Deploying Avaya Call Management System

Release 19.2
Issue 1
March 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Hosted Service

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

Licenses

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

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

License type(s)

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use

Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying a new Avaya Call Management System (CMS) server.

Note:

If you are deploying CMS on Amazon Web Services (AWS), you must use the procedures found in *Deploying Avaya Call Management System on Amazon Web Services*.

If you are upgrading an existing CMS server, you must use the procedures found in *Upgrading Avaya Call Management System*.

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

This document includes a description of virtualization architecture, how to plan for the deployment, a checklist of configuration data you must get, how to deploy the OVA, how to verify the installation, and procedures for configuring the CMS software.

The primary audience for this document is anyone who installs, upgrades, and configures CMS at a customer site. The audience includes implementation engineers, field technicians, business partners, solution providers, and customers.

Chapter 2: Virtualized environment architecture overview

Avaya Customer Experience Virtualized Environment overview

Avaya Customer Experience Virtualized Environment integrates Avaya contact center applications with VMware virtualized server architecture.

Avaya Customer Experience Virtualized Environment provides the following benefits:

- Simplifies IT management by providing common software administration and maintenance
- Requires fewer servers and racks which reduces the footprint
- Lowers power consumption and cooling requirements
- Enables capital equipment cost savings
- Lowers operational expenses
- Uses standard operating procedures for both Avaya and non-Avaya products
- Allows customers to deploy Avaya products in a virtualized environment on customer-specified servers and hardware.
- Allows businesses can scale rapidly to accommodate growth and to respond to changing business requirements.

For existing customers who have a VMware IT infrastructure, Avaya Customer Experience Virtualized Environment allows upgrading to the next release level of collaboration using its own VMware infrastructure.

The Avaya Customer Experience Virtualized Environment project is only for VMware and is not intended to include any other industry hypervisor.

Note:

This document uses the following terms, and at times, uses the terms interchangeably:

- Server and host
- Reservations and configuration values

Deployment of customer-provided hardware

Deployment into the blade, cluster, and server is managed by vCenter Server and vSphere Client.

The customer provides the servers and the VMware infrastructure including the VMware licenses.

Deployment of Avaya-provided Avaya Solutions Platform hardware

The Avaya-provided Avaya Solutions Platform 130 Appliance hardware is delivered to the customer site. The servers contain preloaded VMware ESXi and the RHEL operating system.

Software delivery

The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS). Each OVA contains the following components:

- the application software and operating system.
- preset configuration details for
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Patches and upgrades

A minimum patch level can be required for each supported application. See the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx for more information regarding the application patch requirements.

Important:

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

Performance and capacities

The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

Modifying these values can have a direct impact on the performance, capacity, and stability of the virtual machine. It is the responsibility of the customer to understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) may not be able to assist in fully resolving a problem if the resource allocation has been changed for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

Virtualized components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.

Table continues…

Software component	Description
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface. The installable vSphere Client is not available in vSphere 6.5 and later releases.
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available in vSphere 6.0 or later. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.

Functional differences when installing CMS in a virtualized environment

When deploying CMS in a virtualized environment, it operates almost identically as a CMS deployed on a traditional hardware server provided by Avaya using the Linux operating system. This section describes a few of the functional areas that are different when deploying CMS in a virtualized environment.

Hardware

CMS supports both customer-provided VMware servers or Avaya-provided Avaya Solutions Platform 130 Appliance VMware servers.

Software media

You must download an OVA file to deploy CMS in a virtualized environment. You do not receive a software disc with the OVA file, operating system software, or CMS software. The OVA file contains the operating system and a specific CMS load. Because you do not receive a software disc, you must make a backup copy of the OVA file in the event you must restore the system. Store the backup copy of the OVA file in a safe location so you can get it quickly if you must restore your system.

Chapter 3: Planning an OVA deployment

About planning an OVA deployment

This chapter provides planning information for the deployment of CMS on VMware-based servers. You can deploy the CMS OVA on either a customer-provided VMware system or on an Avaya Solutions Platform 130 Appliance server.

Note:

The profile of the Avaya Solutions Platform 130 Appliance hardware server you install depends on the sizing tool specification. You must determine the configuration size before starting the OVA deployment because the configuration is based on whether the system is small, medium, or large.

Planning checklist

Ensure that the following activities are complete before deploying the virtual appliance:

Action	Notes	✔
Assess the vSphere Infrastructure resource requirements.	Key factors are: • CPU usage • Memory usage • Storage requirements • Network usage • Supported capacity	
Coordinate deployment activities with service providers.		
Buy all required VMware licenses and make all OVA files accessible.	You must separately license each CMS instance, that is, each installation of an OVA. To install multiple instances of CMS, customers or business partners must order a separate CMS license for each instance.	

Table continues…

Action	Notes	✔
Get the WebLM license server details and install the CMS license.	Avaya products use a Web-based License Manager (WebLM) Release 8.0 or later to manage product licenses obtained using the Avaya Product Licensing and Delivery System (PLDS). For more information, see Installing a license file on a WebLM server on page 23	
Buy and install all required hardware.		
Plan and resource all staging and verification activities.		

Note:

You can deploy a configuration that consists of a mixture of CMS servers hosted on VMware platforms and CMS servers hosted on non-VMware platforms.

Deployment guidelines

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

Important:

The values for performance, occupancy, and usage can vary. However, a virtual machine might run at 50% occupancy. If the CPU occupancy exceeds 60% or the CMS real time report mismatches the refresh rates, you can experience performance issues.

Supported hardware for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see https://www.vmware.com/guides.html.

CMS virtualized environment configurations

When deploying CMS in a virtualized environment, you can configure your deployment as a small, medium, or large configuration. The medium configuration is the default configuration. Contact Avaya engineering support to determine which configuration you should install.

High Availability for customer-provided VMware

High Availability (HA) CMS and Survivable CMS are Avaya product offers that are different from VMware vSphere High Availability. Contact your Avaya account team to discuss the deployment options for HA CMS and Survivable CMS.

VMware vSphere HA is a specific approach to VMware deployment. Customers implement HA in a specific VMware environment.

HA CMS and Survivable CMS

Avaya offers an HA CMS package and a Survivable CMS package. With HA CMS, you deploy two CMS servers and provision the systems to both receive the same call data from the same Communication Manager system. The deployment of two CMS servers provides reliability and duplication of ACD call data across both systems for better reliability if the network fails or a server fails.

The Survivable CMS option expands reliability by providing data collection from the Communication Manager Survivable Core and Survivable Remote technology. Survivable CMS has two options. There is a Dual Role CMS option where the HA CMS supports a connection from the Communication Manager system and the Survivable Core or Survivable Remote, and the option for a separate Survivable CMS where only the Survivable Core or Survivable Remote connects to a Survivable CMS. The deployment of the Survivability option allows users to continue working if the main site is not operational because of network failures or server failures.

To have multiple CMS servers in an HA CMS, Survivable CMS, or an HA CMS and Survivable CMS combination deployment when using VMware, you must deploy separate CMS OVA files for each CMS. The reason you need separate OVA files is because all CMS virtual machines must be provisioned as active, licensed systems.

In addition to redundancy of ACD data provided by HA CMS or the resiliency of data provided by Survivable CMS, Avaya requires a feature that synchronizes the administrative data from a primary CMS to the HA CMS or Survivable CMS deployment. This feature allows all systems to remain synchronized with up-to-date administrative data.

Contact your Avaya account team for more information about HA CMS and Survivable CMS.

VMware vSphere HA

VMware vSphere HA provides automatic detection of hardware failures, server failures, and operating system failures. If a physical server fails, affected virtual machines restart automatically on another production server that has spare capacity. If an operating system fails, vSphere HA restarts the affected virtual machine on the same server. The restart takes several minutes, but the system does recover.

VMware HA ensures that capacity is always available to restart all virtual machines affected by a server failure. HA continuously and intelligently monitors capacity use and reserves spare capacity to restart virtual machines. VMware HA helps VMware vSphere users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions with suggested steps for correction.

Contact your Avaya account team for more information about HA CMS and Survivable CMS.

CMS software requirements

All CMS releases support deployments on VMware.

Avaya packages the CMS VMware environment as a virtual appliance ready for deployment on VMware-certified hardware.

VMware software requirements

CMS supports the following VMware software versions:

- VMware vSphere ESXi 6.5
- VMware vSphere ESXi 6.7
- VMware vSphere ESXi 7.0
- VMware vCenter Server 6.5
- VMware vCenter Server 6.7
- VMware vCenter Server 7.0

Important:

VMware vSphere 5.0, 5.1, 5.5, and 6.0, and VMware vCenter 5.0, 5.1, 5.5, and 6.0 are only supported by permissive use agreement with Avaya.

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

Virtual machine resource requirements and average utilization

Before deploying the CMS virtual machine, ensure that the host can support the configuration you want. After deployment and during normal operation, monitor your resource use to ensure that the proper level of resources remains available.

Important:

Customers that deploy an OVA on their own VMware systems can initially choose to start with the minimum memory allocation, minimum memory reservation allocation, and minimum disk space. However, to maintain support from Avaya, Avaya might require you to later increase the memory allocations (to no more than the recommended maximum value) if Avaya finds that problems related to memory usage occur and cause failures on the CMS.

Minimum required resources for configurations

VMware resource	Small configuration	Medium configuration	Large configuration	Notes
vCPU Cores (CPU)	2	8	16	The number of single core virtual CPUs.
Cores per Socket	2	8	16	The number of CPUs per socket. All cores are assigned to one (1) socket. Therefore, the number of vCPU Cores are the number of logical CPUs.
vCPU reservation	1,200 MHz	4,800 MHz	9,600 MHz	Guaranteed CPU allocation: 25% of vCPU capacity. Calculation: vCPUs x processor clock speed (2400Mhz)/4
Minimum CPU speed	2.1 GHz Xeon E5620 or better, 2.4 GHz recommended	2.1 GHz Xeon E5620 or better, 2.4 GHz recommended	2.1 GHz Xeon E5620 or better, 2.4 GHz recommended	2.1 GHz is supported with a 10% reduction in stated capacities. For capacity details, see *Avaya Call Management System Overview and Specification*.
Memory	8 GB Customer-provided VMware minimum is 4 GB	32 GB Customer-provided VMware minimum is 16 GB	64 GB Customer-provided VMware minimum is 16 GB	The memory size represents the maximum that a CMS deployment might consume. The medium and large configuration memory sizes match real hardware machines. The real hardware memory configuration considers future memory growth.

Table continues…

VMware resource	Small configuration	Medium configuration	Large configuration	Notes
Memory reservation	8,192 MB Customer-provided VMware minimum is 4,096 MB	32,768 MB Customer-provided VMware minimum is 16,384 MB	65,536 MB Customer-provided VMware minimum is 16,384 MB	These are the recommended values for Memory Reservation for both the Avaya Solutions Platform 130 Appliance servers and a customer-provided server. If the memory is not reserved and there is contention (with other VMware applications) for additional memory resource, sufficient memory may not be available resulting in CMS failure. Avaya might require you to increase your memory allocations to no more than the recommended maximum value if testing finds that your system capacity requirements have increased and that problems related to memory usage occur.
Storage	800 GB	1,200 GB	1,800 GB	If the recommended storage value on the medium and large configurations is not administered, sufficient storage may not be available resulting in CMS failure. **Note:** For medium and large configurations, you will configure two disks. Follow the procedures given in “Configuring the virtual machine for different configuration sizes”.
IOPS	200	300	600	The IOPS data is based on the real CMS hardware machines with 50% read and 50% write.
Shared NICs	Two @ 1000 Mbps	Two @ 1000 Mbps	Two @ 1000 Mbps	A typical CMS deployment only requires two Ethernet ports, but many hardware options provide a four-port NIC.

The OVA contains many of the virtual machine resource requirements, such as vCPU reservation and memory reservation. The target virtual machine confirms that the required resources in the OVA are available before deploying the OVA.

Caution:

Adhere to the resource specification mentioned in the above table, because any changes in the allocated resources can impact the performance, capacity, and stability of the CMS virtual machine. To run at full capacity, you must meet these resource size requirements. Removing or downsizing the reserved space can put this requirement at risk. Any deviation in the requirements is at customer’s own risk.

Average resource and network utilization for standard configurations

Average resource usage	Small configuration	Medium configuration	Large configuration	Notes
CPU consumed	600 MHz	2 GHz	8 GHz	
Memory consumed	500 MB	2 GB	4 GB	
Network consumed	0.252 Mbps	0.512 Mbps	1.696 Mbps	
IOPS	12	18	28	IOPS is higher during nightly summarization.

Requirements for expanding large configurations on customer-provided VMware

To accommodate CMS deployments that require larger databases, you must increase the amount of disk space on the virtual machine. Use the following table to determine the amount of disk space required by the database to support a larger number of agent skill pairs at interval lengths of 15 or 30 minutes.

Note:

The values in the following table assume 31 days of interval storage, five years of daily storage (1825 days), and three agent shifts every 24 hours when you have one time zone. You can optionally administer a second time zone for an ACD.

Do the following procedure to get space estimates:

1. Log on to the CMS server as `cms`.
2. Run the **`cms`** command.
3. Navigate to **System Setup** > **Data Storage Allocation** and **System Setup** > **Free Space Allocation** to get space estimates.

Agent skill pairs	200,000		400,000		600,000		800,000	
Interval length (minutes)	15	30	15	30	15	30	15	30
Minimum virtual machine disk size (TB)	1.8	1.2	2.2	1.9	2.9	2.6	3.8	3.3

For that second time zone, the Free Space Allocation feature automatically accounts for the second time zone. This is also true with tenancy. For more information, see *About time zone archiving with additional time zones* in *Maintaining and Troubleshooting Avaya Call Management System* and *Free Space Allocation* in *Administering Avaya Call Management System*.

Hyper-threading

Some confusion can arise in relation to the processor core count on systems that have hyper-threading enabled CPUs where the logical core count increases above the physical core count, usually by a factor of two.

For Avaya contact center deployments, only the physical cores count towards the total number of processor cores on an ESXi host that can be assigned as vCPUs.

Hyper-threading is supported enabled or disabled on CPU types that offer the feature. If hyper-threading is enabled, the additional logical cores do not increase the host's number of vCPUs available for provisioning.

Testing conducted on hosts with hyper-threading enabled concluded that scheduling problems can occur when provisioning vCPUs counts greater than the number of physical cores on the host resulting in a degradation of performance of the contact center applications, for example, slower call setup times and degraded media quality.

Capacities

Important:

Use this table to determine the configuration you must use for a deployment. You must select the size that provides the capacities you require. If any capacity requires a larger configuration, you must go to that larger configuration. For example, if you only need 100,000 agent skill pairs but your peak busy-hour call volume is 200,000, you must select the medium configuration.

Parameter	Small	Medium	Large
Peak busy-hour call volume	30,000	200,000	400,000
Concurrent CMS Supervisor sessions[1]	50	200	1,600[2]
Concurrent agents	500	5,000	10,000
Third-party software	3	5	7
Agent skill pairs	100,000	200,000	800,000[3]
Reports per CMS Supervisor session	3	5	10
Report elements	5	5	12
Percentage of supervisors that can run reports with a three-second refresh rate	10%	50%	100%
Active agent traces	250	1,000	5,000
Internal Call History (ICH) records	4,000 per 20 minutes	4,000 per 20 minutes	4,000 per 20 minutes
External Call History (ECH) records	10,000 per 20 minutes	60,000 per 20 minutes	300,000 per 20 minutes

[1] This value is the total number of active CMS Supervisor PC Client and Web Client sessions.
[2] Of the 1600 sessions supported, only 800 can be CMS Supervisor Web Client sessions
[3] Supporting 800,000 agent skill pairs requires greatly increased disk space for interval data. Customers should create up to 8 additional disk volumes.

Customer configuration data worksheets

The following worksheet identifies the key customer configuration information that you must enter when deploying the OVA file. Plan your configuration data before you begin the deployment.

Parameter	Your value
Location of OVA template file on your computer	
Virtual machine template name	
Virtual machine location	
Destination storage location for virtual machine files	
Disk format to store the virtual disks	Thick Provision

The following worksheet identifies the key customer networking information that you must enter when you run the **`/cms/toolsbin/netconfig`** command.

Parameter	Example	Your value
Network interface name	eth0	
Host name for the CMS server. Use only the short host name, not the FQDN. The host name cannot have upper-case letters. **Important:** The CMS backup process automatically assigns time-stamped file names that truncate the CMS server host name if the host name is longer than 15 characters. To avoid confusion between the backup files for multiple CMS servers, do not use the same first 15 characters for a host name when you have multiple CMS servers in your deployment.	vm_cms1	
Domain name	CompanyName.com	
IP address	123.45.67.89	
Netmask	255.255.255.0	
Default gateway IP address	123.45.67.254	
DNS IP addresses, up to 3, separated with a space	123.1.0.1 123.1.0.2 123.1.0.3	
DNS search domains separated with a space	AltCompanyName.com OtherCompanyName.com	

Chapter 4: Deploying CMS software using an OVA file

Deploying CMS software checklist

Action	Notes	✔
Activate the license for the CMS server.	Activating the license for a CMS server on page 21	
Install the license file on the WebLM server.	Installing a license file on a WebLM server on page 23	
Download the OVA software.	Download the software from the Avaya PLDS website at https://plds.avaya.com. For more information, see Downloading software from PLDS on page 24.	
Deploy the OVA software.	For more information, see Deploying the OVA on page 25.	

