Deploying Avaya Call Management System

Release 21.0
Issue 5
April 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

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

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

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

© 2015-2026, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose 7
Change history 7
Chapter 2: Deployment planning 9
Planning checklist 9
Deployment guidelines 10
Functional differences when installing CMS in a virtualized environment 11
High Availability for customer-provided VMware 11
Virtual machine resource requirements and average utilization 12
Capacities 14
Customer configuration data worksheets 15
Chapter 3: Preparing OVA deployment 17
Preparing OVA deployment checklist 17
Cloned and copied OVAs are not supported 17
Activating the license for a CMS server 17
Installing a license file on a WebLM server 19
Downloading software from PLDS 20
Chapter 4: Deploy CMS OVA on a VMware server 22
Deploying CMS software checklist 22
Deploying the OVA 22
Configuring the virtual machine automatic startup settings on VMware 26
Configuring the virtual machine for different configuration sizes 27
Configuring the virtual machine as a small configuration 27
Configuring the virtual machine as a medium configuration 28
Configuring the virtual machine as a large configuration 29
Chapter 5: Deploy CMS OVA on a KVM server 32
Planning checklist for CMS KVM deployment 32
Preparing the CMS KVM file 33
Importing the CMS virtual machine 34
Chapter 6: Configuring system features 36
Configuring system features checklist 36
Opening a hypervisor console 36
Verifying that CMS is installed 37
Powering up the virtual machine 37
Setting the root password 38
Configuring the system network 39
Disk encryption 42
Configuring WebLM, EASG, and the encryption passphrases 42
Installing CMS patches 45
Updating Linux RPMs 45

Running the CMS security script ... 46
Turning on IDS and adding disk space for medium and large configurations ... 46
Configuring the encryption passphrases ... 47
Verifying system startup and remote access ... 50
Chapter 7: Configuring CMS features ... 52
Configuring CMS features checklist ... 52
Assigning passwords to the default CMS login IDs ... 52
Viewing CMS authorizations ... 53
Activating the CMS Supervisor Web Client software ... 53
Managing certificates for Web Client software ... 53
Installing the root certificate and any intermediate certificate for the Web Client software ... 55
Installing the root certificate and any intermediate certificate in the browser ... 56
Starting the Web Client software ... 56
Storage requirements for CMS backups ... 57
Calculating data space requirements for CMSADM backups ... 57
Calculating data space requirements for CMS full maintenance backups ... 58
Setting up the Alarm Origination Manager ... 59
Configuring an Alarm Destination ... 59
Configuring an SNMP User ... 62
Configuring an Alarm ID ... 65
Configuring a Customer ID ... 66
Sending an AOM Test Alarm ... 66
Clearing SNMP Alarms ... 67
CMS SNMP alarm information ... 68
Locating and installing the CMS-MIB.txt file ... 72
Setting up AOM configuration for alarming using Socket/SAL ... 72
Chapter 8: Setting up CMS ... 76
About configuring the CMS software ... 76
Setting up CMS interactively ... 76
Editing a flat file ... 79
Setting up CMS using the flat file ... 80
Chapter 9: Performing the customer handover ... 83
CMS customer handover checklist ... 83
Verifying the system date and time ... 84
Forwarding CMS warning messages ... 84
Checking free space allocation ... 84
Testing the ACD link ... 85
Assigning customer passwords ... 86
Testing the CMS software ... 87
Finalizing the on-site installation ... 90
Appendix A: Flat file example ... 91
Example of a flat file ... 91
Appendix B: Resources ... 101

Documentation 101
Finding documents on the Avaya Support website 103
Avaya Documentation Center navigation 103
Viewing Avaya Mentor videos 105
Support 105
Using the Avaya InSite Knowledge Base 105
Glossary 107

Chapter 1: Purpose

This document is for implementation engineers and other personnel who deploy CMS. They can use this document to install a Avaya Call Management System (CMS) server as a virtual machine on a hypervisor server.

The supported options are:

Avaya Solutions Platform	Platform Hypervisor	CMSR20.x	CMS R21.x
ASP 130 R6	KVM	–	✓
ASP 130 R5	VMware	✓	✓

Alternate hypervisor deployment options

- You can deploy CMS as a virtual machine on Amazon Web Services (AWS) or Google Cloud Platform (GCP). Refer to the separate *Deploying Avaya Call Management System in an Infrastructure as a Service Environment* manual.
- When deploying CMS on a customer-provided hypervisor, you can use VMware. This is supported on:
  - VMware vSphere ESXi 7.0 update 2
  - VMware vCenter Server 7.0 update 2
  - VMware vSphere ESXi 8.0
  - VMware vCenter Server 8.0

Change history

The following table outlines the key changes in this document for Release 21.x:

Issue	Date	Summary of changes
5	April 2026	Updated the following: • Powering up the virtual machine. • Configuring WebLM, EASG, and the encryption passphrases. • Verifying system startup and remote access. Added the following: • Configuring the encryption passphrases.
4	May 2025	• Updated the "Initializing the CMS database" topic to remove incorrect information. • Corrected content related to KVM and VMware across the document.
3	November 2024	• Added Red Hat KVM information and rewrote Avaya Solutions Platform information throughout the document. • Cleaned up outdated information. • Revised and restructured information throughout the document. For example, the relevant content in the Architecture overview chapter has been merged with the Planning chapter.
2	August 2024	• Removed outdated information about configuring the encryption passphrase. • Removed outdated information in "Running the CMS security script". • Revised a command output example in "Calculating data space requirements for CMSADM backups". • Revised old information in Setting up CMS interactively.
1	June 2024	• Updated VMware versions. • Revised outdated IBM references. • Revised encryption information and removed outdated procedures. • Updated various examples.

