Deploying Avaya Session Border Controller for Enterprise on an Amazon Web Services Platform

Release 8.1.X
Issue 3
August 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes the procedures to:

- Convert the Avaya Session Border Controller for Enterprise Open Virtualization Application (OVA) software image to the Amazon Machine Image (AMI) software image.
- Deploy the converted Avaya SBCE AMI software image using the Amazon Web Services Management console.
- Deploy Avaya SBCE on Amazon Web Services as a simplex or High Availability (HA) configuration.

This document is intended for people who install and configure Avaya SBCE AMI at a customer site.

Important:

To install High Availability (HA), you must use Avaya SBCE Release 8.1.1 or later.

Change history

Issue	Date	Summary of changes
3	August 2021	Updated the following items: • Planning checklist on page 13 • Configuring the EMS and SBCE deployment types and the network interfaces on page 30 • About licensing requirements on page 44 • Avaya SBCE licensed features on page 45

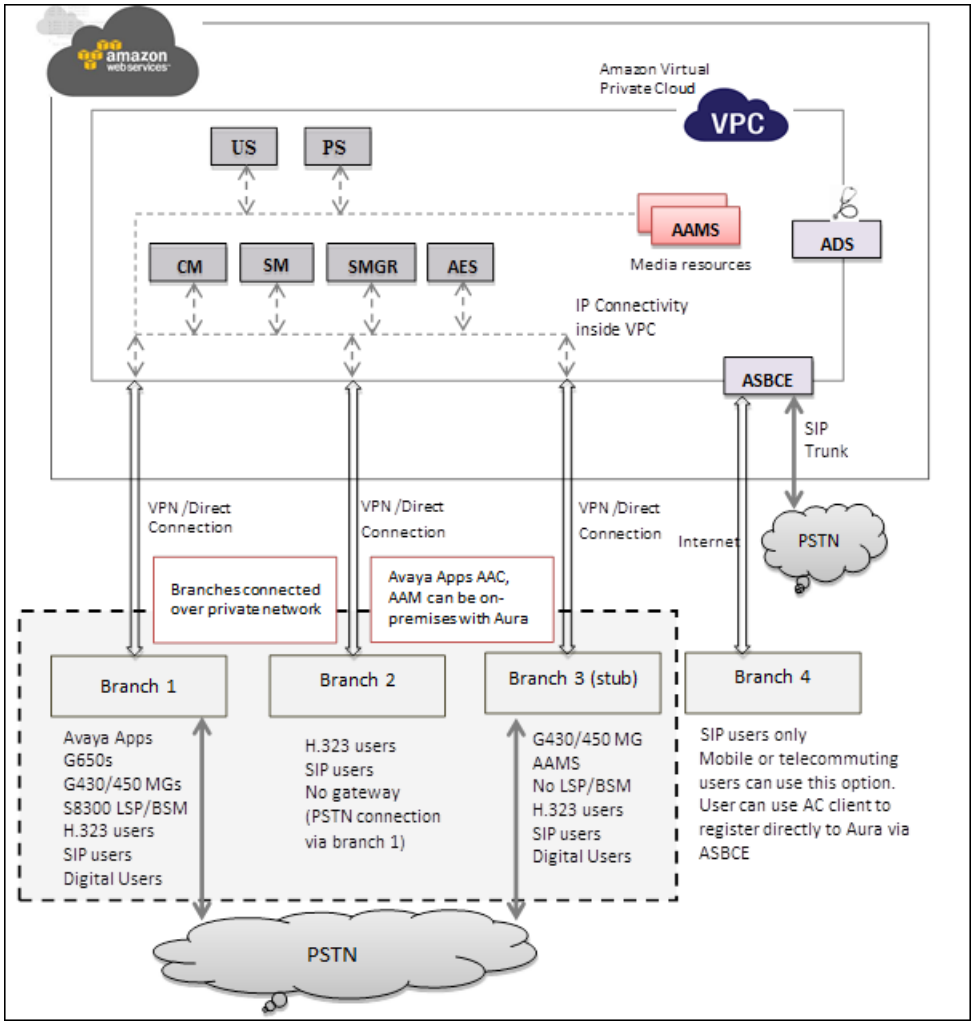
Table continues…

Issue	Date	Summary of changes
2	December 2020	Updated the following items: • Added the file name for the 8.1.2 software to download. • Added the new AWS C5n instance types to Supported instance types for footprints on page 14. • Updated the network interface port numbering in Network interfaces on page 15. • Updated the default password in Password policies on page 15. • Updated the procedures in Deploying EMS and SBCE on a single server using CLI on page 31, Deploying EMS on a dedicated server using CLI on page 34, and Deploying SBCE on a dedicated server using CLI on page 37. • Moved the troubleshooting information to *Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise*.

Chapter 2: Architecture overview

Topology

This network topology diagram depicts the architecture of Avaya applications on Amazon Web Services. The topology diagram is an example of a possible configuration that Avaya offers. The configuration does not need to include all the applications, but must follow the AWS deployment guidelines.



Networking considerations for connecting Avaya applications

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

AWS has some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon Virtual Private Cloud (Amazon VPC) limits, see the AWS documentation at https://docs.aws.amazon.com/vpc/.

Important:

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

Avaya is not responsible for network connections between AWS and customer premises.

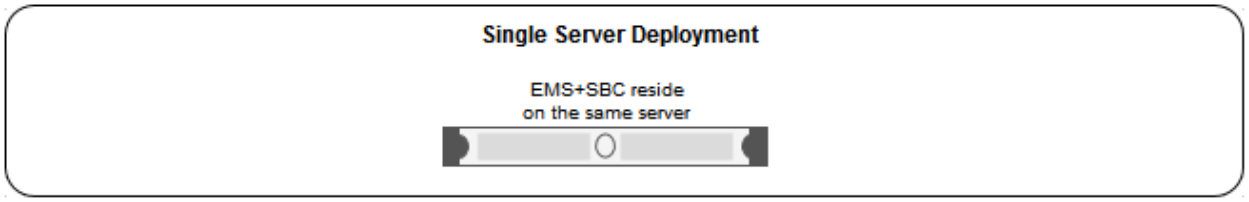
Connection types

You can connect applications in a hybrid network on the Amazon VPC in the following ways:

Connection type	Resource
VPN connection	For information about VPN connections, see: https://docs.aws.amazon.com/vpc/
Direct connection	For information about AWS direct connections, see: https://aws.amazon.com/directconnect/.

