Deploying Avaya CMS in an Infrastructure as a Service Environment

Release 21.0.2
Issue 2
September 2025

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

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: Introduction 6
Purpose 6
Software delivery 6
Release details of CMS application OVAs 6
Change history 6
Part 1: Deploying CMS on AWS 7
Chapter 2: Avaya Call Management System on AWS overview 8
Prerequisites 8
Networking considerations for Avaya Call Management System deployment in AWS 9
Types of network connections 9
Location of CMS in the VPC 9
Number of direct connections 10
Unsupported features for Avaya Call Management System AWS instances 10
Chapter 3: Planning 11
Planning checklist 11
Instance types and capacities for an AWS deployment 11
High Availability 13
HA CMS and Survivable CMS 13
Chapter 4: Converting an OVA file to an AMI file 15
Checklist for converting an OVA file to an AMI file 15
Creating a bucket for uploading an OVA for AMI conversion 15
Uploading the CMS OVA to the AWS console 16
Creating a Linux Amazon EC2 virtual server instance 16
Obtaining the virtual server instance user ID 18
Importing the OVA for AMI conversion 19
Creating a key pair 22
Launching an Amazon EC2 instance 22
Creating a user access key 23
Chapter 5: Deployment process 24
Deployment checklist 24
Deploying the CMS application AMI 24
Configuring the CMS software 26
Verifying CMS on the AWS instance 26
Chapter 6: Maintenance operations 28
Restoring CMS on a virtual machine 28
Starting an Amazon Web Services instance 29
Stopping an Amazon Web Services instance 30
Rebooting an Amazon Web Services instance 30

Part 2: Deploying CMS on Google Cloud Platform 31
Chapter 7: GCP deployment process 32
Avaya Call Management System deployment on Google Cloud Platform (GCP) 32
GCP deployment checklist 32
Importing CMS into GCP 33
Uploading the CMS OVA file to GCP Cloud Storage 33
Importing the CMS OVA file into GCP 33
Connecting to CMS on the GCP instance 34
Configuring the CMS software 35
Part 3: Resources 36
Documentation 36
Amazon Web Services documentation 38
Finding documents on the Avaya Support website 38
Viewing Avaya Mentor videos 39
Support 40
Using the Avaya InSite Knowledge Base 40

Chapter 1: Introduction

Purpose

This document is for users deploying Avaya Call Management System (CMS) as a virtual machine on Amazon Web Services (AWS) or Google Cloud Platform (GCP).

- If you are deploying CMS on VMware or KVM, see *Deploying Avaya Call Management System*.
- If you are upgrading an existing CMS server, see *Upgrading Avaya Call Management System*.

Software delivery

Download the Open Virtualization Appliance (OVA) file for CMS deployment from the Avaya Product Licensing and Download System (PLDS) website. The OVA includes the CMS application software and the Linux operating system for the virtual machine.

You can use the OVA on AWS and GCP.

Release details of CMS application OVAs

Download the CMS OVA from the Avaya PLDS website at https://plds.avaya.com/.

Avaya packages the CMS software as an OVA file, ready for conversion and deployment on AWS and GCP.

Change history

Issue	Date	Summary of changes
2	November 2024	Performed updates for CMS R21 Feature Pack.
1	June 2024	Revised disk encryption and software delivery information.

Part 1: Deploying CMS on AWS

Chapter 2: Avaya Call Management System on AWS overview

AWS is a cloud services platform that enables enterprises to securely run applications in the cloud. Key components of AWS include Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Hosting Avaya applications on the AWS Infrastructure as a Service (IaaS) platform offers the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure by enabling a shift to operational expense (OPEX).
- Reduces the cost of maintaining data centers.
- Provides a unified platform for application deployment.
- Offers a flexible environment to meet evolving business requirements.

You can connect the following applications to CMS instances on AWS from the on-premises environment:

- Avaya Aura® Communication Manager
- Avaya Professional Services solutions

Related links

Prerequisites on page 8
Networking considerations for Avaya Call Management System deployment in AWS on page 9
Types of network connections on page 9
Unsupported features for Avaya Call Management System AWS instances on page 10

Prerequisites

Before deploying the product, ensure that you have the following:

Knowledge of:

- AWS setup
- Linux® operating system
- Avaya Aura® Communication Manager

Skills to:

- Administer the AWS Management Console
- Manage CMS applications

Networking considerations for Avaya Call Management System deployment in AWS

When you deploy an Avaya application at a main or branch location on AWS, ensure you follow the required networking requirements, including WAN topology, bandwidth, and latency considerations for Avaya applications. Comply with the Avaya network recommendations and AWS networking rules.

AWS has limitations for establishing VPNs and direct connections. For more information about Amazon Virtual Private Cloud (VPC) limits, see the AWS documentation at http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

Important:

Use a direct connection combined with a private WAN and Service Level Agreement (SLA) measures to ensure network quality for signaling and voice traffic. Avaya is not responsible for network connectivity between AWS and customer premises.

