Deploying Avaya Session Border Controller for Enterprise on Amazon Web Services

Release 7.2.1
Issue 6
April 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE 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. 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. Note, unless otherwise stated, that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document describes the procedures to:

- Convert the Avaya SBCE OVA to Amazon Machine Image (AMI).
- Deploy the Avaya SBCE AMI by using the Amazon Web Services Management console.

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

Change history

Issue	Date	Summary of changes
1	June 2017	Release 7.2 document
2	July 2017	Removed the supported capacity information.
3	July 2017	• Updated the supported footprints for Avaya SBCE on AWS table. • Updated the unsupported features for Avaya SBCE AWS instance topic.
4	November 2017	Updated configuring the Avaya SBCE instance topic with default username and password.
5	December 2017	Updated the document for following Release 7.2.1 changes: • Added a new chapter of Licensing. • Added a new topic for configuring the Avaya SBCE instance for Release 7.2.1 and later.
6	April 2018	Added the Supported capacity topic

Prerequisites

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

To administer the AWS Management console and Avaya Aura® applications.

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

Chapter 2: Avaya Aura® on Amazon Web Services overview

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

You can deploy the following Avaya Aura® applications on Amazon Web Services:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya WebLM
- Presence Services using Avaya Breeze™
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Device Services
- Avaya Aura® Application Enablement Services (Software only)
- Avaya Aura® Media Server (Software only)
- Avaya Diagnostic Server (Software only)

The supported Avaya Aura® AWS applications can also be deployed on-premises.

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

- Avaya Aura® Conferencing Release 8.0 and later
- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway, G450 Branch Gateway, and G650 Media Gateway

Topology

The following diagram depicts the architecture of the Avaya applications on the Amazon Web Services platform. This diagram is an example setup of possible configuration offered by Avaya. The setup must follow the AWS deployment guidelines, but does not need to include all the applications.