Chapter 2: Deployment planning

This chapter provides planning information and other deployment guidelines. You can deploy CMS on an Avaya Solutions Platform ASP 130 R6 server or in a customer-provided virtual environment.

As of CMS R21.x, the VMware information in this document only applies to customer-provided systems. New CMS deployments on an Avaya Solutions Platform server use Red Hat KVM on the ASP 130 R6.

Note:

- The profile of the Avaya Solutions Platform hardware server you install depends on the sizing tool specification. You must determine the configuration size before starting the 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:

No	Task	Notes	✔
1.	Assess the infrastructure resource requirements for your deployment.	Key factors are: • CPU usage • Memory usage • Storage requirements • Network usage • Supported capacity	
2.	Plan and resource all staging and verification activities.	This includes IP addressing, naming conventions, and application-specific configuration.	

Table continues…

No	Task	Notes	✔
3.	Purchase the appropriate order codes and licenses.	For customer-provided deployments: You must separately license each CMS instance, that is, each installation of an OVA. Ensure that all OVA files are accessible. For Avaya Solutions Platform deployments: You no longer need a license key, but you must have a record in the Avaya Product Licensing and Delivery System (PLDS) of each instance of the server hypervisor.	
4.	Get the WebLM license server details and install the CMS license.	Use Avaya WebLM to manage product licenses obtained from PLDS. For more information, see Installing a license file on a WebLM server on page 19.	
5.	Ensure that you have the CMS software image for deployment.	A CMS R21.x VMware OVA is available on the Avaya Support website. You can use this to deploy CMS on your own customer-provided server. For deployments on Avaya Solutions Platform, download the OVA with the CMS KVM images from the Avaya Support website. The KVM OVA can be used for Avaya Solutions Platform deployments and customer-provided deployments.	

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 this affects performance.
- Monitor the server, host, and virtualized environment performance.

Important:

The values for performance, occupancy, and usage can vary. 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 could experience performance issues.

Functional differences when installing CMS in a virtualized environment

When deploying CMS in an virtualized environment, it operates almost identically to a CMS deployment on a hardware server 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 deployment on VMware supports both customer-provided servers or Avaya-provided Avaya Solutions Platform 130 R5 servers. For more information about Avaya Solutions Platform hardware, refer to the *Avaya Solutions Platform 130/S8300 Overview and Specification* documentation.

For VMware-certified compatibility guides and product interoperability matrices, see https://www.vmware.com/guides.html.

Software media for Avaya Solutions Platform deployments

As of CMS Release 21.x, you can use the KVM OVA for Avaya Solutions Platform deployments and customer-provided deployments.

High Availability for customer-provided VMware

CMS HA is different from VMware vSphere HA. VMware vSphere HA is a specific approach to VMware deployment.

CMS HA

CMS HA provides redundancy to reduce the potential loss of call center data. You can configure HA if you have two CMS servers. The CMS servers connect to an ACD system. With HA, one CMS server is designated as a primary server and the other is designated as a secondary server. When the primary server goes down, the secondary server takes over.

- You can optionally configure a dual-IP CMS server, where two IP addresses are administered. One connects to the main ACD system and the other connects to an Enterprise Survivability Server (ESS).
- For detailed information about CMS HA, see *Avaya Call Management System High Availability Connectivity, Upgrade and Administration*.

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.

Virtual machine resource requirements and average utilization

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

Important:

- If deploying on a customer provided virtual host platform, you can start with the minimum memory, minimum memory reservation, and minimum disk space allocations. However, Avaya will require you to increase the memory allocations if Avaya finds that reported CMS problems relate to memory usage.

Minimum required resources for virtual machine configurations

The following table outlines the virtual machine resource requirements for different CMS profiles.

VM resource	Small	Medium	Large	Extended	Notes
vCPU Cores (CPU)	2	8	16	32	The number of single core virtual CPUs.
Cores per Socket	2	8	16	32	The number of CPUs per socket. All cores are assigned to one socket. Therefore, the number of vCPU cores are the number of logical CPUs.
vCPU reservation	1200 MHz	4800 MHz	9600 MHz	9600 MHz	Guaranteed CPU allocation: 25% of vCPU capacity. Calculation: vCPUs x processor clock speed (2400Mhz)/4.

Table continues…

VM resource	Small	Medium	Large	Extended	Notes
Memory	8 GB	32 GB	64 GB	64 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.
" minimum for customer-provided VM	4 GB	16 GB	32 GB	–	
Memory reservation	8 GB	32 G	64 GB	64 GB	If the memory is not reserved and there is contention with other VM applications for additional memory resources, sufficient memory might not be available, resulting in CMS failures.
" minimum for customer-provided VM	4 GB	16 GB	32 GB	–	
Storage	800 GB	1200 GB	1800 GB	6000 GB	If the recommended storage value on the medium and large configurations is not administered, sufficient storage might not be available resulting in CMS failure. **Note:** For medium and large configurations, you will configure two disks.
IOPS	200	300	600	600	The IOPS data is based on real CMS hardware machines with 50% read and 50% write data.
Shared NICs	Two @ 1000 Mbps	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.

Average resource and network utilization for standard configurations

Average resource usage	Small	Medium	Large	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	

Table continues…

Average resource usage	Small	Medium	Large	Notes
IOPS	12	18	28	IOPS is higher during nightly summarization.

