password of OS**, type the root user password.
   e. **(Optional)** Click **Test Connection**.

      The system logs in to the platform by using the credentials to test the platform connectivity. If connectivity is established, the system displays the message: `Test Connection Successful`.
   f. Click **OK**.

7. Click **Next**.
8. To select the required application, on the **ISO** tab, click one of the following:
   - **SW Library** / **Select from software library**: Select the local library where the *ISO image* is available.

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

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

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

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

   If you do not provide the Communication Manager Release 10.2 bin file at the time of deploying the Communication Manager, the system displays the following message:

   ```
   Installation of the latest <application> patch is mandatory. Are
   you sure you want to skip the patch installation? If Yes, ensure to
   manually install the <application> patch later.
   ```
10. In **Flexi Footprint**, select the footprint size for the application.
11. In Test Your Operating System Compatibility Against Element Software Package, click **Test Environment Compatibility**.

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

    Note:

    If the browser hangs, the system provides the option to end the script or wait. Always click **Wait**.
12. **(Optional)** To view the installer compatibility results in a separate window, click **View Output**.

The system displays the Environment Check Output window.

13. Click **Next**.
14. On the Configuration Parameters page, provide all the information required.
15. Click **Deploy**.
16. On the EULA Acceptance window, click **Accept**.

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

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

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

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

Result

When you deploy the Communication Manager duplex pair through Solution Deployment Manager Application Management, Solution Deployment Manager creates the Active Communication Manager and Standby Communication Manager element entries using the IP Address or FQDN of the respective Communication Manager on the System Manager **Services** > **Inventory** > **Manage Elements** page. To perform the Communication Manager synchronization and other operations, you must edit the Active Communication Manager server entry as following:

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

Patch Installation or Patch Updates

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

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

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

Chapter 6: Configuration

Entering initial system translations

Before you begin

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

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

Procedure

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

Configuration and administration checklist

Use the following checklist to configure the Communication Manager.

#	Action	Link	✔
1	Configure the Communication Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 51	
2	Set up network configuration.	Administering network parameters on page 52	

Table continues…

#	Action	Link	✔
3	Apply the latest Communication Manager patch.	Patch Installation or Patch Updates on page 49	
4	Set the date and time.	Setting the date and time on page 52	
5	Configure the time zone.	Setting the time zone on page 53	
6	Set up the network time protocol.	Setting up the network time protocol on page 53	
7	Direct Communication Manager to the WebLM server.	Configuring the WebLM server on page 56	
8	Create a user account.	Adding an administrator account on page 54	

Configuring the virtual machine automatic startup settings on VMware

About this task

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

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

Before you begin

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

Procedure

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

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

Administering network parameters

Procedure

1. In the vSphere client, start the Communication Manager virtual machine console and log in as `privileged administrator for Communication Manager`.
2. On first attempt log in as `privileged administrator for Communication Manager`, you must type the following details according to the prompts:
   a. In the **IPv4 IP address** field, type the IP address.
   b. In the **IPv4 subnet mask** field, type the network mask IP address.
   c. In the **IPv4 Default Gateway address** field, type the default gateway IP address.
3. In the **Are these correct** field, verify the IP address details and type `y` to confirm the IP address details.
4. When the system prompts to create a customer privileged administrator account, enter the login details to create an account.
5. In the **Enable Avaya Services EASG Access**, enter:
   - `y` to enable EASG.
   - `n` to disable EASG.

   Note:

   By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.
6. To configure the additional network settings, log in to Communication Manager System Management Interface and navigate to **Administration** > **Server (Maintenance)** > **Network Configuration**.

   Note:

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

Setting the date and time

About this task

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

Procedure

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

Setting the time zone

Procedure

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

Note:

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

Setting up the network time protocol

About this task

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

Procedure

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

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

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

Adding an administrator account

About this task

When you deploy the Communication Manager using the bash or Solution Deployment Manager, perform the following procedure after the ISO deployment.

Note:

When you deploy the Communication Manager using bash or Solution Deployment Manager, the system prompts you to configure an administrator account. You can also use this procedure to add other administrator accounts.

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.

- **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 using the bash or Solution Deployment Manager, perform the following procedure after the ISO 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.
2. On the **Administration** menu, click **Licensing**.
3. In the left navigation pane, click **WebLM Configuration**.

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

   Note:

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

IPv6 configuration

Enabling IPv6

About this task

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

Procedure

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

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

Note:

Restart Communication Manager after enabling IPv6.

Disabling IPv6

About this task

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

Procedure

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

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

Note:

Restart Communication Manager after disabling IPv6.

Network port considerations

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

Related links

Accessing the port matrix document on page 90

Communication Manager virtual machine configuration

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

- Server Role: Indicate the type of virtual machine: main, survivable core, or survivable remote.
- Network configuration: Use to configure the IP-related settings for the virtual machine. On the Network Configuration page, the fields are prepopulated with data generated during the installation.

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

Related links

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

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

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

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

Important:

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

Related links

Communication Manager virtual machine configuration on page 57

Configuring Server Role

Procedure

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

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

   Note:

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

Related links

Communication Manager virtual machine configuration on page 57

Server Role field descriptions

Server Settings

Name	Description
This Server is	Specifies the role of the server. Select from the following roles: • **a main server:** For a primary virtual machine. • **an enterprise survivable server (ESS):** For a survivable core virtual machine. • **a local survivable server (LSP):** For a survivable remote virtual machine.

Table continues…

Name	Description
SID	Specifies the system ID. This ID must be the same for the main server and each survivable server. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form. System ID must be set to default value of 1.
MID	Specifies the module ID. The main server module ID must be 1 and the ID of the other server must be unique and 2 or more. For a survivable remote server, the MID must match the Cluster ID or MID for that server.

Configure Survivable Data

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

Configure Memory

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

Button	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes.

Table continues…

Button	Description
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 57

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.

Related links

Configuring load balancer on Microsoft Azure on page 71

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, the system displays additional fields. You can use the same values to duplicate the data on the second Communication Manager virtual machine.

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

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

   Note:

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

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

Network Configuration field descriptions

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

Table continues…

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

Button descriptions

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

Duplication parameters configuration

Duplication parameters

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

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

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

Configuring duplication parameters

Procedure

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

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

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

   For field descriptions, see the *Duplication Parameters field descriptions* section.

5. Add a duplicate server and fill in the required fields, such as host name and IP address.
6. Click **Change**.
7. Click **Restart CM**.

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

Duplication Parameters field descriptions

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

Table continues…

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

Button descriptions

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

Configuring duplex Communication Manager deployed on Amazon Web Services

Before you begin

You must install two Communication Manager instances for Duplex configuration, DuplexCM1 and DuplexCM2.

Procedure

1. Open an SSH session to the new Communication Manager system with the IP address that you provided in the **IP address** field on the Configure Instance Details page.
2. Log in with the user name as `configuser` and password as `configuser01`.

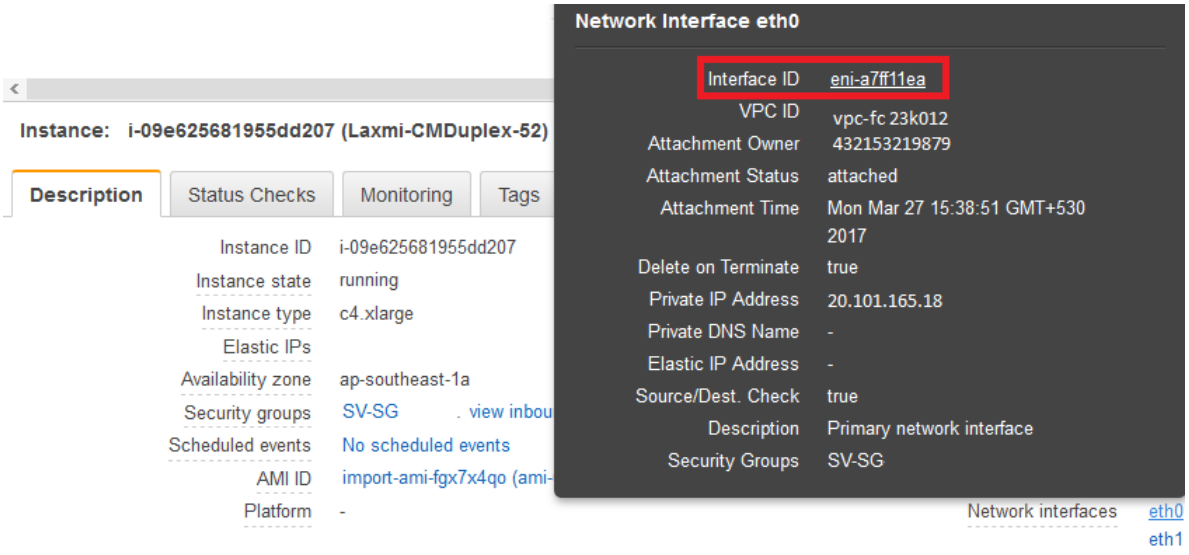
   Note:

   You must log in with `configuser` credentials when logging in for the first time. Once you log in, Communication Manager enables all other user logins and disables `configuser`.
3. In **Do you accept the terms of this EULA? (Y)es/(N)o**, type `y`.
4. In **Enter region of AWS**, type the region name.
5. In **Enter this VM network interface id mentioned on AWS EC2 console**, type the eth0 network interface ID of the Communication Manager DuplexCM1.

   Warning:

   The duplex Communication Manager instances require HTTPS access to Amazon EC2 APIs (ec2.<region>.amazonaws.com) to reconfigure the virtual IP address on interchange.

   In private VPC with no NAT or virtual private gateway, it is possible to use AWS Private Link in an interface VPC endpoint allowing private access to Amazon EC2 without the need of a NAT gateway. If the DNS cannot be configured to map ec2.<region>.amazonaws.com to the new interface VPC endpoint, then use the /etc/hosts file to associate the EC2 FQDN to the new VPC endpoint.



6. In **Enter other VM network interface id mentioned on AWS EC2 console**, type the eth0 network interface ID of the other Communication Manager DuplexCM2.

7. In **Enter the alias/floating ip**, type the floating IP address of the Duplex Communication Manager.

   The system configures the settings and then reboots automatically.
8. Log in with the user name as `craft` and password as `craft01`.
9. When the system prompts to create a customer privileged administrator account, enter the login details to create an account.

   From Communication Manager Release 7.1 onwards, during the initial configuration, 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.
10. 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.
11. After the configuration is complete, log in to the Communication Manager System Management Interface with the Communication Manager privileged administrator credentials.

Next steps

Perform the same procedure for the Communication Manager DuplexCM2. In this case, the values in Step 5 and Step 6 must be reversed.

Configuring duplex Communication Manager deployed on Microsoft Azure

Before you begin

1. You must install the Communication Manager instances Duplex CM1 and Duplex CM2 for Duplex configuration.
2. Keep the following information ready:
   - Three IP addresses for CM1, CM2, and Alias IP. Ensure that all IP addresses belong to the same network.
   - Two more IP addresses in a different network to communicate between duplex CM1 and duplex CM2.

Procedure

1. Log in to Duplex CM1 System Management Interface as a Privileged user.
2. Navigate to **Server Configuration** > **Network Configuration.**
3. On the Network Configuration page, do the following:
   a. In **CM1**, under **Server ID**, enter a number.

      Note:

      You should not enter the same number in CM2.

   b. In **eth0**, under **IP configuration**, enter the **IPv4 Address** and **Subnet Mask** of CM1. This is the same IP address that is used when deploying CM1.
   c. Under **Alias IP**, enter the IP address to access the Duplex Communication Manager.
   d. In **eth1**, enter the IP address that belongs to a different network.
4. Log in to Duplex CM2 System Management Interface as a Privileged user.
5. Navigate to **Server Configuration** > **Network Configuration.**
6. On the Network Configuration page, do the following:
   a. In CM2, under **Server ID**, enter a number.

      Note:

      You should not enter the same number that you entered in CM1.

   b. In **eth0**, under **IP configuration**, enter the IPv4 Address and Subnet Mask of CM2. This is the same IP address that is used when deploying CM2.
   c. Under **Alias IP**, enter the IP address to access the Duplex Communication Manager. The Alias IP must be the same in CM1 and CM2.
7. In **eth1**, enter the IP address that belongs to a different network. The IPv4 address you enter in **eth1** for CM2 must be different from the IPv4 address used in **eth1** in CM1.
8. Navigate to **Server Configuration** > **Duplication Parameters** page and do the following:
   a. For CM1 configuration, do the following steps:
      - In **Hostname**, enter the hostname of CM2.
      - In **Server ID**, enter the Server ID of CM2.
      - In **Corporate LAN/PE IP**, enter the IP address of CM2. This IP address is the same IP address used to deploy CM2.
      - In **Duplication IP**, enter the IP address that you entered in CM2 under the Network Configuration page in the **eth1 IP configuration** field.
      - In **IP address for PE health check**, enter the Gateway IP address. This IP address is the same for CM1 and CM2.

b. For CM2 configuration, do the following steps:

- In **Hostname**, enter the hostname of CM1.
- In **Server ID**, enter the Server ID of CM1.
- In **Corporate LAN/PE IP**, enter the IP address of CM1. This IP address is the same IP address that is used to deploy CM1.
- In **Duplication IP**, enter the IP address that you entered in CM1 under the Network Configuration page in the **eth1 IP configuration** field.
- In **IP address for PE health check**, enter the Gateway IP address. This IP address is the same for CM1 and CM2.