Single server non-HA deployment

In a single server non-HA deployment, the Element Management System (EMS) and SBCE software are installed on a single server. Use this deployment scenario when you want to deploy Avaya SBCE in a basic mode.



Important:

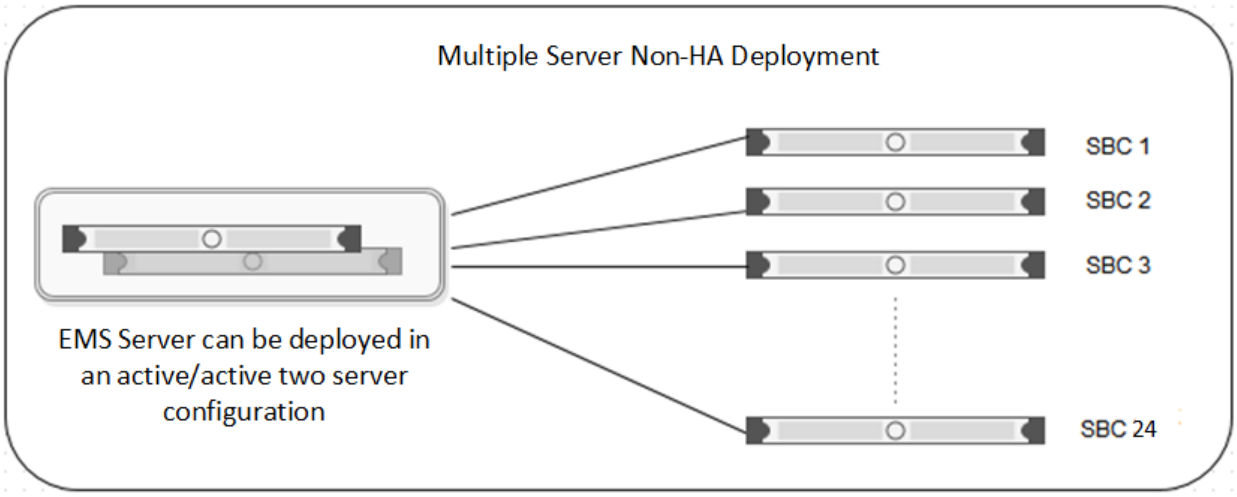
All hardware server types, virtualized environment platforms, and cloud platforms support the single-server non-HA deployment type.

Multiple server non-HA deployment

In a multiple server deployment, the EMS and SBCE software are installed on separate servers.

In a non-HA multiple server deployment, you can have one or more SBCE servers controlled by a single EMS server or a replicated EMS HA pair. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. When using a single EMS server, the EMS server is configured as Primary.

You can have up to 24 individual Avaya SBCE servers in this type of configuration.



If you start with a non-HA deployment and want to later move to an HA deployment, you must completely reconfigure the deployment.

Important:

All hardware server types (except Portwell servers), virtualized environment platforms, and cloud platforms support the multi-server non-HA deployment type.

Multiple server HA deployment

In a multiple server deployment, the EMS and SBCE software are installed on separate servers.

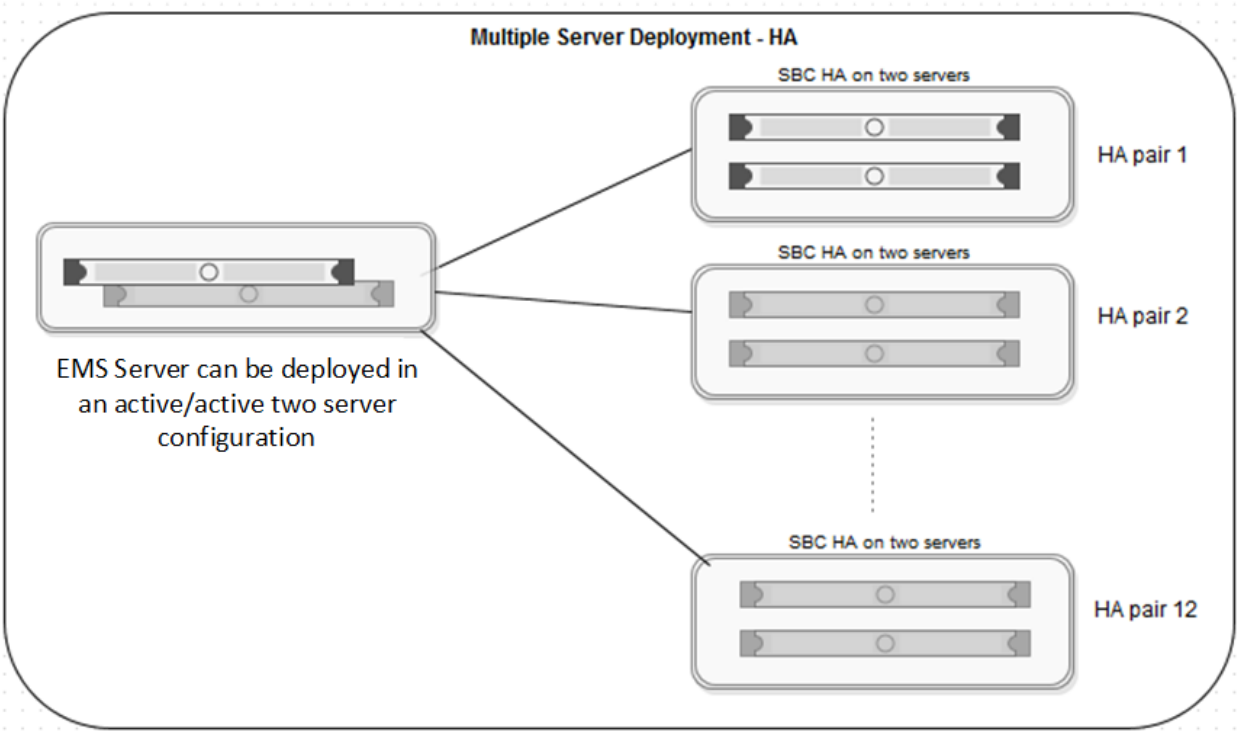
In an HA deployment, SBCE servers are deployed in pairs. Each pair has one SBCE server configured as Primary while the other is configured as Secondary.