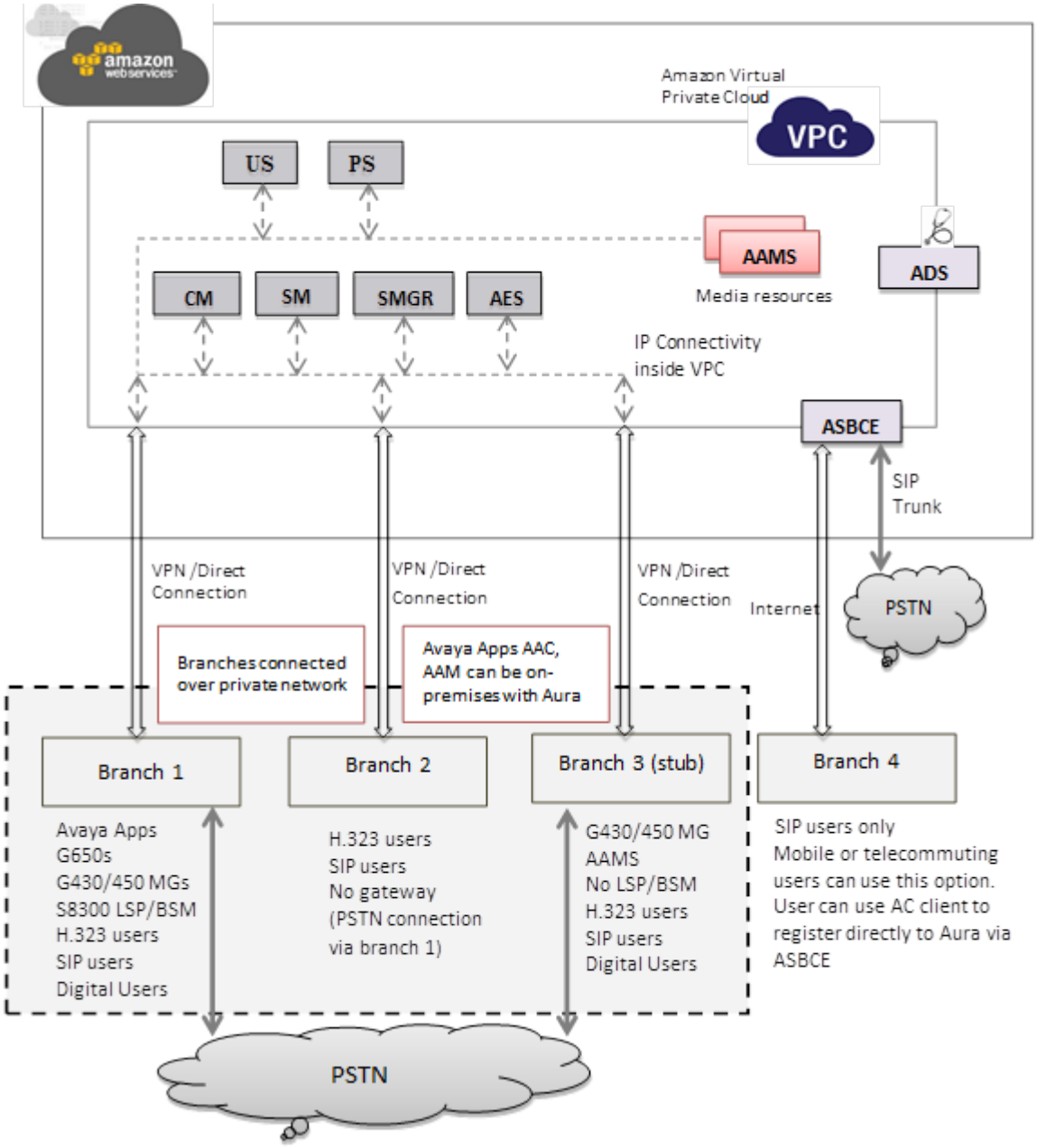

Figure 1: Avaya Aura® applications on Amazon Web Services

Networking considerations for connecting Avaya applications

When you deploy an Avaya application at 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 VPC Limits, see the AWS documentation at http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

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 Virtual Private Cloud (VPC) in the following ways:

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

Chapter 3: Planning and configuration

Planning checklist

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

No.	Task	Link/Notes	✔
1.	Download the required software.	See “Configuration tools and utilities”. See Downloading software from Avaya PLDS on page 14.	
2.	Purchase the required licenses. Register for PLDS and perform the following • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
3.	Log on to the Amazon Web Services Management console.	See Signing in to the Amazon Web Services Management console on page 16.	
4.	Create a key pair.	See Creating a key pair on page 16.	

Release details of Avaya SBCE OVA

You can download the following OVAs from the Avaya PLDS website at http://plds.avaya.com/.

Product name	Material code	Release version and Service pack	AWS OVA
Avaya SBCE	392036	Release: 7.2.0.0	`sbce-7.2.0.0-15-13590-aws-001.ova`

Supported footprints for Avaya SBCE on AWS

Footprint	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
EMS	c4.xlarge	4	7.5	160	2
Avaya SBCE standalone with 4 NIC - Medium	c4.2xlarge	8	15	160	4
Avaya SBCE standalone with 6 NIC - Large	c4.4xlarge	16	30	160	6
EMS+SBCE standalone with 4 NIC - Medium	c4.2xlarge	8	15	160	6
EMS+SBCE with 6 NIC - Large	c4.4xlarge	16	30	160	6

Supported capacity

Server Type	Number of Remote Worker Registrations	Non-encrypted Calls with Trunking	Encrypted Remote Worker Sessions
AWS	5000 registrations	900 calls	1800 sessions

Configuration 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:

- Avaya SBCE OVAs, see “Release version of Avaya SBCE OVAs.”
- A browser for accessing the Amazon Web Services Management Console.
- PuTTY, PuTTYgen, WinSCP, and WinZip

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.

Supported browsers for Amazon Web Console

For information about supported browser list and version, see https://aws.amazon.com/console/faqs/#browser_support on the AWS website.

Signing in to the Amazon Web Services Management console

Before you begin

Ensure that you have an AWS account.

Procedure

1. In your web browser, type the URL https://aws.amazon.com/.
2. Click **Sign In to the Console**.

   The system displays the Amazon Web Service page and auto-populates the **Account** field.
3. In the **User Name** field, type the user name or registered email ID.
4. In the **Password** field, type the password.
5. Click **Sign In**.

   The system displays the AWS Management Console page.

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.

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.

Unsupported features for Avaya SBCE AWS instance

Avaya SBCE AWS instances do not support the following features:

- EMS primary and secondary High Availability (HA) deployment
- Avaya SBCE HA deployment

Chapter 4: Converting OVA to AMI

Checklist for converting Avaya SBCE OVA to an Amazon Machine Image

Ensure that you complete the following before converting the Avaya SBCE OVA to an Amazon Machine Image (AMI).

No.	Task	Link/Notes	✔
1.	Create a bucket for uploading the OVAs.	Creating a bucket for uploading the OVAs for AMI conversion on page 18	
2.	Upload the <Application name> OVA.	Upload the Avaya SBCE OVA	
3.	Create an Amazon EC2 virtual server instance.	Creating a Linux Amazon EC2 virtual server instance on page 19	
4.	Create an access key.	Creating a user access key on page 21	
5.	Obtain the virtual server instance user id.	Obtaining the virtual server instance user ID on page 21	
6.	Import the OVA for AMI conversion.	Importing the OVA for AMI conversion on page 22	

Creating a bucket for uploading the OVAs for AMI conversion

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **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.