Related links

Configuring load balancer on Microsoft Azure on page 71

Configuring load balancer on Microsoft Azure

About this task

For duplex configuration on Microsoft Azure, you must configure load balancer.

Before you begin

Before installing load balancer, install duplex Communication Manager on respective virtual machines to be included in load balancer rule.

Note:

If you install duplex Communication Manager on virtual machines after installing the load balancer, the installation fails as Communication Manager installer cannot reach repository servers because of load balancer rule.

Procedure

1. Create a load balancer of Type=Internal and SKU=standard that has a static front-end IP address that matches the CM alias IP address.
2. Create a backend pool with the 2 Communication Manager virtual machine and use the eth0 IP address on each machine.
3. Create a TCP health probe using port 443 or 9968, use the minimum values of 5 seconds interval and 2 probes.

   Note:

   For the Communication Manager Duplex on AXP Private (Azure Cloud), use of load balancer for the eth0:0 alias IP address allocation requires the additional port 9968 to be opened in Communication Manager application.
4. Create a load balancing rule using the Front-end, back-end and probes defined above and select HA ports and Floating IP enabled.

Related links

Configuring duplex Communication Manager deployed on Microsoft Azure on page 69

Configuring Communication Manager deployed on Google Cloud Platform

About this task

From Release 10.1.0.2 onwards, Communication Manager supports duplex deployment on Google Cloud Platform.

Procedure

1. Create a health check.
2. Create an instance.
3. Configure load balancer on TCP, UDP, or both, as required.

Related links

[Creating a health check on Google Cloud Platform](#) on page 72
[Creating an instance group on Google Cloud Platform](#) on page 73
[Load balancer configuration on Google Cloud Platform](#) on page 73

Creating a health check on Google Cloud Platform

About this task

Google Cloud Platform enables you to create or select a health check when you complete the back-end configuration of the load balancer in the console. A Health check decides whether back-end configurations respond properly to traffic.

You can use the same health check for configuring the TCP and UDP load balancers.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Compute Engine** > **Health checks**.
3. Click **Create a health check**.
4. On the Create a health check page, provide the following information:

- **Name**: Name for the health check.
- **Description**: Description of the health check.
- **Scope**: Choose `Regional` and select **Region**.
- **Protocol**: Select `TCP`.
- **Port**: Enter `443`.
- **Check interval**: Define the duration from the start of one probe to the start of the next one as `1 second`.
- **Timeout**: Define the duration for which Google Cloud waits for a response to a probe as `1 second`.

- **Healthy threshold**: Define the duration that Google Cloud waits for a response to a probe as 2.
- **Unhealthy threshold**: Define the number of sequential probes that must fail for the VM instance to be considered unhealthy as 2.

5. Click **Create**.

Creating an instance group on Google Cloud Platform

About this task

An instance group is a group of virtual machine instances managed as a single entity.

For duplex Communication Manager, create two instance groups. Create one instance group for primary Communication Manager and the other for secondary Communication Manager.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Compute Engine** > **Instance Groups**.
3. Click **Create instance group**.
4. Click **New unmanaged instance group**.
5. On the Create instance group page, provide the following information:

- **Name**: Name of the instance group.
- **Zone**: Select the zone for the primary Communication Manager.
- **Region**: Select the region of your servers.
- **Network**: Select the network for your virtual machine.
- **Subnetwork**: Select the subnetwork for your virtual machine.
- **Select VMs**: Select the primary Communication Manager virtual machine from the list.

6. Click **Create**.
7. Repeat steps 1 to 5 to create another instance group. For **Zone** and **Select VMs** fields, select secondary Communication Manager.

Load balancer configuration on Google Cloud Platform

From Release 10.1.0.2 onwards, Communication Manager supports configuring the load balancer on the Google Cloud Platform.

TCP load balancer is used for the following:

- SIP solutions
- SSH access

UDP load balancer is used for the following:

- H.323 solutions

- SNMP browsing
- LSP/ESS

Related links

Configuring load balancer using TCP on Google Cloud Platform on page 74
Configuring load balancer using UDP on Google Cloud Platform on page 75

Configuring load balancer using TCP on Google Cloud Platform

Before you begin

- Create a health check, if it is not already created.
- Create an instance group, if it is not already created.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Network services** > **Load balancing** and click **Create load balancer**.
3. For **TCP Load Balancing**, click **Start configuration**.
4. For **Internet facing or internal only**, select **Only between my VMs**.
5. For **Multiple regions or single region**, select **Single region only** and click **Continue**.
6. For **Backend Services**, enter **Name** and **Region**.
7. For **Network**, select the required network from the list.
8. For **Backend configuration**, do the following:
    a. For new back-ends, choose the instance group that you added and click **Done**.
    b. Click **Add backend**.
    c. Choose another instance group that you added and select **Use this instance group as a failover group for backup**.
    d. Click **Done**.
    e. Select **Health check**.
    f. For **Drop traffic**, toggle on the **Enable (Drop new connections if no healthy VMs)** option.
    g. For **Connection draining on failover**, toggle off the **Enable connection draining on failover** option.
9. For **Frontend configuration,** do the following:
    a. Enter **Name**.
    b. Select **Subnetwork** from the list.
    c. From **Internal IP**, choose **Shared**.

    If you reserve your IP, choose **ephemeral Custom** and provide the reserved IP.

d. To create a new IP address, click **Reserve a static internal IP address**.

   Enter the **Name** and from the **Static IP address** drop-down list, select **Let me choose** to provide your IP address.

e. Click **Reserve**.

f. For **Ports**, do one of the following:

   - If you know the port numbers, select **Multiple** and enter comma-separated port numbers. For example, for SIP TLS signaling group, enter `5061`.
   - If you do not know the port numbers, select **All**.

g. Click **Done**.

10. Click **Create**.

Related links

Creating a health check on Google Cloud Platform on page 72
Creating an instance group on Google Cloud Platform on page 73

Configuring load balancer using UDP on Google Cloud Platform

Before you begin

- Create a health check, if it is not already created.
- Create an instance group, if it is not already created.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Network services** > **Load balancing** and click **Create load balancer**.
3. For **UDP Load Balancing**, click **Start configuration**.
4. For **Internet facing or internal only**, select **Only between my VMs** and click **Continue**.
5. For **Backend Services**, enter **Name** and **Region**.
6. For **Network**, select the required network from the list.
7. For **Backend configuration**, do the following:
   a. For new back-ends, choose the instance group that you added and click **Done**.
   b. Click **Add backend**.
   c. Choose another instance group that you added and select **Use this instance group as a failover group for backup**.
   d. Click **Done**.
   e. Select **Health check**.
   f. For **Drop traffic**, toggle on **Enable (Drop new connections if no healthy VMs)**.

8. For **Frontend configuration,** do the following:
    a. Enter **Name**.
    b. Select **Subnetwork** from the list.
    c. From **Internal IP**, choose **Shared** and select the IP address reserved for the TCP load balancer.
    d. For **Ports**, choose **Single** and enter the **Port number** as `443`.
    e. Click **Done**.
9. Click **Create**.

Related links

Creating a health check on Google Cloud Platform on page 72
Creating an instance group on Google Cloud Platform on page 73

Creating a Firewall rule on Google Cloud Platform

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **VPC network** > **Firewall** > **CREATE FIREWALL RULE**.
3. In the **Name** field, assign a name to the firewall rule.
4. In the **Network** field, select the network.
5. In the **Direction of traffic** field, select **ingress**.
6. In the **Action on Match** field, select **Allow**.
7. In the **Target tags** field, enter `allow-health-checksl`.
8. In the **Source IP4 ranges** field, enter `130.211.0.0/22` and `35.191.0.0/16`.
9. In the **Protocols and ports** field, select **TCP**, **UDP** and in the **Other protocols** field, enter `icmp`.
10. Click **Create**.

Adding Network tags for duplex Communication Manager on Google Cloud Platform

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Compute Engine** > **VM instances**.
3. Click the duplex Communication Manager instance.
4. Click **Edit**.
5. In the **Network tags** field, enter `allow-health-checks`.

6. Click **Save**.
7. Repeat Steps 3 to 6 for other duplex Communication Manager instances.

Chapter 7: Postinstallation verification

Installation tests

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

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

Note:

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

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

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

Verifying the license status

Accessing Communication Manager System Management Interface

About this task

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

Procedure

1. Open a compatible web browser.

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

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

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

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

   Note:

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

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

   Note:

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

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

Related links

Supported browsers on page 21

Viewing the license status

About this task

Use this procedure to view the Communication Manager license status.

Procedure

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

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

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

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

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

   Note:

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

   Note:

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

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

   - Normal mode
   - Normal mode (≤ 90 days of license expiration)
     - ```
       The Communication Manager license expires in 90 days.
       Contact Your Service Representative at the earliest to renew the license
       before the expiration date to avoid service disruption and daily late fee
       penalties.
       ```
   - Normal mode (≤ 60 days of license expiration)
     - ```
       The Communication Manager license expires in 60 days.
       Contact Your Service Representative at the earliest to renew the license
       before the expiration date.
       Failure to renew will result in the inability to make or receive phone calls
       in 90 days and incur daily late fees starting in 60 days.
       ```
   - License Error
     - ```
       System Administration and Call Processing Will Be Blocked in Approximately
       30 days.
       Contact Your Service Representative Immediately.
       ```
   - No License
     - ```
       System Administration and Call Processing Is Blocked.
       Contact Your Service Representative Immediately.
       ```

License Status field descriptions

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

Table continues…

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

Verifying the software version

Procedure

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

Verifying the 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

Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

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

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, remove, restore or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.
2. To enable EASG, do the following:
   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message:

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

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the
      ```

```
Avaya support site (https://support.avaya.com/ registration)
for additional information for registering products and
establishing remote access and alarming.
```

b. When the system prompts, type `yes`.

The system displays the message: `EASG Access is enabled`.

3. To disable EASG, do the following:

a. Run the command: **`EASGManage --disableEASG`**.

The system displays the following message:

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

b. When the system prompts, type `yes`.

The system displays the message: `EASG Access is disabled`.

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

Procedure

Log in to the application CLI interface.

EASG product certificate expiration

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

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

EASG site certificate

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

Managing site certificates

Before you begin

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

Procedure

1. Log in to the CLI interface as an administrator.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.

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

3. To view information about a particular certificate, run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates currently installed on the system.

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
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

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

Related links

Finding documents on the Avaya Support website on page 89
Accessing the port matrix document on page 90
Avaya Documentation Center navigation on page 90

Finding documents on the Avaya Support website

Procedure

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

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

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

Related links

Communication Manager documentation on page 87

Accessing the port matrix document

Procedure

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

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

Related links

Communication Manager documentation on page 87

Avaya Documentation Center navigation

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

Important:

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

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

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

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.

- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Related links

Communication Manager documentation on page 87

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
71201V	Integrating Avaya Aura® Core Components

Table continues…

Course code	Course title
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Users and groups

The Communication Manager installer requires certain Red Hat RPMs that may not be present on the server. Those rpms are listed as dependencies in the avaya-cm-setup- <version>.noarch.rpm file and may create users. For example the Apache webserver creates an Apache user and group. During the installation, the Communication Manager software-only installer also creates Linux users and groups, and removes others as listed below.

Users

The following users are added by the installer:

- acpsnmp:x:5783:555::/var/home/acpsnmp:/sbin/nologin
- csadmin:x:2000:555::/opt/avaya/common_services:/bin/bash
- <admin_user>:x:5784:555::/var/home/mimmi:/bin/bash

Note:

<admin_user> is an admin user that is created using the user configured login and password during the installation time.

Optionally, the following EASG users are added by the installer:

- craft:x:5780:555::/var/home/craft:/bin/bash
- init:x:5778:555::/var/home/init:/bin/bash
- inads:x:5779:555::/var/home/inads:/bin/bash
- rasaccess:x:5782:888::/var/home/rasaccess:/etc/ppp/ppp-login
- sroot:x:0:0::/var/home/sroot:/bin/bash

Note:

EASG users are used by Avaya Services. However, access to these users is managed by the customer.