Optionally, the EMS software can be replicated in an active/active HA pair deployment. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. An EMS HA pair must be reachable to each other and with the SBCE servers, and can be in different geographical locations.

One EMS server or an active/active pair of EMS servers can control up to 12 separate pairs of SBCE servers.

Note:

When deploying an HA configuration on Amazon Web Services, you only have to configure the SBCE software on the primary device



Important:

All hardware server types (except Portwell servers), virtualized environment platforms, and cloud platforms support the multi-server HA deployment type.

Although the HA pairs and non-HA deployments are shown separately in this figure, EMS can control both an SBCE HA server pair as well as a single SBCE server.

SBCE HA server pairs must adhere to the following requirements:

- You can enable and use the HA deployment feature only if the license file contains an HA license.
- The HA pair servers must reachable by the EMS or EMS HA pair servers over the Management Plane (M1).
- The HA pair servers must be reachable between the devices over the Management link (M1) .

- The HA pair servers must have the HA link (M2) reachable between the HA pair servers.
- The HA pair servers must set up to have all the data interfaces between the servers replicated so that the servers are connected in same subnets. For example, the A1 data interface in one SBCE server should be in the same subnet as the A1 data interface of the paired SBCE server. This allows you to meet the requirement that failover be functional in an active/standby mode.
- In a multiple server HA virtualized deployment, when there are multiple HA pairs and automatic IP addressing is being used on the HA link (M2), every HA pair should either have their own isolated vSwitch or each HA pair should use different IP addresses reachable with their HA pairs as stated previously for M2 connectivity.

Chapter 3: Planning and preconfiguration

Planning checklist

Ensure that you complete the following before deploying Avaya SBCE on Amazon Web Services Management console:

Task	Link/Notes	✔
Read all of the topics in this chapter.		
Download the OVA software image file from the Avaya Support Site or from the Avaya PLDS website. For Release 8.1.3.0: • `sbce-8.1.3.0-31-21052-aws-001.ova` For Release 8.1.2.0: • `sbce-8.1.2.0-31-19809-aws-001.ova` For Release 8.1.1.0: • `sbce-8.1.1.0-26-19214-aws-002.ova` For Release 8.1.0.0: • `sbce-8.1.0.0-14-18490-aws-001.ova`	https://support.avaya.com/downloads/ https://plds.avaya.com	
Purchase the required Avaya SBCE licenses. Register for PLDS and perform the following • Obtain the license file. If you are using HA, you must get and install HA licenses. • Activate license entitlements in PLDS.	https://plds.avaya.com	
Log on to the Amazon Web Services Management console.	See Signing in to the AWS Management console on page 17.	
Create a key pair.	See Creating a key pair on page 17.	

Prerequisite knowledge, skills, and tools

Before deploying the product, ensure that you have the following knowledge, skills, and tools.

Knowledge

- Amazon Web Services setup
- Linux® Operating System
- Avaya SBCE

Skills

Ability to administer the AWS Management console, Avaya Aura® applications, and Avaya SBCE.

Tools and utilities

To convert the Avaya SBCE OVA to AMI, to deploy the AMI, and to configure the applications, you need the following tools and utilities:

- A browser for accessing the AWS Management Console.
- AWS CLI, PuTTY, PuTTYgen, WinSCP, and WinZip.

Supported instance types for footprints

Footprint	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
EMS	c4.xlarge	4	7.5	160	2
SBCE	c4.4xlarge	16	30	160	6
EMS+SBCE	c4.4xlarge	16	30	160	6
EMS	c5n.xlarge	4	10	160	2
SBCE	c5n.4xlarge	16	43	160	6
EMS+SBCE	c5n.4xlarge	16	43	160	6

Important:

High Availability (HA) is not supported on the C5n instance type.

Capacities

Number of Remote Worker Registrations	Non-encrypted Calls with Trunking	Encrypted Remote Worker Sessions
5000	5000	1800

Network interfaces

The number of network interfaces that you set up depends the type of Avaya SBCE instance that you are deploying.

The following table shows the relationship between the number of network interfaces and Avaya SBCE deployment configurations:

Number of network interfaces	Type of Avaya SBCE configuration	Interface ports
2	EMS only	M1, M2
4	Small SBCE	M1, A1, B1, M2
6	EMS+SBCE	M1, A1, B1, M2, A2, B2
6	For all other deployment types, such as High Availability (HA)	M1, A1, B1, M2, A2, B2

Supported browsers for Amazon Web Console

For information about supported browsers, see the following website:

https://aws.amazon.com/

Password policies

The root and ipcs passwords are set during product installation. The EMS GUI has a separate password. The default user IDs and passwords are:

- `root/Avaya_123`
- `ucsec/ucsec`

Security alert:

You must change the default passwords for the CLI root and ipcs login IDs after first boot during the installation procedure. You are prompted to enter and confirm the new password. Password restrictions are enforced on the root, ucsec, and ipcs accounts. The new password must meet the following criteria:

- Minimum of 8 characters.
- One uppercase letter, one lowercase letter, and one number.
- One special character from the following: hyphen (-), underscore (_), at sign (@), asterisk (*), or exclamation point (!).You must not use the number sign (#), dollar sign ($), or ampersand (&).