Requirements for expanding large configurations on customer-provided virtual machines

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.

The values in the table assume 62 days of interval storage and five years of daily storage (1825 days) when you have a one time zone. You can configure data storage allocation and view free space allocation information from CMS Supervisor as described in *Administering Avaya Call Management System*.

Agent skill pairs	200000		400000		600000		800000		1000000		1500000	
Interval length (minutes)	15	30	15	30	15	30	15	30	15	30	15	30
Minimum virtual machine disk size (TB)	1.8	2.2	2.2	1.9	2.9	2.6	3.8	3.3	4.0	2.5	5.9	3.7

Capacities

Use this table to determine the configuration to use for your deployment.

- Select the size that provides the capacities you require.
- If any capacity requires a larger configuration, use the larger configuration option.
  - For example: If you need 100000 agent skill pairs but your peak busy-hour call volume is 200000, you must select the medium configuration.
- The Extended capacity option is only applicable for the AXP Private – Extended Scale ACD.
- Deployments on Avaya Solutions Platform support the small, medium, and large configuration options only.

Parameter	Small	Medium	Large	Extended
Peak busy-hour call volume	30000	200000	400000	500000
Concurrent CMS Supervisor sessions[1]	50	200	2999	2999
Concurrent agents	500	5000	10000	30000
Third-party software	3	3	3	3
Agent skill pairs	100000	200000	800000 [2]	1500000[2]
Reports per CMS Supervisor session	3	5	10 [3]	15[3]

Table continues…

Parameter	Small	Medium	Large	Extended
Report elements [4]	5	5	12	12
Percentage of supervisors that can run reports with a three-second refresh rate	10%	50%	100%	100%
Active agent traces	250	1000	5000	5000
Internal Call History (ICH) records - per 20 minutes	4000	4000	4000	4000
External Call History (ECH) records - per 20 minutes	10000	60000	300000	300000

1. This value is the total number of active CMS Supervisor PC Client and Web Client sessions.
2. For actual capacity details, see *Avaya Call Management System Overview and Specification*.
3. For actual capacity details, see *Avaya Call Management System Overview and Specification*.
4. For a definition of Report elements, see *Avaya Call Management System Overview and Specification*.

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*	

Table continues…

Parameter	Example	Your value
Hostname for the CMS server Use only the short hostname, not the FQDN. The hostname cannot have upper-case letters. **Important:** The CMS backup process automatically assigns time-stamped file names that truncate the CMS server hostname if it 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 hostname when you have multiple CMS servers in your deployment.	*vm_cms1*	
Domain name	`example.com`	
IP address	`123.45.67.89`	
Netmask	`255.255.255.0`	
Default gateway IP address	`123.45.67.254`	
DNS IP addresses Uup to 3 addresses 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 3: Preparing OVA deployment

Preparing OVA deployment checklist

No	Task	Notes	✔
1.	**Activate the license for the CMS server.**	Activating the license for a CMS server on page 17	
2.	**Install the license file on the WebLM server.**	Installing a license file on a WebLM server on page 19	
3.	**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 20.	

Cloned and copied OVAs are not supported

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

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 19.
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 through PLDS. For CMS licensing, use either a standalone WebLM server or install the WebLM server on a coresident Avaya Aura® System Manager. Licenses installed for WebLM must support SHA256 digital signatures and a 14-character host ID.

Important:

Use Centralized licensing for CMS. Enterprise licensing is not supported. This means that 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 the information about license file installation errors in *Administering standalone Avaya WebLM*.

Procedure

1. Log in 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 various reasons. For example, the digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.

An error can also occur if the current capacity use exceeds the capacity in the installed license.

6. Enable Centralized licensing as described 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 to assign to the CMS.
9. Select the license file to associate with the CMS.

Downloading software from PLDS

About this task

- For deployment to a VMware server, download the ova file with the CMS major and minor release name, such as `CMS-R21.0.0.1.ab.b-e810-00-1.ova`.
- For deployment to a KVM server, download the ova file with the kvm designation, such as `CMS-R21.0.0.1.ab.b-kvm-e810-00-1.ova`.

Procedure

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

   Note:

   The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download

(stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

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

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

Chapter 4: Deploy CMS OVA on a VMware server

Deploying CMS software checklist

No	Task	Notes	✔
1.	**Deploy the OVA software.**	For more information, see Deploying the OVA on page 22.	
2.	**Configure the virtual machine for automatic startup.**	Configuring the virtual machine automatic startup settings on VMware on page 26	
3.	**Configure the virtual machine configuration.**	Configuring the virtual machine as a small configuration on page 27 Configuring the virtual machine as a medium configuration on page 28 Configuring the virtual machine as a large configuration on page 29	
4.	**Power up the virtual machine for the first time.**	For more information, see Powering up the virtual machine on page 37.	

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.

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 the signed 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 or VMFS6 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.

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**.

Chapter 5: Deploy CMS OVA on a KVM server

This section of the document covers the processes for deploying CMS as a new virtual machine on a KVM server.

Note:

- For the ASP 130 R6 you cannot use Solution Deployment Manager for the installation of CMS KVM images, Feature Packs, Service Packs, Patches, and Hot fixes. You must follow the CLI instructions for installation of those artifacts.

Planning checklist for CMS KVM deployment

Ensure that the customer completes the following before deploying the Avaya application KVM images on Avaya-supplied ASP 130 R6.