Types of network connections

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

Connection type	Resource
VPN Connection	For information about VPN Connections, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html.
Direct Connection	For information about AWS Direct Connections, see https://aws.amazon.com/directconnect/.

Location of CMS in the VPC

The primary function of CMS is to provide reporting for Avaya Aura® Call Center Elite on Communication Manager. To optimize performance, deploy CMS on AWS in the same region as or as close as possible to Communication Manager. Co-location of CMS and Communication Manager in the same AWS Virtual Private Cloud (VPC) is ideal.

You do not need to deploy both CMS and Communication Manager in AWS. CMS can run in AWS while Communication Manager remains on the customer premise or vice versa.

Supervisors access CMS using the CMS Web client or the CMS PC Supervisor client. All supervisors require network connectivity to the CMS deployment in AWS. If a VPN connection is in use, network latency may impact performance.

Important:

Avaya recommends using a direct connection combined with a private WAN connection and SLA measures to ensure network quality for signaling and voice traffic. Avaya is not responsible for network connectivity between AWS and customer premises.

Number of direct connections

You must separate the Supervisor user traffic to CMS from the traffic between Communication Manager and CMS.

Unsupported features for Avaya Call Management System AWS instances

Do not use AWS infrastructure management tools such as Chef, Ansible, and Puppet to automate deployment and configuration tasks.

Chapter 3: Planning

Planning checklist

Complete the following steps before deploying virtual applications in the AWS Management Console:

No.	Task	References	Notes	✔
1	Download the CMS OVA file.	See Release details of CMS application OVAs on page 6.	--	
2	Upload the OVA file to AWS, then convert it to the AMI format.	See the *Converting an OVA file to an AMI file* chapter.	--	
3	Deploy the CMS AMI file into the required AWS configuration.	--	License each CMS instance separately. Each instance corresponds to an OVA installation. To deploy multiple CMS instances, order a separate license for each one.	
4	Configure the required and optional CMS features to complete the installation.	See *Deploying Avaya Call Management System* for the required features and *Maintaining and Troubleshooting Avaya Call Management System* for the optional features.	--	

Instance types and capacities for an AWS deployment

Instance types

The following table lists the minimum resources required for each CMS deployment size.

When selecting an instance type for a CMS deployment, ensure that it meets or exceeds the minimum resource requirements. These resources are necessary to support the capacities described in the table following the instance types.

Important:

- The resource requirements do not match the instance types offered by Amazon. Deploy CMS on an AWS instance type that meets or exceeds the minimum resource requirements.
- Avoid downsizing the resource allocation, as it can impact CMS performance. CMS is a read and write-intensive application. Avaya recommends using the EBS-optimized storage from Amazon.

Server type	Small	Medium	Large
AWS Instance Type	m4.large m5.large	m4.2xlarge m5.2xlarge	m4.4xlarge m5.4xlarge
AWS vCPU	2	8	16
AWS RAM (GB)	8	16	64
Hard Disk Drive (GB)	800	1200	1800
NICs	3	4	4

- The m4.large and m5.large instance types offer moderate network performance. For high network performance, use m4.2xlarge or m5.2xlarge. Consistent network performance is essential to maintain fast refresh rates for reporting.
- The m4.2xlarge, m5.2xlarge, m4.4xlarge, and m5.4xlarge instance types provide more CPU and memory than required for small configurations. When selecting an instance type, evaluate the trade-offs between network performance and instance cost.

Capacities

The AWS instance types listed above support the capacities shown in the following table:

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

- Select the configuration size that provides your required capacities.
- 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, select the medium configuration.

Parameter	Small	Medium	Large
Peak busy-hour call volume	30000	200000	400000
Concurrent CMS Supervisor sessions[1]	50	200	2999
Concurrent agents	500	5000	10000
Third-party software	3	3	3
Agent skill pairs	100000	200000	800000 [2]
Reports per CMS Supervisor session	3	5	10 [3]
Report elements [4]	5	5	12
Percentage of supervisors that can run reports with a three-second refresh rate	10%	50%	100%

Table continues…

Parameter	Small	Medium	Large
Active agent traces	250	1000	5000
Internal Call History (ICH) records - per 20 minutes	4000	4000	4000
External Call History (ECH) records - per 20 minutes	10000	60000	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*.

High Availability

High Availability (HA) CMS and Survivable CMS are Avaya product offers that differ from the duplication or redundancy features provided by AWS.

Contact your account team to discuss deployment options for HA CMS and Survivable CMS.

HA CMS and Survivable CMS

Avaya offers two reliability-focused options for CMS: High Availability (HA) CMS and Survivable CMS.

With HA CMS, you deploy two CMS systems that both receive identical call data from the same Communication Manager. This setup ensures redundancy by duplicating the Automatic Call Distribution (ACD) data across both systems, improving reliability during network or server failures.