Downloading software from Avaya PLDS

About this task

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements. In addition to PLDS, you can download the product software from http://support.avaya.com/ by navigating to the Support by Product menu at the top of the page.

Procedure

1. To access the Avaya PLDS website, type http://plds.avaya.com/ in your web browser.
2. Type your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. In **Download Pub ID**, type the download pub ID.
8. In the **Application** field, click the application name.
9. In the **Download type** field, click one of the following:
   - **Software Downloads**
   - **Firmware Downloads**
   - **Language Packs**
   - **Miscellaneous**
10. In the **Version** field, click the version number.
11. Click **Search Downloads**.
12. Scroll down to the entry for the download file, and click the **Download** link.
13. Select a location where you want to save the file, and click **Save**.
14. **(Optional)** On Internet Explorer, if you receive an error message, click the install ActiveX message at the top of the page to start the download.

Latest software updates and patch information

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

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

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

Signing in to the AWS Management console

About this task

There are many different ways you can sign in to your AWS account, so step-by-step procedures are not given here. See the following website for more information:

https://aws.amazon.com/premiumsupport/knowledge-center/sign-in-console/

Before you begin

Ensure that you have an AWS account.

Creating a key pair

About this task

A key pair is a set of public and private keys. The public key is used to encrypt data, such as the login password. The private key is used to decrypt the encrypted data. You provide this key pair when you create a CloudFormation stack, and use it for SSH access to the Amazon Machine Instances.

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 Create Key Pair dialog box, 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 on your computer. You can also view the created 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 will not be able to access the instance.

Chapter 4: Converting OVA to AMI

Checklist for converting Avaya SBCE OVA to an AMI

Task	Link/Notes	✔
Create a bucket for uploading the OVAs.	Creating a bucket for uploading an OVA for AMI conversion on page 19	
Upload the Avaya SBCE OVA.	Uploading Avaya SBCE OVA on page 20	
Create an Amazon EC2 virtual server instance.	Creating a Linux Amazon EC2 virtual server instance on page 20	
Create an access key.	Creating a user access key on page 22	
Obtain the virtual server instance user id.	Obtaining the virtual server instance user ID on page 23	
Import the OVA for AMI conversion.	Importing the OVA for AMI conversion on page 23	

Creating a bucket for uploading an OVA for AMI conversion

About this task

For more details about creating a bucket, selecting a region, and administering other options, see 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.

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

Uploading Avaya SBCE OVA

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. From the **All Buckets** section, select a bucket.
4. Click **Upload**.

   The system displays the Upload - Select Files and Folders dialog box.
5. Click **Add Files**.
6. On the Choose File to Upload dialog box, select the Avaya SBCE 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 use the AWS CLI, this procedure is not required.

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**.

   You must 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 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 will not be able to 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`.

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 on 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, you must save it. If you lose the security access key, you cannot retrieve it.

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.

   Example:

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

   The user name 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”.
- Converting the `*.pem` file to the `*.ppk` format and configure PuTTY for establishing 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 command: `aws`.
4. To configure the AWS details, run the 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 command: `aws s3 ls`.

   The system displays the S3 bucket that you created.

6. To view the content of the S3 bucket, run the command: `aws s3 ls s3://<nameofbucket>`.

   Note:

   If DNS resolution for the VPC is disabled, the execution of the **`aws s3 ls s3://<nameofbucket>`** command fails.