To view the list of EASG users, run the following command: `/sbin/EASGManage –listUsers`

Username	Enabled	Locked
craft	Yes	No
init	Yes	No
inads	Yes	No

Table continues…

Username	Enabled	Locked
rasaccess	No	Yes
sroot	Yes	No

The following users are removed by the installer:

- lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
- sync:x:5:0:sync:/sbin:/bin/sync
- shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
- halt:x:7:0:halt:/sbin:/sbin/halt
- operator:x:11:0:operator:/root:/sbin/nologin
- games:x:12:100:games:/usr/games:/sbin/nologin

Groups

The following groups are added by the installer:

- susers:x:555:craft,acpsnmp,init,inads
- remote:x:888:rasaccess
- avcommonos:x:1000:init,inads,craft,rasaccess,<admin_user>
- CDR_User:x:10999:
- prof0:x:10000:init
- prof1:x:10001:inads
- prof2:x:10002:
- prof3:x:10003:craft
- prof17:x:10017:acpsnmp
- prof18:x:10018:<admin_user>
- prof19:x:10019:

The following group is removed by the installer:

- lp:x:7:

Appendix B: System configuration file changes

Communication Manager software only installer makes modification to the system configuration files. Change methods are as follows:

- Delta: Added to the existing file.
- Replace: Old file is replaced with a new file.
- User choice: Customer can choose for them or Avaya application to own.

The following table lists the files that are modified along with the reason for modification:

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/passwd /etc/group /etc/shadow /etc/gshadow	Delta	Add users and groups required by Communication Manager. Remove groups that are not required.	Yes	No	The SMI Web page **Administrator Accounts** allows the user to create or remove Communication Manager administrators. Communication Manager also creates Services accounts.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/snmp/snmpd.conf /var/lib/net-snmp/snmpd.conf /etc/snmp/snmptrapd.conf /var/lib/net-snmp/snmptrapd.conf	Delta	Administer SNMP communities (v1/v2c) and users (v3). Administer SNMP incoming traps.	Yes	No	The SMI Web interface allows the user to create or remove SNMP users. Also, allow configuration of the trap receiver, fault, and performance filters.
/etc/hosts	Delta	Entries are added for current host and duplicated server	Yes	No	The SMI Web interface allows configuration of host names.
/etc/hostname	Replace	Update hostname with the value configured during install.	Yes	No	The SMI Web interface allows configuration of host names.
/etc/aliases	Delta	Remove decode alias.	Yes	No	Security vulnerability.
/etc/sysconfig/network-scripts/route-eth<n>	Delta	Configuration of static routes.	Yes	No	The SMI Web page **Static Routes** allows configuration of static routes.
/etc/sysconfig/network-scripts/ifcfg-eth<0-2>	Delta	Configuration of the Ethernet interfaces IP addresses.	No	No	The SMI Web interface allows configuration of IP addresses. The files should not be changed.
/etc/chrony.conf	Replace	Configuration of NTP servers.	Yes	No	The SMI Web interface allows configuration of NTP servers.
/etc/systemd/system/multi-user.target.wants/chronyd.service remove /etc/ntp/drift	Replace	Enable NTP.	No	Yes	Enable NTP service.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/resolv.conf	Delta	Configure DNS and domain.	Yes	No	The SMI Web page **Network Configuration** and installation choices allows configuration of DNS, domain, search domain.
/etc/syconfig/network	Delta	Configure hostname and default gateways.	Yes	No	The SMI Web page **Login Account Policy** allows configuration of Web and CLI inactivity timeouts.
/etc/profile.d/umask.sh	Replace	Comments only. No operating system changes.	No	No	The file is for documentation purposes only.
/etc/login.defs	Delta	Updates UID_MIN to 1000, to keep Communication Manager logins separate. Updates the password aging control. Set password expiration and lockout periods.	Yes	No	The SMI Web page **Login Account Policy** allows configuring the 'Credential Expiration parameters'.
/etc/security/limits.conf /etc/security/pwquality.conf	Replace	Configure max number of logins and user's password complexity.	Yes See Note	No	The SMI Web page **Login Account Policy** allows configuration of password complexity. **Note:** After installation, set the entry 'CustomPamFiles enabled' in /etc/ecs.conf, if custom changes to PAM files are desired.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/localtime /etc/sysconfig/clock	Replace	Configure the time zone.	Yes	No	The SMI Web page **Time Zone configuration** allows configuration of the time zone.
/etc/pam.d/mv-auth /etc/pam.d/crond /etc/pam.d/cm /etc/pam.d/smi_web /etc/pam.d/hp-sshd	Replace	Set authorization and account policies for SSH and Web access.	Yes See Note	No	**Note:** After installation set the entry 'CustomPamFiles enabled' in /etc/ecs.conf, if custom changes to PAM files are desired.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/pam.d/atd /etc/pam.d/chfn /etc/pam.d/chsh /etc/pam.d/config-util /etc/pam.d/crond /etc/pam.d/login /etc/pam.d/passwd /etc/pam.d/polkit-1 /etc/pam.d/ppp /etc/pam.d/remote /etc/pam.d/screen /etc/pam.d/smtp /etc/pam.d/smtp.postfix /etc/pam.d/sshd /etc/pam.d/su /etc/pam.d/sudo /etc/pam.d/systemd-user /etc/pam.d/vlock	Delta	Set authorization and account policies for SSH and Web access. use Communication Manager PAM stack.	Yes See Note	No	**Note:** After installation set the entry 'CustomPamFiles enabled' in /etc/ecs.conf, if custom changes to PAM files are desired.
/etc/ssh/sshd_config /etc/ssh/hp-sshd_config /etc/ssh/ssh_config	Replace	Configure SSH access to bash and SAT.	Yes See Note	No	**Note:** After installation set the entry 'CustomSSHFiles enabled' in /etc/ecs.conf, if custom changes to SSH files are desired.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/shells	Delta	Add shells: 'nologin', 'eula_shell', and 'ppp-login'.	Yes	No	Required by Communication Manager.
/etc/nsswitch.conf	Replace	Configure LDAP access.	Yes See Note	No	**Note:** After installation set the entry 'CustomLDAPFiles enabled' in /etc/ecs.conf, if custom changes to LDAP are desired.
/etc/rc.d/init.d/*	Replace	Communication Manager adds initialization scripts.	No	Yes	These are the initialization scripts required for Communication Manager to start after a reboot
/etc/rc.modules	Replace	Make sure upper level SCSI and software watchdog are present.	Yes	Yes	
/etc/sysconfig/iptables /etc/sysconfig/ip6tables	Replace	Configure firewall for all Communication Manager connections.	Yes See Note	No	**Note:** After installation set the entry 'CustomFirewall enabled' in /etc/ecs.conf, if custom changes to Firewall are desired.
/etc/rsyncd.conf	Replace	Required for synchronization of Communication Manager configuration files.	No	Yes	
/etc/at.deny /etc/cron.deny /etc/cron.allow	Delta	Remove 'at' and 'cron' capability for some service logins. Only root is allowed to run cron.	Yes	No	Security related change.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/ld.so.conf	Delta	Add paths to Communication Manager libraries.	Yes	No	
/etc/issue /etc/issue.avaya	Replace	Add default Communication Manager login banner.	Yes	No	
/etc/syslog.conf /etc/sysconfig/rsyslog	Replace	Syslog configuration.	Yes	Yes	The SMI Web page **Syslog Server** allows configuration of syslog.
/etc/selinux/config	Delta	Disable SELinux.	Yes See Note	No	**Note:** Communication Manager provides a script to enable SELinux and auditd with safe settings: **`setCMSelinux [-f] <disabled | permissive | enforcing>`**. Note that enabling this will cause a small performance loss.
/etc/audit/auditd.conf /etc/audit/rules.d/audit.rules	Replace	Configure operating system level auditing. Disabled by default.	Yes See Note	Yes	**Note:** Communication Manager provides a script to enable auditd: **`setCMAuditd [ -f] <enabled | disabled>`**. Note that enabling this will cause a small performance loss.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/services	Replace	Older version of the file with added Communication Manager services (SAT, H.248, messaging).	Yes	Yes	
/etc/logrotate.conf /etc/logrotate.d/chistory /etc/logrotate.d/httpd /etc/logrotate.d/krm_rotate /etc/logrotate.d/syslog /etc/logrotate.d/syslog_rotate /etc/logrotate.d/avaya.logrotate	Replace	Configure a log rotation period and disk usage.	Yes	Yes	Changes may be lost after a Communication Manager update. Some files are for Communication Manager specific logs only.
/etc/nscd.conf	Replace	Configure Name Services cache by removing caching of hosts.	Yes	Yes	
/etc/sysctl.conf /etc/sysctl.d/99-sysctl.conf	Replace	Customized operating system and networking parameters.	Yes	Yes	Should not be changed.
/etc/httpd/conf/httpd.conf /etc/httpd/conf.d/ssl.conf	Delta	Configure the Apache HTTP service for SMI Web interface.	No	Yes	Communication Manager requires control of the httpd configuration for the SMI Web interface. Communication Manager also adds configuration files in the same /etc/httpd/conf.d directory.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/ppp/options /etc/ppp/ip-up.local /etc/ppp/ip-down.local /etc/ppp/ppp-login	Replace	Set global PPP options.	Yes	Yes	
/etc/sysconfig/crond	Replace	Turn off all mail from cron job.	Yes	Yes	Cron configuration files are also added to /etc/cron.d
/etc/sysconfig/init	Replace	Change the terminal font for success, failure, and warning to bold that is easier to see in color.	Yes	Yes	
/etc/fstab	Delta	Add security setting for cdrom, floppy, tmpfs, sysfs if present.	Yes	No	
/etc/php.ini	Replace	Configure PHP used by the SMI and other Communication Manager scripts.	Yes	Yes	

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/systemd/system/rsyslog.socket /etc/systemd/system/rsyslog.service /etc/systemd/system/nbsyslog.socket /etc/systemd/system/nbsyslog.service /etc/systemd/system/hp-sshd.service /etc/systemd/system/httpd.service /etc/systemd/system/fixFstab.service /etc/systemd/system/rngd.service /etc/systemd/system/auto_upgr.service	Replace (add)	Services initialization scripts for systemd.	Yes	Yes	Services needed by Communication Manager.

Table continues…

File	Change method (Delta | Replace | User choice)	Reason for change	Can be edited afterwards by customer ?	File can change in service packs and feature packs	Comments
/etc/aide.conf /etc/cron.daily/aide	Replace	Configuration files for the AIDE intrusion detection.	Yes (See Note)	No	To enable or disable AIDE, use the command: **`setCMAide <enabled | disabled>`** **Note:** After installation, set the entry 'CustomAIDEFiles enabled' in /etc/ecs.conf, if custom changes to AIDE are desired
/etc/termcap	Replace (add)	This configures terminal capability for legacy terminals.	Yes	Yes	
/etc/vimrc	Replace (add)	System wide vim initializations.	Yes	Yes	
/etc/sysconfig/apm-scripts/apmcontinue /etc/sysconfig/harddiskhda /etc/sysconfig/harddiskhdc /etc/sysconfig/i18n /etc/sendmail.cf /etc/man.config	Replace (add)	These files are no longer used or needed by the operating system.	Yes	Yes	

Appendix C: List of required RPMs on RHEL 8.4

The complete list of required RPMs is included in the `Dependencies.txt` in the ISO.

Note:

RPM versions listed are those available at the time of Release 10.2 ISO. Newer version of the RPMs are allowed.

To see Avaya™ Product Support Notice (PSN) for Avaya Aura® 10.2.x Software-only RPM updates, click PSN020617u.

The deployment of Avaya Aura® applications as Software Only is limited and unavailable for the net new deployments. The existing Avaya Aura® customers that run their deployments as software only, remain supported in Avaya Aura® 10.2, however, the customers are advised to migrate to a supported deployment platform by Aura 10.3. For queries, you can get in touch with the Avaya™ Sales or Accounts team.