No.	Task	Notes	✔
1.	**Check the hardware platform**	For ASP 130 R6, A1SC configurator output should be utilized to determine which applications are to be deployed on which server/host.	
2.	**Plan the staging and verification activities and assign the resources**	This must include network topology, IP addressing, naming conventions, and application specific configuration and administration.	
3.	**Purchase the appropriate order codes**	Reach out to the Avaya account team for detailed information on ordering ASP 130 R6. Note that with the introduction of ASP 130 R6, there is no longer a license key present on the server. However, it is imperative that customers have a record in PLDS for each instance of the ASP 130 R6 server as customers and Avaya are subject to audits to ensure right to use royalties have been paid.	
4.	**Read the Avaya server documentation**	Navigate to https://support.avaya.com and search for Avaya Solutions Platform, Release ASP 130 R6.	

Table continues…

No.	Task	Notes	✔
5.	**Download the latest CMS software**	Reference the CMS R21 Release Notes, Product Correction Notices, and software downloads for specific PLDS IDs links to the CMS KVM images. The deployment process for Feature Packs, Service Packs, patches, and hot-fixes is the same regardless of the underlying hypervisor.	

Preparing the CMS KVM file

About this task

Avaya supplies the KVM files as an KVM OVA file. That file contains a `.qcow2` file you can use to create a CMS virtual machine.

Before you begin

- Download the CMS KVM OVA file from Avaya PLDS. For example, `CMS-R21.0.0.1.ab.b-kvm-e810-00-1.ova`.

Procedure

1. Login to KVM CLI as the *custadm* user.
2. Run `sudo ls -ld /var/lib/libvirt/staging`.
3. Check that the directory `/var/lib/libvirt/staging` is listed.
   - If the directory does not exist, create it by running the following commands:

     ```
     sudo mkdir /var/lib/libvirt/staging
     sudo chown custadm:wheel /var/lib/libvirt/staging
     ```
4. Check that the directory permissions shown as match `drwxr-x---`.
   - If the permissions do not match, change them using the following command. This allows *custadm* to write into the directory folder using **sudo** commands.
   - `sudo chown custadm:wheel /var/lib/libvirt/staging`
5. Verify there is sufficient free-space to copy the size of the KVM image. There needs to be a minimum of 800 GB free space.
6. Copy the downloaded `CMS-R21.0.0.1.ab.b-kvm-e810-00-1.ova` file into the `/var/lib/libvirt/staging` directory.
7. Extract the contents of the ova using the command:

   `tar -xvf CMS-R21.0.0.1.ab.b-kvm-e810-00-1.ova`

This extracts the following files

- `CMS-R21.0.0.1.ab.b-kvm.ovf`
- `CMS-R21.0.0.1.ab.b-kvm.mf`
- `CMS-R21.0.0.1.ab.b-kvm-1.qcow2`

8. The `.qcow2` file is in thin provisioning format. To create a copy that is thick provisioned file, run the command:

   ```
   sudo qemu-img convert -O qcow2 -o preallocation=full CMS-R21.0.0.1.ab.b-kvm-1.qcow2 CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2
   ```

   This operation takes around 45 minutes.

9. Verify that the thick provision copy is 800 GB by running the command:

   ```
   sudo qemu-img info CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2
   ```

10. Move the thick provisioned file image to the virtual machine images directory:

    ```
    sudo mv -i CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2 /var/lib/libvirt/images
    ```

11. Change the file owner and file permission by running following commands:

    ```
    sudo chown qemu:qemu /var/lib/libvirt/imagesCMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2
    sudo chmod 640 /var/lib/libvirt/images/CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2
    ```

12. You can now delete the downloaded `CMS-R21.0.0.1.ab.b-kvm-e810-00-1.ova` file and extracted files from the `/var/lib/libvirt/staging` folder.

Next steps

- You can now use the KVM image file to create a CMS virtual machine. See Importing the CMS virtual machine on page 34.

Importing the CMS virtual machine

About this task

Use this process to use the `.qcow2` file as the virtual drive for a new CMS virtual machine.

Before you begin

- Prepare the CMS `.qcow2` disk image. See Preparing the CMS KVM file on page 33.

Procedure

1. Login to the KVM web console in the following format: `https://<IP address or FQDN of KVM host>:9090`
   - Use the same credentials that you used to access the KVM host by SSH.

- If your web console session shows "Limited Access", click **Turn on administrative access**. This is equivalent to using sudo and web console may prompt you for your credentials.

2. Navigate to **System** > **Virtual machines** > **Import VM**.
3. In the **Name** field, enter a name for the CMS virtual machine.
4. In the **Disk Image** field, enter `/var/lib/libvirt/images` and select the `CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2` image.
5. In the **Operating system** field, select **RHEL 8.10**.
6. In the **Memory** field, select the required memory in MB format.
   - For more information on footprints, see Virtual machine resource requirements and average utilization on page 12.
7. Click **Import and edit**.
8. In the **CPU** field, click **edit**.
   a. Increase the values in the **vCPU Maximum** and **vCPU Count** fields to match the footprint requirement (see Virtual machine resource requirements and average utilization on page 12). Set the same value in each field.
   b. Click **Apply**.
9. In the **Firmware** field, select **BIOS** and click **Save**.
10. Under the **Disks** section:,
    a. Check that the `CMS-R21.0.0.1.ab.b-kvm-1-THICK.qcow2` image disk image size is correctly displayed in the **Capacity** field.
    b. Click **Edit**.
    c. In the **Bus** field select **scsi**.
    d. In the **Cache** field select **directsync**.
    e. Click **Save**.
11. In the **Networking** section:
    a. Click on **Edit**.
    b. Select the required **Network Bridge** and click **Save**.
12. On the virtual machine, click **Run** to start the CMS virtual machine.