7. To allow 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 where the OVA is stored:

   ```
   {
   "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 above.

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 above command.

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

9. To check the status of the import image, run the 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 the Step 8. For example: `import-ami-ffmanv5x`.

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

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 product-specific Avaya Aura® AMI, and click **Launch**.

Chapter 5: Deploying and configuring Avaya SBCE

Deploying an Avaya SBCE AMI software image on AWS

Before you begin

Convert the Avaya SBCE AWS OVA to AMI. For more information, see Checklist for converting Avaya SBCE OVA to an AMI on page 19.

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 **IMAGES** > **AMIs**.

   The system displays the list of AMIs.
4. Select the Avaya SBCE AMI, and click **Launch**.
5. On the Choose an Instance Type page, select an instance type, and click **Next: Configure Instance Details**.

   You must select the correct instance type for deploying the AMI. If you select an incorrect instance type, usability of the system might be impacted. For information about the instance type, see Supported instance types for footprints on page 14.

   For deploying EMS, select c4.xlarge instance type.

   For deploying an SBCE, select c4.4xlarge instance type.
6. On the Configure Instance Details page, do the following:
   a. In the **Network** field, click a VPC network.
   b. In the **Network interfaces** section, assign an IP address.
7. Click **Next: Add Storage**.
8. On the **Add Storage** page, select the **Delete on termination** check box.

   If you select **Delete on termination**, the allocated resources for the instance are deleted when you terminate the instance.

9. Click **Next: Configure Security Group**.
10. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.
11. On the Configure Security Group page, create a new security group or select an existing security group, and click **Review and Launch**.

    You must 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/.
12. Assign an IP address from the subnet, which will be reserved to be assigned from DHCP and used as management IP for this Avaya SBCE instance.
13. 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 will not be able to 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.
14. 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`.

Managing AWS instances

Using the EC2 Management Console, you can start, stop, reboot, and terminate an AWS instance.

Note:

With the stop and start operations, the instance might move to a different host that might change the IP Address and MAC Address if not statically allocated. Rebooting the instance will not change the host, IP Address, and MAC Address in AWS.

Starting an AWS instance

About this task

For more information, see the following website:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html

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 one or more instance, 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 AWS instance

About this task

For more information, see the following website:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html

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 one or more instance, 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 AWS 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 left navigation pane, click **Instances**.
4. Select one or more instance, click **Actions** > **Instance State** > **Reboot**.

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

Configuring the EMS and SBCE deployment types and the network interfaces

Before you begin

Create three different subnets, one each for Avaya SBCE Management, Avaya SBCE external, and Avaya SBCE internal networks.

Create and configure AWS network ACLs for Avaya SBCE to deny network communication of Avaya SBCE external subnet with other subnets of Avaya SBCE and with other subnets of Avaya Aura® instances.

Create five elastic network Interfaces, from the EC2 GUI console by using information available at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html. The network interface name must contain netwrok identifier name, for example, SBC_M2, SBC_A1, SBC_A2, SBC_B1, SBC_B2.

Procedure

1. Verify that you can SSH to the Avaya SBCE instance from the subnet which is enabled for your VPC.

   For example:

   `ssh root@`*`xxx.xxx.xxx.xxx`*` -p 22`

   Where *xxx.xxx.xxx.xxx* is the IP address of the Avaya SBCE instance on AWS.
2. Enter the password `Avaya_123`.

3. Run the following command:

   `CloudConfigurator.py -s`

   The system displays a prompt to accept the EULA agreement and then displays a configuration screen similar to configuration on VMware platforms and hardware platforms. For more information, see *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform* and *Deploying Avaya Session Border Controller for Enterprise on a Hardware Platform*.
4. Select EMS or SBCE as the deployment type.
5. Add the EMS_M2 network interface for an EMS deployment type.
6. Add five network interfaces for the SBCE in the following order:

- For 8.1.2 release - M2, A1, A2, B1, B2
- For 8.1.3 release - A1, B1, M2, A2, B2

7. Reboot the Avaya SBCE instance.
8. Log in to the server as root user by using the password `Avaya_123`.

Deploying EMS and SBCE on a single server using CLI

About this task

Use this task when you want to deploy the EMS and SBCE software on the same physical or virtual server.

Procedure

1. Turn on the system.
2. Wait for the configuration menu to appear.

   The options are:

   - 1-configure: Command line mode
   - 2-Reboot SBCE
   - 3-Shutdown SBCE
   - 4-SBCE Shell Login
3. Type `4` for Shell login.
4. Run the following command:

   `CloudConfigurator.py -s`
5. Select the **Add Cloud Region** option and set it to the region where the system is located.

6. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press `Enter`:

   - IPv4
   - DUAL STACK

   Voice interfaces (A1, A2, B1, B2) support both IPv4 and IPv6 address configurations. If you are using dual stack for any of the data interfaces, then configure the system with dual stack. The IP Address on Management interface (M1) supports only IPv4 addresses — it does not depend on the type of **IP Mode**.

7. Type the **Appliance Type** as `EMS+SBCE` and press `Enter`.
8. Type a name for the appliance in the **Appliance Name** and press `Enter`.
9. Type the management IP address in the **Management IP address** field and press `Enter`.
10. Type the subnet mask in the **Management subnet mask** field and press `Enter`.
11. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press `Enter`.
12. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

13. Type the prefix length in the **Management subnet network prefix length** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

14. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

15. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press `Enter`.
16. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

17. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.

    You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.

18. Type the domain suffix in the **Domain Suffix** field and press `Enter`.

19. Type appropriate value in the **First and Last Name** field and press `Enter`.
20. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
21. Type a name of your organizational unit in the **Organizational Unit** field and press `Enter`.
22. Type your organization name in the **Organization** field and press `Enter`.
23. Type your city or locality name in the **City or Locality** field and press `Enter`.
24. Type your state or province name in the **State or Province** field and press `Enter`.
25. Type the two characters code of your country in the **Country Code** field and press `Enter`.
26. Type the number of your country in the **Please select a country** field to select your country from the list.
27. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
28. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
29. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

    ```
    Is the above information OK?
    ```

    Note:

    If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:

30. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
31. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
32. Type and confirm the password for root user and then press `Enter`.
33. Type and confirm the same password for the ipcs user and press `Enter`.

    Use this password for secure shell (ssh) to gain access to Avaya SBCE.

34. Type and confirm the grub password, and press `Enter`.

    A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

Deploying EMS on a dedicated server using CLI

About this task

Use this procedure when you want dedicated EMS servers. For EMS, you must deploy at least one EMS server, which is called the Primary EMS. You can optionally deploy a Secondary EMS server.

Caution:

When deploying the Secondary EMS server, verify that the software version of the Secondary EMS server matches the software version of the Primary EMS server. If the software versions do not match, the system will not work properly.