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

A

acl-2.2.53-1.el8.x86_64	acpid-2.0.30-2.el8.x86_64
aide-0.16-14.el8_5.1.x86_64	alsa-lib-1.2.4-5.el8.x86_64
annobin-9.72-1.el8_5.2.x86_64	apr-1.6.3-11.el8.x86_64
apr-util-1.6.1-6.el8_8.1.x86_64	apr-util-bdb-1.6.1-6.el8_8.1.x86_64
apr-util-openssl-1.6.1-6.el8_8.1.x86_64	at-3.1.20-11.el8.x86_64
audispd-plugins-3.0-0.17.20191104git1c2f876.el8.x86_64	audit-3.0-0.17.20191104git1c2f876.el8.x86_64
audit-libs-3.0-0.17.20191104git1c2f876.el8.i686	audit-libs-3.0-0.17.20191104git1c2f876.el8.x86_64
augeas-libs-1.12.0-6.el8.x86_64	authselect-1.2.2-3.el8.x86_64
authselect-compat-1.2.2-3.el8.x86_64	authselect-libs-1.2.2-3.el8.x86_64
avahi-libs-0.7-20.el8.x86_64	

B

basesystem-11-5.el8.noarch	bash-4.4.19-14.el8.x86_64
bash-completion-2.7-5.el8.noarch	bc-1.07.1-5.el8.x86_64
bind-export-libs-9.11.36-8.el8_8.1.x86_64	bind-libs-9.11.36-8.el8_8.1.x86_64
bind-libs-lite-9.11.36-8.el8_8.1.x86_64	bind-license-9.11.36-8.el8_8.1.noarch
bind-utils-9.11.36-8.el8_8.1.x86_64	binutils-2.30-108.el8_5.1.x86_64
biosdevname-0.7.3-2.el8.x86_64	brotli-1.0.6-3.el8.i686
brotli-1.0.6-3.el8.x86_64	bubblewrap-0.4.0-1.el8.x86_64
buildah-1.29.1-1.module+el8.8.0+18195+471da4bb.x86_64	bzip2-1.0.6-26.el8.x86_64
bzip2-libs-1.0.6-26.el8.i686	bzip2-libs-1.0.6-26.el8.x86_64

C

c-ares-1.13.0-6.el8_8.2.x86_64	ca-certificates-2020.2.41-80.0.el8_2.noarch
cairo-1.15.12-6.el8.x86_64	checkpolicy-2.9-1.el8.x86_64
chkconfig-1.19.1-1.el8.x86_64	chrony-3.5-2.el8.x86_64
clevis-15-1.el8.x86_64	clevis-dracut-15-1.el8.x86_64
clevis-luks-15-1.el8.x86_64	clevis-systemd-15-1.el8.x86_64
compat-openssl10-1.0.2o-4.el8_6.i686	conmon-2.1.6-1.module+el8.8.0+18098+9b44df5f.x86_64
container-selinux-2.205.0-2.module+el8.8.0+18438+15d3aa65.noarch	containernetworking-plugins-1.2.0-1.module+el8.8.0+18060+3f21f2cc.x86_64
containers-common-1-64.module+el8.8.0+18571+eed59fc4.x86_64	coreutils-8.30-8.el8.x86_64
coreutils-common-8.30-8.el8.x86_64	cpio-2.12-11.el8.x86_64
cracklib-2.9.6-15.el8.i686	cracklib-2.9.6-15.el8.x86_64
cracklib-dicts-2.9.6-15.el8.x86_64	criu-3.15-3.module+el8.8.0+18060+3f21f2cc.x86_64
cronie-1.5.2-4.el8.x86_64	cronie-anacron-1.5.2-4.el8.x86_64
crontabs-1.11-17.20190603git.el8.noarch	crypto-policies-20210209-1.gitbfb6bed.el8_3.noarch
crypto-policies-scripts-20210209-1.gitbfb6bed.el8_3.noarch	cryptsetup-2.3.3-4.el8_5.1.x86_64
cryptsetup-libs-2.3.3-4.el8_5.1.x86_64	cups-libs-2.2.6-51.el8_8.1.x86_64
curl-7.61.1-30.el8_8.3.x86_64	cyrus-sasl-lib-2.1.27-6.el8_5.i686
cyrus-sasl-lib-2.1.27-6.el8_5.x86_64	

D

dbus-1.12.8-24.el8_8.1.x86_64	dbus-common-1.12.8-24.el8_8.1.noarch
dbus-daemon-1.12.8-24.el8_8.1.x86_64	dbus-glib-0.110-2.el8.x86_64
dbus-libs-1.12.8-24.el8_8.1.x86_64	dbus-tools-1.12.8-24.el8_8.1.x86_64
dejavu-fonts-common-2.35-7.el8.noarch	dejavu-sans-fonts-2.35-7.el8.noarch
desktop-file-utils-0.23-8.el8.x86_64	device-mapper-1.02.175-5.el8.x86_64
device-mapper-event-1.02.175-5.el8.x86_64	device-mapper-event-libs-1.02.175-5.el8.x86_64
device-mapper-libs-1.02.175-5.el8.x86_64	device-mapper-persistent-data-0.8.5-4.el8.x86_64
dhcp-client-4.3.6-49.el8.x86_64	dhcp-common-4.3.6-49.el8.noarch
dhcp-libs-4.3.6-49.el8.x86_64	dialog-1.3-13.20171209.el8.x86_64
diffutils-3.6-6.el8.x86_64	dmidecode-3.3-4.el8_8.1.x86_64
dnf-4.7.0-4.el8.noarch	dnf-data-4.7.0-4.el8.noarch
dnf-plugin-spacewalk-2.8.5-11.module+el8.1.0+3455+3ddf2832.noarch	dnf-plugins-core-4.0.21-3.el8.noarch
dos2unix-7.4.0-3.el8.x86_64	dosfstools-4.1-6.el8.x86_64
dracut-049-135.git20210121.el8.x86_64	dracut-config-rescue-049-135.git20210121.el8.x86_64
dracut-live-049-135.git20210121.el8.x86_64	dracut-network-049-135.git20210121.el8.x86_64
dracut-squash-049-135.git20210121.el8.x86_64	dwz-0.12-9.el8.x86_64

E

e2fsprogs-1.45.6-5.el8.x86_64	e2fsprogs-libs-1.45.6-5.el8.x86_64
ed-1.14.2-4.el8.x86_64	efi-filesystem-3-3.el8.noarch
efi-srpm-macros-3-3.el8.noarch	efibootmgr-16-1.el8.x86_64
efivar-37-4.el8.x86_64	efivar-libs-37-4.el8.x86_64
elfutils-debuginfod-client-0.182-3.el8.x86_64	elfutils-default-yama-scope-0.182-3.el8.noarch
elfutils-libelf-0.182-3.el8.i686	elfutils-libelf-0.182-3.el8.x86_64
elfutils-libs-0.182-3.el8.x86_64	emacs-filesystem-26.1-10.el8_8.2.noarch
ethtool-5.8-5.el8.x86_64	expat-2.2.5-10.el8_7.1.i686
expat-2.2.5-10.el8_7.1.x86_64	expect-5.45.4-5.el8.x86_64

F

file-5.33-20.el8.x86_64	file-libs-5.33-20.el8.x86_64
filesystem-3.8-3.el8.x86_64	findutils-4.6.0-20.el8.x86_64
fipscheck-1.5.0-4.el8.x86_64	fipscheck-lib-1.5.0-4.el8.x86_64
firewalld-0.8.2-6.el8.noarch	firewalld-filesystem-0.8.2-6.el8.noarch

Table continues…

flac-libs-1.3.2-9.el8_8.1.x86_64	fontconfig-2.13.1-3.el8.x86_64
fontpackages-filesystem-1.44-22.el8.noarch	freetype-2.9.1-9.el8.x86_64
fribidi-1.0.4-9.el8.x86_64	fstrm-0.6.0-3.el8.1.x86_64
fuse-2.9.7-12.el8.x86_64	fuse-common-3.2.1-12.el8.x86_64
fuse-libs-2.9.7-12.el8.x86_64	fuse-overlayfs-1.10-1.module+el8.8.0+18060+3f21f2cc.x86_64
fuse3-3.2.1-12.el8.x86_64	fuse3-libs-3.2.1-12.el8.x86_64
fwupd-1.5.9-1.el8_4.x86_64	fxload-2008_10_13-10.el8.x86_64

G

gawk-4.2.1-2.el8.x86_64	gc-7.6.4-3.el8.x86_64
GConf2-3.2.6-22.el8.x86_64	gd-2.2.5-7.el8.x86_64
gdb-8.2-15.el8.x86_64	gdb-headless-8.2-15.el8.x86_64
gdbm-1.18-1.el8.i686	gdbm-1.18-1.el8.x86_64
gdbm-devel-1.18-1.el8.x86_64	gdbm-libs-1.18-1.el8.i686
gdbm-libs-1.18-1.el8.x86_64	gdisk-1.0.3-11.el8.x86_64
gdk-pixbuf2-2.36.12-5.el8.x86_64	GeoIP-1.6.12-7.el8.x86_64
gettext-0.19.8.1-17.el8.x86_64	gettext-libs-0.19.8.1-17.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch	glib2-2.56.4-159.el8.i686
glib2-2.56.4-159.el8.x86_64	glibc-2.28-164.el8_5.3.i686
glibc-2.28-164.el8_5.3.x86_64	glibc-all-langpacks-2.28-164.el8_5.3.x86_64
glibc-common-2.28-164.el8_5.3.x86_64	glibc-devel-2.28-164.el8_5.3.x86_64
glibc-headers-2.28-164.el8_5.3.x86_64	glibc-langpack-en-2.28-164.el8_5.3.x86_64
glx-utils-8.4.0-5.20181118git1830dcb.el8.x86_64	gmp-6.1.2-10.el8.i686
gmp-6.1.2-10.el8.x86_64	gnupg1-1.4.23-15.el8.x86_64
gnupg2-2.2.20-3.el8_6.x86_64	gnupg2-smime-2.2.20-3.el8_6.x86_64
gnutls-3.6.16-6.el8_7.i686	gnutls-3.6.16-6.el8_7.x86_64
go-srpm-macros-2-17.el8.noarch	gobject-introspection-1.56.1-1.el8.x86_64
gpgme-1.13.1-7.el8.x86_64	graphite2-1.3.10-10.el8.x86_64
grep-3.1-6.el8.x86_64	groff-1.22.3-18.el8.x86_64
groff-base-1.22.3-18.el8.x86_64	grub2-common-2.02-142.el8_7.1.noarch
grub2-efi-x64-2.02-142.el8_7.1.x86_64	grub2-pc-2.02-142.el8_7.1.x86_64
grub2-pc-modules-2.02-142.el8_7.1.noarch	grub2-tools-2.02-142.el8_7.1.x86_64
grub2-tools-extra-2.02-142.el8_7.1.x86_64	grub2-tools-minimal-2.02-142.el8_7.1.x86_64
grubby-8.40-41.el8.x86_64	gsm-1.0.17-5.el8.x86_64
gstreamer1-1.16.1-2.el8.x86_64	gstreamer1-plugins-bad-free-1.16.1-1.el8.x86_64

Table continues…

gstreamer1-plugins-base-1.16.1-2.el8.x86_64	guile-2.0.14-7.el8.x86_64
gzip-1.9-13.el8_5.x86_64	

H

hardlink-1.3-6.el8.x86_64	harfbuzz-1.7.5-3.el8.x86_64
hdparm-9.54-3.el8.x86_64	hicolor-icon-theme-0.17-2.el8.noarch
hostname-3.20-6.el8.x86_64	httpd-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64
httpd-filesystem-2.4.37-56.module+el8.8.0+19808+379766d6.7.noarc	httpd-tools-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64
hwdata-0.314-8.8.el8.noarch	

I

ima-evm-utils-1.3.2-12.el8.x86_64	info-6.5-6.el8.x86_64
initscripts-10.00.15-1.el8.x86_64	ipcalc-0.2.4-4.el8.x86_64
iproute-5.9.0-4.el8.x86_64	iprutils-2.4.19-1.el8.x86_64
ipset-7.1-1.el8.x86_64	ipset-libs-7.1-1.el8.x86_64
iptables-1.8.4-17.el8.x86_64	iptables-ebtables-1.8.4-17.el8.x86_64
iptables-libs-1.8.4-17.el8.x86_64	iputils-20180629-7.el8.x86_64
irqbalance-1.4.0-6.el8.x86_64	isl-0.16.1-6.el8.x86_64
iso-codes-3.79-2.el8.noarch	

J

jansson-2.11-3.el8.x86_64	jbigkit-libs-2.1-14.el8.x86_64
jose-10-2.el8.x86_64	jq-1.5-12.el8.x86_64
json-c-0.13.1-3.el8.x86_64	json-glib-1.4.4-1.el8.x86_64

K

kbd-2.0.4-10.el8.x86_64	kbd-legacy-2.0.4-10.el8.noarch
kbd-misc-2.0.4-10.el8.noarch	kernel-4.18.0-477.27.1.el8_8.x86_64
kernel-core-4.18.0-477.27.1.el8_8.x86_64	kernel-devel-4.18.0-477.27.1.el8_8.x86_64
kernel-headers-4.18.0-477.27.1.el8_8.x86_64	kernel-modules-4.18.0-477.27.1.el8_8.x86_64
kernel-tools-4.18.0-477.27.1.el8_8.x86_64	kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64
kexec-tools-2.0.20-57.el8.x86_64	keyutils-libs-1.5.10-6.el8.i686
keyutils-libs-1.5.10-6.el8.x86_64	kmod-25-17.el8.x86_64
kmod-libs-25-17.el8.x86_64	kpartx-0.8.4-37.el8.x86_64
krb5-libs-1.18.2-22.el8_7.i686	krb5-libs-1.18.2-22.el8_7.x86_64