Deployment of cloned and copied OVAs

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

Activating the license for a CMS server

About this task

Important:

Each CMS deployment must have its own license file on a WebLM Release 8.0 or later server and must use Centralized Licensing. Enterprise licensing is not supported for CMS. That is, multiple CMS deployments cannot share one license file.

Before you begin

Get the following information:

- SAP order number
- WebLM server host ID

Note:

The SAP order number and the WebLM server host ID must be listed under the same Company ID.

Procedure

1. In a browser window, navigate to the PLDS site:

   https://plds.avaya.com

2. Log on to PLDS using your customer ID and password.
3. Navigate to **Assets** > **View Entitlements**.

   PLDS displays the Search Entitlements screen.
4. Search for your license entitlement using one of the following criteria:
   - SAP order number
   - Sold to number
   - License activation code

   You can also use **Advanced Search** to find a license entitlement.
5. Click **Search Entitlements**.

   PLDS displays the known license entitlements based on the search criteria.
6. For the customer's entitlement record, click **Options** > **Activate**.

   PLDS displays a list of possible entitlements.
7. Select the entitlement for CMS release for which you are installing or upgrading.
8. Click **Activate**.

   PLDS displays the Search License Hosts screen. The available license hosts for the Company ID are displayed on this screen.

   Note:

   You can also download a license file and install the file manually. For more information, see Installing a license file on a WebLM server on page 23.
9. Select one of the displayed license hosts or create a new host by clicking **Add a License Host**.
10. Click **Next**.

    PLDS displays a registration summary screen.

11. Click **Next**.

    PLDS displays the Activate Entitlements screen.

12. Select the quantity of each entitlement you want to activate.
13. Click **Next**.
14. Add notes for the activation, if needed.
15. Click **Finish**.

Installing a license file on a WebLM server

About this task

Avaya products use WebLM Release 8.0 or later to manage product licenses obtained using PLDS. For CMS licensing, the customer must use either a standalone WebLM server or have the WebLM server installed on a coresident Avaya product, such as Avaya Aura® System Manager.

Licenses installed for WebLM must support SHA256 digital signatures and a 14-character host ID.

Important:

You must use Centralized Licensing when licensing CMS. Enterprise licensing is not supported for CMS. That is, multiple CMS deployments cannot share one license file. After enabling Centralized Licensing, you must assign every license file to the license ID in WebLM.

For more information about installing license files, see the following documents:

- *Administering Avaya Aura® System Manager*
- *Administering standalone Avaya WebLM*

Before you begin

Ensure that the XML license file is present in the computer.

Use the uninstall functionality of WebLM to remove any existing license file from the WebLM server before you install a new license file. The system displays an error message if an older license file is still available. For a centralized license file, the system automatically overwrites the older license file during installation. If you experience problems while installing the license file, see “License file installation errors” in *Administering standalone Avaya WebLM*.

Procedure

1. Log on to the standalone WebLM web console or the System Manager console with administrator privilege credentials.
2. In the navigation pane, click **Install license**.
3. On the Install license page, click **Choose File** and browse to the directory of the XML license file that you saved on your computer.
4. Read the terms and conditions and click **Accept the License Terms & Conditions**.

5. Click **Install**.

   WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as the digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file. Another error could be caused by the current capacity use exceeds the capacity in the installed license.

6. Enable Centralized Licensing as describe in WebLM documentation.

   With Centralized Licensing, you must assign every license file to the license ID in WebLM.

7. Click **New**.
8. Enter a name you want to assign to that CMS.
9. Select the license file you want to associate with that CMS.

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **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. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
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.

Deploying the OVA

CMS supports the following VMware deployment options:

- Deploying the OVA on customer-provided VMware servers using vSphere.
- Deploying the OVA on Avaya Solutions Platform 130 Appliance VMware servers using ESXi.

Related links

[Deploying the OVA on a customer-provided VMware server](#) on page 25
[Deploying the OVA on an Avaya Solutions Platform server](#) on page 27

Deploying the OVA on a customer-provided VMware server

About this task

Note:

Based on the vSphere version, you might observe minor differences in the interface.

Before you begin

Download the OVA from PLDS and deploy the OVA on the VMware server. Note down the folder and file name.

Determine the web browser. VMware recommends using Google Chrome or Mozilla Firefox.

Important:

Customers that deploy an OVA on their own VMware systems can initially choose to start with the minimum memory allocation, minimum memory reservation allocation, and minimum disk space. However, to maintain support from Avaya, Avaya might require you to later increase the memory allocations (to no more than the recommended maximum value) if Avaya finds that problems related to memory usage occur and cause failures on the CMS.

Important:

You must separately license each CMS instance, that is, each installation of OVA. To install multiple instances of CMS, customers or business partners must order a separate CMS license for each instance.

Procedure

1. To start the vSphere client software, do one of the following:

   - In your web browser, enter `https://<hostname>.company.com/vsphere-client/?csp`.
   - In your web browser, enter `https://<hostname>/ui/#/login`.

2. In the **User Name** field, enter the vCenter Single Sign On user name that has permissions on vCenter Server.
3. In the **Password** field, enter the password.

4. Click **Login**.
5. If you see a warning message on untrusted SSL certificate, select the appropriate action based on your security policy based on the following security policy:
   - To ignore the security for this login session only, click **Ignore**.
   - To ignore the security warning for this login session and install the default certificate, select **Install this certificate and do not display any security warnings for this server**, and click **Ignore**.

     Select this option only if you do experience any security problem in the default certificate in your environment.
   - To install a signed certificate before proceeding, click **Cancel** and ensure that thesigned certificate is installed on the vCenter Server system before you attempt to connect again.
6. In the Home navigation pane, click **Hosts and Clusters**.
7. In the Host and Clusters tree, select an ESXi host where you want to deploy the OVA.
8. Select **Actions**, and then click **Deploy OVF Template**.
9. In the Deploy OVF Template window, do the following steps:
   a. Select **Local File**, and then click **Browse**.
   b. Browse to the location of the CMS OVA file, select the OVA file, and then click **Open**.
   c. Click **Next**.
   d. In the Select a name and folder window, enter the virtual machine name and click **Next**.
   e. Select the destination compute resource and click **Next**.
   f. In the Review Details window, verify the details of the OVA file, including the CMS version number, and then click **Next**.
10. In the End User License Agreement window, review the license agreement.
11. In the End User License Agreement window, click **Accept** and click **Next**.
12. From the **Select virtual disk format** drop-down list, select `Thick Provision`.

    Important:

    Customers that deploy an OVA on their own VMware systems can initially choose to start with the minimum memory allocation, minimum memory reservation allocation, and minimum disk space. However, to maintain support from Avaya, Avaya might require you to later increase the memory allocations (to no more than the recommended maximum value) if Avaya finds that problems related to memory usage occur and cause failures on the CMS.
13. From the **VM Storage Policy** drop-down list, select `Datastore Default`.
14. From the **Datastore** table, select `Datastore` and click **Next**.

Important:

The data store type that you select must use the VMFS5 format.

15. In the Select networks window, choose a network from the **Destination Network** drop-down, and then click **Next**.
16. In the Ready to Complete window verify the deployment settings, and click **Finish**.

    The Deploy OVF window closes and installation begins, the Recent Tasks pane displays information for tasks **Deploy OVF template and Import OVF package**, the Status column shows the percentage complete, and the installation should last 10-20 minutes depending on the processing power of the server.

Deploying the OVA on an Avaya Solutions Platform server

About this task

Interfaces on different VMware ESXi versions might differ.

Before you begin

Download the file to the computer where you execute the vSphere client. Note down the folder and the file name for the download.

Decide on the browser to use for gaining access to the vSphere client. VMware recommends using Google Chrome or Mozilla Firefox.

Note:

For an Avaya Solutions Platform server, Avaya or Business Partner personnel downloads the OVA from PLDS and deploy the OVA on the Avaya Solutions Platform server.

Procedure

1. On your web browser, type the VMware ESXi URL.
2. In the **User name** field, type your user name.
3. In the **Password** field, type your password.
4. Click **Login**.
5. (Optional) If the VMware ESXi client browser displays a warning message about an untrusted SSL certificate, select the appropriate action based on your security policy below:
   - To ignore the security for this login session only, click **Ignore**.
   - To ignore the security warning for this login session, and install the default certificate so that the warning does not appear again, select **Install this certificate and do not display any security warnings for this server** and click **Ignore**.

     Select this option only if the default certificate does not present a security problem in your environment.

- To install a signed certificate before proceeding, click **Cancel** and ensure that a signed certificate is installed on the vCenter Server system before you attempt to connect again.

6. In the Home navigation pane, click **Host**.
7. In the Host window, select **Create/Register VM**.
8. In the **Select creation type** window, select **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.
9. In the **Select OVF and VMDK files** window, do the following:
   a. Enter the name of the virtual machine.
   b. Select the **Click to select files or drag/drop** check box.
   c. Browse to the location of the CMS OVA file, select the OVA file, click **Open**.
   d. Click **Next**.
10. In the **Select storage** window, click the storage resource and then click **Next**.
11. In the End User License Agreement window, review the license agreement. If you agree to the terms, click **I agree** and then click **Next**.
12. In the Deployment options window, implement the following settings.
    a. From the **Network Mapping** drop-down list, select a subnetwork.
    b. From the **Disk Provisioning** drop-down list, select `Thick`.
    c. Select the **Power on automatically** check box.
    d. Click **Next**.
13. In the Additional settings window, click **Next**.
14. In the Ready to Complete window, verify the deployment settings and then click **Finish**.

    The Deploy OVF window closes and installation begins, the **Recent Tasks** pane displays information for tasks **Upload disk (Target VM name) and Import VApp package**, the Completed column shows the percentage complete, and the installation should last 10-15 minutes depending on the processing power of the server.

Chapter 5: Configuring system features

Configuring system features checklist

Task	Procedure reference	✔
Configure the virtual machine for automatic startup.	Configuring the virtual machine automatic startup settings on VMware on page 30	
Configure the virtual machine as a small, medium, or large configuration.	Configuring the virtual machine as a small configuration on page 30 Configuring the virtual machine as a medium configuration on page 31 Configuring the virtual machine as a large configuration on page 33	
Power up the virtual machine for the first time.	For more information, see Powering up the virtual machine on page 34.	
Verify that CMS is installed.	Verifying that CMS is installed on page 35	
Set the root password.	Setting the root password on page 36	
Configure the system network.	Configuring the system network on page 36	
Configure WebLM, EASG, and initial encryption passphrase rules.	Configuring WebLM, EASG, and the encryption passphrases on page 40	
Install any CMS patches that apply to the CMS release.	Installing CMS patches on page 42	
Update the Linux RPMs for your CMS release, if required.	Updating Linux RPMs on page 43	
Turn on IDS and initialize Informix.	Turning on IDS and adding disk space for medium and large configurations on page 44	
Configure the encryption passphrases.	Configuring the encryption passphrases on page 45	
Verify that the system starts up properly and that you can access the system remotely.	Verifying system startup and remote access on page 48	

Configuring the virtual machine automatic startup settings on VMware

About this task

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

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

Before you begin

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

Procedure

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

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

Configuring the virtual machine for different configuration sizes

Configuring the virtual machine as a small configuration

About this task

Note:

Interfaces on different vSphere versions might differ.

Caution:

Do not change the resource settings, because any changes in the allocated resources can impact the performance, capacity, and stability of the CMS virtual machine. To run at full capacity, you must meet these resource size requirements. Removing or downsizing the

reserved space can put this requirement at risk. Any deviation in the requirements is at customer's own risk.

Before you begin

Turn off the virtual machine.

Procedure

1. On your web browser, type the vSphere vCenter URL and press **Enter**.
2. In the **User name** field, type your user name.
3. In the **Password** field, type your password.
4. Click **Login**.
5. On the vSphere Web Client home page, select one of the following icons:
   - **Hosts and Clusters**
   - **VMs and Templates**
6. In the navigation pane, click **CMS Virtual Machine**.
7. Click **Actions** > **Edit Settings**.
8. In the Edit Settings dialog box, do the following:
   a. In the navigation pane, select **CPU** and click **2**.
   b. In the content pane, select **Cores per Socket** and then click **2**.
   c. In the navigation pane, select **Reservation** and then click **1200 MHz**.
   d. In the content pane, select **Memory** and then click **8 GB**.

      For a customer-provided OVA deployment, the minimum value allowed is 4 GB.
   e. In the navigation pane, select, select **Reservation** and then click **8192 MB**.

      For a customer-provided OVA deployment, the minimum value allowed is 4,096 MB.
   f. Click **OK**.

Configuring the virtual machine as a medium configuration

About this task

Note:

Interfaces on different vSphere versions might differ.

Caution:

Do not change the resource settings, because any changes in the allocated resources can impact the performance, capacity, and stability of the CMS virtual machine. To run at full capacity, you must meet these resource size requirements. Removing or downsizing the

reserved space can put this requirement at risk. Any deviation in the requirements is at customer's own risk.

Important:

Avaya recommends that customers increase this storage space by 400 GB to provide 1,200 GB total disk space. Deviating from this recommendation is at the customer's own risk.

Before you begin

Turn off the virtual machine.

Procedure

1. On your web browser, type the vSphere vCenter URL and press **Enter**.
2. In the **User name** field, enter your user name.
3. In the **Password** field, enter your password.
4. Click **Login**.
5. On the vSphere Web Client home page, select one of the following icons:
   - **Hosts and Clusters**
   - **VMs and Templates**
6. In the navigation pane, click **CMS Virtual Machine**.
7. Click **Actions** > **Edit Settings**.
8. In the Edit Settings dialog box, do the following:
   a. In the navigation pane, select **CPU** and then click **8**.
   b. In the content pane, select **Cores per Socket** and then click **8**.
   c. In the navigation pane, select **Reservation** and then click **4800 MHz**.
   d. In the content pane, select **Memory** and then click **32 GB**.

      For a customer-provided OVA deployment, the minimum value allowed is 16 GB.
   e. Select **Reservation** and then click **32,768 MB**.

      For a customer-provided OVA deployment, the minimum value allowed is 16,384 MB.
   f. Click **OK**.
9. In the vSphere Web Client left pane, select the CMS virtual machine.
10. On the vSphere Client browser, click **Actions** and select **Edit Settings**.

    The system displays the Edit Settings window.
11. In the Edit Settings window, click **ADD NEW DEVICE**.

    The system displays a drop-down list.
12. From the drop-down list, select **Hard Disk**.

13. Select **New Hard disk** and click to expand.
14. Enter 400 in the **Size** field.
15. Click **Disk Provisioning** and select **Thick Provision**.

    Important:

    Customers that deploy an OVA on their own VMware systems can initially choose to start with the minimum memory allocation, minimum memory reservation allocation, and minimum disk space. However, to maintain support from Avaya, Avaya might require you to later increase the memory allocations (to no more than the recommended maximum value) if Avaya finds that problems related to memory usage occur and cause failures on the CMS.
16. Select **OK**.

Configuring the virtual machine as a large configuration

About this task

Note:

Interfaces on different vSphere versions might differ.

Caution:

Do not change the resource settings, because any changes in the allocated resources can impact the performance, capacity, and stability of the CMS virtual machine. To run at full capacity, you must meet these resource size requirements. Removing or downsizing the reserved space can put this requirement at risk. Any deviation in the requirements is at customer's own risk.

Important:

Avaya recommends that customers increase this storage space by 1,000 GB to provide 1,800 GB total disk space. Deviating from this recommendation is at the customer's own risk.

Before you begin

Turn off the virtual machine.

Procedure

1. On your web browser, type the vSphere vCenter URL and press **Enter**.
2. In the **User name** field, type your user name.
3. In the **Password** field, type your password.
4. Click **Login**.
5. On the vSphere Web Client home page, select one of the following icons:
   - **Hosts and Clusters**
   - **VMs and Templates**

6. In the navigation pane, click **CMS Virtual Machine**.
7. Click **Actions** > **Edit Settings**.
8. In the Edit Settings dialog box, do the following:
   a. In the navigation pane, select **CPU** and then click **16**.
   b. In the content pane, select **Cores per Socket** that then click **16**.
   c. In the navigation pane, select **Reservation** and then click **9600 MHz**.
   d. In the content pane, select **Memory** and then click **64 GB**.