For example, a version mismatch might occur if the Primary EMS server was deployed but the Secondary EMS server was not deployed until a later time. If the Primary EMS server gets a software update before you deploy the Secondary EMS server, a version mismatch occurs.

Before you begin

Verify that the server you are deploying for EMS has the Avaya SBCE software installed. To confirm that the primary and secondary EMS servers have the same version of software, do the following steps:

1. Turn on the primary EMS server.
2. Wait for the configuration menu to appear.
3. From the menu, select **4** to go to the shell prompt.
4. Run the following command: **`rpm -qa | grep sbce`**
5. Repeat these steps on the secondary EMS server.
6. Compare the software versions. If the versions do not match, you must reinstall the Avaya SBCE software on one or both servers so that the same software version is on both EMS servers. If you need to reinstall the Avaya SBCE software, see the software installation instructions given earlier in this document.

Procedure

1. Turn on the system.
2. Wait for the configuration menu to appear.

   The options are:

   - 1-configure: Command line mode
   - 2-Reboot SBCE
   - 3-Shutdown SBCE
   - 4-SBCE Shell Login
3. Type `4` for Shell login.
4. Run the following command:

   `CloudConfigurator.py -s`

5. Select the **Add Cloud Region** option and set it to the region where the system is located.
6. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press `Enter`:

   - IPv4
   - DUAL STACK

   If you are using dual stack for any of the data interfaces, then configure the system with dual stack. The IP Address on Management interface (M1) or (M2) supports only IPv4.address, it does not depend on the type of **IP Mode**.
7. Type the **Appliance Type** as `EMS` and press `Enter`:
8. Type the passphrase in the **Network Passphrase** field and press `Enter`.
9. Type a name for the appliance in the **Appliance Name** field and press `Enter`.
10. Type the installation type for EMS in the **Installation Type** field from the following choices and press `Enter`:

    - Primary
    - Secondary

    Caution:

    When deploying the Secondary EMS server, verify that the software version of the Secondary EMS server matches the software version of the Primary EMS server. If the software versions do not match, the system will not work properly.

    For more information, see *Before you begin*.
11. Type the management IP address in the **Management IP address** field and press `Enter`.
12. Type the subnet mask in the **Management subnet mask** field and press `Enter`.
13. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press `Enter`.
14. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
15. Type the prefix length in the **Management subnet network prefix length** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
16. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

17. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press `Enter`.
18. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
19. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.

    You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.
20. Type the domain suffix in the **Domain Suffix** field and press `Enter`.
21. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
22. Type appropriate value in the **First and Last Name** field and press `Enter`.
23. Type a number of your organizational unit in the **Organizational Unit** field and press `Enter`.
24. Type your organization name in the **Organization** field and press `Enter`.
25. Type your city or locality name in the **City or Locality** field and press `Enter`.
26. Type your state or province name in the **State or Province** field and press `Enter`.
27. Type the two characters code of your country in the **Country Code** field and press `Enter`.
28. Type the name of your country in the **Please select a country** field to select your country from the list.
29. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
30. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
31. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

    ```
    Is the above information OK?
    ```

    Note:

    If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:
32. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
33. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
34. Type and confirm the password for root user and then press `Enter`.
35. Type and confirm the same password for the ipcs user and press `Enter`.

    Use this password for secure shell (ssh) to gain access to Avaya SBCE.
36. Type and confirm the grub password, and press `Enter`.

A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

37. Repeat this procedure if you are installing a Secondary EMS.

Deploying SBCE on a dedicated server using CLI

About this task

Use this procedure when you want dedicated Avaya SBCE servers. For Avaya SBCE, you can deploy several non-HA servers or several pairs of HA servers.

Before you begin

Ensure that the EMS server is accessible over the network when deploying Avaya SBCE.

Procedure

1. Turn on the system.
2. Wait for the configuration menu to appear.

   The options are:

   - 1-configure: Command line mode
   - 2-Reboot SBCE
   - 3-Shutdown SBCE
   - 4-SBCE Shell Login
3. Type `4` for Shell login.
4. Run the following command:

   `CloudConfigurator.py -s`
5. Select the **Add Cloud Region** option and set it to the region where the system is located.
6. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press `Enter`:

   - IPv4
   - DUAL STACK

   Voice interfaces (A1, A2, B1, B2) support both IPv4 and IPv6 address configuration. If you are using dual stack for any of the data interfaces, then configure the system with dual stack and the IP Address on Management interface (M1) must be the IPv4.address.
7. Type the **Appliance Type** as `SBCE`.
8. Type a name for the appliance in the **Appliance Name** field and press `Enter`.

9. Type the management IP address in the **Management IP address** field and press `Enter`.
10. Type the subnet mask in the **Management subnet mask** field and press `Enter`.
11. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press `Enter`.
12. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
13. Type the IP address of the EMS in **EMS IP address (IPv4)** and press `Enter`.
14. Type the IPv6 address of the EMS in **EMS IP address (IPv6)** and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
15. Type the prefix length in the **Management subnet network prefix length** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
16. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
17. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press `Enter`.
18. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.

    This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
19. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.

    You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.
20. Type the domain suffix in the **Domain Suffix** field and press `Enter`.
21. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
22. Type appropriate value in the **First and Last Name** field and press `Enter`.
23. Type a name of your organizational unit in the **Organizational Unit** field and press `Enter`.
24. Type your organization name in the **Organization** field and press `Enter`.
25. Type your city or locality name in the **City or Locality** field and press `Enter`.

26. Type your state or province name in the **State or Province** field and press `Enter`.
27. Type the two characters code of your country in the **Country Code** field and press `Enter`.
28. Type the number of your country in the **Please select a country** field to select your country from the list.
29. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
30. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
31. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

    ```
    Is the above information OK?
    ```

    Note:

    If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:
32. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
33. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
34. Type and confirm the password for root user and then press `Enter`.
35. Type and confirm the same password for the ipcs user and press `Enter`.

    Use this password for secure shell (ssh) to gain access to Avaya SBCE.
36. Type and confirm the grub password, and press `Enter`.

    A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

Next steps

After configuring Avaya SBCE, take a snapshot of the Avaya SBCE configuration. For information about backing up the Avaya SBCE database, see *Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise*.

Appliance and management interface field descriptions

Appliance Configuration field descriptions

Name	Description
Appliance Name	A descriptive name assigned to the EMS or Avaya SBCE. **Note:** Ensure that the appliance name is unique.
Domain Suffix (Optional)	The domain within which this server is deployed.
List of DNS Servers	The IP address of each Domain Name Server (DNS). **Note:** The list of DNS server names must be comma-separated, with no spaces. Only two IP addresses are allowed here.