L

langpacks-en-1.0-12.el8.noarch	lcms2-2.9-2.el8.x86_64
less-530-1.el8.x86_64	libICE-1.0.9-15.el8.x86_64
libSM-1.2.3-1.el8.x86_64	libX11-1.6.8-5.el8.x86_64
libX11-common-1.6.8-5.el8.noarch	libX11-xcb-1.6.8-5.el8.x86_64
libXau-1.0.9-3.el8.x86_64	libXdamage-1.1.4-14.el8.x86_64
libXext-1.3.4-1.el8.x86_64	libXfixes-5.0.3-7.el8.x86_64
libXft-2.3.3-1.el8.x86_64	libXi-1.7.10-1.el8.x86_64
libXpm-3.5.12-9.el8_7.x86_64	libXrender-0.9.10-7.el8.x86_64
libXtst-1.2.3-7.el8.x86_64	libXv-1.0.11-7.el8.x86_64
libXxf86vm-1.1.4-9.el8.x86_64	libacl-2.2.53-1.el8.x86_64
libaio-0.3.112-1.el8.x86_64	libarchive-3.3.3-5.el8.x86_64
libassuan-2.5.1-3.el8.x86_64	libasyncns-0.8-14.el8.x86_64
libatasmart-0.19-14.el8.x86_64	libatomic_ops-7.6.2-3.el8.x86_64
libattr-2.4.48-3.el8.x86_64	libbabeltrace-1.5.4-3.el8.x86_64
libblkid-2.32.1-27.el8.i686	libblkid-2.32.1-27.el8.x86_64
libblockdev-2.24-5.el8.x86_64	libblockdev-crypto-2.24-5.el8.x86_64
libblockdev-fs-2.24-5.el8.x86_64	libblockdev-loop-2.24-5.el8.x86_64
libblockdev-mdraid-2.24-5.el8.x86_64	libblockdev-part-2.24-5.el8.x86_64
libblockdev-swap-2.24-5.el8.x86_64	libblockdev-utils-2.24-5.el8.x86_64
libbytesize-1.4-3.el8.x86_64	libcap-2.48-5.el8_8.i686
libcap-2.48-5.el8_8.x86_64	libcap-ng-0.7.9-5.el8.i686
libcap-ng-0.7.9-5.el8.x86_64	libcgroup-0.41-19.el8.x86_64
libcom_err-1.45.6-5.el8.i686	libcom_err-1.45.6-5.el8.x86_64
libcomps-0.1.11-5.el8.x86_64	libcroco-0.6.12-4.el8_2.1.x86_64
libcurl-7.61.1-30.el8_8.3.i686	libcurl-7.61.1-30.el8_8.3.x86_64
libcurl-devel-7.61.1-30.el8_8.3.i686	libdaemon-0.14-15.el8.x86_64
libdatrie-0.2.9-7.el8.x86_64	libdb-5.3.28-40.el8.i686
libdb-5.3.28-40.el8.x86_64	libdb-devel-5.3.28-40.el8.x86_64
libdb-utils-5.3.28-40.el8.x86_64	libdnet-1.12-26.el8.x86_64
libdnf-0.63.0-3.el8.x86_64	libdrm-2.4.103-1.el8.x86_64
libdvdnav-5.0.3-8.el8.x86_64	libdvdread-5.0.3-9.el8.x86_64
libedit-3.1-23.20170329cvs.el8.x86_64	libestr-0.1.10-1.el8.x86_64
libevdev-1.10.0-1.el8.x86_64	libevent-2.1.8-5.el8.x86_64
libfastjson-0.99.8-2.el8.x86_64	libfdisk-2.32.1-27.el8.x86_64
libffi-3.1-22.el8.i686	libffi-3.1-22.el8.x86_64

Table continues…

libgcab1-1.1-1.el8.x86_64	libgcc-8.5.0-4.el8_5.i686
libgcc-8.5.0-4.el8_5.x86_64	libgcrypt-1.8.5-7.el8_6.i686
libgcrypt-1.8.5-7.el8_6.x86_64	libglvnd-1.3.2-1.el8.x86_64
libglvnd-egl-1.3.2-1.el8.x86_64	libglvnd-gles-1.3.2-1.el8.x86_64
libglvnd-glx-1.3.2-1.el8.x86_64	libgomp-8.5.0-4.el8_5.x86_64
libgpg-error-1.31-1.el8.i686	libgpg-error-1.31-1.el8.x86_64
libgudev-232-4.el8.x86_64	libgusb-0.3.0-1.el8.x86_64
libibverbs-32.0-4.el8.i686	libibverbs-32.0-4.el8.x86_64
libicu-60.3-2.el8_1.x86_64	libidn-1.34-5.el8.x86_64
libidn2-2.2.0-1.el8.i686	libidn2-2.2.0-1.el8.x86_64
libinput-1.16.3-3.el8_6.x86_64	libipt-1.6.1-8.el8.x86_64
libjose-10-2.el8.x86_64	libjpeg-turbo-1.5.3-12.el8.x86_64
libkcapi-1.2.0-2.el8.x86_64	libkcapi-hmaccalc-1.2.0-2.el8.x86_64
libksba-1.3.5-9.el8_7.x86_64	libluksmeta-9-4.el8.x86_64
libmaxminddb-1.2.0-10.el8.x86_64	libmbim-1.20.2-1.el8.x86_64
libmetalink-0.1.3-7.el8.x86_64	libmnl-1.0.4-6.el8.x86_64
libmodulemd-2.13.0-1.el8.x86_64	libmount-2.32.1-27.el8.i686
libmount-2.32.1-27.el8.x86_64	libmpc-1.1.0-9.1.el8.x86_64
libmspack-0.7-0.3.alpha.el8.4.x86_64	libndp-1.7-5.el8.x86_64
libnet-1.1.6-15.el8.x86_64	libnetfilter_conntrack-1.0.6-5.el8.x86_64
libnfnetlink-1.0.1-13.el8.x86_64	libnftnl-1.1.5-4.el8.x86_64
libnghttp2-1.33.0-3.el8_2.1.i686	libnghttp2-1.33.0-3.el8_2.1.x86_64
libnl3-3.5.0-1.el8.i686	libnl3-3.5.0-1.el8.x86_64
libnl3-cli-3.5.0-1.el8.x86_64	libnsl-2.28-164.el8_5.3.i686
libnsl-2.28-164.el8_5.3.x86_64	libnsl2-1.2.0-2.20180605git4a062cf.el8.i686
libnsl2-1.2.0-2.20180605git4a062cf.el8.x86_64	libogg-1.3.2-10.el8.x86_64
libpath_utils-0.2.1-39.el8.x86_64	libpcap-1.9.1-5.el8.i686
libpcap-1.9.1-5.el8.x86_64	libpciaccess-0.14-1.el8.x86_64
libpipeline-1.5.0-2.el8.x86_64	libpkgconf-1.4.2-1.el8.x86_64
libpng-1.6.34-5.el8.x86_64	libprelude-5.2.0-1.el8.x86_64
libpsl-0.20.2-6.el8.i686	libpsl-0.20.2-6.el8.x86_64
libpwquality-1.4.4-3.el8.i686	libpwquality-1.4.4-3.el8.x86_64
libqmi-1.24.0-1.el8.x86_64	librepo-1.14.0-2.el8.x86_64
libreport-filesystem-2.9.5-15.el8.x86_64	libretls-3.7.0-1.el8.x86_64
librhsm-0.0.3-4.el8.x86_64	librsvg2-2.42.7-4.el8.x86_64
libseccomp-2.5.1-1.el8.x86_64	libsecret-0.18.6-1.el8.x86_64

Table continues…

libselinux-2.9-5.el8.i686	libselinux-2.9-5.el8.x86_64
libselinux-utils-2.9-5.el8.x86_64	libsemanage-2.9-6.el8.x86_64
libsepol-2.9-3.el8.i686	libsepol-2.9-3.el8.x86_64
libsigsegv-2.11-5.el8.x86_64	libslirp-4.4.0-1.module+el8.8.0+18060+3f21f2cc.x86_64
libsmartcols-2.32.1-27.el8.x86_64	libsmbios-2.4.1-2.el8.x86_64
libsmi-0.4.8-23.el8.x86_64	libsndfile-1.0.28-12.el8.x86_64
libsolv-0.7.19-1.el8.x86_64	libsrtp-1.5.4-8.el8.x86_64
libss-1.45.6-5.el8.x86_64	libssh-0.9.6-10.el8_8.i686
libssh-0.9.6-10.el8_8.x86_64	libssh-config-0.9.6-10.el8_8.noarch
libstdc++-8.5.0-4.el8_5.i686	libstdc++-8.5.0-4.el8_5.x86_64
libsysfs-2.1.0-24.el8.x86_64	libtalloc-2.3.1-2.el8.x86_64
libtasn1-4.13-4.el8_7.i686	libtasn1-4.13-4.el8_7.x86_64
libteam-1.31-2.el8.x86_64	libthai-0.1.27-2.el8.x86_64
libtheora-1.1.1-21.el8.x86_64	libtiff-4.0.9-28.el8_8.x86_64
libtirpc-1.1.4-4.el8.i686	libtirpc-1.1.4-4.el8.x86_64
libtool-ltdl-2.4.6-25.el8.x86_64	libudisks2-2.9.0-9.el8.x86_64
libunistring-0.9.9-3.el8.i686	libunistring-0.9.9-3.el8.x86_64
libusb-0.1.5-12.el8.x86_64	libusbx-1.0.23-4.el8.x86_64
libuser-0.62-23.el8.x86_64	libutempter-1.1.6-14.el8.x86_64
libuuid-2.32.1-27.el8.i686	libuuid-2.32.1-27.el8.x86_64
libverto-0.3.0-5.el8.i686	libverto-0.3.0-5.el8.x86_64
libvisual-0.4.0-25.el8.x86_64	libvorbis-1.3.6-2.el8.x86_64
libwacom-1.6-2.el8.x86_64	libwacom-data-1.6-2.el8.noarch
libwayland-client-1.21.0-1.el8.x86_64	libwayland-cursor-1.21.0-1.el8.x86_64
libwayland-egl-1.21.0-1.el8.x86_64	libwayland-server-1.21.0-1.el8.x86_64
libwebp-1.0.0-8.el8_7.x86_64	libxcb-1.13.1-1.el8.x86_64
libxcrypt-4.1.1-4.el8.i686	libxcrypt-4.1.1-4.el8.x86_64
libxcrypt-devel-4.1.1-4.el8.x86_64	libxkbcommon-0.9.1-1.el8.x86_64
libxkbcommon-x11-0.9.1-1.el8.x86_64	libxml2-2.9.7-16.el8_8.1.i686
libxml2-2.9.7-16.el8_8.1.x86_64	libxmlb-0.1.15-1.el8.x86_64
libxshmfence-1.3-2.el8.x86_64	libxslt-1.1.32-6.el8.x86_64
libyaml-0.1.7-5.el8.x86_64	libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64
libzstd-1.4.4-1.el8.x86_64	lm_sensors-libs-3.4.0-22.20180522git70f7e08.el8.x86_64
lockdev-1.0.4-0.28.20111007git.el8.x86_64	logrotate-3.14.0-4.el8.x86_64

Table continues…

lsof-4.93.2-1.el8.x86_64	lsscsi-0.32-2.el8.x86_64
ltrace-0.7.91-28.el8.x86_64	lua-libs-5.3.4-12.el8.x86_64
luksmeta-9-4.el8.x86_64	lvm2-2.03.11-5.el8.x86_64
lvm2-libs-2.03.11-5.el8.x86_64	lz4-libs-1.8.3-3.el8_4.i686
lz4-libs-1.8.3-3.el8_4.x86_64	lzo-2.08-14.el8.x86_64

M

mailcap-2.1.48-3.el8.noarch	make-4.2.1-10.el8.x86_64
man-db-2.7.6.1-17.el8.x86_64	man-pages-4.15-6.el8.x86_64
man-pages-overrides-8.3.0.2-2.el8.noarch	mariadb-connector-c-3.1.11-2.el8_3.x86_64
mariadb-connector-c-config-3.1.11-2.el8_3.noarch	mdadm-4.1-15.el8.x86_64
memstrack-0.1.11-1.el8.x86_64	mesa-libEGL-20.3.3-2.el8.x86_64
mesa-libGL-20.3.3-2.el8.x86_64	mesa-libgbm-20.3.3-2.el8.x86_64
mesa-libglapi-20.3.3-2.el8.x86_64	microcode_ctl-20210216-1.20210608.1.el8_4.x86_64
mod_http2-1.15.7-8.module+el8.8.0+18751+b4557bca.3.x86_64	mod_ssl-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64
ModemManager-glib-1.10.8-2.el8.x86_64	mokutil-0.3.0-11.el8_6.1.x86_64
mozjs60-60.9.0-4.el8.x86_64	mpfr-3.1.6-1.el8.x86_64
mtdev-1.1.5-12.el8.x86_64	mtools-4.0.18-14.el8.x86_64