      For a customer-provided OVA deployment, the minimum value allowed is 16 GB.
   e. Select **Reservation** and then click **65,536 MB**.

      For a customer-provided OVA deployment, the minimum value allowed is 16,384 MB.
   f. Click **OK**.
9. In the vSphere Web Client left pane, select the CMS virtual machine.
10. On the vSphere Client browser, click **Actions** and select **Edit Settings**.

    The system displays the Edit Settings window.
11. In the Edit Settings window, click **ADD NEW DEVICE**.

    The system displays a drop-down list.
12. From the drop-down list, select **Hard Disk**.
13. Select **New Hard disk** and click to expand.
14. Enter 1000 in the **Size** field.
15. Click **Disk Provisioning** and select **Thick Provision**.

    Important:

    Customers that deploy an OVA on their own VMware systems can initially choose to start with the minimum memory allocation, minimum memory reservation allocation, and minimum disk space. However, to maintain support from Avaya, Avaya might require you to later increase the memory allocations (to no more than the recommended maximum value) if Avaya finds that problems related to memory usage occur and cause failures on the CMS.
16. Select **OK**.

Powering up the virtual machine

About this task

Use this procedure to power up the virtual machine, verify that the OVA deployed successfully, and that the Linux OS boots properly.

Note:

Interfaces on different vSphere versions might differ when you power up the system.

Procedure

1. On your web browser, type the vSphere vCenter URL.

   The system displays the login prompt.
2. In the **User name** field, type your user name.
3. In the **Password** field, type your password.
4. Click **Login**.
5. On the vSphere Web Client home page, click one of the following icons:
   - **Hosts and Clusters**
   - **VMs and Templates**
6. Click one of the following icons:
   - **Launch Web Console**
   - **Launch Remote Console**

   The system displays the following message:

   ```
   Please enter passphrase for disk Virtual_disk (/cms)!:
   ```
7. Enter a default encryption passphrase.

   You can choose from either of the following default encryption passphrases:
   - cmsdefault
   - cmssvcdefault

   The system displays the Linux command prompt.

Verifying that CMS is installed

Procedure

1. Log on to Linux as root. At this point, no password is requested.
2. Enter the following command:

   `rpm -qa cms`

   The system displays the version of the CMS RPM.

Setting the root password

About this task

You must create a password for the root user ID. Record this password for when you turn the system over to the customer.

Security alert:

Remind the customer to change and record the root password after the system is turned over to them.

Procedure

1. Log on as root. You are not prompted for a password.
2. Enter the following command to assign a password to the root user ID:

   `passwd root`

   The system displays the following message:

   ```
   Changing password for user root.
   New password:
   ```

3. Enter the new password for the root user ID.

   The system displays the following message:

   ```
   Retype new password:
   ```

4. Enter the new password for the root user ID a second time.

   The system displays the following message:

   ```
   passwd: all authentication tokens updated successfully.
   ```

Configuring the system network

About this task

This procedure shows example default entries and variables as `<variable>`. The actual information you enter must match your network setup.

Note:

This procedure describes how to configure the system network using IPv4. To configure IPv6 support, see the chapter “Installing and configuring optional software” in *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. Log on to Linux as a root user.

Important:

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Enter the following command:

   /cms/toolsbin/netconfig

   The system displays the following prompt:

```
 WARNING: This tool only supports IPv4

 Enter the network interface name from following name(s): eth0 eth1 eth2 eth3
(default <ethX>)

ENTER>
```

3. Accept the default value `eth0` and press **Enter**.

   The system displays the following prompt:

```
 You have entered [ eth0 ]. Is this correct? (y|n)
```

4. Enter **y**, then press **Enter**.

   The system displays the following prompt:

```
Enter the host name of the CMS system (default <cms_hostname>)

ENTER>
```

5. Enter the host name of the CMS server and press **Enter**.

   Host name for the CMS server. Use only the short host name, not the FQDN. The host name cannot have upper-case letters.

   Important:

   The CMS backup process automatically assigns time-stamped file names that truncate the CMS server host name if the host name is longer than 15 characters. To avoid confusion between the backup files for multiple CMS servers, do not use the same first 15 characters for a host name when you have multiple CMS servers in your deployment.

   The system displays the following prompt:

```
You have entered [ <cms_hostname> ]. Is this correct? (y|n)
```

6. If you have entered the correct host name, enter **y**, then press **Enter**.

   The system displays the following prompt:

```
Enter the domain name of the CMS system (default <cms.domain.com>)

ENTER>
```

7. Enter the domain name of the CMS server and press **Enter**.

The system displays the following prompt:

```
You have entered [ <cms.domain.com> ]. Is this correct? (y|n)
```

8. If you have entered the correct domain name, enter **y**, then press **Enter**.

   The system displays the following prompt:

   ```
   Enter the IP address of the network interface (default <IP_address>)

   ENTER>
   ```

9. Enter the IP address of the CMS server network interface and press **Enter**.

   The system displays the following prompt:

   ```
   You have entered [ <IP_address> ]. Is this correct? (y|n)
   ```

10. If you entered the correct IP address, enter **y**, then press **Enter**.

    The system displays the following prompt:

    ```
    Enter the netmask for the subnet of the network interface (default <netmask_IP>)

    ENTER>
    ```

11. Enter the netmask for the subnet of the CMS server network interface and press **Enter**.

    The system displays the following prompt:

    ```
    You have entered [ <netmask_IP> ]. Is this correct? (y|n)
    ```

12. If you entered the correct IP address, enter **y**, then press **Enter**.

    The system displays the following prompt:

    ```
    Enter the gateway of the CMS system (default <Gateway_IP>)

    ENTER>
    ```

13. Enter the gateway for the CMS server network interface and press **Enter**.

    The system displays the following prompt:

    ```
    You have entered [ <Gateway_IP> ]. Is this correct? (y|n)
    ```

14. If you entered the correct default gateway, enter **y**, then press **Enter**.

    The system displays the following prompt:

    ```
    Enter the DNS server(s) seperated by space (up to three servers) (default
    <Maximum_Three_DNS_Servers_IP>)

    ENTER>
    ```

15. Enter the DNS servers of the CMS server and press **Enter**.

    The system displays the following prompt:

    ```
    You have entered [ <Maximum_Three_DNS_Servers_IP> ]. Is this correct? (y|n)
    ```

16. If you entered the correct DNS server(s), enter **y**, then press **Enter**.

    The system displays the following prompt:

    ```
    Enter the search domains separated by space (default <Search_Domains>, "" for
    none)
    ```

```
ENTER>
```

17. Enter the search domain(s) of the CMS server and press **Enter**.

    The system displays the following prompt:

    ```
    You have entered [ <Search_Domains> ]. Is this correct? (y|n)
    ```

18. If you entered the correct search domains, enter **y**, then press **Enter**.

    The system displays the network configuration options you have entered, for example:

    ```
    Interface: eth0
    CMS Hostname: cmshostname
    Domainname: tmp.domain.com
    CMS IP address: 10.10.10.10
    Netmask: 255.255.255.0
    Gateway: 10.20.30.40
    DNS Server1: 40.30.20.10
    DNS Server2: 100.200.300.400
    DNS Server3:
    Search domains: tmp.domain1.com tmp.domain2.com

    Are the above inputs correct? (y|n)
    ```

19. Perform one of the following actions:

    - If any of the network configuration entries are not correct, enter **n**, then press **Enter**.

      The network configuration process returns to step 3.

    - If the network configuration entries are correct, enter **y**, then press **Enter**.

      The system attempts to bring up the network and if successful, displays a successfully finished message.

      ```
      Bring the network up. Please wait...

      <timestamp> /cms/toolsbin/netconfig successfully finished
      ```

20. If the network configuration was not successful, troubleshoot the network for outages and repeat this procedure. If the network configuration fails again, escalate through normal channels. Test your network settings to ensure that the network settings are working properly using the following commands:

    `ifconfig` <*ethX*> (use your actual Ethernet port)

    `ping` <*system on your local network*>

    Press `Control+C` to exit the ping command.

    Note:

    If the network does not respond, enter **`ifup`** <*ethX*>. If the network still does not respond, repeat this procedure and verify that the values entered are correct.

Configuring WebLM, EASG, and the encryption passphrases

About this task

When you execute the **cmssvc** command for the first time after deploying an OVA, the system does not display the normal CMS Services menu. Instead, the system automatically prompts you to set up the following features:

- WebLM
- Enhanced Access Security Gateway (EASG)
- Encryption passphrases

For WebLM licensing, you have 30 days to provide a valid host name to a WebLM Release 8.0 or later server where the CMS license is installed. If you cannot provide a valid host name, CMS enters the License Error mode for 30 days. After 30 days, CMS enters the License Restricted mode.

The Enhanced Access Security Gateway (EASG) package is integrated into CMS and provides secure authentication and auditing for all remote access into the maintenance ports.

EASG authentication is based on a challenge/response algorithm using a token-based private key-pair cryptographic authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful log on, failed log on, errors, and exceptions.

EASG allows Avaya to control Avaya service engineer privileges when accessing customer products. EASG controls permission levels, such as init, inads, and craft, used by the service engineers.

CMS automatically encrypts the data partitions on the storage disk drive during an OVA deployment. Encryption is not optional — the data partitions on the storage disk drive are always encrypted. A newly-deployed or upgraded system is assigned two default encryption passphrases. You can choose from either of the following default encryption passphrases:

- cmsdefault
- cmssvcdefault

The customer must decide whether they will require an encryption passphrase to be entered on the console after the system has shut down and rebooted. This includes shutdowns for administrative or maintenance procedures such as turning FIPS on and off, CMSADM restore, LAN restore, RPM update, software upgrades, and regular maintenance reboots as recommended by Avaya. It also includes unplanned shutdowns such as a system crash.

Before you begin

Confirm that a valid CMS license has been obtained and installed on the WebLM server used with your deployment. This can be a standalone WebLM server or a System Manager server. When you install a license on the WebLM server, you must map the license by giving it a License ID. This license ID can be any value. For more information, see Standalone WebLM documentation or System Manager WebLM documentation.

Consult with the customer to find out whether they want to require an encryption passphrase after a shutdown and reboot. The customer can always change this decision.

Procedure

1. Log on as root to the CMS server.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Enter:

   cmssvc

   The system displays the following message:

   ```
   cmssvc: Warning IDS off-line. It will take approx 45 seconds to
   start cmssvc. IDS can be turned on with the run_ids command on
   the cmssvc menu.
   You are required to set the WebLM server before proceeding.

   Please enter the hostname for the WebLM license server.
   If you do not have a WebLM license server, enter <CR>:
   ```

3. Enter the host name or IP address of the WebLM server where the CMS license is installed.

4. Press **Enter**.

   If you entered the correct WebLM server host name or IP address, the system displays the following message:

   ```
   Please enter the CMS server license ID: (default: <LicenseID>)
   ```

   Note:

   If you entered an incorrect WebLM server host name or IP address, the system displays the following message:

   ```
   Cannot connect to host: <HostName>

   Do you want to enter another hostname? (y/n):
   ```

   Enter **y** and enter the correct WebLM server host name.

5. Enter the CMS server license ID. This is an ID created when the license was installed on the WebLM server.

6. Press **Enter**.

   The system displays the following message:

   ```
   Web hostname is now authorized as https://<Host_Name or IP_Address>:<Port_Number>/
   WebLM/LicenseServer.

       EASG User Access

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

               In addition to enabling the Avaya Logins, this product should
   ```

```
            be registered with Avaya and technically onboarded for remote
            connectivity and alarming. Please see the Avaya support site
            (support.avaya.com/registration) for additional information for
            registering products and establishing remote access and alarming.

Would you like to enable Avaya EASG? (Recommended)
[yes/no]:
```

7. Do one of the following steps:
   - Enter **yes** to enable EASG. This is the recommended setting. The customer can always disable EASG if required.
   - Enter **no** to keep EASG in the disabled state.

     Note:

     If you do not enable EASG now, you can enable it later using the **cmssvc** command.

```
Avaya EASG is now enabled

Disk encryption is implemented on all CMS data partitions.

Select one of the following:
  1) Require the encryption passphrase to be manually entered on the system
     console whenever the system is rebooted
  2) Enable auto-unlocking to allow the system to use a CMS generated local
     key file to start up unattended without needing to enter the encryption
     passphrase
Enter choice (1-2):
```

8. Select one of the following options based on what the customer wants:
   - Select 1 if the customer wants to require an encryption passphrase after a shutdown and reboot.
   - Select 2 if the customer wants to allow the system to use a CMS-generated local key file to boot up without an encryption passphrase. During deployment, you should select option 2 since you might be rebooting the system a few times. The customer can change this after you have turned the system over to the customer.

Installing CMS patches

About this task

After installing CMS for the first time, download the latest CMS patches and install them on the system. For procedure on installing CMS patches, see *Maintaining and Troubleshooting Avaya Call Management System*.

Updating Linux RPMs

Avaya provides updated Linux RPMs with new CMS releases, be it a major, minor, feature pack, or service pack release. When you install or upgrade to the new release, you follow a procedure to manually update the Linux RPMs.

It is important to update the Linux RPM packages because the updates might contain new Linux operating system updates for security and system operation. Avaya provides the Linux RPM updates on the CMS media used for upgrades. For hardware, it is a software disc. For VMware, it is an ISO image.

Avaya also releases RPM updates outside of normal CMS releases. Those RPM updates are documented in PSN005673u. This PSN describes how to update a CMS release with a new set of Linux RPMs. This PSN will contain specific update instructions for specific CMS releases. You should check the Avaya support site to see if there are any new Linux RPM updates for your release of CMS by searching on PSN005673u.

https://support.avaya.com/

Running the CMS security script

About this task

As part of installing or upgrading CMS software, you must install the CMS security options using the CMS security script **cms_sec**. The security script must be run after you have updated the RHEL RPMs. You can run the security script at any time, but any customer customizations are overwritten.

Important:

You can log in to the console as root only after you run the CMS security script. If you are logging into the system remotely, log on as another user and then use **su - root** to log in as root.

Before you begin

Verify that you are logged in to the system as root.

Procedure

1. Verify the current services running on the system and save the list for comparison with the listing after the security script run. To capture the current services and preserve the output to a file, enter:

   chkconfig --list > /tmp/current_chkconfig.txt

2. Run the security script by entering:

   /storage/cms_dvd/security/cms_sec

The system configures your security settings and displays the following message:

```
Avaya CMS security configuration completed: <date>
```

Note:

If the system displays a configuration failed message, contact your Avaya services representative.

3. To capture the new services and preserve the output to a different file, enter:

   chkconfig --list > /tmp/new_chkconfig.txt

4. Run the following command to check for any services that need to be reenabled:

   diff /tmp/current_chkconfig.txt /tmp/new_chkconfig.txt

5. View the output from the **diff** command and reenable the services that are displayed. To reenable any customer used services, enter:

   diff /tmp/current_chkconfig.txt /tmp/new_chkconfig.txt

   For example:

   chkconfig --level 2345 snmpd on

Turning on IDS and adding disk space for medium and large configurations

Procedure

1. Log on as root.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Enter:

   cmssvc

   The system displays the following menu:

```
Avaya(TM) Call Management System Services Menu

Select a command from the list below.
 1) auth_display   Display feature authorizations
 2) weblm_set      Set up the connection to the WebLM
 3) run_ids        Turn Informix Database on or off
 4) run_cms        Turn Avaya CMS on or off
 5) setup          Set up the initial configuration
 6) swinfo         Display switch information
 7) swsetup        Change switch information
 8) uninstall      Remove the CMS rpm from the machine
 9) patch_rmv      Backout an installed CMS patch
```

```
10) back_all       Backout all installed CMS patches from machine
11) security       Administer CMS security features
Enter choice (1-11) or q to quit:
```

3. Choose the **run_ids** option to turn on the Informix Database Server.

   The system displays the following menu:

```
Select one of the following
  1) Turn on IDS
  2) Turn off IDS
Enter choice (1-2):
```

4. Choose the **Turn on IDS** option.
5. For a medium or large configuration, type the following command to add disk space:

   /opt/informix/bin/dbinit.sh add_disks

   Important:

   Do not run this command on a small configuration.

   Verify that the disk space was added successfully. If the procedure fails, contact Avaya support.

Configuring the encryption passphrases

About this task

CMS automatically encrypts the data partitions on the storage disk drive during an OVA deployment. Encryption is not optional — the data partitions on the storage disk drive are always encrypted. A newly-deployed or upgraded system is assigned two default encryption passphrases. You can choose from either of the following default encryption passphrases:

- cmsdefault
- cmssvcdefault

The customer must decide whether they will require an encryption passphrase to be entered on the console after the system has shut down and rebooted. This includes shutdowns for administrative or maintenance procedures such as turning FIPS on and off, CMSADM restore, LAN restore, RPM update, software upgrades, and regular maintenance reboots as recommended by Avaya. It also includes unplanned shutdowns such as a system crash.