Chapter 6: Configuring system features

Following deployment of a new CMS virtual machine, use the processes in this section of the documentation to start and initially configure CMS.

Configuring system features checklist

No	Task	Procedure reference	✔
1.	Verify that CMS is installed by checking the version	Verifying that CMS is installed on page 37	
2	Initialize the CMS database	See Powering up the virtual machine on page 37.	
3.	Set the root password.	Setting the root password on page 38	
4.	Configure the system network.	Configuring the system network on page 39	
5.	Configure WebLM and EASG.	Configuring WebLM, EASG, and the encryption passphrases on page 42	
6.	Install any CMS patches that apply to the CMS release.	Installing CMS patches on page 45	
7.	Update the Linux RPMs for your CMS release, if required.	Updating Linux RPMs on page 45	
8.	Turn on IDS and initialize Informix.	Turning on IDS and adding disk space for medium and large configurations on page 46	
9.	Verify that the CMS system starts up properly and that you can access it remotely.	Verifying system startup and remote access on page 50	
10.	Proceed to configuring CMS features.	See Configuring CMS features checklist on page 52.	

Opening a hypervisor console

About this task

Perform the following steps in a virtual machine (VM) hypervisor console.

Procedure

1. To open a VMware VM console:
   a. Log on to the vSphere web client.
   b. Locate the CMS VM.
   c. Open the remote console or web console.
2. To open a KVM VM console:
   a. Log on to the KVM web client.
   b. Click **virtual machines**.
   c. Select the CMS VM.
   d. Click **Console Expand**.

Verifying that CMS is installed

About this task

Use this process to check the installed CMS version.

Procedure

1. Using the hypervisor console for the CMS virtual machine, log in as *root*. At this point, no password has been set.
2. Enter the following command:

   ```
   rpm -qa cms
   ```

3. Confirm that the displayed version matches the expected CMS version.

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
   - cms190941

   The system displays the Linux command prompt.

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**.

   Hostname for the CMS server

   Important:

   The CMS backup process automatically assigns time-stamped file names that truncate the CMS server hostname if it 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 hostname 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.

Disk encryption

By default, CMS no longer encrypts disks and partitions with CMS data using LUKS encryption. This encryption is generally redundant because supported cloud providers encrypt by default and VMware supports disk encryption natively.

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
- cms190941

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

The following process is exclusive to CMS servers installed from an Avaya provided OVA image. 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 ISO image used for upgrades.

Avaya also releases RPM updates outside of normal CMS releases. In this case, a 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. Check the Avaya Support site to see if there are any new Linux RPM updates for your release of CMS.

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_sec** security script. 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.

Procedure

1. Ensure that you are logged in to CMS with root privileges.
2. Run the following security script command to configure your security settings:

```
/storage/cms_dvd/security/cms_sec
```

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
- cms190941

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
   - cms190941

   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 7: Configuring CMS features

Configuring CMS features checklist

No.	Task	Notes	✔
1.	Assign passwords for the CMS login IDs.	Assigning passwords to the default CMS login IDs on page 52	
2.	View the CMS authorizations to confirm that your licensed features are authorized.	Viewing CMS authorizations on page 53	
3.	Activate the Supervisor web client.	Activating the CMS Supervisor Web Client software on page 53	
4.	Calculate storage requirements for backups.	Calculating data space requirements for CMSADM backups on page 57 Calculating data space requirements for CMS full maintenance backups on page 58	
5.	Set up the Alarm Origination Manager to report alarms to Avaya support or customer management systems.	Setting up the Alarm Origination Manager on page 59	

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 enables 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*.

Managing certificates for Web Client software

About this task

To encrypt communication between browsers and the Web client CMS server you must install a security certificate. Use the following procedure to obtain a signed security certificate.

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. To create and move to a temporary work directory, use the following commands:

   ```
   mkdir /opt/cmsweb/cert/custom
   ```

   ```
   cd /opt/cmsweb/cert/custom
   ```

3. To generate a private key, use the following command:

   ```
   keytool -genkey -alias cmsweb1
   -keyalg RSA -keysize 2048
   -keystore cmsweb.p12
   -dname "CN=[fqdn],OU=CMS,O=Avaya,L=Thornton,ST=Colorado,C=US"
   -ext "SAN=IP:[ip],DNS:[fqdn]"
   ```

   - In the `-dname` part, replace the `[fqdn]` with the FQDN for CMS.
   - In the `-ext` part, replace the `[fqdn]` and `[ip]` with the values for CMS.
   - The `-alias` value must be `cmsweb1` as shown.
   - The `-keystore` value must be `cmsweb.p12` as show.
   - All other values (`-keyalg`, `-kesize`) must be as shown.

4. Enter the keystore password: `cmsweb`.

5. To generate a Certificate Signing Request (CSR), enter:

   ```
   keytool -certreq -keyalg RSA -alias cmsweb1 -file cmsweb.csr
   -keystore cmsweb.p12
   ```

6. To obtain a signed certificate, submit the CSR to the Certificate Authority (CA) using your organization's regular certificate signing procedure.

   - You can use the Avaya System Manager CA function to sign the certificate.