N

ncurses-6.1-9.20180224.el8_8.1.x86_64	ncurses-base-6.1-9.20180224.el8_8.1.noarch
ncurses-libs-6.1-9.20180224.el8_8.1.i686	ncurses-libs-6.1-9.20180224.el8_8.1.x86_64
net-snmp-5.8-27.el8.x86_64	net-snmp-agent-libs-5.8-27.el8.x86_64
net-snmp-libs-5.8-27.el8.x86_64	net-snmp-perl-5.8-27.el8.x86_64
net-snmp-utils-5.8-27.el8.x86_64	net-tools-2.0-0.52.20160912git.el8.x86_64
nettle-3.4.1-7.el8.i686	nettle-3.4.1-7.el8.x86_64
network-scripts-10.00.15-1.el8.x86_64	network-scripts-team-1.31-2.el8.x86_64
NetworkManager-1.32.10-4.el8.x86_64	NetworkManager-config-server-1.32.10-4.el8.noarch
NetworkManager-libnm-1.32.10-4.el8.x86_64	NetworkManager-tui-1.32.10-4.el8.x86_64
nftables-0.9.3-18.el8.x86_64	npth-1.5-4.el8.x86_64
nspr-4.35.0-1.el8_8.i686	nss-3.79.0-11.el8_7.x86_64
nss-pam-ldapd-0.9.9-3.el8.x86_64	nss-softokn-3.79.0-11.el8_7.x86_64
nss-softokn-freebl-3.79.0-11.el8_7.x86_64	nss-util-3.79.0-11.el8_7.i686
numactl-libs-2.0.12-11.el8.x86_64	

O

oddjob-0.34.7-1.el8.x86_64	oniguruma-6.8.2-2.el8.x86_64
openal-soft-1.18.2-7.el8.x86_64	openldap-2.4.46-16.el8.i686
openldap-clients-2.4.46-16.el8.x86_64	openssh-clients-8.0p1-19.el8_8.x86_64
openssl-1.1.1k-9.el8_7.x86_64	openssl-libs-1.1.1k-9.el8_7.x86_64
openssl-pkcs11-0.4.10-2.el8.x86_64	orc-0.4.28-3.el8.x86_64

P

p11-kit-0.23.22-1.el8.i686	p11-kit-trust-0.23.22-1.el8.x86_64
pam-1.3.1-14.el8.x86_64	parted-3.2-38.el8.x86_64
patch-2.7.6-11.el8.x86_64	pciutils-libs-3.7.0-1.el8.x86_64
pcre-8.42-6.el8.x86_64	pcre2-10.32-3.el8_6.x86_64
perl-5.26.3-419.el8.x86_64	perl-Archive-Tar-2.30-1.el8.noarch
perl-Attribute-Handlers-0.99-419.el8.noarch	perl-Business-ISBN-3.005-4.el8.noarch
perl-CPAN-2.18-397.el8.noarch	perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
perl-Carp-1.42-396.el8.noarch	perl-Compress-Bzip2-2.26-6.el8.x86_64
perl-Compress-Raw-Zlib-2.081-1.el8.x86_64	perl-DB_File-1.842-1.el8.x86_64
perl-Data-Dumper-2.167-399.el8.x86_64	perl-Data-Perl-0.002009-17.el8.noarch
perl-Devel-Caller-2.06-15.el8.x86_64	perl-Devel-LexAlias-0.05-16.el8.x86_64
perl-Devel-Peek-1.26-419.el8.x86_64	perl-Devel-Size-0.81-2.el8.x86_64
perl-Devel-StackTrace-2.03-2.el8.noarch	perl-Digest-HMAC-1.03-17.module+el8.3.0+6498+9eecfe51.noarch
perl-Digest-SHA-6.02-1.el8.x86_64	perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-Env-1.04-395.el8.noarch	perl-Expect-1.35-10.el8.noarch
perl-Exporter-Tiny-1.000000-4.el8.noarch	perl-ExtUtils-Command-7.34-1.el8.noarch
perl-ExtUtils-Install-2.14-4.el8.noarch	perl-ExtUtils-MakeMaker-7.34-1.el8.noarch
perl-ExtUtils-Miniperl-1.06-419.el8.noarch	perl-File-Fetch-0.56-2.el8.noarch
perl-File-Listing-6.04-17.module+el8.3.0+6498+9eecfe51.noarch	perl-File-Temp-0.230.600-1.el8.noarch
perl-Filter-1.58-2.el8.x86_64	perl-GD-2.71-1.el8.x86_64
perl-Getopt-Long-2.50-4.el8.noarch	perl-HTML-Parser-3.72-15.module+el8.3.0+6498+9eecfe51.x86_64

Table continues…

perl-HTTP-Cookies-6.04-2.module+el8.3.0+6498+9eecfe51.noarch	perl-HTTP-Date-6.02-19.module+el8.3.0+6498+9eecfe51.noarch
perl-HTTP-Negotiate-6.01-19.module+el8.3.0+6498+9eecfe51.noarch	perl-Hash-FieldHash-0.15-9.el8.x86_64
perl-IO-Compress-2.081-1.el8.noarch	perl-IO-Socket-IP-0.39-5.el8.noarch
perl-IO-Tty-1.12-11.el8.x86_64	perl-IPC-Cmd-1.02-1.el8.noarch
perl-IPC-System-Simple-1.25-17.el8.noarch	perl-JSON-2.97.001-2.el8.noarch
perl-LWP-MediaTypes-6.02-15.module+el8.3.0+6498+9eecfe51.noarch	perl-List-MoreUtils-XS-0.428-3.el8.x86_64
perl-Locale-Maketext-1.28-396.el8.noarch	perl-MIME-Base64-3.15-396.el8.x86_64
perl-MRO-Compat-0.13-4.el8.noarch	perl-Math-BigInt-1.9998.11-7.el8.noarch
perl-Math-BigRat-0.2614-1.el8.noarch	perl-Memoize-1.03-419.el8.noarch
perl-Module-CoreList-5.20181130-1.el8.noarch	perl-Module-Load-0.32-395.el8.noarch
perl-Module-Loaded-0.08-419.el8.noarch	perl-Module-Runtime-0.016-2.el8.noarch
perl-MooX-0.101-19.el8.noarch	perl-MooX-late-0.015-19.el8.noarch
perl-NTLM-1.09-17.module+el8.3.0+6498+9eecfe51.noarch	perl-Net-LibIDN-0.12-35.el8.x86_64
perl-Net-SSLeay-1.88-1.module+el8.3.0+6446+594cad75.x86_64	perl-PadWalker-2.3-2.el8.x86_64
perl-Params-Util-1.07-22.el8.x86_64	perl-Perl-OSType-1.010-396.el8.noarch
perl-Pod-Checker-1.73-395.el8.noarch	perl-Pod-Html-1.22.02-419.el8.noarch
perl-Pod-Perldoc-3.28-396.el8.noarch	perl-Pod-Usage-1.69-395.el8.noarch
perl-Scalar-List-Utils-1.49-2.el8.x86_64	perl-Socket-2.027-3.el8.x86_64
perl-Storable-3.11-3.el8.x86_64	perl-Sub-Exporter-Progressive-0.001013-5.el8.noarch
perl-Sub-Quote-2.006003-3.el8.noarch	perl-Term-ANSIColor-4.06-396.el8.noarch
perl-TermReadKey-2.37-7.el8.x86_64	perl-Test-Fatal-0.014-9.el8.noarch
perl-Test-Simple-1.302135-1.el8.noarch	perl-Text-Diff-1.45-2.el8.noarch
perl-Text-ParseWords-3.30-395.el8.noarch	perl-Text-Tabs+Wrap-2013.0523-395.el8.noarch
perl-Thread-Queue-3.13-1.el8.noarch	perl-Time-Local-1.280-1.el8.noarch
perl-TimeDate-2.30-15.module+el8.3.0+6498+9eecfe51.noarch	perl-Type-Tie-0.014-5.el8.noarch
perl-URI-1.73-3.el8.noarch	perl-Unicode-Normalize-1.25-396.el8.x86_64
perl-XML-Parser-2.44-11.el8.x86_64	perl-bignum-0.49-2.el8.noarch

Table continues…

perl-devel-5.26.3-419.el8.x86_64	perl-experimental-0.019-2.el8.noarch
perl-interpreter-5.26.3-419.el8.x86_64	perl-libnetcfg-5.26.3-419.el8.noarch
perl-libwww-perl-6.34-1.module+el8.3.0+6498+9eecfe51.noarch	perl-macros-5.26.3-419.el8.x86_64
perl-parent-0.237-1.el8.noarch	perl-podlators-4.11-1.el8.noarch
perl-strictures-2.000006-6.el8.noarch	perl-threads-shared-1.58-2.el8.x86_64
perl-version-0.99.24-1.el8.x86_64	php-cli-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64
php-fpm-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64	php-xml-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64
pinentry-1.1.0-2.el8.x86_64	pkgconf-1.4.2-1.el8.x86_64
pkgconf-m4-1.4.2-1.el8.noarch	platform-python-3.6.8-51.el8_8.1.i686
platform-python-pip-9.0.3-20.el8.noarch	plymouth-0.9.4-9.20200615git1e36e30.el8.x86_64
plymouth-scripts-0.9.4-9.20200615git1e36e30.el8.x86_64	podman-catatonit-4.4.1-8.module+el8.8.0+18438+15d3aa65.x86_64
policycoreutils-python-utils-2.9-14.el8.noarch	polkit-libs-0.115-13.el8_5.2.x86_64
popt-1.18-1.el8.x86_64	ppp-2.4.7-26.el8_1.x86_64
protobuf-c-1.3.0-6.el8.x86_64	publicsuffix-list-dafsa-20180723-1.el8.noarch
pulseaudio-libs-glib2-14.0-2.el8.x86_64	python-srpm-macros-3-41.el8.noarch
python3-augeas-0.5.0-12.el8.noarch	python3-cffi-1.11.5-5.el8.x86_64
python3-configobj-5.0.6-11.el8.noarch	python3-dateutil-2.6.1-6.el8.noarch
python3-decorator-4.2.1-2.el8.noarch	python3-dnf-4.7.0-4.el8.noarch
python3-dnf-plugins-core-4.0.21-3.el8.noarch	python3-firewall-0.8.2-6.el8.noarch
python3-gpg-1.13.1-7.el8.x86_64	python3-hwdata-2.3.6-3.el8.noarch
python3-libcomps-0.1.11-5.el8.x86_64	python3-librepo-1.14.0-2.el8.x86_64
python3-libs-3.6.8-51.el8_8.1.x86_64	python3-libsemanage-2.9-6.el8.x86_64
python3-linux-procfs-0.6.3-1.el8.noarch	python3-newt-0.52.20-11.el8.x86_64
python3-perf-4.18.0-477.27.1.el8_8.x86_64	python3-pip-wheel-9.0.3-20.el8.noarch
python3-policycoreutils-2.9-14.el8.noarch	python3-pwquality-1.4.4-3.el8.x86_64
python3-pycparser-2.14-14.el8.noarch	python3-pysocks-1.6.8-3.el8.noarch
python3-pyyaml-3.12-12.el8.x86_64	python3-rhn-client-tools-2.8.16-13.module+el8.1.0+3455+3ddf2832.x86_64
python3-rpm-4.14.3-19.el8_5.2.x86_64	python3-schedutils-0.6-6.el8.x86_64
python3-setuptools-39.2.0-6.el8_7.1.noarch	python3-six-1.11.0-8.el8.noarch
python3-slip-dbus-0.6.4-11.el8.noarch	python3-unbound-1.16.2-5.el8.x86_64

Table continues…

python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64	

Q

qrencode-libs-3.4.4-5.el8.x86_64	qt5-qtbase-common-5.15.2-4.el8.noarch
qt5-qtdeclarative-5.15.2-2.el8.x86_64	qt5-srpm-macros-5.15.3-1.el8.noarch

R

rdma-core-32.0-4.el8.x86_64	readline-7.0-10.el8.i686
redhat-logos-httpd-84.5-1.el8.noarch	redhat-release-eula-8.4-0.6.el8.x86_64
rhn-client-tools-2.8.16-13.module+el8.1.0+3455+3ddf2832.x86_64	rootfiles-8.1-22.el8.noarch
rpm-4.14.3-19.el8_5.2.x86_64	rpm-libs-4.14.3-19.el8_5.2.x86_64
rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64	rsync-3.1.3-19.el8.x86_64
rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64	rust-srpm-macros-5-2.el8.noarch