   For more information about creating a bucket and selecting a region, see Amazon S3 Documentation.

6. Click **Create**.

Uploading Avaya SBCE OVA

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Storage**, and click **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

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Compute**, and click **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**.
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:
      a. From the **Select a key pair** drop-down list, select a key pair.
      b. 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:
      a. In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
      b. Click **Download Key Pair**.
      c. 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`.

Next steps

Import the OVA for AMI conversion.

Creating a user access key

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Security, Identity & Compliance**, and click **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. Go to **Services** > **Compute**, and click **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 CM-Simplex-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 CM-Simplex-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. Go to **Services** > **Compute**, and click **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. Go to **Services** > **Compute**, and click **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 the Avaya SBCE AMI

Deploying Avaya SBCE AMI

Before you begin

Convert the Avaya SBCE AWS OVA to AMI. See “Checklist for converting OVA to an Amazon Machine Image”.

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Compute**, and click **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 footprints for Avaya SBCE on AWS”.

   For deploying Avaya SBCE, select c4.4xlarge instance type.

   For deploying EMS, select c4.large 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:
        a. From the **Select a key pair** drop-down list, select a key pair.
        b. 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:
        a. In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
        b. Click **Download Key Pair**.
        c. 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`.

Amazon Web Services instance management

Using EC2 Management Console, you can start, stop, reboot, and terminate an 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

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Compute**, and click **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

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services** > **Compute**, and click **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. Go to **Services** > **Compute**, and click **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**.

Chapter 6: Configuring the Avaya SBCE instance

Interfaces and Avaya SBCE deployment

The number of network interfaces that you set up determines the type of Avaya SBCE instance that you can install on the system .

The following table shows the relationship between the number of network interfaces and Avaya SBCE configuration types:

Number of network interfaces	Type of Avaya SBCE configuration
2	EMS
4	Standalone, that is, EMS + SBCE
6	Multiserver deployment, or one EMS and a number of Avaya SBCE instances

Configuring the Avaya SBCE instance for Release 7.2 and earlier

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. Name the interfaces by following any naming convention, for example, SBC_A1, SBC_B1, SBC_A2, SBC_B2, SBC_M2.

Procedure

1. Verify that you can SSH to the Avaya SBCE instance from the subnet which is enabled for your VPC by using the password @V@Y@_123.

   For example, ssh root@xxx.xxx.xxx.xxx -p 22, by using password @V@Y@_123.

2. After logging in as root, run the command: **`VMconfig.py`**.

   The system displays a prompt to accept the EULA agreement, and then displays a message to add network interfaces if the interfaces have not been added.

3. Do one of the following:

   - For EMS, attach one network interface. For example, SBCE_M2.
   - For medium, large, or standalone Avaya SBCE: Three or five network interfaces in the following order - SBC_A1, SBC_B1, SBC_A2, SBC_B2, SBC_M2.

4. Log in to the server again as root, and run the command **`VMconfig.py`**.

   The system installs the Avaya modified kernel and powers off the machine.

5. Log in to the server as root user by using the password @V@Y@_123.
6. Run the command **`VMconfig.py`** and proceed with configuration similar to configuration on VMware and hardware
7. Wait for 5 minutes till you receive the message for completion of boot process and then power off and power on the machine again from the EC2 Management Console page.
8. Use any Windows machine deployed in AWS and Accessible as RDP from client machine to configure the Avaya SBCE instance from EMS.

   You can access EMS from `https://<Avaya SBCE IP address>/` by using following credentials:

   - Username : ucsec
   - Password: ucsec

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

   Note:

   At your first login, you must change the default password.

   Disable Avaya SBCE **Media Anchoring** and use **Media Tromboning Only** in **Call Type for Media Unanchoring** for remote worker Avaya SBCE configuration on Amazon Web Services. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Configuring the Avaya SBCE instance for Release 7.2.1 and later

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. Name the interfaces by following any naming convention, for example, SBC_A1, SBC_B1, SBC_A2, SBC_B2, SBC_M2.

Procedure

1. Verify that you can SSH to the Avaya SBCE instance from the subnet which is enabled for your VPC by using the password Avaya_123.

   For example, ssh root@xxx.xxx.xxx.xxx -p 22, by using password Avaya_123.

2. After logging in as root, run the command: **`VMconfig.py`**.

   The server will go down, and then displays a message to add network interfaces if the interfaces have not been added.