Survivable CMS enhances system reliability by collecting call data from the Communication Manager Survivable Core and Survivable Remote technologies. Survivable CMS supports the following deployment models:

- Dual Role CMS: The HA CMS connects to Communication Manager and Survivable Core or Remote.
- Dedicated Survivable CMS: A separate CMS connects only to Survivable Core or Remote.

Survivable CMS helps users stay productive and minimizes service disruption even if the main site becomes unavailable due to network or server failures.

When deploying HA CMS, Survivable CMS, or a combination on AWS, each CMS must have its own OVA file. Each virtual machine must be set up as an active, licensed CMS to function correctly.

Along with the ACD data redundancy offered by HA CMS and the data resiliency provided by Survivable CMS, Avaya includes a feature that synchronizes administrative data from the primary

CMS to the HA CMS or Survivable CMS deployment. This synchronization ensures that all systems stay aligned with the latest administrative data.

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

Chapter 4: Converting an OVA file to an AMI file

Checklist for converting an OVA file to an AMI file

Use the following checklist to help you convert the CMS OVA file to an Amazon Machine Image (AMI):

Task	Link/Notes	✔
Create a bucket to upload the OVAs.	Creating a bucket for uploading an OVA for AMI conversion on page 15	
Upload the CMS OVA file.	Uploading the CMS OVA to the AWS console on page 16	
Create an Amazon EC2 virtual server instance.	Creating a Linux Amazon EC2 virtual server instance on page 16	
Create an access key.	Creating a user access key on page 23	
Obtain the virtual server instance user ID.	Obtaining the virtual server instance user ID on page 18	
Import the OVA for AMI conversion.	Importing the OVA for AMI conversion on page 19	

Creating a bucket for uploading an OVA for AMI conversion

About this task

To learn more about creating a bucket, choosing a region, and managing other settings, visit the following website: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-bucket.html

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Storage** > **S3**.

   The system displays the S3 Management Console page.

3. Click **Create bucket**.

   The system displays the Create bucket dialog box.
4. In **Bucket name**, type a unique bucket name.

   Use lowercase letters throughout the name.
5. In the **Region** field, click a region for your bucket.
6. Click **Create bucket**.

Uploading the CMS OVA to the AWS console

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Storage** > **S3**.

   The system displays the S3 Management Console page.
3. In All Buckets, click a bucket name.
4. Click **Upload**.

   The system displays the Upload - Select Files and Folders dialog box.
5. Click **Add Files**.
6. In the Choose File to Upload dialog box, select the CMS OVA file from your local system, and click **Open**.
7. Click **Upload**.

Creating a Linux Amazon EC2 virtual server instance

About this task

If you are using the AWS CLI, you do not need to follow this procedure.

Procedure

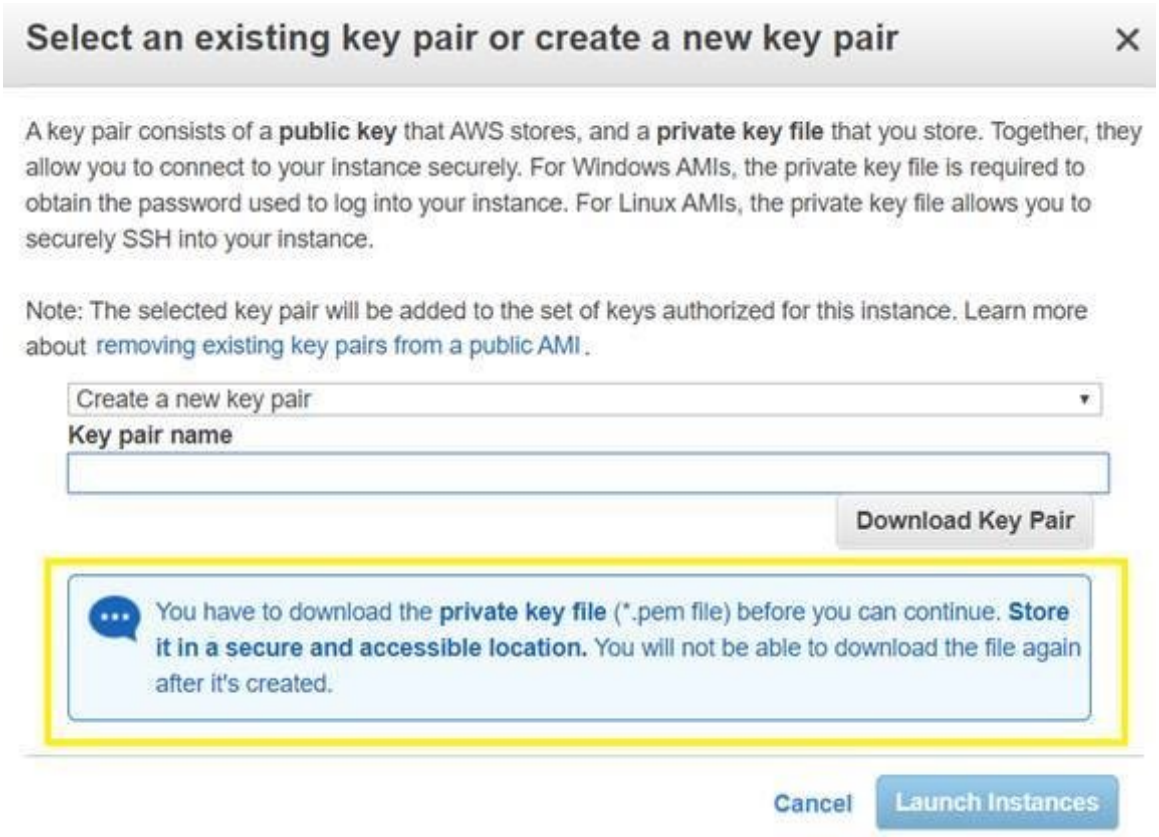
1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Compute** > **EC2**.