S

sed-4.5-2.el8.x86_64	selinux-policy-targeted-3.14.3-80.el8_5.2.noarch
setup-2.12.2-6.el8.noarch	sg3_utils-libs-1.44-5.el8.x86_64
shadow-utils-subid-4.6-17.el8.x86_64	shim-x64-15.6-1.el8.x86_64
slirp4netns-1.2.0-2.module+el8.8.0+18060+3f21f2cc.x86_64	soundtouch-2.0.0-3.el8.x86_64
sqlite-libs-3.26.0-18.el8_8.i686	squashfs-tools-4.3-20.el8.x86_64
ssldump-1.8-1.el8.x86_64	sudo-1.8.29-8.el8_7.1.x86_64
syslinux-nonlinux-6.04-5.el8.noarch	systemd-239-74.el8_8.2.x86_64
systemd-libs-239-74.el8_8.2.x86_64	systemd-udev-239-74.el8_8.2.x86_64

T

tar-1.30-6.el8_7.1.x86_64	tcp_wrappers-7.6-96.el8.x86_64
teamd-1.31-2.el8.x86_64	timedatex-0.5-3.el8.x86_64
tpm2-abrmd-2.3.3-2.el8.i686	tpm2-abrmd-selinux-2.3.1-1.el8.noarch
tpm2-tss-2.3.2-3.el8.i686	traceroute-2.1.0-6.el8.x86_64
trousers-lib-0.3.15-1.el8.x86_64	tzdata-2023c-1.el8.noarch

U

unbound-libs-1.16.2-5.el8.x86_64	unzip-6.0-44.el8.x86_64
usermode-1.113-1.el8.x86_64	util-linux-2.32.1-27.el8.x86_64
uuid-1.6.2-43.el8.x86_64	

V

virt-what-1.18-6.el8.x86_64	

W

webrtc-audio-processing-0.3-9.el8.x86_64	which-2.21-12.el8.x86_64
words-3.0-28.el8.noarch	

X

xcb-util-0.4.0-10.el8.x86_64	xcb-util-keysyms-0.4.0-7.el8.x86_64
xcb-util-wm-0.4.1-12.el8.x86_64	xdg-utils-1.1.2-5.el8.noarch
xkeyboard-config-2.28-1.el8.noarch	xmlsec1-1.2.25-4.el8.x86_64
xz-5.2.4-4.el8_6.x86_64	xz-libs-5.2.4-4.el8_6.x86_64

Y

yum-4.7.0-4.el8.noarch	

Z

zip-3.0-23.el8.x86_64	zlib-1.2.11-19.el8_6.x86_64

Appendix D: List of required RPMs on RHEL 8.10

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

A

acl	ACP	acpconf-unused-vmware	acpid
aide	alsa-firmware	alsa-lib	alsa-tools-firmware
annobin	apr	apr-util	apr-util-bdb
apr-util-openssl	at	audispd-plugins	audit
audit-libs	augeas-libs	authselect	authselect-compat
authselect-libs	avahi-libs	avaya-os-tools	avaya-vm-tools

B

basesystem	bash	bash-completion	bc
bind-export-libs	bind-libs	bind-libs-lite	bind-license
bind-utils	binutils	biosdevname	bison
brotli	bubblewrap	buildah	bzip2
bzip2-libs			

C

ca-certificates	cairo	c-ares	checkpolicy
chkconfig	chrony	clamav	clamav-filesystem
clamav-lib	clamav-update	clevis	clevis-dracut
clevis-luks	clevis-systemd	compat-openssl10	conmon
containernetworking-plugins	containers-common	container-selinux	coreutils
coreutils-common	cpio	cpp	cracklib
cracklib	cracklib-dicts	criu	cronie
cronie-anacron	crontabs	crypto-policies	crypto-policies-scripts

Table continues…

cryptsetup	cryptsetup-libs	cups-libs	curl
cyrus-sasl-lib	cyrus-sasl-lib		

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts
desktop-file-utils	device-mapper	device-mapper-event	device-mapper-event-libs
device-mapper-libs	device-mapper-persistent-data	dhcp-client	dhcp-common
dhcp-libs	dialog	diffutils	dmidecode
dnf	dnf-data	dnf-plugins-core	dnf-plugin-spacewalk
dos2unix	dosfstools	dracut	dracut-config-rescue
dracut-live	dracut-network	dracut-squash	dwz

E

e2fsprogs	e2fsprogs-libs	easg	ed
efibootmgr	efi-filesystem	efi-srpm-macros	efivar
efivar-libs	elfutils-debuginfod-client	elfutils-default-yama-scope	elfutils-libelf
elfutils-libelf-devel	elfutils-libs	emacs-filesystem	ethtool
expat	expect		

F

file	file-libs	filesystem	findutils
fipscheck	fipscheck-lib	firewalld	firewalld-filesystem
flac-libs	flex	fontconfig	fontpackages-filesystem
freetype	fribidi	fstrm	fuse
fuse3	fuse3-libs	fuse-common	fuse-libs
fuse-overlayfs	fwupd	fxload	

G

gawk	gc	gcc	gcc-gdb-plugin
gcc-plugin-annobin	GConf2	gd	gdb
gdb-headless	gdbm	gdbm	gdbm-devel
gdbm-libs	gdbm-libs	gdisk	gdk-pixbuf2
genisoimage	GeoIP	gettext	gettext-libs
ghc-srpm-macros	glib2	glib2	glibc
glibc	glibc-all-langpacks	glibc-common	glibc-devel

Table continues…

glibc-gconv-extra	glibc-gconv-extra	glibc-headers	glibc-langpack-en
glx-utils	gmp	gmp	gnupg1
gnupg2	gnupg2-smime	gnutls	gnutls
gobject-introspection	go-srpm-macros	gpgme	gpg-pubkey
gpg-pubkey	graphite2	grep	groff
groff-base	grub2-common	grub2-efi-x64	grub2-computer
grub2-computer-modules	grub2-tools	grub2-tools-efi	grub2-tools-extra
grub2-tools-minimal	grubby	gsm	gstreamer1
gstreamer1-plugins-bad-free	gstreamer1-plugins-base	guile	gzip

H

hardlink	harfbuzz	hdparm	hicolor-icon-theme
hostname	httpd	httpd-filesystem	httpd-tools
hwdata			

I

ima-evm-utils	information	initscripts	ipcalc
iproute	iprutils	ipset	ipset-libs
iptables	iptables-ebtables	iptables-libs	iputils
irqbalance	isl	iso-codes	

J

jansson	jbigkit-libs	jkc-image	jose
jq	json-c	json-glib	

K

kbd	kbd-previous	kbd-misc	kernel
kernel-core	kernel-devel	kernel-headers	kernel-modules
kernel-tools	kernel-tools-libs	kexec-tools	keyutils-libs
keyutils-libs-devel	kmod	kmod-libs	kpartx
krb5-devel	krb5-libs		

L

langpacks-en	lcms2	less	libacl
libaio	libarchive	libassuan	libasyncns
libatasmart	libatomic_ops	libattr	libbabeltrace
libblkid	libblockdev	libblockdev-crypto	libblockdev-fs

Table continues…

libblockdev-loop	libblockdev-mdraid	libblockdev-part	libblockdev-swap
libblockdev-utils	libbpf	libbytesize	libcap
libcap-ng	libcgroup	libcom_err	libcom_err-devel
libcomps	libcroco	libcurl	libcurl-devel
libdaemon	libdatrie	libdb	libdb-devel
libdb-utils	libdnet	libdnf	libdrm
libdvdnav	libdvdread	libedit	libestr
libevdev	libevent	libfastjson	libfdisk
libffi	libgcab1	libgcc	libgcrypt
libglvnd	libglvnd-egl	libglvnd-gles	libglvnd-glx
libgomp	libgpg-error	libgudev	libgusb
libibverbs	libICE	libicu	libidn
libidn2	libinput	libipt	libjose
libjpeg-turbo	libkadm5	libkcapi	libkcapi-hmaccalc
libksba	libluksmeta	libmaxminddb	libmbim
libmetalink	libmnl	libmodulemd	libmount
libmpc	libmspack	libndp	libnet
libnetfilter_conntrack	libnfnetlink	libnftnl	libnghttp2
libnl3	libnl3-cli	libnsl	libnsl2
libogg	libpath_utils	libpcap	libpciaccess
libpipeline	libpkgconf	libpng	libprelude
libpsl	libpwquality	libqmi	librepo
libreport-filesystem	libretls	librhsm	librsvg2
libseccomp	libsecret	libselinux	libselinux-devel
libselinux-utils	libsemanage	libsepol	libsepol-devel
libsigsegv	libslirp	libSM	libsmartcols
libsmbios	libsmi	libsndfile	libsolv
libsrtp	libss	libssh	libssh-config
libstdc++	libsysfs	libtalloc	libtasn1
libteam	libthai	libtheora	libtiff
libtirpc	libtool-ltdl	libudisks2	libunistring
libusal	libusb	libusbx	libuser
libutempter	libuuid	libverto	libverto-devel
libwayland-client	libwayland-cursor	libwayland-egl	libwayland-server
libwebp	libX11	libX11-common	libX11-xcb
libXau	libxcb	libxcrypt	libxcrypt-devel

Table continues…

libXdamage	libXext	libXfixes	libXft
libXi	libxkbcommon	libxkbcommon-x11	libxml2
libxmlb	libXpm	libXrender	libxshmfence
libxslt	libXtst	libXv	libXxf86vm
libyaml	libzip	libzstd	libzstd-devel
linux-firmware	lm_sensors-libs	lockdev	logrotate
lsof	lsscsi	ltrace	lua-libs
luksmeta	lvm2	lvm2-libs	lz4-libs
lzo			

M

m4	mailcap	make	man-db
man-pages	man-pages-overrides	mariadb-connector-c	mariadb-connector-c-config
mdadm	memstrack	mesa-libEGL	mesa-libgbm
mesa-libGL	mesa-libglapi	MessageTracer	microcode_ctl
ModemManager-glib	mod_http2	mod_ssl	mokutil
mozjs60	mpfr	mtdev	mtools

N

ncurses	ncurses-base	ncurses-libs	net-snmp
net-snmp-agent-libs	net-snmp-libs	net-snmp-perl	net-snmp-utils
nettle	net-tools	NetworkManager	NetworkManager-config-server
NetworkManager-initscripts-updown	NetworkManager-libnm	NetworkManager-team	NetworkManager-tui
network-scripts	network-scripts-team	newt	nftables
nginx-filesystem	npth	nscd	nspr
nss	nss-pam-ldapd	nss-softokn	nss-softokn-freebl
nss-sysinit	nss-util	numactl-libs	

O

ocaml-srpm-macros	oddjob	oddjob-mkhomedir	oniguruma
openal-soft	openblas-srpm-macros	openldap	openldap-clients
openssh	openssh-clients	openssh-server	openssl
openssl-devel	openssl-libs	openssl-pkcs11	open-vm-tools
opus	orc	os-prober	

P

p11-kit	p11-kit-trust	pam	pango
parted	passwd	patch	pciutils
pciutils-libs	pcre	pcre2	pcre2-devel
pcre2-utf16	pcre2-utf32	perl	perl-Algorithm-Diff
perl-Archive-Tar	perl-Archive-Zip	perl-Attribute-Handlers	perl-autodie
perl-B-Debug	perl-bignum	perl-Business-	perl-Business--Data
perl-Carp	perl-Class-Method-Modifiers	perl-Compress-Bzip2	perl-Compress-Raw-Bzip2
perl-Compress-Raw-Zlib	perl-Config-Perl-V	perl-constant	perl-
perl--Meta	perl--Meta-Requirements	perl--Meta-YAML	perl-Data-Dump
perl-Data-Dumper	perl-Data-OptList	perl-Data-Perl	perl-Data-Section
perl-DB_File	perl-devel	perl-Devel-Caller	perl-Devel-GlobalDestruction
perl-Devel-LexAlias	perl-Devel-Peek	perl-Devel-PPPort	perl-Devel-SelfStubber
perl-Devel-Size	perl-Devel-StackTrace	perl-Digest	perl-Digest-
perl-Digest-MD5	perl-Digest-SHA	perl-Encode	perl-Encode-devel
perl-Encode-Locale	perl-encoding	perl-Env	perl-Errno
perl-Expect	perl-experimental	perl-Exporter	perl-Exporter-Tiny
perl-ExtUtils-CBuilder	perl-ExtUtils-Command	perl-ExtUtils-Embed	perl-ExtUtils-Install
perl-ExtUtils-MakeMaker	perl-ExtUtils-Manifest	perl-ExtUtils-Miniperl	perl-ExtUtils-MM-Utils
perl-ExtUtils-ParseXS	perl-File-Fetch	perl-File-HomeDir	perl-File-Listing
perl-File-Path	perl-File-Temp	perl-File-Which	perl-Filter
perl-Filter-Simple	perl-GD	perl-GD-Barcode	perl-Getopt-Long
perl-GnuPG-Interface	perl-Hash-FieldHash	perl-HTML-Parser	perl-HTML-Tagset
perl-HTTP-Cookies	perl-HTTP-Daemon	perl-HTTP-Date	perl-HTTP-Message
perl-HTTP-Negotiate	perl-HTTP-Tiny	perl-Import-Into	perl-inc-latest
perl-interpreter	perl-I/O	perl-I/O-Compress	perl-I/O-HTML
perl-I/O-Socket-IP	perl-I/O-Socket-SSL	perl-I/O-Tty	perl-I/O-Zlib
perl--Cmd	perl--System-Simple	perl--SysV	perl-JSON
perl-JSON-PP	perl-libnet	perl-libnetcompare	perl-libs
perl-libwww-perl	perl-List-MoreUtils	perl-List-MoreUtils-XS	perl-Locale-Codes
perl-Locale-Maketext	perl-Locale-Maketext-Simple	perl-local-lib	perl--MediaTypes
perl-macros	perl-Mail-Sender	perl-Math-BigInt	perl-Math-BigInt-FastCalc
perl-Math-BigRat	perl-Math-Complex	perl-Memoize	perl--Base64