NTP Server IP Address (ipv4)	The IPv4 IP address of the Network Time Protocol (NTP) server. If no NTP is present, configure manually. Only one IP address can be configured. For an HA pair, both Avaya SBCE servers must have the NTP address. You must configure **NTP Server IP Address (ipv4)** if TLS or encryption is enabled.
Network Passphrase	A unique password that the EMS server and Avaya SBCE security devices deployed throughout the network will use for authentication. This field is displayed for Avaya SBCE-only installations. **Important:** The same passphrase must be configured on all the SBCE instances that are managed by an EMS and on the managing EMS as well. Different passphrases prevent the EMS and Avaya SBCE security devices from communicating with one another.

Management Interface Setup field descriptions

Name	Description
Management IP Address (ipv4)	The IPv4 address of the management network.
Management Network Mask	The network mask of the management network.
Management Gateway IP Address (ipv4)	The IPv4 address of the gateway to the management network.
Management IP Address (ipv6)	The IPv6 address of the management network. The system displays this field only when you select **Dual Stack** on the Management IP Configuration screen. **Note:** In **Dual Stack** the IPv6 address is optional but the IPv4 address is compulsory.
Management Network Pfx length	The length of the prefix for the management network IPv6 address. The system displays this field only when you select Dual Stack on the Management IP Configuration screen.
Management Gateway IP Address (ipv6)	The IPv6 address of the gateway to the management network. The system displays this field only when you select **Dual Stack** on the Management IP Configuration screen. **Note:** In **Dual Stack** the IPv6 address is optional but the IPv4 address is compulsory.
EMS Server IP Address (ipv4)	The IP address of the EMS server. This field is displayed for Avaya SBCE only installations.
Self-signed certificate fields	
First and Last Name	The name used to refer to or identify the company or group creating the certificate.
Organizational Unit	The group within the company organization creating the certificate.
Organization	The name of the company or organization creating the certificate.
City or Locality	The city or locality where the certificate is being created.

Table continues…

Name	Description
State or Province	The state or province where the certificate is being created.
Country Code	The number to identify the country where the certificate is being created.

Important:

- When using SSL or VPN is configured on the M1 interface, the IP address associated with the M1 interface will need *outbound* internet access. The M1 interface requires *outbound* internet access to initiate connectivity with the Avaya VPN Gateway (AVG) server. M1 is the management interface that is the required interface for SSL or VPN.
- All the self-signed certificate fields are applicable only on the management interface, for communication with the user interface and with the Avaya Aura® components. The values for self signed certificate are optional, if you will not provide any value then certificate will be generated by using the default values of the fields.

Note:

For security reasons for Voice Over IP (VoIP) systems, segment the data or data management network from the voice network. For Avaya SBCE deployments, segmentation means configuring the Management Interface (M1) on a separate subnet from the subnet used for the Voice Interfaces (A1, A2, B1, and B2). Avoid placing M1 IP address on a PBX core network. For more information about this recommendation, see

- Avaya: *Security Best Practices Checklist*.
- Network Security Agency: *Recommended IP Telephony Architecture*.
- National Institute of Standards and Technology (NIST): *Security Considerations for Voice Over IP Systems*.

Configuring Avaya SBCE

About this task

When deploying an HA configuration, you only have to do this on the primary device.

Procedure

1. Log on to the EC2 Management Console.
2. Power off and power on the virtual machine again from the EC2 Management Console page.
3. Use any Windows machine deployed in AWS and Accessible as RDP from client machine to configure the Avaya SBCE instance from EMS.

You can log on the EMS GUI from `https://<Avaya SBCE IP address>/` using following credentials:

- Username : ucsec
- Password: ucsec

You can log on to the Avaya SBCE instance CLI by using port 222 and ipcs user with the password set during installation.

Note:

When you log on the first time, you must change the default password.

4. Configure Avaya SBCE with network, media, signalling interfaces, and other standard Avaya SBCE features.

   For more information, see *Administering Avaya Session Border Controller for Enterprise*.

5. Disable Avaya SBCE **Media Anchoring** and use **Media Tromboning Only** in **Call Type for Media Unanchoring** for a remote worker Avaya SBCE configuration on AWS.

6. On the AWS EC2 Management Console, attach the elastic public IP address to the A1/A2 interface of the device. If you are deploying an HA configuration, you only have to do this on the primary device. The secondary device will be automatically configured.

   Use the **Allow Reassignment** option for the elastic public IP address. Avaya SBCE data interfaces A1/A2 and B1/B2 should have secondary IP addresses. These secondary IP addresses are used for all media and signalling configurations.

   Important:

   Ensure that the InstanceId for a particular SBCE is stored in the **aws_instance_id** column of the Global_nodes table. If the InstanceId is not administered, manually run the following command to store the InstanceId:

   `CloudConfigurator.py -i` <*InstanceId*>

   For more information, see the following website:

   https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

Dual data center configuration

For configuring the applications in a dual data center environment, the instances must be configured in the same network region in two zones on the same Virtual Private Cloud (VPC).

Chapter 6: Licensing requirements

About licensing requirements

Avaya SBCE uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBCE software. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBCE:

- Standard Services delivers non-encrypted SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication, and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBCE.

Avaya SBCE uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBCE license file on a primary Element Management System (EMS) using the Device Management page.

Important:

You must not enable the local WebLM option and install an Avaya SBCE license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **Grace Period State**.

Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBCE works normally during the grace period.

Important:

Licenses and a WebLM server are required for new installations or upgrades.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

The primary host ID of WebLM is used for creating the license file.

- Licensed features
- Licensed capacity

All hardware Avaya SBCE devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

For integration with Microsoft® Teams, Avaya SBCE requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBCE requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

Avaya SBCE licensed features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.

Table continues…

License feature	Description
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBCE. This license is required when using any advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBCE encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

License installation

You can install Avaya SBCE license on either of the following servers:

- The WebLM server on System Manager
- The local WebLM server

Installing a license on WebLM server on System Manager

Before you begin

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/.

About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering standalone Avaya WebLM*.

Procedure

1. Log in to the System Manager web interface.
2. On the home page, in the **Services** section, click **Licenses**.
3. In the left navigation pane, click **Install license**.
4. Browse to the location where you saved the license file, and select the file to upload.
5. Click **Install**.
6. Verify that the license is installed. If the installation is successful, a new menu item named ASBCE appears in the left navigation pane. Click **ASBCE** to view the licensed features.

Installing a license file on the local WebLM server

Procedure

1. Log in to the WebLM application. If you are logging in for the first time, the system prompts you to change the default password.
2. In the left navigation pane, click **Install License**.

   The system displays the Install License page.
3. In the **Enter license path** field, select the downloaded license from your computer and click **Install**.

   After the license is successfully installed, the system displays a new menu **ASBCE**.
4. Click **ASBCE** to view the license information.

Configuring the WebLM server IP address using the EMS web interface

Before you begin