Caution:

If the customer requires an encryption passphrase after a shutdown, that passphrase must be entered on the system console. The passphrase cannot be entered remotely after the system has rebooted. You can work around this requirement by temporarily enabling auto-unlocking before doing the reboot, but you must remember to disable auto-unlocking after the reboot is complete.

Important:

Whether the customer requires the encryption passphrase after a shutdown and reboot, the customer must change the passphrases from the default to passphrases known only to the customer and Avaya services. The customer must record the new encryption passphrases in a safe, secure location.

Before you begin

Consult with the customer to find out whether they want to require an encryption passphrase after a shutdown and reboot. The customer can always change this decision.

Procedure

1. Log on as root.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Enter:

   cmssvc

   The system displays the following menu:

```
Avaya(TM) Call Management System Services Menu

Select a command from the list below.
 1) auth_display   Display feature authorizations
 2) weblm_set      Set up the connection to the WebLM
 3) run_ids        Turn Informix Database on or off
 4) run_cms        Turn Avaya CMS on or off
 5) setup          Set up the initial configuration
 6) swinfo         Display switch information
 7) swsetup        Change switch information
 8) uninstall      Remove the CMS rpm from the machine
 9) patch_rmv      Backout an installed CMS patch
10) back_all       Backout all installed CMS patches from machine
11) security       Administer CMS security features
Enter choice (1-11) or q to quit:
```

3. Enter the number that corresponds to the **security** command.

   The system displays the following menu:

```
Select one of the following:
   1) FIPS 140-2 mode
   2) Firewall
   3) Enhanced Access Security Gateway (EASG)
   4) Disk encryption
Enter choice (1-4) or q to quit:
```

4. Enter the number that corresponds to the **Disk encryption** command.

   The system displays the following menu:

```
Disk encryption auto-unlocking is enabled.

Select one of the following
  1) Change encryption passphrase
  2) Enable auto-unlocking
```

```
  3) Disable auto-unlocking
Enter choice (1-3) or q to quit:
```

5. To change an encryption passphrase, do the following steps:

   Important:

   Whether the customer requires the encryption passphrase after a shutdown and reboot, the customer must change the passphrases from the default to passphrases known only to the customer and Avaya services. The customer must record the new encryption passphrases in a safe, secure location.

   a. Enter the number that corresponds to the **Change encryption passphrase** command.

      The system displays the following message:

      ```
      Select one of the following
        1) Primary encryption passphrase
        2) Secondary encryption passphrase
      Enter choice (1-2) or q to quit:
      ```

   b. Select either the primary or secondary encryption passphrase option.

      The system displays the following message:

      ```
      Enter current encryption passphrase:
      ```

   c. Enter a current encryption passphrase and press **Enter**.

      The system displays the following message:

      ```
      Enter new encryption passphrase:
      ```

   d. Enter the new encryption passphrase and press **Enter**.

      The system displays the following message:

      ```
      Re-enter new encryption passphrase:
      ```

   e. Re-enter the new encryption passphrase and press **Enter**.

      The system displays messages similar to the following example:

      ```
      Changing passphrase for disk partition /dev/sda3 ...
      Changing passphrase for disk partition /dev/sda7 ...
      Changing passphrase for disk partition /dev/sda10 ...
      Changing passphrase for disk partition /dev/sda11 ...
      ```

   f. Repeat these steps for the second passphrase.

6. To enable encryption auto-unlocking, do the following steps:

   a. Enter the number that corresponds to the **Enable auto-unlocking** command.

      The system displays the following message:

      ```
      Enter an existing encryption passphrase:
      ```

   b. Enter the current encryption passphrase and press **Enter**.

      The system displays messages similar to the following example:

      ```
      Adding auto-unlocking key file to partition /dev/sda3 ...
      Adding auto-unlocking key file to partition /dev/sda7 ...
      ```

```
Adding auto-unlocking key file to partition /dev/sda10 ...
Adding auto-unlocking key file to partition /dev/sda11 ...
Changing reboot setting ...

Auto-unlocking enabled successfully.
```

7. To disable encryption auto-unlocking, do the following steps:

   Caution:

   If the customer requires an encryption passphrase after a shutdown, that passphrase must be entered on the system console. The passphrase cannot be entered remotely after the system has rebooted. You can work around this requirement by temporarily enabling auto-unlocking before doing the reboot, but you must remember to disable auto-unlocking after the reboot is complete.

   a. Enter the number that corresponds to the **Disable auto-unlocking** command.

      The system displays the following message:

      ```
      Enter an existing encryption passphrase:
      ```

   b. Enter the current encryption passphrase and press **Enter**.

      The system displays messages similar to the following example:

      ```
      Changing reboot setting ...
      Removing auto-unlocking key file from partition /dev/sda3 ...
      Removing auto-unlocking key file from partition /dev/sda10 ...
      Removing auto-unlocking key file from partition /dev/sda7 ...
      Removing auto-unlocking key file from partition /dev/sda11 ...
      ```

Verifying system startup and remote access

About this task

After you configure the system features, use this task to verify that the system starts up properly and that you can access the system remotely.

Before you begin

If the default passphrases have been changed, get those new passphrases.

Procedure

1. Reboot the system using the following command:

   `shutdown -r now`

   The remote console displays the reboot sequence. If you did not configure encryption auto-unlocking, the system displays the following message:

   ```
   Please enter passphrase for disk Virtual_disk (/cms)!:
   ```

2. Enter a default or new encryption passphrase.

You can choose from either of the following default encryption passphrases:

- cmsdefault
- cmssvcdefault

The system displays the Linux login prompt.

3. Log on to Linux as root.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

4. From another system, verify that you can access the new system using tools such as puTTY or SSH.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

Chapter 6: Configuring CMS features

Configuring CMS features checklist

Task	Procedure reference	✔
Assign passwords for the CMS login IDs.	Assigning passwords to the default CMS login IDs on page 50	
View the CMS authorizations to confirm that your licensed features are authorized.	Viewing CMS authorizations on page 51	
Calculate storage requirements for backups.	Calculating data space requirements for CMSADM backups on page 55 Calculating data space requirements for CMS full maintenance backups on page 56	
Set up the Alarm Origination Manager to report alarms to Avaya support or customer management systems.	Setting up the Alarm Origination Manager on page 58	

Assigning passwords to the default CMS login IDs

Procedure

1. To assign a password for the cms login ID, enter: `passwd cms`

   The system displays the following message:

   ```
   New password:
   ```

2. Enter the password for the cms login ID.

   The system displays the following message:

   ```
   Re-enter new password:
   ```

3. Enter the password for the cms login ID a second time.

   The system displays the following message:

   ```
   passwd: password successfully changed for cms
   ```

4. To assign a password for the cmssvc login ID, enter: `passwd cmssvc`

The system displays the following message:

```
New password
```

5. Enter the password for the cmssvc login ID.

   The system displays the following message:

   ```
   Re-enter new password
   ```

6. Enter the password for the cmssvc login ID a second time.

   The system displays the following message:

   ```
   passwd: password successfully changed for cmssvc
   ```

Viewing CMS authorizations

About this task

This section describes how to view CMS capacities authorized based on the license file and the status of CMS optional feature packages and security settings.

Procedure

1. Enter: `cmssvc`

   The system then displays the Avaya Call Management System Services menu.

2. Enter the number associated with the **auth_display** option.

Activating the CMS Supervisor Web Client software

The CMS Supervisor Web Client software is installed on the same server as the CMS software. The Web Client is browser-based and allows customers to access CMS administration and reports without install client software on your PC. For more information, see *Avaya Call Management System Overview and Specification* and *Avaya CMS Supervisor Clients Installation and Getting Started*.

Related links

Starting the Web Client software on page 52
Managing certificates for Web Client software on page 52
Generating a certificate for the Web Client server on page 53
Installing the root certificate for the Web Client software on page 54

Starting the Web Client software

Procedure

1. Log on as root on the CMS server.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Enter the following command to start the Web Client software:

   cmsweb start

   The system displays the following message:

   ```
   starting cmsweb...
   ```

3. Enter the following command to verify that the correct version of the Web Client software is installed:

   rpm –qa cmsweb

   The system displays a message similar to the following example:

   ```
   cmsweb-R19-web19xx.x.x86_64
   ```

Managing certificates for Web Client software

A security certificate must be installed to encrypt communication between browsers and the Web Client CMS server. When you first install the Web Client package, a self-signed certificate is automatically generated by the installation process based on the host name and domain name of the host server. You can view the URL or Common Name used in this certificate by running the following command:

/opt/cmsweb/bin/showcrt.sh

The URL or Common Name should be used to access the Web Client user interface from a browser. If the URL does not appear correct due to the network and host setup, use the following command to change it:

/opt/cmsweb/bin/chgcrt.sh

This command prompts you for a new URL. The default value for this command is your host name and domain name (if a domain name is configured on your host). Press **Enter** to accept the default or type in your preferred URL.

If you change the Web Client certificate, you must restart the Web Client software on the CMS server to accept the changes. To restart the Web Client software, run the following commands:

cmsweb stop

cmsweb start

Generating a certificate for the Web Client server

Procedure

1. Log on as root on the CMS server.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Use the following command to create a directory to put the certificate:

   mkdir /opt/cmsweb/cert/custom

3. Move to the new directory:

   cd /opt/cmsweb/cert/custom

4. Use the following command to generate a new key and keystore:

   keytool -genkey -alias cmsweb -keyalg RSA -keysize 2048 -keystore cmsweb.jks

   The system prompts you for a keystore password and other information.

5. For the password, enter `cmsweb`. For the first and last name, enter the domain name of the CMS server. For example:

```
Enter keystore password: cmsweb
Re-enter new password: cmsweb
What is your first and last name?
  [Unknown]: company.com
What is the name of your organizational unit?
  [Unknown]: DirectSales
What is the name of your organization?
  [Unknown]: Sales
What is the name of your City or Locality?
  [Unknown]: Buffalo
What is the name of your State or Province?
  [Unknown]: New York
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=company.com, OU=DirectSales, O=Sales, L=Buffalo, ST=New York, C=US correct?
Y

Enter key password for <cmsweb>
        (RETURN if same as keystore password
```

6. Use the following command to generate a certificate request:

   keytool -certreq -keyalg RSA -alias cmsweb -file certreq.csr -keystore cmsweb.jks

7. For the password, enter `cmsweb`.

8. Use the certificate request in file `certreq.csr` to get a certificate from the certificate authority (CA) of your choice.

Installing the root certificate for the Web Client software

About this task

Sometimes the CA also issues an intermediate CA certificate. If the CA issues an intermediate certificate, import the intermediate CA certificate using the steps in this procedure. If you do not have an intermediate certificate, skip those optional steps.

Procedure

1. Copy and paste the root certificate into a file, for example, `cmsweb.crt`.
2. Use the following command to import the certificate:

   `keytool -import -alias cmsweb -keystore cmsweb.jks -trustcacerts -file cmsweb.crt`
3. For the password, enter `cmsweb`.

Note:

Do Steps 4–6 if the intermediate certificates are published and required by the CA.

4. Copy and paste the intermediate certificate into a file, for example, `intermediate.crt`.
5. Use the following command to import the certificate:

   `keytool -import -alias intermediate -keystore cmsweb.jks -trustcacerts -file intermediate.cert`
6. For the password, enter `cmsweb`.
7. Copy and paste the new certificate into a file, for example, `cmsweb.cert`.
8. Use the following command to import the certificate:

   `keytool -import -alias cmsweb -keystore cmsweb.jks -trustcacerts -file cmsweb.cert`
9. For the password, enter `cmsweb`.
10. Use the following command to stop the Web Client software:

    `cmsweb stop`
11. Copy the keystore in the correct location, for example:

    `cp /opt/cmsweb/cert/custom/cmsweb.jks /opt/cmsweb/cert`
12. Use the following command to start the Web Client software:

    `cmsweb start`

Storage requirements for CMS backups

Calculating data space requirements for CMSADM backups

Procedure

1. Log on as root to Linux.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Run the following command:

   df -Th

   The system displays information similar to the following example:

```
Filesystem       Type       Size  Used Avail Use% Mounted on
devtmpfs         devtmpfs   7.8G     0  7.8G   0% /dev
tmpfs            tmpfs      7.8G     0  7.8G   0% /dev/shm
tmpfs            tmpfs      7.8G  113M  7.7G   2% /run
tmpfs            tmpfs      7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/sda2        ext4       9.8G  1.6G  7.7G  18% /
/dev/sda1        ext4       546M  106M  400M  21% /boot
/dev/sda6        ext4        87G  2.7G   80G   4% /storage
/dev/sda9        ext4        16G   45M   15G   1% /tmp
/dev/sda8        ext4        26G  240M   24G   1% /var
/dev/dm-0        ext4        32G   49M   30G   1% /export/home
/dev/dm-1        ext4        12G  1.8G  9.3G  16% /opt
/dev/dm-2        ext4       9.8G  354M  8.9G   4% /cms
tmpfs            tmpfs      1.6G     0  1.6G   0% /run/user/0
cms-store:/store nfs4       2.2T  1.5T  554G  74% /nfsbu
```

3. Add the disk space from the `Used` column for all of the `ext4` filesystems, except for the `/storage` or `/tmp` directories.

   In this example, that would include the following directories:

   - `/`
   - `/boot`
   - `/var`
   - `/export/home`
   - `/opt`
   - `/cms`

4. Calculate the space you need, for example:

Directory	Used space
/	1.6 GB

Table continues…

Directory	Used space
/boot	106 MB
/var	240 MB
/export/home	49 MB
/opt	1.8 GB
/cms	354 MB
TOTAL	4.15 GB

Note:

The **df -Th** command gives a current snapshot of disk space usage of the CMS server. You must run additional checks periodically to see if your storage needs have changed to ensure you have enough backup space.

Calculating data space requirements for CMS full maintenance backups

Procedure

1. Log on as root to Linux.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

2. Set the Informix environment by entering the following command:

   . /opt/informix/bin/setenv

3. Run the following command:

   onstat -d

   The system displays information similar to the following example:

```
IBM Informix Dynamic Server Version 12.10.FC11 -- On-Line -- Up 142 days 18:48:53
-- 8634236 Kbytes

Dbspaces
address          number   flags      fchunk   nchunks  pgsize   flags    owner
name
44c10028         1        0x4030001  1        1        2048     N  BA    informix
rootdbs
462e31f8         2        0x4030001  2        1        2048     N  BA    informix
physdbs
462e3438         3        0x4020001  3        1        2048     N  BA    informix
logdbs
462e3678         4        0x4020001  4        1        8192     N  BA    informix
dbtemp
462e38b8         5        0x4020001  5        1        8192     N  BA    informix
cmsdbs
 5 active, 2047 maximum
```

```
Chunks
address           chunk/dbs     offset      size        free        bpages      flags
pathname
44c10268          1       1     0           128000      107807                  PO-
B-- /cmsdisk
463dc028          2       2     128000      327680      0                       PO-
B-- /cmsdisk
463dd028          3       3     455680      65536       0                       PO-
B-- /cmsdisk
463de028          4       4     521216      655360      655307                  PO-
B-- /cmsdisk
463df028          5       5     3142656     77413632    77290429                PO-
B-- /cmsdisk
 5 active, 32766 maximum

NOTE: The values in the "size" and "free" columns for DBspace chunks are
      displayed in terms of "pgsize" of the DBspace to which they belong.


Expanded chunk capacity mode: always
```

4. Use the output generated from running this command and the formulas at the bottom of the following tables to calculate how much database space is required for a CMS full maintenance backup.

   The data in this table is dynamic, and changes as database space is used.

Platform	pgsize	Full disk size of cmsdbs Dbspace	Total Disk cmsdbs Dbspace (Bytes)	Total Disk cmsdbs Dbspace (rounded in GB)	Total Full Maintenance Backup space Required if cmsdbs Dbspace is full (GB)[4]
Dell R630	8,192	32,861,440	269,200,916,480	250.71	8.36
Dell R730	8,192	179,072,256	1,466,959,921,152	1,366.21	45.54
HP DL380P G9	8,192	179,072,256	1,466,959,921,152	1,366.21	45.54
HP DL20 G9	8,192	43,844,355	359,172,956,160	334.5	11.15

   Bytes to GB conversion factor = 1,073,741,824

   Full Maintenance Backup compression ratio = 30 (approximation)

   Note:

   The **`onstat -d`** command gives a current snapshot of disk space usage of the CMS server. You must run additional checks periodically to see if your storage needs have changed to ensure you have enough backup space.

Example

Dell R630 (300 GB) example:

[4] If ontape is being used for binary backups this value must be multiplied by 30 since ontape does not compress data.