   The system displays the EC2 Management Console page.
3. Click **Launch Instance**.
4. On the Choose an Amazon Machine Image (AMI) page, search for a Linux AMI, and click **Select**.

Select an image that includes the AWS command line tools.

5. On the Choose an Instance Type page, select an instance type, and click **Next: Configure Instance Details**.
6. On the Configure Instance Details page, do the following:
   a. In the **Network** field, click a Virtual Private Cloud (VPC) network.
   b. In the **Network interfaces** section, assign an IP address.
7. Click **Next: Add Storage**.
8. On the Add Storage page, leave the default settings, and click **Next: Add Tags**.
9. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.
10. On the Configure Security Group page, create a new security group or select an existing security group, and click **Review and Launch**.
11. On the Review Instance Launch page, review the details of each configuration, and then click **Launch**.

    The system displays the following screen:



12. On the Select an existing key pair or create a new key pair dialog box, select one of the following options:
    - **Choose an existing key pair**: If you select this option, perform the following:
      - From the **Select a key pair** drop-down list, select a key pair.
      - Select the **I acknowledge that I have access to the selected private key file (<example.pem>), and that without this file, I won't be able to log into my instance** check box.
    - **Create a new key pair**: If you select this option, perform the following:
      - In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
      - Click **Download Key Pair**.
      - Save the file in a secure and accessible location.

        Note:

        You cannot download the file again.
    - **Proceed without a key pair**: If you select this option, select the **I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI** check box.
13. Click **Launch Instances**.

    The system creates the virtual server instance.
14. Click **Launch Status**, and click **View instance**.

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

Obtaining the virtual server instance user ID

Procedure

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

   The system displays the EC2 Management Console page.
3. In the left navigation pane, click **Instances**.
4. Select a server instance, and click **Connect**.
5. On the Connect To your Instance page, view the user ID.

   For example:

   ```
   ssh -i "example.pem" ec2-user@<IP address>
   ```

The username is `ec2-user`. Use this user ID to connect to the Linux server.

Importing the OVA for AMI conversion

Before you begin

- Create an access key. For more information, see Creating an access key.
- Obtain the user id. For more information, see Obtaining the virtual server instance user id.
- Convert the `*.pem` file to the `*.ppk` format and configure PuTTY to establish an SSH connection. For more information, see Configuring PuTTY.

Procedure

1. Open an SSH session.
2. In **Host Name (or IP address)**, type the IP Address of the virtual server instance, and click **Open**.
3. Log in to the Linux server, and run the following command: **`aws`**.
4. To configure the AWS details, run the following command: **`aws configure`**, and do the following:
   a. In **AWS Access Key ID**, type the AWS access key ID.
   b. In **AWS Secret Access Key**, type the AWS secret access key ID.
   c. In **Default region name**, type the region name.

      For example: us-west-2.

   d. In **Default output format**, type `text` or `json`.
5. To check whether the EC2 instance is ready to use, run the following command: **`aws s3 ls`**.

   The system displays the S3 bucket that you created.
6. To view the content of the S3 bucket, run the following command: **`aws s3 ls s3://<nameofbucket>`**.

   Note:

   The **`aws s3 ls s3://<nameofbucket>`** command fails if the Virtual Private Cloud (VPC) has DNS resolution disabled.
7. To enable importing files into the EC2 instance, create a vmimport role and attach policies as mentioned in the following sub-steps:
   a. Create a file named `trust-policy.json` with the following policy:

```
{ "Version":"2012-10-17", "Statement":[ { "Sid":"", "Effect":"Allow",
"Principal":{ "Service":"vmie.amazonaws.com" }, "Action":"sts:AssumeRole",
"Condition":{ "StringEquals":{ "sts:ExternalId":"vmimport" } } } ] }
```

b. Use the **create-role** command to create a role named `vmimport` and give VM Import/Export access to it.