Install the Avaya SBCE license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Licensing**.
3. Do one of the following tasks:
   - For a WebLM server or standalone server installed on System Manager , in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

     The URL format of the WebLM server installed on System Manager is:

     `https://<SMGR_server_IP>:52233/WebLM/LicenseServer`

     The URL format of the standalone WebLM server is:

     `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.
   - For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.
4. Click **Refresh Existing License** to refresh the existing licenses.
5. Click **Verify Existing License** to verify the existing WebLM license to confirm it is trusted.

   If the WebLM license is trusted, a pop window will display the certificate details. Otherwise, you can select the option to trust the WebLM certificate manually.
6. On the Dashboard screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows `OK`.
7. Click the **Devices** tab.
8. Locate the Avaya SBCE device you configured, and click **Edit**.

   The EMS server displays the Edit Device dialog box.
9. In the **Standard Sessions**, **Advanced Sessions**, **Scopia Video Sessions**, and **CES Sessions** fields, type the number of licensed sessions depending on the license you purchased.
10. Click **Finish**.

Configuring the WebLM server IP address using CLI

Before you begin

Install the Avaya SBCE license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log on to the CLI with administrator credentials.
2. Run the following command to configure an external WebLM server URL:

   `sbceconfigurator.py config-weblm-url <WebLM URL>`

About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBCE connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBCE setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBCE setup.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBCE.

Note:

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBCE setup.

Chapter 7: Verifying a successful deployment

You can verify the successful deployment of EMS using one of the following methods:

- Access the EMS server using the web interface.
- Access the EMS server through console.
- Establish a CLI session through a secure shell session (SSH).

Logging on to the EMS web interface

Procedure

1. Open a new browser tab or window.
2. Type the following URL:

   `https://<Avaya EMS IP address>`
3. Press **Enter**.

   The system displays a message indicating that the security certificate is not trusted.
4. Accept the system message and continue to the next screen.

   If the Welcome screen is displayed, the EMS is operating normally and available for use. You can log in to EMS and perform normal administrative and operational tasks. See *Administering Avaya Session Border Controller for Enterprise*.
5. Type the username and password as `ucsec`.

   On first login, system prompts you to change the password.
6. Enter a new password and login with the new password.

Installing and verifying successful installation of EMS and SBCE

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.

   Note:

   The following step is not applicable for the single server deployment of Avaya SBCE.
3. On the Device Management page, do the following:
   a. In the **Devices** tab, click **Add**.
   b. In the Add Devices window, enter the Avaya SBCE details, such as the host name and the management IP address.
   c. Click **Finish**.

   On the Device Management page, the **Status** column of the Avaya SBCE device displays Registered.
4. Click **Install**.
5. In the Install Wizard, enter the configuration. For more information, see *Administering Avaya Session Border Controller for Enterprise*.
6. Click **Finish**.

   In the **Devices** tab, the **Status** column of the device displays **Commissioned** indicating that the device is successfully deployed and configured.

Logging in to the EMS using SSH

Procedure

1. Log in to SSH client using PuTTy.
2. Type the IP address for Avaya SBCE.
3. Specify the port as **222**.
4. Select the connection type as SSH and press `Enter`.
5. Enter the user name and password to log in.

   Note:

   You cannot gain access to shell with user account `ucsec`.

User account `ipcs` or user accounts that have shell access can be used for logging in to Avaya SBCE.

Chapter 8: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Design		
Avaya Session Border Controller for Enterprise Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBCE.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller for Enterprise Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller for Enterprise on a Hardware Platform	Describes how to plan and deploy an Avaya SBCE system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBCE system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on an Avaya Aura® Appliance Virtualization Platform	Describes how to plan and deploy an Avaya SBCE system on a virtualized appliance.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller for Enterprise on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBCE system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBCE system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller for Enterprise Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller for Enterprise	Describes how to upgrade to the latest release of Avaya SBCE.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller for Enterprise	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise	Describes troubleshooting and maintenance procedures for Avaya SBCE.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller for Enterprise and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBCE with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller for Enterprise Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBCE Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller for Enterprise Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBCE Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

For Portwell documentation, go to https://portwell.com/.

Finding documents on the Avaya Support website

Procedure

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

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

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

Accessing the port matrix document

Procedure

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

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

Avaya Documentation Center navigation

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

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

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

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

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

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

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
20600W	Avaya SBCE 8.1.x Technical Delta
21098W	Avaya SBCE 8.0.x Technical Delta
20660W	Administering Avaya SBCE Release 8 for SIP Trunking
60660W	Administering Avaya SBCE Release 8 for Remote Worker
20660T	Administering Avaya SBCE Release 8 Test
20800C	Implementing and Supporting Avaya SBCE — Platform Independent
20800T	Avaya SBCE Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBCE — Platform Independent
26160W	Avaya SBCE Fundamentals
7008T	Avaya SBCE for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBCE for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Appendix A: Appendix

Configuring PuTTY

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

Before you begin

Download the PuTTYGen software.

Procedure

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

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

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

Configuring PuTTY for an SSH session

Before you begin

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

Procedure

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

Signing in to the Amazon EC2 virtual server instance

Before you begin

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

Procedure

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

Identifying the SSH user name of the RHEL instance on AWS

About this task

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

Before you begin

Create RHEL instance on Amazon Web Services.

Procedure

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

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

Glossary

Availability Zone	A distinct location within a region that is insulated from failures in other availability zones and provides inexpensive low latency network to other availability zones in the same region. A Virtual Private cloud (VPC) can extend across availability zones, but each availability zone uses a different IP subnet.
Region	A named set of AWS regions in the same geographical area. A region comprises availability zones. VPCs cannot extend across regions.
Virtual Private Cloud	An elastic network populated by infrastructure, platform, and application services that share common security and interconnection. For more information about Amazon Virtual Private Cloud (VPC), go to the Amazon Web Services website at https://aws.amazon.com/vpc/.

Index

M

N

O

P

R

S

T

U

V

W