Db spaces address	numbers	flags	fchunk	nchunks	pgsize	flags	owner	name
c64a5358	5	0x60001	5	1	8192	N B	informix	cmsdbs

Chunks address	chunk	dbs	offset	size	free	bpages	flags	pathname
c64a5ac0	5	5	31,426,56	34,679,882	29,584,364		PO-B-	/cmsdis

Full Dbspace size of cmsdbs = ((8,192 * 34,679,882) / 1,073,741,824) = 264.59 GB

Full Dbspace size of cmsdbs available for Full maintenance backups = (((8192 * 34,679,882) / 1,073,741,824) / 30) = 8.82 GB

Space required for backup = (((8,192 * (34,679,882 - 29,584,364)) / 1,073,741,824) / 30) = 14.01 GB

Setting up the Alarm Origination Manager

Use this section to set up the Alarm Origination Manager (AOM) on the CMS server. The aom_tool is used to configure AOM. You can use the AOM feature to enable alarming to Avaya and this capability is available only for CMS servers with a current maintenance agreement in effect. You can optionally use AOM to send SNMP alarms to customer provided Network Management Systems (NMS). You can enable SNMP alarms to a customer provided NMS even if a current Avaya maintenance agreement is not in effect.

Note:

CMS supports only SNMP v3 in this release

Important:

There are multiple phases to completing the AOM configuration. You must configure an Alarm ID, and you must configure an Alarm ID and a Customer ID if SNMP alarming to SAL is intended. To use SNMP, you must configure an SNMP user. Finally, you must configure an Alarm Destination.

Prerequisites

Before you set up AOM, perform the following tasks:

- Obtain an Alarm ID number and Sold To Functional Location (FL) number. You can obtain an Alarm ID by registering the CMS server. You can register a CMS server using the Avaya Global Registration Tool (GRT) tool at https://support.avaya.com/grt. If you cannot register the system using the GRT tool, call 1800-242-2121, extension 15265, for assistance. If the system does not have an Avaya maintenance agreement in effect and you are going to configure optional SNMP alarming in a customer NMS, accept the default values that are pre-populated.

Note:

During AOM configuration, use the Alarm ID referred to here as the Alarm ID and use the Sold To Functional Location (FL) number as the Customer ID.

- Log on as root.

Important:

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **su - root** to log on with root privileges.

Related links

Configuring an Alarm Destination on page 59
Configuring an SNMP User on page 62
Configuring an Alarm ID on page 65
Configuring a Customer ID on page 65
Sending an AOM Test Alarm on page 66
Clearing SNMP Alarms on page 67
CMS SNMP alarm information on page 68
Locating and installing the CMS-MIB.txt file on page 72
Setting up AOM configuration for alarming using Socket/SAL on page 72

Configuring an Alarm Destination

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Configure the Alarm Destination** option, and press **Enter**.

   The system displays the following message:

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

   Note:

   Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the `SNMP/SAL` option, and press **Enter**.

The system displays a list of SNMP configuration options:

```
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q):
```

4. Enter the number associated with the **Add an SNMP connection** option, and press **Enter**.

   The system displays the **Adding an SNMP connection** option followed by an input prompt for destination type:

   ```
   Adding an SNMP connection
   Select a destination type:
   1) SAL
   2) NMS
   Enter choice (1-2):
   ```

5. Enter the number associated with SAL or NMS, and press **Enter**.

   The system displays the input prompt for the destination IP address:

   ```
   What is the destination IP address?
   ```

6. Enter the destination IP address, for example, `192.168.123.256`, and press **Enter**.

   The system displays the input prompt for the port number:

   ```
   What is the destination port number?
   ```

7. Enter the destination port number, for example, `162`, and press **Enter**.

   The system displays the input prompt for the notification type of trap or inform:

   ```
   Select a notification type:
   1) trap
   2) inform
   Enter choice (1-2):
   ```

8. Enter the number associated with the notification type, and press **Enter**.

   Note:

   You must select **Trap as Trap** is the recommended selection. **Inform** is a trap with a receipt acknowledgement.

   The system displays the input prompt for the SNMP user:

   ```
   Select an SNMP user:
   1) cmssnmp
   Enter choice (1-1):
   ```

9. Enter The system displays a list of defined users. Select an SNMP user, and press **Enter**.

   The system displays the input prompt for Alarm ID along with the default Alarm ID value:

   ```
   What is the Alarm ID (10 digit alarm ID)? (default:3000004043)
   ```

10. Enter the Alarm ID or accept the default value, and press **Enter**.

The system displays the input prompt for Customer ID along with the default Customer ID value:

```
What is the Customer ID (10 digit customer code)? (default:0004558769)
```

11. Enter the Customer ID value or accept the default value, and press **Enter**.

    The system displays the input prompt for Customer Name along with the default Customer Name value:

    ```
    What is the Customer Name? (default:Avaya)
    ```

12. Enter the Customer Name or accept the default value, and press **Enter**.

    The system displays the input prompt for running a test alarm:

    ```
    Run a test alarm when done?(y/n)
    ```

13. Enter `y` or `n`, and press **Enter**.

    The system displays the following messages:

    ```
    You have selected to configure AOM using SNMP.

    Add an SNMP Connection

    Destination Type: SAL
    Destination IP: 198.1.1.2
    Destination port: 162
    Notification Type: inform
    User Name: salcmsuser
    Alarm ID: 3000004043
    Customer ID: 0004558769
    Customer NAME: Avaya

    A test alarm will be sent at the end.
    Press [Enter] to continue or [q] to quit
    ```

    Note:

    The SAL SNMP option requires a Notification Type of inform and notify in the `dest.cfg` file.

14. Press **Enter**.

    The system displays the following messages:

    ```
    Configuring dest.cfg
    [started]
    done
    reset AOM
    [started]
    done
    Clearing all current alarms.
    [started]
    done
    Sending test alarm.
    [started]
    done
    done
    Do you want to
    1) Add an SNMP Connection
    2) Delete an SNMP Connection
    3) Modify an SNMP Connection
    ```

```
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q): q
```

15. Enter `q` to quit, and press **Enter**.

    The system displays the following message:

```
Quitting
```

Configuring an SNMP User

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Configure the Alarm Destination** option, and press **Enter**.

   The system displays the Welcome to Avaya CMS Alarm Origination main menu options:

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

   Note:

   Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the **SNMP/SAL** option, and press **Enter**.

   The system displays the list of SNMP configuration options:

```
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q):
```

4. Enter the number associated with the **Add an SNMP User** option, and press **Enter**.

The system displays the input prompt for SNMP user name:

```
Adding an SNMP user
What is the SNMP user name?
```

5. Enter the SNMP user name, and press **Enter**.

   The system displays the **Select the SNMP version** option:

   ```
   Select the SNMP version:
   1) v3
   Enter choice (1-1):
   ```

6. Enter the number associated with the v3 option, and press **Enter**.

   The system displays the **Select the access level** option:

   ```
   Select the access level:
   1) rouser: Read Only
   2) rwuser: Read/Write
   Enter choice (1-2):
   ```

7. Enter the number associated with the level of access to assign to the user, and press **Enter**.

   The system displays the **Select the security level** option based on the FIPS status:

   - If the FIPS mode is off:

     ```
     Select the security level:
     1) noAuthNoPriv: Unauthenticated/Unencrypted (not allowed in FIPS mode)
     2) authNoPriv: Authenticated/Unencrypted (not allowed in FIPS mode)
     3) authPriv: Authenticated/Encrypted
     Enter choice (1-3):
     ```

   - If the FIPS mode is on:

     ```
     Select the security level:
     3) authPriv: Authenticated/Encrypted
     Enter choice (1-1):
     ```

8. Enter the number associated with the level of security to assign to the user, and press **Enter**. .

   The system displays the **Select the authentication protocol option** based on the FIPS status:

   - If the FIPS mode is off:

     ```
     Select the authentication protocol:
     1) MD5 ( not allowed in FIPS mode)
     2) SHA
     Enter choice (1-2):
     ```

   - If the FIPS mode is on:

     ```
     Select the authentication protocol:
     1) SHA
     Enter choice (1-1):
     ```

9. Enter the number associated with the authentication protocol to assign to the user, and press **Enter**.

Note:

Authentication utilizes the defined authentication password to sign the messages that are sent during authentication. The encryption protocol for this can be either MD5 or SHA.

The system displays the authentication password prompt:

```
Enter authentication password (min 8 chars):
```

10. Enter the authentication password to assign to the user, and press **Enter**.

    The system displays the **Select the encryption protocol** option:

```
Select the encryption protocol:
1) AES
2) DES
Enter choice (1-2):
```

11. Enter the number associated with the encryption protocol to assign to the user, and press **Enter**.

    Note:

    Authentication utilizes the defined encryption password to encrypt the data portion of the SNMP messages. The encryption protocol for this may be either AES or DES.

    The system displays the encryption password prompt:

```
Enter encryption password (min 8 chars):
```

12. Enter the encryption password to assign to the user, and press **Enter**.

    The system displays information about the choices entered:

```
CMS was last rebooted 11 day(s) ago.
You have selected to configure AOM using SNMP.
Add an SNMP User
User Name: TestSNMP
SNMP version: v3
SNMP Access Level: rouser
SNMP Security Level: authPriv
SNMP authentication protocol: MD5
SNMP authentication password: ******
SNMP encryption protocol: AES
SNMP encryption password: ******
Press [Enter] to continue or [q] to quit
```

13. Press **Enter** to save the choices displayed, or press `q` to quit. .
14. If you press **Enter**, the system saves the choices and displays the following messages: .

```
Configuring /cms/aom/data/admin/user.cfg
[started]
Done
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
```

```
q) Quit
Enter choice (1-7, q):
```

- To add another user, repeat Steps 3-13.
- To modify a user, enter the number associated with the Modify an SNMP User option, and press **Enter**. Make any desired changes to the configuration of the user.

15. Enter `q` to quit, and press **Enter**.

    The system displays the following message:

```
Quitting
```

Configuring an Alarm ID

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Set a Test Alarm** option, and press **Enter** .

   The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

```
Clearing all current alarms.
[started]
done
Sending test alarm.
[started]
done
#
```

Configuring a Customer ID

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Customer ID** option, and press **Enter**

   The system displays the Customer ID prompt:

   ```
   What is the Customer ID (10 digit customer code)? (default:0004558769)
   ```

3. Enter the Customer ID value, and press **Enter**.

   The default Customer ID is normally the last value entered. CMS servers have a pre-defined default value that must be changed if the customer has an Avaya maintenance agreement.

   The system displays the Customer Name prompt:

   ```
   What is the Customer Name? (default:Avaya)
   ```

4. Enter the Customer Name, and press **Enter**.

   After you have configured the Customer name, the system displays the following messages, and the tool returns to the command line prompt:

   ```
   reset AOM
   [started]
   Done
   #
   ```

Sending an AOM Test Alarm

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

   ```
   Welcome to Avaya CMS Alarm Configuration Main Menu.
   1) Set Alarm ID
   2) Set Customer ID
   3) Configure Alarm Destination
   4) Send a Test Alarm
   q) Quit
   Enter choice (1-4, q):
   ```

2. Enter the number associated with the **Send a Test Alarm** option, and press **Enter** .

   The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

   ```
   Clearing all current alarms.
   [started]
   done
   Sending test alarm.
   [started]
   done
   #
   ```

Clearing SNMP Alarms

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

   ```
   Welcome to Avaya CMS Alarm Configuration Main Menu.
   1) Set Alarm ID
   2) Set Customer ID
   3) Configure Alarm Destination
   4) Send a Test Alarm
   q) Quit
   Enter choice (1-4, q):
   ```

2. Enter the number associated with the **Configure the Alarm Destination** option, and press **Enter** .

   The system displays the Welcome to **Avaya CMS Alarm Origination** main menu options

   ```
   Configure the Alarm DestinationWelcome to Avaya CMS Alarm Origination main menu.
   1) SNMP/SAL
   2) Socket/SAL
   q) Quit
   Enter choice (1-2, q):
   ```

   Note:

   Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the **SNMP/SAL** option, and press **Enter**.

   The system displays the list of SNMP configuration options:

   ```
   Do you want to
   1) Add an SNMP Connection
   2) Delete an SNMP Connection
   3) Modify an SNMP Connection
   4) Add an SNMP User
   5) Delete an SNMP User
   6) Modify an SNMP User
   7) Clear SNMP Alarms
   q) Quit
   Enter choice (1-7, q): 7
   ```

4. Enter the number associated with the **Clear SNMP Alarms** option, and press **Enter**

   The system displays active alarms.

5. To close an open alarm, enter `y` at the prompt.

CMS SNMP alarm information

Alarm type	Alarm name	SNMP object identifier	Description
Test Alarm	TEST_ALARM	.1.3.6.1.4.1.6889.2.72.0.1	This Test alarm is generated to verify that CMS alarming is functional. Since this is a test alarm, this alarm does not cause a new alarm ticket to be created with Avaya.
Test Alarm Clear	TEST_ALARM_CLR	.1.3.6.1.4.1.6889.2.72.0.2	This Test alarm clear is generated to verify that CMS alarming is functional. Since this is a test alarm clear, this alarm does not close all alarm tickets with Avaya.
Expert System Alarm	ES_ALARM	.1.3.6.1.4.1.6889.2.72.0.3	Avaya Expert System alarm.
Expert System Alarm Clear	ES_ALARM_CLR	.1.3.6.1.4.1.6889.2.72.0.4	Avaya Expert System alarm clear.
ACD Link Alarm	ACDLINK[1-8]	.1.3.6.1.4.1.6889.2.72.0.5	This ACD Link Alarm is generated if any CMS ACD link experiences trouble.
ACD Link Alarm Clear	ACDLINK[1-8]_CLR	.1.3.6.1.4.1.6889.2.72.0.6	This ACD Link Alarm Clear is generated when an existing ACD Link alarm is cleared.
Archiving Alarm	[H]*ARCH	.1.3.6.1.4.1.6889.2.72.0.7	This Archiving Alarm is generated when the CMS interval, daily, weekly, or monthly data archiver experiences trouble.
Archiving Alarm Clear	[H]*ARCH_CLR	.1.3.6.1.4.1.6889.2.72.0.8	This Archiving Alarm Clear is generated when an existing data archiver alarm is cleared.
Disk Error	DISK _ERR	.1.3.6.1.4.1.6889.2.72.0.9	This disk error alarm is generated when a disk failure occurs.
Disk Error Clear	DISK_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.10	This disk error clear alarm is generated when an existing DISK _ERR alarm is cleared.
ECH Warning Alarm	ECH_WARNING	.1.3.6.1.4.1.6889.2.72.0.11	This ECH Warning Alarm is generated when External Call History experiences a warning.
ECH Warning Alarm Clear	ECH_WARNING_CLR	.1.3.6.1.4.1.6889.2.72.0.12	This ECH Warning Alarm Clear is generated when an existing ECH Warning alarm is cleared.

Table continues…

Alarm type	Alarm name	SNMP object identifier	Description
ECH Failure Alarm	ECH_FAILURE	.1.3.6.1.4.1.6889.2.72.0.13	This ECH Failure Alarm is generated when External Call History experiences a failure.
ECH Failure Alarm Clear	ECH_FAILURE_CLR	.1.3.6.1.4.1.6889.2.72.0.14	This ECH Failure Alarm Clear is generated when an existing ECH Failure alarm is cleared.
Surviving Alarm	SURVIVING	.1.3.6.1.4.1.6889.2.72.0.15	This Surviving Alarm is generated when a survivable CMS in standby mode becomes active.
Surviving Alarm Clear	SURVIVING_CLR	.1.3.6.1.4.1.6889.2.72.0.16	This Surviving Alarm Clear is generated when an existing Surviving Alarm is cleared.
Disk Warning	DISK_WRN	.1.3.6.1.4.1.6889.2.72.0.17	This disk warning alarm is generated when a disk warning occurs. A disk warning indicates a disk failure condition that can exist in the near future.
Disk Warning Clear	DISK_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.18	This disk warning clear alarm is generated when an existing DISK_WRN alarm is cleared.
Battery Error	BATTERY_ERR	.1.3.6.1.4.1.6889.2.72.0.19	This battery error alarm is generated when a RAID battery failure occurs.
Battery Error Clear	BATTERY_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.20	This battery error clear alarm is generated when an existing BATTERY_ERR alarm is cleared.
Battery warning	BATTERY_WRN	.1.3.6.1.4.1.6889.2.72.0.21	This battery warning alarm is generated when a RAID battery warning occurs. A battery warning indicates a RAID battery failure condition that can exist in the near future.
Battery Warning Clear	BATTERY_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.22	This battery warning clear alarm is generated when an existing BATTERY_WRN alarm is cleared.
RAID Error	RAID_ERR	.1.3.6.1.4.1.6889.2.72.0.23	This RAID error alarm is generated when a RAID enclosure failure occurs.
RAID Error Clear	RAID_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.24	This RAID error clear alarm is generated when an existing RAID_ERR alarm is cleared.