7. Obtain a copy of the root certificate of the CA used in the previous step. For example, *<CARootCert>*`.pem`.

8. If the CA also uses intermediate certificates, obtain copies of those certificates.

9. Copy the signed certificate to `/opt/cmsweb/cert/custom directory`.

10. To import the signed certificate, enter:

    ```
    keytool -import -alias cmsweb1 -keystore cmsweb.p12 -file
    <SignedCert>.pem
    ```

11. To copy the keystore containing the certificate to the CMS Web location, enter:

    ```
    cp cmsweb.p12 /opt/cmsweb/cert/cmsweb.p12
    ```

12. To restart the Web client on the CMS server, enter:

    ```
    cmsweb stop
    cmsweb start
    ```

Next steps

- You need to install the CA root certificate, and any intermediate certificates. See Installing the root certificate and any intermediate certificate for the Web Client software on page 55.

Installing the root certificate and any intermediate certificate for the Web Client software

About this task

You can use this process to install a copy of the root certificate obtained from the Certificate Authority (CA) that you used to sign the CMS security certificate.

If the CA issued any intermediate certificate, you must also import those intermediate CA certificates.

Procedure

1. Copy and paste the root certificate into a file. For example, *<CARootCert>*.pem.
2. To import the certificate: , enter:
   a. Enter:

      ```
      keytool -import -alias root -keystore cmsweb.p12 -trustcacerts
      -file <CARootCert>.pem
      ```

   b. For the password, enter cmsweb.
3. If the CA also requires intermediate certificates:
   a. Copy and paste the intermediate certificate into a file, for example, intermediate.cert.
   b. To import the certificate, enter:

      ```
      keytool -import -alias intermediate -keystore cmsweb.p12
      -trustcacerts -file intermediate.cert
      ```

   c. For the password, enter cmsweb.
4. Copy and paste the new certificate into a file, for example, cmsweb.cert.
5. To import the certificate, enter:

   ```
   keytool -import -alias cmsweb -keystore cmsweb.p12 -trustcacerts
   -file cmsweb.cert
   ```

6. For the password, enter cmsweb.
7. To stop the Web Client software, enter:

   ```
   cmsweb stop
   ```

8. Copy the keystore to the correct location, for example:

   ```
   cp /opt/cmsweb/cert/custom/cmsweb.p12 /opt/cmsweb/cert
   ```

9. To restart the Web Client software, enter:

   ```
   cmsweb start
   ```

Next steps

- Configure the browser to trust the CA. See Installing the root certificate and any intermediate certificate in the browser on page 56.

Installing the root certificate and any intermediate certificate in the browser

About this task

Ensure that your browser is configured to trust the CA. If your organization does not automatically configure this setting, you can manually configure the settings for your browser.

Procedure

1. If using Google Chrome or Microsoft Edge:
   a. Open the browser.
   b. Navigate to **Settings** > **Privacy and security** > **Security** > **Manage device certificates**.
   c. On the Certificates window, click the **Trusted Root Certification Authorities** tab.
   d. In the list of certificates, select the CA root certificate and click **Import**.
2. For Mozilla Firefox:
   a. Import the CA to the Firefox certificate store. If you use Windows, you can open the command line `cmd.exe` using the **Run as Administrator** option.
   b. At the command line, you can use the following command:

      ```
      certutil -addstore -enterprise -f "Root" <CARootCert>.pem
      ```

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 –q cmsweb

   The system displays a message similar to the following example:

   ```
   cmsweb-R{XX}-web{XX}xx.x.x
   ```

   The {XX} in this message is the release version.

Storage requirements for CMS backups

Calculating data space requirements for CMSADM backups

About this task

The command described in this procedure provides a snapshot of the current CMS disk space usage. Run additional checks periodically to see if your storage needs have changed to ensure you have enough backup space.

Procedure

1. Log in to the CMS command line interface with root privileges.
2. Run `df -Th` to get a snapshot of the current disk space usage on the CMS server.

   Information such as the following is displayed:

   ```
   Filesystem     Type      Size  Used Avail Use% Mounted on
   devtmpfs       devtmpfs  7.7G     0  7.7G   0% /dev
   tmpfs          tmpfs     7.7G  4.0K  7.7G   1% /dev/shm
   tmpfs          tmpfs     7.7G  105M  7.6G   2% /run
   tmpfs          tmpfs     7.7G     0  7.7G   0% /sys/fs/cgroup
   /dev/sda2      ext4      9.8G  2.4G  6.9G  26% /
   /dev/sda12     ext4       16G  540M   15G   4% /tmp
   /dev/sda8      ext4      2.9G  268M  2.5G  10% /var
   /dev/sda1      ext4      545M  187M  319M  37% /boot
   /dev/sda13     ext4       12G  1.1G   11G  10% /opt
   /dev/sda3      ext4      9.8G  971M  8.3G  11% /cms
   /dev/sda7      ext4       32G   96K   30G   1% /export/home
   /dev/sda9      ext4      2.0G   36K  1.9G   1% /var/tmp
   /dev/sda10     ext4      2.0G   22M  1.8G   2% /var/log
   /dev/sda6      ext4       86G  5.5G   77G   7% /storage
   /dev/sda11     ext4      9.8G  4.5M  9.3G   1% /var/log/audit
   tmpfs          tmpfs     1.6G     0  1.6G   0% /run/user/0
   ```

3. Add the disk space from the Used column for all `ext4` file systems, except for the `/storage` and `/tmp` directories.
4. Calculate the space you need.