Table continues…

perl-Module-Build	perl-Module-CoreList	perl-Module-CoreList-tools	perl-Module-Load
perl-Module-Load-Conditional	perl-Module-Loaded	perl-Module-Metadata	perl-Module-Runtime
perl-Moo	perl-MooX	perl-MooX-HandlesVia	perl-MooX-late
perl-Mozilla-CA	perl--Compat	perl-Net-HTTP	perl-Net-LibIDN
perl-Net-Ping	perl-Net-SSLeay	perl-	perl-open
perl-Package-Generator	perl-PadWalker	perl-Params-Check	perl-Params-Util
perl-parent	perl-PathTools	perl-perlfaq	perl-PerlIO-through-QuotedPrint
perl-Perl-OSType	perl-Pod-Checker	perl-Pod-Escapes	perl-Pod-Html
perl-podlators	perl-Pod-Parser	perl-Pod-Perldoc	perl-Pod-Simple
perl-Pod-Usage	perl-Ref-Util-XS	perl-Role-Tiny	perl-Scalar-List-Utils
perl-SelfLoader	perl-Socket	perl-Software-License	perl-srpm-macros
perl-Storable	perl-strictures	perl-Sub-Exporter	perl-Sub-Exporter-Progressive
perl-Sub-Install	perl-Sub-Quote	perl-Sys-Syslog	perl-Term-ANSIColor
perl-Term-Cap	perl-TermReadKey	perl-Test	perl-Test-Fatal
perl-Test-Harness	perl-Test-Simple	perl-Text-Balanced	perl-Text-Diff
perl-Text-Glob	perl-Text-ParseWords	perl-Text-Tabs+Wrap	perl-Text-Template
perl-Thread-Queue	perl-threads	perl-threads-shared	perl-TimeDate
perl-Time-HiRes	perl-Time-Local	perl-Time-Piece	perl-Try-Tiny
perl-Type-Tie	perl-Type-Tiny	perl-Unicode-Collate	perl-Unicode-Normalize
perl-URI	perl-utils	perl-version	perl--RobotRules
perl-XML-Parser	php	php-cli	php-common
php-fpm	php-process	php-xml	pigz
pinentry	pixman	pkgconf	pkgconf-m4
pkgconf-pkg-config	platform-python	platform-python-pip	platform-python-setuptools
plymouth	plymouth-core-libs	plymouth-scripts	podman
podman-catatonit	policycoreutils	policycoreutils-python-utils	polkit
polkit-libs	polkit-pkla-compat	popt	postfix
ppp	procps-ng	protobuf-c	psmisc
publicsuffix-list-dafsa	pulseaudio-libs	pulseaudio-libs-glib2	python36
python3-audit	python3-augeas	python3-bind	python3-comparei
python3-chardet	python3-configobj	python3-cryptography	python3-dateutil
python3-dbus	python3-decorator	pythona3-dmidecode	python3-dnf

Table continues…

python3-dnf-plugins-core	python3-dnf-plugin-spacewalk	python3-ethtool	python3-firewall
python3-gobject-base	python3-gpg	python3-hawkey	python3-hwdata
python3-idna	python3-libcomps	python3-libdnf	python3-librepo
python3-libs	python3-libselinux	python3-libsemanage	python3-libxml2
python3-linux-procompare	python3-netifaces	python3-newt	python3-nftables
python3-perf	python3-pip	python3-pip-wheel	python3-ply
python3-policycoreutils	python3-prometheus_client	python3-pwquality	python3-pycparser
python3-pyOpenSSL	python3-pyparsing	python3-pysocks	python3-pyudev
python3-pyyaml	python3-requests	python3-rhn-client-tools	python3-rhnlib
python3-rpm	python3-rpm-macros	python3-schedutils	python3-setools
python3-setuptools	python3-setuptools-wheel	python3-six	python3-slip
python3-slip-dbus	python3-syspurpose	python3-systemd	python3-urllib3
python-rpm-macros	python-srpm-macros		

Q

qemu-guest-agent	qrencode-libs	qt5-qtbase	qt5-qtbase-common
qt5-qtbase-gui	qt5-qtdeclarative	qt5-qtmultimedia	qt5-srpm-macros

R

rdma-core	readline	redhat-logos-httpd	redhat-release
redhat-release-eula	redhat-rpm-config	rhn-client-tools	rng-tools
rootfiles	rpcbind	rpm	rpm-build-libs
rpm-libs	rpm-plugin-selinux	rpm-plugin-systemd-inhibit	rsync
rsyslog	rsyslog-gnutls	runc	rust-srpm-macros

S

satyr	sed	selinux-policy	selinux-policy-targeted
sendmail	setools-console	setup	sg3_utils-libs
sgml-common	shadow-utils	shared-mime-info	shim-x64
slang	snappy	sqlite	sqlite-libs
squashfs-tools	sssd-client	strace	subscription-manager
subscription-manager-rhsm-certificates	sudo	systemd	systemd-libs
systemd-libs	systemd-pam	systemd-udev	

T

tar	tcl	tcp_wrappers	tcp_wrappers-libs
teamd	time	timedatex	tmpwatch
tpm2-abrmd	tpm2-abrmd-selinux	tpm2-tools	tpm2-tss
traceroute	trousers	trousers-lib	tuned
tzdata			

U

udisks2	unzip	usbutils	usermode
ustr	util-linux	util-linux-user	uuid

V

vim-minimal	virt-what	volume_key-libs	

W

webhelp-CM-en	webrtc-audio-processing	wget	which
wireshark-cli	words	wpa_supplicant	

X

xcb-util	xcb-util-image	xcb-util-keysyms	xcb-util-renderutil
xcb-util-wm	xdelta	xdg-utils	xfsprogs
xkeyboard-config	xml-common	xmlsec1	xmlsec1-openssl
xz	xz-libs		

Y

yum

Z

zip	zlib	zlib-devel	

Appendix E: Avaya root certificate

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

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

Appendix F: Configuring PuTTY

Converting the *.pem file to the *.ppk format

Before you begin

Download the PuTTYGen software.

Procedure

1. Double-click the downloaded `puttygen.exe` file.
2. In the PuTTY Key Generator dialog box, click **Conversions** > **Import key**.
3. On Load private key, select a `.pem` file from your local computer, and click **Open**.

   The system displays the key in the **Key** section.
4. Click **Generate**.

   The system takes a few minutes.
5. Click **Save private key**.

Configuring PuTTY for an SSH session

Before you begin

Convert the `*.pem` file to the `*.ppk` format.

Procedure

1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click **Connections** > **SSH** > **Auth**.
3. In the **Authentication parameters** section, click **Browse**.
4. On **Select a private key**, select a `.ppk` file from your local computer, and click **Open**.

Signing in to the Amazon EC2 virtual server instance

Before you begin

- Convert the `*.pem` file to the `*.ppk` format.
- Configure PuTTY for an SSH session

Procedure

1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click **Session**.
3. In **Host Name (or IP Address)**, type `admin@<IP_Address>`, where `<IP_Address>` is the IP address of the Amazon EC2 virtual server instance.
4. Click **Open**.

Identifying the SSH user name of the RHEL instance on AWS

About this task

You will require the user name to login to the RHEL instance. This is applicable for software-only deployments.

Before you begin

Create RHEL instance on Amazon Web Services.

Procedure

1. Log on to the Amazon Web Services management console.
2. Click **Servers** > **EC2**.
3. In the right-pane, select the RHEL instance you created.
4. On the top of the page, click **Actions** > **Connect**.

   In the page that opens, under the **Example**, user name of the RHEL instance appears. For example: **`ssh -i "<Key_Pair.pem>" abc-user@<IP address>`**. In this example, “abc-user” is the user name to login to the RHEL instance using SSH.

Appendix G: Creating RHEL virtual machine on Nutanix

Uploading the RHEL ISO to Nutanix server

About this task

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

Note:

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

Procedure

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

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

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

Next steps

Installing RHEL on Nutanix 6.5 and later.

Installing RHEL on the Nutanix server

Before you begin

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

Procedure

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

   For more information about the required CPU, see footprint profile on page 22.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.

   For more information about the required resources, see footprint profile on page 22.
7. Under **Boot Configuration**, select **UEFI**.
8. Under **Disks**, click the Edit icon for the CD-ROM disk type, and do the following:
   a. In the **Type** field, ensure **CD-ROM** is displayed.
   b. In the **Operation** field, select **Clone from Image Service**.
   c. In the **Bus Type** field, Avaya recommends selecting **IDE**.
   d. In the **Image** field, select the RHEL ISO Image.
   e. Click **Update**.

   The CD-ROM and the disk size are displayed.

   Communication Manager requires 64 GiB of hard disk. For more information see footprint profile on page 22.
9. Click **Add New Disk** next to **Disks**, and do the following:
   a. In the **Type** field, select Disk.
   b. In the **Operations** field, select **Allocate on Storage Container**.
   c. In the **Bus Type** field, select the same bus type which you selected while updating the disk.
   d. In the **Storage Container** field, select the appropriate storage container.
   e. In the **Size** field, enter the required GiB size.
   f. Click **Add**.

10. Under **Network Adapters (NIC)**, do the following:
    a. Click **Add New NIC** to add a Network Interface Card (NIC).
    b. In the **Create NIC** window, select the **Subnet Name**.
    c. In the **Network Connection State** field, select **Connected**.
    d. Click **Add**.
    e. To add multiple NICs, repeat 10.a to 10.d.

    Note:

    - Simplex Communication Manager requires two NICs
      - NIC1 is for the Public IP address
      - NIC2 is for the Out of Band Management
    - Duplex Communication Manager requires three NICs
      - NIC1 is for the Public IP address
      - NIC2 is for the duplication network
      - NIC3 is for the Out of Band Management
11. Under **VM Host Affinity**, click **Set Affinity** and do the following:
    a. In the **Set VM Host Affinity** window, select the hosts.

       Select multiple hosts to ensure one node (virtual machine) runs in case another node fails.
    b. Click **Save**.

    After the successful creation of virtual machine, virtual machine appears in the VM page.
12. Select the newly created VM and click **Power On**.
13. Click **Launch Console**.

    Note:

    The **Launch Console** button is enabled only when the virtual machine is Powered On.

    After the RHEL boots, Red Hat Enterprise Linux 8.10 welcome screen appears.
14. Click **Continue**.
15. In the **Installation Summary** screen, under **LOCALIZATION**, click **Language Support** to select the supported language.
16. Click **Time & Date** to set the required timezone.
17. Under **SOFTWARE**, click **Software Selection**.
18. Select **Minimal Install** and then click **Done**.

19. Under **SYSTEM**, click **Installation Destination** and do the following:
    a. Under **Storage Configuration**, select the **Custom** radio button and click **Done**.
    b. In the **Manual Partitioning** window, set the partitioning as required.

       For information on disk partitions and size, see Disk Partitioning on page 40.
    c. Click the **+** icon to create a new mount point.
    d. Select the available partition from the **Mount Point** drop-down menu. To add custom partitions, type the required partition name. For eg:`/etc/opt/defty`.
    e. Enter the capacity in GiB in the **Desired Capacity** field and then click **Add Mount Point**.
    f. In the **Manual Partitioning** window, click **Done**.
    g. In the **Summary of Changes** window, click **Accept Changes**.
    h. Click **Done**.
20. Click **Network & Host Name** and do the following:
    a. Enter a name in the **Host Name** field and click **Apply**.
    b. To configure the IP, click **Configure**.
    c. Click **IPV4 Settings** and select the required option from the **Method** drop-down menu.
    d. Click **Done**.
21. Under **USER SETTINGS**, click **Root Password**.

    In the **Root Password** window, set a password for the root user and then click **Done**.
22. Click **User Creation** and in the Create User window, enter the details and click **Done**.
23. Click **Begin Installation**.

    The RHEL virtual machine is installed on the Nutanix 6.5 server and later.
24. Click **Reboot System** to reboot the RHEL virtual machine.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W