Table continues…

Alarm type	Alarm name	SNMP object identifier	Description
RAID Warning	RAID_WRN	.1.3.6.1.4.1.6889.2.72.0.25	This RAID warning alarm is generated when a RAID enclosure warning occurs. A RAID warning indicates a RAID enclosure failure condition that can exist soon.
RAID Warning Clear	RAID_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.26	This RAID warning clear alarm is generated when an existing RAID_WRN alarm is cleared.
Backup Warning	BACKUP_WRN	.1.3.6.1.4.1.6889.2.72.0.27	This backup warning alarm is generated when a CMS maintenance backup warning occurs. A backup warning indicates that a CMS maintenance backup was not successful.
Backup Warning Clear	BACKUP_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.28	This backup warning clear alarm is generated when an existing BACKUP_WRN alarm is cleared.
Elog Warning Alarm	ELOG_WRN	.1.3.6.1.4.1.6889.2.72.0.29	Warning that the CMS error logging process may be overloaded.
Elog Warning Alarm Clear	ELOG_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.30	CMS ELOG_WRN clear.
ACD Secondary Link Up	ACDSECUP[1-8]	.1.3.6.1.4.1.6889.2.72.0.31	The secondary ACD IP address is being used.
ACD Secondary Link Up Clear	ACDSECUP[1-8]_CLR	.1.3.6.1.4.1.6889.2.72.0.32	The Clear is generated when the ACD Secondary Link Up Alarm is cleared.
Disk Full Warning	DISKFULLINF	.1.3.6.1.4.1.6889.2.72.0.33	This Disk Full Alarm is generated when the disks are 95% full.
Disk Full Warning Clear	DISKFULLINF_CLR	.1.3.6.1.4.1.6889.2.72.0.34	This Disk Full Warning Clear is generated when the Disk Full Warning is cleared.
Disk Full Alarm	DISKFULLWRN	.1.3.6.1.4.1.6889.2.72.0.35	This Disk Full Alarm is generated when the disks are 95% full.
Disk Full Alarm	DISKFULLWRN_CLR	.1.3.6.1.4.1.6889.2.72.0.36	The Disk Full Alarm is cleared.
Firewall Warning Alarm	FIREWALLWRN	.1.3.6.1.4.1.6889.2.72.0.37	This firewall warning is generated when the firewall is disabled.
Firewall Warning Alarm Clear	FIREWALLWRN_CLR	.1.3.6.1.4.1.6889.2.72.0.38	The firewall warning is cleared.
FIPS Warning Alarm	FIPS_WRN	.1.3.6.1.4.1.6889.2.72.0.39	This FIPS warning is generated when FIPS is disabled.

Table continues…

Alarm type	Alarm name	SNMP object identifier	Description
FIPS Warning Alarm Clear	FIPS_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.40	The FIPS Warning Alarm is cleared.
WebLM Warning Alarm	LIC_ERR	.1.3.6.1.4.1.6889.2.72.0.41	This License error is generated when CMS is in license error mode.
WebLM Warning Alarm Clear	LIC_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.42	The license error mode is cleared.
WebLM Warning Alarm	LIC_RESTRICTED	.1.3.6.1.4.1.6889.2.72.0.43	This License Restricted is generated when CMS is in license restricted mode.
WebLM Warning Alarm Clear	LIC_RESTRICTED_CLR	.1.3.6.1.4.1.6889.2.72.0.44	The license restricted mode is cleared.
Web Client Warning Alarm	WEBCRT_WRN	.1.3.6.1.4.1.6889.2.72.0.45	This Web Client certificate warning alarm is generated when the Web Client certificate is about to expire.
Web Client Warning Alarm Clear	WEBCRT_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.46	The Web Client certificate warning alarm is cleared.
Web Client Error Alarm	WEBCRT_ERR	.1.3.6.1.4.1.6889.2.72.0.47	This Web Client certificate error alarm is generated when the Web Client certificate has expired.
Web Client Error Alarm Clear	WEBCRT_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.48	The Web Client certificate expired error alarm is cleared.
EASG Warning Alarm	EASGCRT365_WRN	.1.3.6.1.4.1.6889.2.72.0.49	This EASG certificate warning alarm is generated when the EASG certificate is expiring within 365 days.
EASG Warning Alarm Cleared	EASGCRT365_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.50	The EASG certificate 365 day warning alarm is cleared.
EASG Warning Alarm	EASGCRT180_WRN	.1.3.6.1.4.1.6889.2.72.0.51	This EASG certificate warning alarm is generated when the EASG certificate is expiring within 180 days.
EASG Warning Alarm Cleared	EASGCRT180_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.52	The EASG certificate 180 day warning alarm is cleared.
EASG Warning Alarm	EASGCRT30_WRN	.1.3.6.1.4.1.6889.2.72.0.53	This EASG certificate warning alarm is generated when the EASG certificate is expiring within 30 days.
EASG Warning Alarm Cleared	EASGCRT30_WRN_CLR	.1.3.6.1.4.1.6889.2.72.0.54	The EASG certificate 30 day warning alarm is cleared.

Table continues…

Alarm type	Alarm name	SNMP object identifier	Description
EASG Error Alarm	EASGCRT30_ERR	.1.3.6.1.4.1.6889.2.72.0.55	This EASG certificate error alarm is generated when the EASG certificate has expired.
EASG Error Alarm Cleared	EASGCRT30_ERR_CLR	.1.3.6.1.4.1.6889.2.72.0.56	The EASG certificate expired error alarm is cleared.

Locating and installing the CMS-MIB.txt file

Procedure

1. Download the `CMS-MIB.txt` file from http://support.avaya.com.
2. Install the MIBS file with NMS.

Setting up AOM configuration for alarming using Socket/SAL

The aom_tool is used to configure AOM.

- To set up AOM configuration, continue with Configuring AOM.
- To send a test alarm, continue with Sending an AOM Test Alarm.

Configuring AOM

Configuring AOM for alarming using a modem includes the following:

- Configuring an Alarm Destination
- Configuring an Alarm ID
- Sending an AOM Test Alarm

Configuring an Alarm Destination

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

   ```
   Welcome to Avaya CMS Alarm Configuration Main Menu.
   1) Set Alarm ID
   2) Set Customer ID
   3) Configure Alarm Destination
   4) Send a Test Alarm
   q) Quit
   Enter choice (1-4, q):
   ```

2. Enter the number associated with the **Configure the Alarm Destination** option, and press **Enter**.

   The system displays the following message:

   ```
   Welcome to Avaya CMS Alarm Origination main menu.
   1) SNMP/SAL
   ```

```
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

Note:

Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the `Socket/SAL` option, and press **Enter**.

   Note:

   If the system has been previously configured with an alarming method, the system can prompt for the removal of the configuration.

   The system displays the input prompt for the SAL IP address:

   ```
   What is the SAL ip address?
   ```

4. Enter the SAL IP Address and press **Enter**.

   Do not use any leading zeros in the IP address as this can lead the system to interpret the numbers in the address as octal.

   The system displays the input prompt for the SAL network port and the default network port value:

   ```
   What is the SAL network port? (default:5108)
   ```

5. Enter the SAL network port value or accept the default value and press **Enter**.

   The system displays the input prompt for the Alarm ID and the default Alarm ID:

   ```
   What is the Alarm ID (10 digit product code)?
   ```

6. Enter the Alarm ID or accept the default value, and press **Enter**.

   The system displays the input prompt for running a test alarm:

   ```
   Run a test alarm when done?(y/n)
   ```

7. Enter `y` or `n`, and press **Enter**.

   The system displays the following messages:

   ```
   CMS was last rebooted 1 day(s) ago.
   You have selected to configure AOM using SAL via Socket/Virtual NIU.
   Removing existing socket configuration
   SAL IP Address:
   SAL network port number: 5108
   Alarm ID: 3000004043
   A test alarm will be sent at the end.
   Press [Enter] to continue or [q] to quit
   ```

8. Press **Enter**.

   The system displays the following messages, and the tool returns to the command line prompt:

   ```
   Configuring dest.cfg
   [started]
   done
   reset AOM
   [started]
   ```

```
done
Clearing all current alarms.
[started]
done
Sending test alarm.
[started]
done
done#
```

Configuring an Alarm ID

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

   ```
   Welcome to Avaya CMS Alarm Configuration Main Menu.
   1) Set Alarm ID
   2) Set Customer ID
   3) Configure Alarm Destination
   4) Send a Test Alarm
   q) Quit
   Enter choice (1-4, q):
   ```

2. Enter the number associated with the **Set a Test Alarm** option, and press **Enter** .

   The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

   ```
   Clearing all current alarms.
   [started]
   done
   Sending test alarm.
   [started]
   done
   #
   ```

Sending an AOM Test Alarm

Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`

   The system displays the following messages:

   ```
   Welcome to Avaya CMS Alarm Configuration Main Menu.
   1) Set Alarm ID
   2) Set Customer ID
   3) Configure Alarm Destination
   4) Send a Test Alarm
   q) Quit
   Enter choice (1-4, q):
   ```

2. Enter the number associated with the **Send a Test Alarm** option, and press **Enter** .

   The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

   ```
   Clearing all current alarms.
   [started]
   done
   Sending test alarm.
   [started]
   ```

```
done
#
```

Setting the Informix configuration parameters for CMS

The IDS configuration parameters for CMS are automatically optimized for system performance during the installation of Informix.

Chapter 7: Setting up CMS

About configuring the CMS software

You can choose either of the following ways to configure the CMS software:

- Interactive configuration. If you use the interactive option, the program automatically prompts you for the necessary information to configure the CMS software.
- Flat file configuration. If you use what is called the “flat file” option, you edit a file that contains the necessary configuration data to set up the CMS software. When you execute the install program, the program runs in the background and uses the flat file to configure CMS.

Prerequisites

Before you configure the CMS software, perform the following tasks:

- Verify that you are logged in as root.

  Important:

  You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

- Verify that if TCP/IP is being used to connect to an ACD, the switch/LAN setup is done.
- Verify that all file systems are mounted.

Setting up CMS interactively

About this task

Caution:

Using the CMS **`setup`** option of the **`cmssvc`** command erases all previous setup information. Ensure that you have any old setup information on record when you run the **`setup`** option.

Before you begin

Ensure that CMS is turned off and that IDS is running.

Procedure

1. Enter **`cmssvc`**.

Note:

If you are executing the **cmssvc** command for the first time, the system does not display the menu. Instead, the system automatically prompts for WebLM setup, EASG setup, encryption passphrase setup. For more information, see Configuring WebLM, EASG, and the encryption passphrases on page 40.

The system displays the “Call Management System Services Menu”:

```
Avaya(TM) Call Management System Services Menu

Select a command from the list below.
 1) auth_display   Display feature authorizations
 2) weblm_set      Set up the connection to the WebLM
 3) run_ids        Turn Informix Database on or off
 4) run_cms        Turn Avaya CMS on or off
 5) setup          Set up the initial configuration
 6) swinfo         Display switch information
 7) swsetup        Change switch information
 8) uninstall      Remove the CMS rpm from the machine
 9) patch_rmv      Backout an installed CMS patch
10) back_all       Backout all installed CMS patches from machine
11) security       Administer CMS security features
Enter choice (1-11) or q to quit:
```

2. Type the option number for the **setup** command.

   The system displays the following message:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is compatible. (Upgrade from
any ISO Latin language to any ISO Latin language or from Japanese to Japanese is
supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

Note:

When the **cmssvc** setup command is running, the system does not allow any other **cmsadm** or **cmssvc** commands. The system rejects any attempt to run other **cmsadm** or **cmssvc** commands and the system displays the following error message

```
Please try later, setup is active.
```

Note:

If system setup has already been done, the program responds:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

If the warning message is displayed, perform one of the following actions:

- Enter `n` to exit the setup.
- Enter `y` to continue with the setup.

Caution:

Using the CMS **`setup`** option of the **`cmssvc`** command erases all previous setup information. Ensure that you have any old setup information on record when you run the **`setup`** option.

3. Enter the number associated with the language that is used on the system.

   The system displays the following message if a flat file exists; otherwise, this menu is not displayed:

```
The input will be read from
1) the terminal
2) a flat file
Enter choice (1-2):
```

4. Enter the number associated with the terminal option.

```
## Initializing Customer CMS data . . .
.......................
Customer CMS data successfully initialized.
Creating database tables
.......
Enter a name for this UNIX system (up to 256 characters): (default:)
```

5. Enter the host name of the CMS server. This name was assigned during network setup. For more information, see Configuring the system network on page 36.

   The system displays the following message:

```
Select the type of backup device you are using
1) Tape
2) Other
Enter choice (1-2):
```

6. Enter the type of backup device the system is using.

   The following table lists the supported models of backup devices:

Backup device	Description	Platforms supported
DAT 160	DDS compliant 150 meter 160/320 GB DAT cartridge	Dell R630 Dell R730 HP DL380P G9
DAT 320	DDS compliant 150 meter 320 GB DAT cartridge	Dell R630 Dell R730 HP DL380P G9

Table continues…

Backup device	Description	Platforms supported
LTO-4	820 meter 800 GB 12.65 mm cartridge	Dell R630 Dell R730 HP DL380P G9
LTO-5	820 meter 800 GB 12.65 mm cartridge 846 meter 1.5 TB 12.65 mm cartridge	Dell R630 Dell R730 HP DL380P G9

Note:

Avaya Solutions Platform servers do not have a tape drive option.

The system displays the following message:

```
Enter the default backup device path: (default: 'none')
```

For tape option, use the following steps to determine the device path of the tape drive:

a. Insert a tape into the tape drive.

b. In another xterm window, enter the following commands:

mt -f /dev/st0 status

mt -f /dev/st1 status

The system displays the following message for the DAT 320 tape drive:

```
SCSI 2 tape drive:
File number=-1, block number=-1, partition=0.
Tape block size 0 bytes. Density code 0x4d (no translation).
Soft error count since last status=0
General status bits on (1010000):
ONLINE IM_REP_EN
```

Caution:

You cannot perform backups to `/dev/null`. The `/dev/null` device path allows customers who do not have a backup device to continue configuring CMS.

The `/dev/null` device path is not an option if type “Other” is selected. The CMS administrator needs to provide the path used for type “Other”.

7. Enter the default backup device path.

   The system displays the following message:

   ```
   Enter number of ACDs being administered (1-8): (default: 2)
   ```

8. Enter the number of ACDs (Communication Manager systems) to be administered. This number may be less than the number of ACDs authorized.

   The system displays the following message:

   ```
   Information for ACD 1
   Enter switch name (up to 20 characters):
   ```

9. Enter the name for the Communication Manager system that is being used as ACD 1.

   The system displays the following supported Communication Manager releases.

   ```
   Select the model of switch for this ACD
      1) Communication Mgr 6.x
      2) Communication Mgr 7.x
      3) Communication Mgr 8.x
      4) CM 8.1.2+ Secured
   Enter choice (1-4): 1
   ```

   Important:

   To administer an encrypted link between CMS and a Communication Manager system, you must use the “CM 8.1.2+ Secured” option on CMS and the “R19.1+ (secured)” option on Communication Manager. If you do not want an encrypted link, use the “Communication Mgr 8.x” option on CMS and “R19.0” on Communication Manager.

   For information on switch models, see *Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting*.

10. Choose the Communication Manager release.

    The system displays the following message:

    ```
    Enter the local port assigned to switch. (1-64):
    ```

    Note:

    The standard CMS provisioning procedure is to set the local and remote port assignments equal to the switch processor channel assignment. For example, for switch processor channel 2, the remote and local port assignments would both be set to a value of 2.

11. Enter the local port or channel number on the switch.

    The system displays the following message:

    ```
    Enter the remote port assigned to switch (1-64):
    ```

12. Enter the remote port or channel number on the switch.

    The system displays the following message:

    ```
    Enter switch host name or IP Address:
    ```

13. Enter the host name or IP address of a Communication Manager system that is connected to this CMS server.

    Note:

    If you enter a host name that has not been added to the computer’s `/etc/hosts` file, the system displays the following message:

    ```
    Switch_name has not been administered in a DNS or
    /etc/hosts file. The DNS or /etc/hosts file must be
    corrected or the link to the switch will not work.
    ```

    The system displays the following message:

    ```
    Enter switch TCP port number (minimum-maximum):(default: 5001)
    ```

14. Press **Enter** to use the default TCP port number.

    This number must match the port number administered on the switch.

    The system displays the following message:

    ```
    Number of splits/skills (0-maximum): (default: 350)
    ```

15. Enter the number of splits/skills in this ACD.

    The system displays the following message:

    ```
    Total split/skill members, summed over all splits/skills(0-Maximum):(default 3500)
    ```

16. Enter the maximum number of split/skill members that will be logged into this ACD simultaneously.

    The system logs in sum all agent-skill combinations at the same time. Count the maximum number of skills the supervisors expect to assign to each agent (maximum is 120).

    If it is not possible to sum the number of splits/skills for each agent, you can determine the capacity that is needed by multiplying the total number of agents by the average number of splits/skills per agent.

    The system displays the following message:

    ```
    Number of trunk groups (0-maximum):(default 350)
    ```

17. Enter the number of trunk groups that are associated with this ACD.

    The system displays the following message:

    ```
    Number of trunks (0-maximum):(default 1000)
    ```

18. Enter the number of trunks associated with this ACD.

    The system displays the following message:

    ```
    Number of unmeasured facilities (0-maximum):(default: 500)
    ```

19. Enter the number of unmeasured trunk facilities that are associated with this ACD.

    The recommended assignment per ACD for unmeasured facilities is 50% of the measured trunks.

    If the Communication Manager system supports call work codes, the system displays the following message:

    ```
    Number of call work codes (minimum-maximum):(default 750)
    ```

20. Enter the number of call work codes.

    ```
    Enter number of vectors (0-maximum):(default 350)
    ```

21. Enter the number of vectors.

    ```
    Enter number of VDNs (0-maximum):(default 2000)
    ```

22. Enter the number of VDNs.

    At this point, the program repeats starting at Step 7 based on the number of ACDs entered in Step 6.

After you define the last ACD, the system displays the following message:

```
Updating database.