The example in the following table shows the used space for the relevant `ext4` file system directories:

Directory	Used space
`/`	1.6 GB
`/boot`	106 MB
`/var`	240 MB
`/export/home`	49 MB
`/opt`	1.8 GB
`/cms`	354 MB
Total: 4.15 GB	

Calculating data space requirements for CMS full maintenance backups

Procedure

1. Log on to Linux as *root*.

   Important:

   - If using a remote connection, you cannot directly log on as *root*. Instead, log on using an administered CMS user ID and then then use `su - root` to log on with root privileges.

2. Run the following command to set the Informix environment: **`./opt/informix/bin/setenv`**
3. Run `onstat -d`
4. Use the output generated from running this command to estimate 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.

   Note:

   - Bytes to GB conversion factor = 1,073,741,824.
   - Full Maintenance Backup compression ratio = 30 (approximation). 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 that you have enough backup space.

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.

Configuring an Alarm Destination

About this task

Use this procedure to configure an alarm destination.

Procedure

1. Start the AOM tool by running the 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 SNMP user:

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

8. 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)
   ```

9. 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)
   ```

10. 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)
    ```

11. 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)
    ```

12. 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.

13. 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
```

14. 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 8: 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

When you run `cmssvc` and select the **`setup`** option for setting up CMS, all previous setup information is erased. Before running this command option, ensure that you have any old setup information on record.

Before you begin

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

Procedure

1. Ensure that you are logged in to the CMS server with root privileges.
2. Run the `cmssvc` command.

The Call Management System Services menu is displayed:

```
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:
```

Note:

If you are running `cmssvc` for the first time, the Services menu is not displayed. Instead, you are prompted to set up your system as described in Configuring WebLM, EASG, and the encryption passphrases on page 42.

3. At the command prompt, enter `4` to select the **`run_cms`** option.
4. At the command prompt, enter `2` to turn CMS off and keep the Informix Database Server running.
5. To create a new contact center connection, run the `cmssvc` command again.
6. At the command prompt, enter `5` to select the **`setup`** option.
7. At the command prompt, enter `y` to add a new configuration to CMS.

   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)
```

8. Enter the number corresponding to your language.

   For example, you can enter `1` to select English.

   When CMS is ready for adding a new configuration, a message such as the following is displayed: `Customer CMS data successfully initialized`.

9. At the **Enter a name for this UNIX system** prompt, enter the name of the new system.

   You can enter a maximum of 64 alphanumeric characters.

10. At the **Select the type of backup device you are using** prompt, select the backup device type.

    Note that tape backups are no longer supported.

11. Enter the backup device path when prompted.
12. At the **Enter the number of Automatic Call Distribution systems (ACDs) being administered** prompt, enter `1`.
13. At the **Enter switch name** prompt, enter the name of the new contact center.

    You can enter a maximum of 20 alphanumeric characters.

14. Enter the number corresponding to the switch model you want to select.
15. At the **Enter the local port assigned to switch** prompt, enter the local port number.

    The port number must be in the range of 1 through 64 and match the corresponding value defined for the Routing Core Server during the contact center installation.

16. At the **Enter the remote port assigned to switch** prompt, enter the remote port number.

    The port number must be in the range of 1 through 64 and match the corresponding value defined for the Routing Core Server.

17. At the **Enter switch host name or IP Address** prompt, enter the Routing Core Server IP address.

    For the Simplex deployment, specify the static IP address of the Routing Core Server. For the local HA and geo-redundant HA deployments, specify the virtual IP address of the Routing Core Server. You define the Routing Core Server IP addresses in the **megaconfig.yml** file.

18. At the **Enter switch TCP port number** prompt, enter the TCP port number.

    The port number range is 5001 through 5020.

19. At the **Number of splits/skills** prompt, enter the number of skills in your contact center.

    The value range is 0 through 15,000.

20. At the **Total split/skill members summed over all splits/skills** prompt, enter the number of agents in your contact center.

    The value range is 0 through 1,000,000.

21. At the **Number of trunk groups** prompt, enter the number of trunk groups.

The value range is 0 through 400.

22. At the **Number of trunks** prompt, enter the number of trunks in your contact center.

    The value range is 0 through 200,000.

23. At the **Number of unmeasured facilities** prompt, enter the number of facilities in your contact center.

    The value range is 0 through 100,000.

24. At the **Number of call work codes** prompt, enter the number of call work codes in your contact center.

    The value range is 0 through 1,999.

25. At the **Number of vectors** prompt, enter the number of vectors in your contact center.

    The value range is 0 through 32,000.

26. At the **Number of VDNs** prompt, enter the number of VDNs in your contact center.

    The value range is 0 through 30,000.

    You see the message **Setup completed successfully** displayed in the command output.

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

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

    a. Run the `cmssvc` command.

    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 (Automatic Call Distribution 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 91.

Next steps

Continue with Setting up CMS using the flat file on page 80.

Setting up CMS using the flat file

Before you begin

Verify that you have made all edits in the flat file. For more information, see Editing a flat file on page 79.

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 42.

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.

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 9: Performing the customer handover

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.

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

CMS customer handover checklist

No.	Task	Notes	✔
1.	Check the system date and time.	See Verifying the system date and time on page 84.	
2.	Configure CMS warning email forwarding.	See Forwarding CMS warning messages on page 84.	
3.	Check the free-space allocation.	See Checking free space allocation on page 84.	
4.	Test the ACD link.	See Testing the ACD link on page 85.	
5.	Assign customer password.	See Assigning customer passwords on page 86.	
6.	Test the CMS software.	See Testing the CMS software on page 87.	
7.	Finalize the on-site installation.	See Finalizing the on-site installation on page 90.	