   Ensure that you specify the full path to the location of the `trust-policy.json` file, and prefix `file://` to it:

```
aws iam create-role --role-name vmimport --assume-role-policy-document
file://trust-policy.json
```

c. Create a file named `role-policy.json` with the following policy:

   Where <your_bucket_name> is the bucket that includes the OVA:

```
{
"Version":"2012-10-17",
"Statement":[
{
"Effect":"Allow",
"Action":[
"s3:ListBucket",
"s3:GetBucketLocation"
],
"Resource":[
"arn:aws:s3:::<your_bucket_name>"
]
},
{
"Effect":"Allow",
"Action":[
"s3:GetObject"
],
"Resource":[
"arn:aws:s3:::<your_bucket_name>/*"
]
},
{
"Effect":"Allow",
"Action":[
"ec2:ModifySnapshotAttribute",
"ec2:CopySnapshot",
"ec2:RegisterImage",
"ec2:Describe*"
],
"Resource":"*"
}
]
}
```

d. Use the following **put-role-policy** command to attach the policy to the role created in the preceding step.

   Ensure that you specify the full path to the location of the `role-policy.json` file.

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-
document file://role-policy.json
```

8. To import the OVA for conversion, type the following command: **aws ec2 import-image --cli-input-json "{ \"Description\": \"<Server OVA>\", \"DiskContainers\": [{ \"Description\": \"<text description of task>\", \"UserBucket\": { \"S3Bucket\": \"<your_bucket_name>\", \"S3Key\" : \"<server.ova>\" } }]}"**

Ensure to replace appropriate values wherever brackets <> are present in preceding command.

The system displays the **Status** and the **ImportTaskId** parameters.

9. To check the status of the import image, run the following command: **`aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\": [\"<Your_ImportTaskId>\"], \"NextToken\": \"abc\", \"MaxResults\": 10 } "`**

   Where, **ImportTaskId** is the one from the output of Step 8. For example, `import-ami-ffmanv5x`.

   The conversion process takes up to 30 minutes. You can run the preceding command repeatedly. When the AMI conversion is successful, the system displays the **Status** as `completed` and **ImageId**.

   In the following example, the process is at the update stage and is 30% complete.

   ```
   [ec2-user@ip-10-143-10-81 ~]$ aws ec2 describe-import-image-tasks --cli-input-
   json "{ \"ImportTaskIds\": [\"import-ami-ffgji45r\"], \"NextToken\": \"abc\",
   \"MaxResults\": 10 } " IMPORTIMAGETASKS <Avaya application>-07.1.0.0.xxx-
   aws-001.ova import-ami-ffgji45r 30 active updating
   ```

   In the following example, the process is preparing the AMI and is 76% complete.

   ```
   IMPORTIMAGETASKS x86_64 <Avaya application>-07.1.0.0.xxx-aws-001.ova import-ami-
   ffgji45r BYOL Linux 76 active preparing ami
   ```

   The output format varies depending on the selection of the text or JSON format on the aws CLI configuration.

   For more information, see AWS Import your VM as an image on the AWS website at http://docs.aws.amazon.com/vm-import/latest/userguide/import-vm-image.html.

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

    The system displays the EC2 Management Console page.

12. In the left navigation pane, click **IMAGES** > **AMIs**.

    You can search the converted AMI with **ImageId**. The system displays the newly converted AMI **ImageId** in the **AMI ID** column.

    You can give an appropriate name for the AMI **ImageId**.

Creating a key pair

About this task

A key pair consists of a public key and a private key. The public key encrypts data, such as login credentials, and the private key decrypts it. You provide the key pair when creating a CloudFormation stack and use it to access Amazon Machine Instances through SSH.

For more information, see the following website: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

Procedure

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

   The system generates a `*.pem` file and prompts you to save the file to your computer. You can also view the key pair name in the Key pair name column.
6. Save the `*.pem` file.

   Important:

   When you create a key pair, save it. If you lose the key, you cannot retrieve it, and you cannot access the instance.

Launching an Amazon EC2 instance

Procedure

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

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **IMAGES** > **AMIs**.
4. Select the Avaya Call Management System (CMS) AMI, and click **Launch**.

Creating a user access key

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **Services** > **Security, Identity, & Compliance** > **IAM**.

   The system displays the Welcome to Identity and Access Management page.
3. In the left navigation pane, click **Users**.
4. Click a user name.
5. On the Summary page, click the **Security Credentials** tab.
6. In the Access Keys section, click **Create Access Key**.

   The system displays the message: `Your access key has been created successfully.`

   Important:

   When you create a security access key, save it. If you lose the security access key, you cannot retrieve it.

Chapter 5: Deployment process

Deployment checklist

Task	Notes	✔
Complete all the planning and configuration requirements.	For information about planning and configuring, see the Planning chapter.	
Deploy the AMI converted from the CMS OVA.	Deploying the CMS application AMI on page 24.	
Configure the AWS deployment for a small, medium, or large configuration.	Instance types and capacities for an AWS deployment on page 11.	
Complete the deployment by following the standard CMS deployment process.	Configuring the CMS software on page 26.	

Important:

You must license each CMS instance, that is, each AMI deployment. To deploy multiple CMS AMI instances, customers or business partners must order a separate CMS license for each AMI deployment.

Deploying the CMS application AMI