Creating database tables
.......

Computing space requirements and file system space
availability.

Setup completed successfully.
```

Note:

If the setup determines that you do not have enough file space, the system displays the following warning message:

```
Failed to find sufficient file space for CMS data.

WARNING: You do not currently have sufficient file space for your existing CMS
data. At this point you should turn on CMS, go to the "Data Storage Allocation"
screen, verify/modify the administration, and go to the "Free Space Allocation"
screen and verify your available free space.
Setup completed with warnings.
```

23. To verify that the installation completed successfully, enter:

    `tail /cms/install/logdir/admin.log`

    All failure messages are logged in this file. The CMS software is successfully set up when the system displays a message similar to the following:

    ```
    Setup completed successfully <date/time>
    ```

    You may edit this file and add comments about the packages that were installed or authorized.

24. **(Optional)** If you need to install additional CMS-related feature packages, see "Installing feature packages" in *Maintaining and Troubleshooting Avaya Call Management System*.

25. If you are not installing any other feature packages, perform the following steps:

    a. Enter: **`cmssvc`**

    b. Enter the number associated with the **`run_cms`** option.

    c. Enter the number associated with the **`Turn on CMS`** option.

Editing a flat file

About this task

To configure CMS using a flat file, you must edit a copy of the `cms.inst.skl` installation file and start the setup option of the **`cmssvc`** command.

Important:

This procedure is not necessary if you already configured CMS interactively.

Procedure

1. Use the following command to change to the CMS installation directory:

   `cd /cms/install/cms_install`

2. Use the following command to make a copy of the CMS installation file:

   `cp cms.inst.skl cms.install`

3. Use the following command to change permissions on the copied CMS installation file:

   `chmod 644 cms.install`

4. Use the following command to edit the copied CMS installation file:

   `vi cms.install`

   The file contains a series of questions and value ranges for each possible ACD (Communication Manager system) in your configuration. Enter the appropriate values for your configuration. The entries must be added on the blank lines after each question.

   Caution:

   Use the CMS server host name for the Linux system name. The computer's host name was assigned during network setup.

5. Press **Esc**.
6. Enter:

   `:wq!`

   The system saves and closes the file.

Example

For an example of a flat file that you will edit to set up CMS, see Example of a flat file on page 103.

Next steps

Continue with Setting up CMS using the flat file on page 83.

Setting up CMS using the flat file

About this task

Caution:

Using the CMS **`setup`** option of the **`cmssvc`** command erases all previous setup information. Ensure that you have any old setup information on record when you run the **`setup`** option.

Before you begin

Verify that you have made all edits in the flat file. For more information, see Editing a flat file on page 82.

Ensure that CMS is turned off and that IDS is running.

Procedure

1. Enter **cmssvc**.

   Note:

   If you are executing the **cmssvc** command for the first time, the system does not display the menu. Instead, the system automatically prompts for WebLM setup, EASG setup, encryption passphrase setup. For more information, see Configuring WebLM, EASG, and the encryption passphrases on page 40.

   The system displays the “Call Management System Services Menu”:

```
Avaya(TM) Call Management System Services Menu

Select a command from the list below.
 1) auth_display   Display feature authorizations
 2) weblm_set      Set up the connection to the WebLM
 3) run_ids        Turn Informix Database on or off
 4) run_cms        Turn Avaya CMS on or off
 5) setup          Set up the initial configuration
 6) swinfo         Display switch information
 7) swsetup        Change switch information
 8) uninstall      Remove the CMS rpm from the machine
 9) patch_rmv      Backout an installed CMS patch
10) back_all       Backout all installed CMS patches from machine
11) security       Administer CMS security features
Enter choice (1-11) or q to quit:
```

2. Type the option number for the **setup** command.

   The system displays the following message:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is compatible. (Upgrade from
any ISO Latin language to any ISO Latin language or from Japanese to Japanese is
supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

Note:

When the **cmssvc** setup command is running, the system does not allow any other **cmsadm** or **cmssvc** commands. The system rejects any attempt to run other **cmsadm** or **cmssvc** commands and the system displays the following error message

```
Please try later, setup is active.
```

Note:

If system setup has already been done, the program responds:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

If the warning message is displayed, perform one of the following actions:

- Enter `n` to exit the setup.
- Enter `y` to continue with the setup.

Caution:

Using the CMS **setup** option of the **cmssvc** command erases all previous setup information. Ensure that you have any old setup information on record when you run the **setup** option.

3. Enter the number associated with the language that is used on the system.

   The system displays the following message if a flat file exists; otherwise, this menu is not displayed:

   ```
   The input will be read from
   1) the terminal
   2) a flat file
   Enter choice (1-2):
   ```

4. Enter the number associated with the flat file option.

   The system displays the following message:

   ```
   *** The rest of this command is running in the background ***
   ```

5. Verify that the installation completed successfully by entering: `tail -f /cms/install/logdir/admin.log`

   The -f option in the tail command updates the console as messages are written to the `admin.log` file. All failure messages are logged in this file. The CMS software is successfully set up when you see a message similar to the following:

   ```
   Setup completed successfully <date/time>
   ```

   You can edit this file and add comments about the packages that were installed or authorized.

6. Press **Delete** to exit the **tail -f** command.

7. Choose one of the following:
   - To install additional CMS-related feature packages (such as Forecasting or External Call History), see *Maintaining and Troubleshooting Avaya Call Management System*.
   - If you are not installing any other feature packages, do the following to turn on the CMS software:
     a. Enter: `cmssvc`.

        The system displays the “Avaya Call Management System Services Menu”.
     b. Enter the number associated with the **run_cms** option.
     c. Enter the number associated with the **Turn on CMS** option.

Chapter 8: Turning the system over to the customer

About turning the system over to the customer

This section describes how to test the CMS software to ensure that the application is working properly before the system is turned over to the customer. Perform these procedures after:

- Completing the initial computer installation and CMS setup
- Completing a CMS software package upgrade

Prerequisites

Before you begin the procedures in this section, the technicians must:

- Locate the backup tapes (the set created by provisioning during installation) and set these tapes to write-protect mode if using tape drives for backups.

  Note:

  Avaya Solutions Platform server backup must be done through LAN backup.

- Connect the CMS server to the switch
- Translate the switch with the CMS feature enabled
- Connect the switch to an active link

Verifying the system date and time

Procedure

1. Verify that the RHEL operating system time and the current local time are the same.
2. If the date and times are not correct, see the procedures in “Changing the system date and time” in *Maintaining and Troubleshooting Avaya Call Management System*.

Forwarding CMS warning messages

About this task

The CMS server can forward warning messages to specific customer e-mail addresses. If you do not enable CMS to forward warning messages, the messages will remain in the CMS root e-mail account.

Important:

To use this feature, you must have Avaya Professional Services install either the Admin Paging or Supervisor Paging packages. Contact Avaya support for more information.

Use the following steps to forward CMS warning messages:

Procedure

1. Obtain the e-mail addresses of any customer CMS administrators who want to receive the warning messages.
2. Enter: `cd /`
3. Create the file for the e-mail addresses by entering: `vi /.forward`
4. Enter an e-mail address on a single line in the file.

   You can enter more than one e-mail address but each e-mail address must be on a single line as shown in the following example:

   ```
   admin1@company.com
   admin2@company.com
   admin3@company.com
   ```

5. Save and quit the file by pressing **Esc** and entering: `chmod 600 /.forward`

Checking free space allocation

About this task

Note:

The steps in this section are performed using CMS Supervisor.

Procedure

1. Log on to CMS Supervisor.
2. Navigate to **Administration** > **System Setup** > **Free Space Allocation**.
3. Enter an ACD number (1-8).
4. Click on the **Get Contents** icon.

   The system displays the **Get Contents** screen showing the amount of dbspace allocated for each CMS item for the ACD selected.

For more information about free space allocation, see *Administering Avaya Call Management System*.

If the **Total Free Space** field shows that there is not enough space available, you must modify data storage allocation.

Testing the ACD link

About this task

After the CMS software has been installed or upgraded, the on-site technician must test the link from the CMS server to the switch that is using the Automatic Call Distribution (ACD) feature.

Before you begin

Verify that:

- A virtual console window is open
- CMS is turned on.

Procedure

1. In a virtual console window, log into the system by using a CMS administrator's login ID by entering: `su - cms`

   Enter the correct password if prompted.
2. Enter: `cms`
3. Enter the correct terminal type.

   The CMS Main Menu is displayed.

   The CMS Main Menu has indicators that show whether the link to the ACD is active. The link indicator consists of the carets (\/ and /\) at the right side of the banner line. There should be one caret for each ACD, and all should be pointed up (^).

   Example:

   If you have four ACDs, the link indicator should look like this: ^^^^, which means that all four ACDs are up and operating.
4. Select **Maintenance** from the CMS Main Menu.

   The system displays the **Maintenance** menu.
5. Select **Connection Status** from the **Maintenance** menu.

   The **Connection Status** window displays the following information:

   - The name of the ACD
   - Whether the application is in data transfer
   - Whether the session is in data transfer

- Whether the connection is operational
- The date, time, and any errors

6. Press the **F5** key to exit the screen.

Assigning customer passwords

About this task

This section describes how the customer assigns passwords to each of its logins on the CMS server. The customer must assign passwords to each of the following logins:

- root
- cms
- Any other administration logins that have been added for the customer

Procedure

1. Log in as root.

   Important:

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

2. At the system prompt, have the customer enter: `passwd login`

   where `login` is root, cms, and so on.

   The system displays the following message:

   ```
   New password:
   ```

3. Have the customer enter the new password.

   The system displays the following message:

   ```
   Re-enter new password.
   ```

4. Have the customer enter the password again.

   Note:

   The technician should not know these passwords

5. Repeat this procedure for each customer login.

Testing the CMS software

About this task

After the CMS software has been installed or upgraded, the on-site technician must test the CMS software to verify its sanity.

Before you begin

Verify that:

- The virtual console is active
- CMS is turned on.

Procedure

1. Test the Real-Time Reports subsystem.
    a. Enter: `CMS`

       The system displays the CMS Main Menu.
    b. Select **Reports**.
    c. Select **Real-time**.
    d. Select **Split/Skill**.
    e. Select **Split Status** or **Skill Status**.
    f. Verify that the Split/Skill Status Report input window is displayed.
    g. Enter a valid split number in the Split: or Skill: field.
    h. Select the **Run** action list item, and run the report.
    i. Verify that the system displays the Split or Skill Status Report window.
    j. If the switch link is not operating, the report fields are blank and the status line reads **Switch link down**.
    k. Press the **F3** key to access the Print window screen.
    l. Select **Print window** to send the report to the printer.
    m. Look at the message line near the bottom of the window, and verify that there is a confirmation message about sending the report to the printer.
    n. Verify that the report was printed by checking the printer for the report.
    o. Return to the CMS Main Menu screen by pressing the **F5** key twice.
2. Test the Historical Reports subsystem.
    a. On the CMS Main Menu, select **Reports**.
    b. Select **Historical**.
    c. Select **Split/Skill**.
    d. Select **Status**.

e. Verify that the Split/Skill Status Report input window is displayed.
f. Enter a valid split number in the Split/Skill: field.
g. Enter **-1** in the Date: field.
h. Select the **Run** action list item, and run the report.
i. Verify that the report window is displayed and that the information is displayed in the appropriate fields.

Note:

If no historical data exists, the fields in the report window are blank.

j. Return to the CMS Main Menu by pressing the **F5** key twice.

3. Test the Dictionary subsystem by doing the following from the CMS Main Menu.
   a. On the CMS Main Menu select **Dictionary**.
   b. Select **Login Identifications**
   c. Enter an asterisk (*) in the Login ID field.
   d. Select the **List all** action list item. The system lists all the login IDs.
   e. Verify that the logins are displayed.

Note:

On a new system, the fields are blank.

   f. Return to the CMS Main Menu by pressing the **F5** key twice.
4. Test the Exceptions subsystem.
   a. On the CMS Main Menu screen, select **Exceptions**.
   b. Select **Real-time Exception Log**.
   c. Verify that the window is displayed.

Note:

For a new installation, this window may be blank

   d. Return to the CMS Main Menu by pressing the **F5** key once.
5. Test the Call Center Administration subsystem.
   a. On the CMS Main Menu select **Call Center Administration**.
   b. Select the **Call Work Codes** option.
   c. Press **Enter**.
   d. Select the **List all** action list item, and list all the call work codes currently defined.
   e. Verify that the displayed information is correct.

Note:

On a new system, the fields may be blank.

f. Return to the CMS Main Menu by pressing the **F5** key twice.

6. Test the Custom Reports subsystem.
   a. On the CMS Main Menu select **Custom Reports**.
   b. Select **Real-time**. The system lists the names of the custom reports.
   c. Verify that the names of existing custom reports are listed. If there are no reports, you receive a message saying the submenu is empty.
   d. Return to the CMS Main Menu by pressing the **F5** key once.
7. Test the User Permissions subsystem.
   a. On the CMS Main Menu select **User Permissions**.
   b. Select **User Data**.
   c. Verify that the User Data Input window is displayed.
   d. Return to the CMS Main Menu by pressing the **F5** key once.
8. Test the System Setup subsystem
   a. On the CMS Main Menu select **System Setup**.
   b. Select **CMS state**.
   c. Verify that CMS is operating in the Multi-user mode.
   d. Return to the CMS Main Menu by pressing the **F5** key once.
9. Test the Maintenance subsystem.
   a. On the CMS Main Menu select **Maintenance**.
   b. Select the **Printer Administration** option.
   c. Enter a valid printer name in the CMS printer name: field.
   d. Select the **List all** action list item. The system lists the printer parameters.
   e. Verify that the printer has been administered correctly.
   f. Return to the CMS Main Menu by pressing the **F5** key twice.
10. If the Graphics feature package has been enabled, test the Graphics subsystem.
    a. On the CMS Main Menu select **Graphics**.
    b. Verify that a Real-time Graphics screen can be accessed.
    c. Return to the CMS Main Menu by pressing the **F5** key once.
    d. At each CMS terminal, log in as cms and enter the correct terminal type to verify that the terminals are working properly. To log off, select the Logout option from the CMS Main Menu.

If you encounter a problem that you cannot solve, escalate the problem through normal procedures.

Finalizing the on-site installation

About this task

This section contains the final steps that a technician must perform before turning the system over to the customer.

Procedure

1. Back up the system using a CMSADM backup.

   The CMSADM file system backup saves all local file systems on the computer onto a backup device, including system files, OS programs, and CMS programs. For more information refer to *CMSADM backup* in *Maintaining and Troubleshooting Avaya Call Management System*.

   Caution:

   Use a new set of backup media for this CMSADM file system backup. Do not use the provisioning backup media. Ensure that the customer has the proper media for the new backup.

2. Back up the customer's historical data by doing a full maintenance backup. You can do these backups using the CMS Supervisor maintenance features.

   For more information about maintenance backups, see *Administering Avaya Call Management System*.

3. Set up alarming. For more information about the AOM tool, see Setting up the Alarm Origination Manager on page 58.

4. Have the customer record their log-ins and passwords.

   The technician must not know these login passwords.

5. Remind the customer to configure their data encryption passphrases. For more information, have the customer review Configuring the encryption passphrases on page 45 in this document or see the encryption passphrase information in *Maintaining and Troubleshooting Avaya Call Management System*.

6. Give the passwords, backup media, and software to the customer's CMS administrator.

   Caution:

   For system security and recovery, tell the CMS administrator should store passwords, Informix serial numbers, key license information, encryption passphrases, and the backup media in a secure location.

Chapter 9: Resources

Documentation

CMS and CMS Supervisor Documents

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers, Administrators
Product Privacy Statement for Avaya Call Management System	Describes how personal data is stored and processed by CMS.	Administrators
Design		
Avaya Customer Experience Virtualized Environment Solution Description	Describes the AvayaCustomer Experience Virtualized Environment market solution from a holistic perspective that focuses on the functional view of the solution architecture.	Sales engineers
Installation, upgrades, maintenance, and troubleshooting		
Deploying Avaya Call Management System	Describes how to plan, deploy, and configure CMS on new VMware-based installations.	Avaya support personnel
Deploying Avaya Call Management System on Amazon Web Services	Describes how to plan, deploy, and configure CMS on new Amazon Web Services installations.	Avaya support personnel
Avaya Call Management System Dell® PowerEdge™ R630 and R730 Hardware Installation, Maintenance and Troubleshooting	Describes how to install, maintain, and troubleshoot Dell® servers used with CMS.	Avaya support personnel
Avaya Call Management System HPE DL20 G9 and DL380 G9 Hardware Installation, Maintenance, and Troubleshooting	Describes how to install, maintain, and troubleshoot HPE servers used with CMS.	Avaya support personnel

Table continues…

Title	Description	Audience
Planning for Avaya Call Management System Upgrades	Describes the procedures customers must plan for before and after upgrading to a new CMS release.	Administrators
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release.	Avaya support personnel
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Avaya support personnel, Administrators
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Communication Manager systems used by CMS.	Avaya support personnel, Administrators
Avaya Call Management System Base Load Upgrade	Describes the procedures to upgrade from one base load (for example, 19.1.0.0) to another base load (for example, 19.1.0.1). Not all releases support base load upgrades.	Administrators
Using Avaya Call Management System High Availability	Describes how to install and maintain a CMS HA system.	Avaya support personnel, Administrators
Using Avaya Call Management System LAN Backup	Describes how to back up your CMS data using a LAN connection to a remote server.	Administrators
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Avaya support personnel, Administrators
Using Avaya Call Management System High Availability	Describes how to install and maintain your CMS High Availability (HA) system.	Avaya support personnel, Administrators
Administration		
Administering Avaya Call Management System	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, Report designers

Table continues…

Title	Description	Audience
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, Operations personnel, Report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Avaya support personnel, Administrators
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Avaya support personnel, Administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Administrators, Operations personnel
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Administrators, Operations personnel, Report designers

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	IT Management, sales and deployment engineers, solution architects, support personnel
Installing the Avaya Solutions Platform 130 Appliance	Describes how to install Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes procedures to use the iDRAC9 tools on the Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel

WebLM Documents

Title	Description	Audience
Deploying standalone Avaya WebLM in Virtual Appliance	Deploy the application in virtual appliance environment by using Solution Deployment Manager	Implementation personnel

Table continues…

Title	Description	Audience
Deploying standalone Avaya WebLM in Virtualized Environment	Deploy the application in virtualized environment.	Implementation personnel
Deploying standalone Avaya WebLM in Infrastructure as a Service Environment	Deploy the application on cloud services.	Implementation personnel
Deploying standalone Avaya WebLM in Software-Only Environment	Deploy the application in software-only environment.	Implementation personnel
Upgrading standalone Avaya WebLM	Upgrade the application.	Implementation personnel
Administering standalone Avaya WebLM	Do administration tasks	System administrators

VMware Documents

VMware component or operation	Document description	Document URL
vSphere Virtual Machine Administration	Provides information on managing virtual machines in the VMware vSphere Web Client for vSphere 6.0 or later. This document also provides information of the following: • Deploying OVF templates • Configuring virtual machine hardware and options • Managing Virtual Machines	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-55238059-912E-411F-A0E9-A7A536972A91.html
vSphere Web Client	Provides information on how through a browser vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.	https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html

Note:

If the document description (link) are no longer active, consult VMware for documents associated with the component or operation.

Related links

Finding documents on the Avaya Support website on page 99
Accessing the port matrix document on page 99
Avaya Documentation Center navigation on page 100

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

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

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ( ).

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

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

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

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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **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 key word or key words 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 the topic. 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.

Related links

Using the Avaya InSite Knowledge Base on page 102

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Flat file example

Example of a flat file

The following display shows an example of a flat file used to configure the CMS software for up to eight ACDs (eight Communication Manager systems). Enter data for only the required number of ACDs.

For more information, see About configuring the CMS software on page 76, Editing a flat file on page 82, and Setting up CMS using the flat file on page 83.