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 to 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 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 about backups, see *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. Perform a full maintenance backup to back up historical data.

   You can perform this backup 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 59.

4. Ensure that customer login information and passwords are recorded.

5. Give the passwords, backup media, and software to the CMS administrator.

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

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 Automatic Call Distribution 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 79, and Setting up CMS using the flat file on page 80.

```
# 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):
```

Flat file example

```
# 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
```

Flat file example

```
#    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
```

Flat file example

```
# 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: 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.	All users
Installation and maintenance		
Deploying Avaya Call Management System	Describes how to install and configure CMS in a virtualized VMware or KVM environment.	Implementation engineers, administrators
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
Using Avaya Call Management System High Availability and Admin-Sync	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Upgrading		

Table continues…

Title	Description	Audience
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
Avaya Call Management System Base Load Upgrade	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
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, supervisors
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, support personnel
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, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	All users

Table continues…

Title	Description	Audience
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Avaya Documentation Center navigation

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

Important:

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

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

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

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

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

  You can do the following:

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

  You can do the following:

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

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

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

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

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

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

A

activating
  CMS Supervisor Web Client software ... 53
  license ... 17
adding
  disk space ... 46
alarm destination ... 59, 72
alarm ID ... 65, 74
Alarm Origination Manager
  setting up AOM ... 59
AOM ... 67
AOM configuration ... 59, 62, 65, 66, 72, 74
  using Socket/SAL ... 72
assigning customer passwords ... 86
automatic restart
  virtual machine ... 26
Avaya InSite Knowledge Base ... 105
Avaya support website ... 105
average resource utilization ... 12

C

calculating data space
  CMSADM backup ... 57
  full maintenance backup ... 58
capacities ... 14
certificates
  CMS Supervisor Web Client software ... 53
changing
  root password ... 38
checking free space allocation ... 84
checklist
  configure CMS features ... 52
  configure system features ... 36
  customer handover ... 83
  KVM deployment ... 32
  planning ... 9
  preparing OVA deployment ... 17
  VMware deployment ... 22
clearing SNMP alarms ... 67
clones
  deployment ... 17
CMS configuration
  through a flat file ... 79
CMS login passwords ... 52
CMS patches ... 45
CMS setup
  interactive configuration ... 76
  using a flat file ... 80
CMS SNMP
  alarm information ... 68
CMS software configuration ... 76
CMS Supervisor Web Client software
  activating ... 53
  certificates ... 53
  root certificate ... 55, 56
  starting ... 56
CMS VM ... 11
CMS-MIB.txt file ... 72
collection
  delete ... 103
  edit ... 103
  generating PDF ... 103
  sharing content ... 103
configuration
  customer data ... 15
configuration data ... 15
configure
  CMS features ... 52
  initial configuration ... 36
  system features ... 36
configuring
  EASG ... 42
  encryption passphrases ... 42, 47
  system network ... 39
  virtual machine automatic restart ... 26
  WebLM ... 42
configuring a medium configuration ... 28
configuring AOM ... 72
configuring CMS ... 91
configuring CMS authorizations ... 53
content
  publishing PDF output ... 103
  searching ... 103
  sharing ... 103
  sort by last updated ... 103
  watching for updates ... 103
customer handover ... 83
customer ID ... 66

D

Dell platforms
  for Avaya Solutions Platform ... 11
deploying copies ... 17
deploying OVA
  on Avaya Solutions Platform ... 24
  on customer-provided VMware server ... 22
deployment
  KVM ... 32
  preparing OVA ... 17
  VMware ... 22
deployment guidelines ... 10
deployment overview ... 9
Disk encryption ... 42

disk space
adding 46
document changes 7
document purpose 7
documentation 101
documentation center 103
finding content 103
navigation 103
documentation portal 103
downloading software 11

E

EASG
configuring 42
encryption passphrases
configuring 47

F

finalizing the on-site installation 90
finding content on documentation center 103
flat file example 91
forwarding CMS warning messages 84

H

handover 83
hardware support 11
high availability
VMware 11
hypervisor console 36

I

IDS
starting 46
installation
CMS patches 45
installing
license file 19

K

KB
Support site 105
KVM deployment 32

L

large configuration 29
license 17
limitations 14
Linux RPMs 45

O

opening
hypervisor console 36
OVA 11
OVA deployment 22
OVA deployment options
customer provided OVA 22

P

planning
checklist 9
planning for deployment 9
PLDS
downloading software 20
power up virtual machine 37

Q

QCOW2 11

R

related documentation 101
remote access 50
requirements
virtual machine resources 12
resource requirements 12
root certificate 55, 56
root password 38

S

searching for content 103
security script 46
setting the Informix configuration 75
sharing content 103
small configuration 27
SNMP user 62
software media 11
sort documents 103
starting
CMS Supervisor Web Client software 56
support 105
system startup 50

T

test alarm 66, 74
testing the ACD link 85
testing the CMS software 87

U

update Linux RPMs 45

V

verify
CMS version 37
verifying
remote access 50
system startup 50
verifying the system date and time 84
videos 105
virtual environment 11
virtual machine
automatic restart configuration 26
Powering 37
virtual machine resource average utilization 12
virtual machine resource requirements 12

W

watchlist 103
WebLM
configuring 42
worksheets 15