Before you begin

Convert the CMS OVA to AMI. For more information, see Checklist for converting an OVA file to an AMI file on page 15.

Procedure

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

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **IMAGES** > **AMIs**.

   The system displays the list of AMIs.
4. Select the Contact Center application AMI, and click **Launch**.

5. On the Choose an Instance Type page, select an instance type, and click **Next: Configure Instance Details**.

   Select the correct instance type for deploying the AMI. Selecting an incorrect instance type can affect the usability of the system.

6. On the Configure Instance Details page, do the following:

   a. In the **Network** field, click a Virtual Private Cloud (VPC) network.

   b. In the **Network interfaces** section, assign an IP address.

   On the Configure Instance page, configuration is different for different products. For information about application specific configuration, see the product-specific AWS deployment guide on the Avaya Support website at http://support.avaya.com/.

7. Click **Next: Add Storage**.

8. On the Add Storage page, leave the default settings, and click **Next: Add Tags**.

9. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.

10. On the Configure Security Group page, create a new security group or select an existing security group, and click **Review and Launch**.

    Select the security group that has the required ports enabled. For information about ports, see port matrix on the Avaya Support website at http://support.avaya.com/.

11. On the Select an existing key pair or create a new key pair dialog box, select one of the following options:

    - **Choose an existing key pair**: If you select this option, perform the following:
      - From the **Select a key pair** drop-down list, select a key pair.
      - Select the **I acknowledge that I have access to the selected private key file (<example.pem>), and that without this file, I won't be able to log into my instance** check box.
    - **Create a new key pair**: If you select this option, perform the following:
      - In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
      - Click **Download Key Pair**.
      - Save the file in a secure and accessible location.

        Note:

        You cannot download the file again.
    - **Proceed without a key pair**: If you select this option, select the **I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI** check box.

12. Click **Launch Instances**.

    The system creates the instance and displays it on the Instances page.

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

Configuring the CMS software

About this task

Use the procedures referenced in this section to configure required and optional features on a newly deployed CMS.

Before you begin

Gather the following documents:

- *Deploying Avaya Call Management System*
- *Maintaining and Troubleshooting Avaya Call Management System*

Procedure

1. Complete the procedures in the Configuring system features chapter of *Deploying Avaya Call Management System*.
2. Complete the procedures in the Configuring CMS features chapter of *Deploying Avaya Call Management System*.
3. Set up CMS as described in the Setting up CMS chapter of *Deploying Avaya Call Management System*.
4. Install and configure any optional CMS features as described in the Installing and configuring optional software chapter of *Maintaining and Troubleshooting Avaya Call Management System*.
5. Set the correct time and date on the system as described in *Maintaining and Troubleshooting Avaya Call Management System*.
6. Complete the procedures in the Turning the system over to the customer chapter of *Deploying Avaya Call Management System*.

Verifying CMS on the AWS instance

Procedure

1. Log on to the AWS console.
2. Click **EC2**.
3. On the left pane, click **Instances**.
4. From the drop-down list, click **Instances**.

5. Click on the instance you have created.
6. Click **Actions**.
7. From the drop-down list, click **Instance State**, and click **Start**.

   The system creates the instance and displays it on the Instances page.

   When the system creates an instance, the **Status Checks** column displays the message: `2/2`.
8. SSH to CMS server IP address.
9. Log in as `cms` using the initial password: `avayacloud516`.

   The system displays a console terminal window.
10. Log in as root using the **`su - root`** command.

    To change the System Name, you can use the **`netconfig`** command. For information on the instructions to run the **`netconfig`** command, see *Maintaining and Troubleshooting Avaya Call Management System*.

Chapter 6: Maintenance operations

Backing up CMS on a virtual machine

For information about backing up CMS on a virtual machine, see *Maintaining and Troubleshooting Avaya Call Management System*.

Restoring CMS on a virtual machine

About this task

If your AWS deployment fails or the CMS software becomes corrupted, use this procedure to restore your system.

Procedure

1. Deploy the AMI as a new installation.
2. Set up networking as described in the Configuring the system network section of *Deploying Avaya Call Management System*.
3. Perform a CMSADM restore as outlined in the Restore CMS setup using a CMSADM backup section of *Maintaining and Troubleshooting Avaya Call Management System*.
4. Log in using a CMS user ID. For example, `cms`.
5. Log in as root using the **`su - root`** command.

   The restore process continues automatically. It can fail if the system detects changes in the CMS hardware configuration.

   If the setup fails, the system displays messages similar to the following:

   ```
   <timestamp> ERR:CMS Setup has failed 3 times.
   <timestamp> ERR:View the admin.log file for details on status.