```
# Enter a name for this UNIX system (up to 64 characters):
localhost
# Select the type of backup device you are using
#    1) Tape
#    2) Other
# Enter choice (1-2):

# Default backup device paths based on device type:
# Device                    Default backup path
# Tape                      /dev/st0
# Other                     'none'
# Enter the default backup device path:

# Enter number of ACDs being administered (1-8):

# The following information is required per ACD:
# Information for ACD 1:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):
```

```
# Maximum number of split/skill members based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x                      100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                          360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                 Value
# Communication Mgr 6.x                      12000
# Communication Mgr 7.x                      24000
# Communication Mgr 8.x/CM 8.1.2+ Secured    30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                 Value
# Communication Mgr 6.x                       6000
# Communication Mgr 7.x                      12000
# Communication Mgr 8.x/CM 8.1.2+ Secured    15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 2:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
```

```
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x                        100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                            360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                   Value
# Communication Mgr 6.x                        12000
# Communication Mgr 7.x                        24000
# Communication Mgr 8.x/CM 8.1.2+ Secured      30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                   Value
# Communication Mgr 6.x                         6000
# Communication Mgr 7.x                        12000
# Communication Mgr 8.x/CM 8.1.2+ Secured      15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 3:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
```

```
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x                        100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                            360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                   Value
# Communication Mgr 6.x                        12000
# Communication Mgr 7.x                        24000
# Communication Mgr 8.x/CM 8.1.2+ Secured      30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                   Value
# Communication Mgr 6.x                         6000
# Communication Mgr 7.x                        12000
# Communication Mgr 8.x/CM 8.1.2+ Secured      15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
```

```
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 4:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x                        100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                            360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                   Value
# Communication Mgr 6.x                        12000
# Communication Mgr 7.x                        24000
# Communication Mgr 8.x/CM 8.1.2+ Secured      30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                   Value
# Communication Mgr 6.x                         6000
# Communication Mgr 7.x                        12000
# Communication Mgr 8.x/CM 8.1.2+ Secured      15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
```

```
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 5:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x                         100000
# Communication Mgr 7.x/Communication Mgr 8.x   360000
# CM 8.1.2+ Secured                             360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x                       12000
# Communication Mgr 7.x                       24000
# Communication Mgr 8.x/CM 8.1.2+ Secured     30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                  Value
# Communication Mgr 6.x                        6000
# Communication Mgr 7.x                       12000
```

```
# Communication Mgr 8.x/CM 8.1.2+ Secured   15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 6:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x                      100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                          360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                  Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
```

```
# Release(s)                                  Value
# Communication Mgr 6.x                       12000
# Communication Mgr 7.x                       24000
# Communication Mgr 8.x/CM 8.1.2+ Secured     30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                  Value
# Communication Mgr 6.x                        6000
# Communication Mgr 7.x                       12000
# Communication Mgr 8.x/CM 8.1.2+ Secured     15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                        Value
# Communication Mgr 6.x/Communication Mgr 7.x           1
# Communication Mgr 8.x/CM 8.1.2+ Secured               1
# Maximum number of call work codes based on switch type:
# Release(s)                                        Value
# Communication Mgr 6.x/Communication Mgr 7.x        1999
# Communication Mgr 8.x/CM 8.1.2+ Secured            1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                        Value
# Communication Mgr 6.x/Communication Mgr 7.x        8000
# Communication Mgr 8.x/CM 8.1.2+ Secured            8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                        Value
# Communication Mgr 6.x/Communication Mgr 7.x       30000
# Communication Mgr 8.x/CM 8.1.2+ Secured           30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 7:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type:
# Release(s)                                        Value
# Communication Mgr 6.x/Communication Mgr 7.x        8000
# Communication Mgr 8.x/CM 8.1.2+ Secured            8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                       Value
# Communication Mgr 6.x                           100000
# Communication Mgr 7.x/Communication Mgr 8.x     360000
```

```
# CM 8.1.2+ Secured                              360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x/Communication Mgr 7.x     2000
# Communication Mgr 8.x/CM 8.1.2+ Secured         2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                   Value
# Communication Mgr 6.x                        12000
# Communication Mgr 7.x                        24000
# Communication Mgr 8.x/CM 8.1.2+ Secured      30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                   Value
# Communication Mgr 6.x                         6000
# Communication Mgr 7.x                        12000
# Communication Mgr 8.x/CM 8.1.2+ Secured      15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x/Communication Mgr 7.x        1
# Communication Mgr 8.x/CM 8.1.2+ Secured            1
# Maximum number of call work codes based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x/Communication Mgr 7.x     1999
# Communication Mgr 8.x/CM 8.1.2+ Secured         1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x/Communication Mgr 7.x     8000
# Communication Mgr 8.x/CM 8.1.2+ Secured         8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                     Value
# Communication Mgr 6.x/Communication Mgr 7.x    30000
# Communication Mgr 8.x/CM 8.1.2+ Secured        30000
# Enter number of VDNs (0-Maximum):

# Information for ACD 8:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD
#    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x
#    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):
```

Flat file example

```
# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x                        100000
# Communication Mgr 7.x/Communication Mgr 8.x  360000
# CM 8.1.2+ Secured                            360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured        2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)                                   Value
# Communication Mgr 6.x                        12000
# Communication Mgr 7.x                        24000
# Communication Mgr 8.x/CM 8.1.2+ Secured      30000
# Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)                                   Value
# Communication Mgr 6.x                         6000
# Communication Mgr 7.x                        12000
# Communication Mgr 8.x/CM 8.1.2+ Secured      15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x       1
# Communication Mgr 8.x/CM 8.1.2+ Secured           1
# Maximum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured        1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x    8000
# Communication Mgr 8.x/CM 8.1.2+ Secured        8000
# Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)                                    Value
# Communication Mgr 6.x/Communication Mgr 7.x   30000
# Communication Mgr 8.x/CM 8.1.2+ Secured       30000
# Enter number of VDNs (0-Maximum):
```

Appendix B: Deploying CMS software on a Dell or HPE hardware server

About deploying CMS software on hardware servers

Use the procedures in this appendix when upgrading CMS on Dell or HPE hardware servers. These procedures show you how to install the RHEL Linux operating system (OS), the CMS software, and security options . The purpose of having this information in the *Deploying Avaya Call Management System* is that for upgrades, you must also do several procedures that are included in this document around configuring the system and setting up CMS.

Do only those chapters and tasks as directed from *Upgrading Avaya Call Management System*.

Installing the CMS security script and changing the cmssvc password

About this task

As part of installing or upgrading CMS software, you must install the CMS security options using the **cms_sec** script. As part of the security script, you are also prompted to change the default cmssvc user ID password the first time you run this script. If you have previously changed the default password for the cmssvc user ID, you are not prompted to enter a new password.

Important:

You can log in to the console as root only after you run the CMS security script. If you are logging on to the system remotely, log on as another user and then use **su - root** to log in as root.

Before you begin

Get the CMS software disc.

Procedure

1. Verify that you are logged in to the system as root.
2. Verify the current services running on the system and save the list for comparison with the listing after the security script run.

Note:

It is necessary to find out which services in the list of differences are used by the customer.

3. To capture the current services and preserve the output to a file, enter:

   chkconfig --list > /tmp/current_chkconfig.txt

4. Insert the CMS software disc and close the disc drive.
5. Change to the root directory by entering:

   cd /

6. Mount the disc by entering:

   mount /dev/dvd/mnt

7. Run the security script by entering:

   /mnt/security/cms_sec

   The system displays the following message if you have not already changed the default password for cmssvc user ID:

```
Avaya CMS security configuration started: Thu Jan 28 19:53:46 EST 2021
The backup directory for this run is: /cms/install/logdir/security/bkup_10338
Password change is required for user cmssvc
New password:
```

8. Enter and reenter a new password for the cmssvc user ID. You must follow standard password requirements as documented in *Avaya Call Management System Security*.

   The system displays messages similar to the following example:

```
Force password reset for user: cmssvc successfully executed.
File: /etc/cron.d/cron.allow already exists
Changed: permissions on /etc/cron.d/cron.allow to 644
File: /etc/cron.d/at.allow already exists
Changed: permissions on /etc/cron.d/at.allow to 644
File: /etc/init.d/umask already exists
Changed: permissions on /etc/init.d/umask to 744
Changed: group on /etc/init.d/umask to sys
File: /etc/rc1.d/S00umask already exists
Note: Forwarding request to 'systemctl disable sendmail.service'.
Disabled: sendmail
File: /etc/mail/sendmail.cf already exists, will overwrite
Copied: sec_files/sendmail.cf to /etc/mail/sendmail.cf
Line: ->PermitRootLogin no<- already in file: /etc/ssh/sshd_config
Line: ->PermitRootLogin no<- already in file: /etc/ssh/sshd_config
Service: sshd restarted
Disabled: time-dgram
Disabled: time-stream
Disabled: echo-dgram
Disabled: echo-stream
Disabled: discard-dgram
Disabled: discard-stream
Disabled: daytime-dgram
Disabled: daytime-stream
Disabled: chargen-dgram
Disabled: chargen-stream
Updated user informix shell to /sbin/nologin
```

```
Only 1 kernel exists, remove old kernels not required
Avaya CMS security configuration completed: Thu Jan 28 19:54:04 EST 2021
```

Note:

If the system displays a configuration failed message, contact your Avaya services representative.

9. To capture the new services and preserve the output to a different file, enter:

   chkconfig --list > /tmp/new_chkconfig.txt

10. Run the following command to check for any services that need to be reenabled:

    diff /tmp/current_chkconfig.txt /tmp/new_chkconfig.txt

11. View the output from the **diff** command and reenable the services that are displayed. To reenable any customer used services, enter:

    chkconfig [--level levels] <*Service name*> <*on*|*off*|*reset*>

    For example:

    chkconfig --level 2345 snmpd on

Next steps

Continue with the upgrade of the Dell or HPE servers as described in *Upgrading Avaya Call Management System*.

Installing Linux and CMS on hardware servers for an upgrade

About this task

Use this task to install the Linux OS and CMS software on a Dell or HPE hardware server as part of an upgrade.

Important:

Do not use this procedure on any VMware servers.

Before you begin

Get the following discs:

- RHEL Kickstart DVD
- CMS software DVD

Confirm that you have done the following tasks as shown in *Upgrading Avaya Call Management System*:

- Backed up the old system.
- Recorded all of the old information from the old system.

- Extracted the data from the old system.

Procedure

1. Insert the RHEL Kickstart DVD into the disc drive.
2. At the Linux prompt, enter:

   reboot

   The system boots from disc and displays a series of messages ending with the following message:

```
############################## IMPORTANT!! ##########################
## PROCEEDING WILL INSTALL A NEW OPERATING SYSTEM.                  ##
## ALL DATA WILL BE LOST!! PROCEED WITH CAUTION.                    ##
####################################################################
USAGE:
Type “ks” then press <enter> to install preconfigured Linux and
copy CMS software to the disk.
Type “rs” then press <enter> to install preconfigured Linux and
make the system ready to restore from a CMSADM backup.
Type “rescue” then press <enter> to rescue installed system
```

3. Enter:

   ks

   The kickstart process rebuilds the system by loading the Linux OS. When the process is finished, the system displays the following message:

```
####################################################################
## Please insert the CMS DVD into the drive.                      ##
####################################################################
```

4. Remove the RHEL Kickstart DVD, insert the CMS software DVD, and close the disc drive.

   The system automatically loads the CMS software. You will see a series of messages ending with a message similar to the following example:

```
Unpacking files please wait…
Extracting the tar…

Installing Avaya ™ Call Management System (cms) version rXXxx.x
Creating CMS group id
Creating dbaccess group id
Proceeding with install…

Preparing ########################################### [100 %]
1:cms ############################################## [100 %]

CMS is installed.
CMS installation successfully finished

                                Complete

Congratulations, your Red Hat Enterprise Linux installation is
complete.
Please reboot to use the installed system. Note that updates may
be available to ensure the proper functioning of your system and
installation of these updates is recommended after the reboot.

                                Reboot
```

5. Remove the CMS software DVD from the disc drive.
6. Press **Enter** to reboot the system.

   The system reboots to the logon prompt.
7. Log on to the system as `root`. There is no password required on the first logon.
8. Assign a root password by entering:

   `passwd`
9. When prompted, enter a password to use with the root logon ID.

Glossary

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.

Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Web Client	The vSphere Web Client is an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based Web client version is VMware 6.5 and later.

Index

E

F

H

I

L

M

O

P

R

S

T

U

V

W