   <timestamp> ERR:You will need to manually resolve the problem.
   <timestamp> ERR:The most likely cause is an error in or problem
   <timestamp> ERR:with the CMS Setup flat file.
   <timestamp> ERR:CMS Restore failed to complete.
   ```

6. To verify that the license file authorizes the CMS hardware feature, do the following:
   a. Enter `cmssvc`.
   b. Enter the number for the **auth_display** option.

c. Review the list of authorizations and confirm the authorization of the CMS hardware feature.

7. To turn off IDS, do the following:
   a. Enter `cmssvc`.
   b. Enter the number of the **run_ids** option.
   c. Enter the number of the **Turn off IDS** option.
8. To set up CMS, enter `/cms/install/bin/restore database`.
9. To confirm that the installation completed successfully, do the following:
   a. Enter `tail /cms/install/logdir/admin.log`.

      The system logs all failure messages in this file. The CMS software setup is successful when the system displays `Setup completed successfully <date/time>`.

   b. If the CMS setup fails, check that the flat file is correct and rerun Step a. If the CMS setup fails again, escalate through the standard support channels.
10. Perform a maintenance restore as described in the Restore CMS data using a CMS Maintenance restore topic of *Maintaining and Troubleshooting Avaya Call Management System*.

Starting an Amazon Web Services instance

Procedure

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

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **Instances**.
4. Select one or more instance, and then click **Actions** > **Instance State** > **Start**.

   The system displays a message to start the instances.
5. Click **Yes, Start**.

   When the system starts the instance, the **Instance State** column displays the state as Running.

Stopping an Amazon Web Services instance

Procedure

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

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **Instances**.
4. Select one or more instance, and then click **Actions** > **Instance State** > **Stop**.

   The system displays a message to stop the instances.
5. Click **Yes, Stop**.

   When the system stops the instance, the Instance State column displays the state as Stopped.

Rebooting an Amazon Web Services instance

Procedure

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

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **Instances**.
4. Select one or more instance, and then click **Actions** > **Instance State** > **Reboot**.

   The system displays a message to reboot the instances.
5. Click **Yes, Reboot**.

Part 2: Deploying CMS on Google Cloud Platform

Chapter 7: GCP deployment process

Avaya Call Management System deployment on Google Cloud Platform (GCP)

Google Cloud Platform (GCP) is a set of cloud computing services. You can use these services to install, configure, and deploy CMS on GCP.

The primary function of CMS is to provide reporting features for Avaya Aura® Call Center Elite functionality on Avaya Aura® Communication Manager. To optimize performance, store the CMS GCP deployment in the same zone as, or as close as possible to, Communication Manager.

You do not have to deploy CMS and Communication Manager in GCP. You can deploy CMS in GCP and Communication Manager on-premise, or vice versa.

Note:

Supervisors can access CMS using CMS Supervisor Web (Web client) or CMS Supervisor (PC client). All users with the Supervisor profile require adequate network access to the CMS deployment in GCP. If supervisors use a VPN connection to access CMS in GCP, they may experience performance issues due to network latency.

Therefore, supervisors must use a direct connection over a private WAN connection, with adequate Service Level Agreement (SLA) measures, to ensure that the network quality is appropriate for signaling and voice traffic.

GCP deployment checklist

Task	Notes	✔
Download the CMS OVA file from the Avaya Support site.	See Importing CMS into GCP on page 33.	
Create a Google Cloud project in the Google Cloud Console.	Follow the instructions to create a Google Cloud project on the Google Cloud docs library.	
Download Google Cloud CLI (gcloud CLI).	Follow the instructions to download and install gcloud CLI on the Google Cloud Docs library.	
Complete the deployment by following the standard CMS deployment process.	See Configuring the CMS software on page 26.	

Importing CMS into GCP

To import CMS into GCP, perform the following steps:

1. Upload the CMS OVA to GCP Cloud Storage.
2. Import the CMS OVA into GCP.

Note:

Ensure that you have stored the CMS R20.0 Cloud OVA file at a location accessible from the GCP console. The file name includes the term `cloud`. For example:

`CMS-R20.0.0.0.ba.o-cloud-e88-00-1.ova`

You can download the CMS R20.0 Cloud OVA file from the Avaya PLDS website at http://plds.avaya.com/.

Related links

Uploading the CMS OVA file to GCP Cloud Storage on page 33
Importing the CMS OVA file into GCP on page 33

Uploading the CMS OVA file to GCP Cloud Storage

Procedure

1. Log in to the GCP console.
2. From the Select a project list, select your project.
3. Navigate to **Navigation menu** > **Cloud Storage** > **Buckets**.
4. To upload the CMS OVA file to a bucket, click the appropriate bucket.
5. Click **Upload Files**.
6. Select the CMS OVA file to upload and click **Open**.

   The GCP Cloud Storage Bucket displays the uploaded CMS OVA file.

Related links

Importing CMS into GCP on page 33

Importing the CMS OVA file into GCP

Before you begin

Ensure that you have installed the Google Cloud CLI (gcloud CLI).

Procedure

1. Log in to the gcloud CLI.
2. To import the CMS OVA file from the Cloud Storage Bucket to Google Console Compute Engine, use the following command:

```
gcloud compute instances import <name of VM>
--os=rhel-8 --source-uri=<gsPATH_TO_OVA_FILE>
```

```
--network=<network to use> --subnet=<subnet to use>
--project=<project ova loaded into>
--zone=<GCP Zone>
```

For example:

```
gcloud compute instances import "cms20"
--os=rhel-8
--source-uri=gs://cms-bucket/CMS-R20.0.0.0.ba.o-cloud-e88-00-1.ova
--network=cms --subnet=cms --project=Avaya-cms --zone="us-east1-b"
```

Related links

Importing CMS into GCP on page 33

Connecting to CMS on the GCP instance

Before you begin

Ensure that:

- The imported VM instance has a firewall rule that enables TCP ingress traffic in the IP range of `35.235.240.0` through `35.235.240.20`, `port: 22`.
- You have installed the Google Cloud CLI (gcloud CLI).

Procedure

1. Log in to the gcloud CLI.
2. To authorize gcloud to access the Cloud Platform with Google user credentials, enter the following command:

   `gcloud auth login`

3. To enable SSH into the CMS virtual machine, enter the following command:

   ```
   gcloud compute ssh <cms user>@<name of VM> --zone=<GCP Zone>
   --project=<project ova loaded into>
   ```

   For example:

   ```
   gcloud compute ssh cms@cms20 --zone "us-east1-b" --project "avaya-cms"
   ```

4. To log in, use the following credentials:

   username: `cms`

   password: `avayacloud516`

5. To log in as root, use the following command:

   `su - root`

Configuring the CMS software

About this task

Use the procedures referenced in this section to configure required and optional features on a newly deployed CMS.

Before you begin

Gather the following documents:

- *Deploying Avaya Call Management System*
- *Maintaining and Troubleshooting Avaya Call Management System*

Procedure

1. Complete the procedures in the Configuring system features chapter of *Deploying Avaya Call Management System*.
2. Complete the procedures in the Configuring CMS features chapter of *Deploying Avaya Call Management System*.
3. Set up CMS as described in the Setting up CMS chapter of *Deploying Avaya Call Management System*.
4. Install and configure any optional CMS features as described in the Installing and configuring optional software chapter of *Maintaining and Troubleshooting Avaya Call Management System*.
5. Set the correct time and date on the system as described in *Maintaining and Troubleshooting Avaya Call Management System*.
6. Complete the procedures in the Turning the system over to the customer chapter of *Deploying Avaya Call Management System*.

Part 3: 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

Table continues…

Title	Description	Audience
Upgrading		
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

Amazon Web Services documentation

For information about the Amazon Web Services documentation, go to the AWS documentation website at https://aws.amazon.com/documentation/.

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.

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.

Index

A

Amazon EC2 virtual server instance
    create 16
AMI installation 24
application software 6
Avaya InSite Knowledge Base 40
Avaya PLDS
    OVA file 6
Avaya support website 40
AWS console 26
AWS instance 11
AWS management 8
AWS virtual instances 24

B

backing up 28

C

capacities 11
CAPEX 8
change history 6
checklist
    converting OVA to AMI 15
    Google Cloud Platform deployment 32
    OVA to Amazon Machine Image 15
CMS AMI
    deploy 24
CMS deployment
    GCP 32
    Google Cloud Platform 32
CMS installation 10
CMS on GCP instance
    connecting 34
CMS OVA
    upload 33
CMS software
    configuring 26, 35
CMS version 28
CMS web client 9
Communication Manager 13
configuring
    CMS software 26, 35
connecting to CMS
    GCP instance 34
creating
    bucket 15
    user access key 23
creating a key pair 22

D

deploy
    CMS AMI 24
deploying CMS
    GCP 32
    Google Cloud Platform 32
documentation 36

E

EC2 30
EC2 management 30

G

GCP deployment
    checklist 32

H

hybrid network connection
    Direct Connection 9
    VPN connections 9

I

importing CMS
    GCP 33
importing CMS OVA 33
importing OVA for conversion 19
instance state 26, 29, 30

K

KB
    Support site 40
key pair
    creating 22

L

launching
    Amazon EC2 instance 22
Linux 8

N

network topology 9

O

obtaining
virtual server instance user ID 18
OVA
upload to the AWS console 16
OVA file 6, 13
AWS 11
OVA to AMI conversion 19
overview 8

R

reboot 30
redundancy 13
related documentation 36
Amazon Web Services 38
AWS 38
restoring 28
restoring CMS 28

S

services 29
supervisor users 10
support 40
survivable CMS 13

U

unique identifier 28
unsupported features for AWS instances 10
upload CMS OVA
GCP Cloud Storage Bucket 33
uploading CMS OVA file 33

V

videos 39
VPN 9

W

WAN connection 9