3. Add three network interfaces for small Avaya SBCEand five network interfaces for large Avaya SBCEin the following order: SBC_A1, SBC_B1, SBC_A2, SBC_B2, SBC_M2.

   Network interface for EMS is not required as by default one network interface is present.

4. Log in to the server as root user by using the password Avaya_123.

5. Run the command **`VMconfig.py`**.

   The system displays a prompt to accept the EULA agreement and then displays a configuration screen similar to configuration on VMware and hardware

6. Wait for 5 minutes till you receive the message for completion of boot process and then power off and power on the machine again from the EC2 Management Console page.

7. Use any Windows machine deployed in AWS and Accessible as RDP from client machine to configure the Avaya SBCE instance from EMS.

   You can access EMS from `https://<Avaya SBCE IP address>/` by using following credentials:

   - Username : ucsec
   - Password: ucsec

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

   Note:

   At your first login, you must change the default password.

   Disable Avaya SBCE **Media Anchoring** and use **Media Tromboning Only** in **Call Type for Media Unanchoring** for remote worker Avaya SBCE configuration on Amazon Web Services. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

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 7: Post-installation verification

Verifying EMS operation

You can verify the operational status of the EMS by:

- Attempting to access the EMS server using the web interface.
- Establishing a CLI session via a secure shell session (SSH) and manually checking the status of various internal processes.

If the Avaya SBCE installation fails, you can restore the system data. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Logging on to the EMS web interface

Procedure

1. Open a new browser tab or window by using any of the following web browsers:
   - Microsoft Internet Explorer (5) 9.0+
   - Microsoft Edge 13.0+
   - Mozilla Firefox 38+ / 38.0 ESR+
   - Google Chrome 47.0+
   - Apple Safari (4) 7.0+
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.

Verifying successful installation of EMS and Avaya SBCE

Before you begin

Deploy EMS and Avaya SBCE, and configure EMS and Avaya SBCE.

About this task

Use this procedure to add an Avaya SBCE device.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **System Management**.
3. On the System Management page, do the following:
   a. In the **Devices** tab, click **Add**.
   b. In the Add Devices window, type the Avaya SBCE details, such as the host name and the management IP address.
   c. Click **Finish**.

   On the System Management page, the **Status** column of the Avaya SBCE device displays Registered.
4. Click **Install**.
5. In the Install Wizard, type the configuration.
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 EMS through SSH connection

Before you begin

Ensure that Avaya SBCE is installed and available on the network.

Procedure

1. Open an SSH client, such as 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: Troubleshooting

Avaya SBCE takes a long time to install

Condition

After you click **Launch instances**, Avaya SBCE takes a long time to install.

During installation, the instance is unreachable through RDP for Windows and SSH for Linux. Therefore, investigating the issue might be difficult. To counter this, Amazon Web Services provides instance screenshots and system logs for visibility of the current state of the instance during installation.

Solution

1. Select the instance and right-click.
2. To view the instance screenshot, click **Instance Settings** > **Get Instance Screenshot**.
3. To view the system logs, click **Instance Settings** > **Get System Log**.

System reachability checks do not pass

Condition

System reachability checks do not pass. Therefore, screenshots do not provide sufficient information to investigate and correct the issue.

Solution

Do one of the following:

- Detach the volume and attach it to another virtual machine. Then, go through the logs to troubleshoot.
- Remove interfaces from all the instances. Reboot and log in by using new root password and port number 222 to investigate and troubleshoot.

Related links

Attaching the volume to a virtual machine on page 37
Detaching the volume from AWS on page 37

Detaching the volume from AWS

Before you begin

Unmount the device by using `[ec2-user~] umount -d /dev/sda1` command.

Procedure

1. Open the Amazon Web Services Management console at https://console.aws.amazon.com/ec2/.
2. Go to **Services** > **Compute**, and click EC2.

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **Volumes**.
4. In the navigation pane, click **Volumes**.
5. Select a volume, click **Actions** > **Detach Volume**.
6. In the confirmation dialogue box, click **Yes, Detach**.

   AWS detaches the specified volume.

Next steps

Attach the volume to another virtual machine.

Attaching the volume to a virtual machine

About this task

Use the following procedure to attach the volume to another virtual machine for troubleshooting after detaching it from AWS.

Before you begin

Attach the volume to the instance which is available in the same zone.

Procedure

1. Open the Amazon Web Services Management console at https://console.aws.amazon.com/ec2/.
2. Go to **Services** > **Compute**, and click EC2.

   The system displays the EC2 Management Console page.
3. In the navigation pane, click **Volumes**.
4. In the navigation pane, click **Volumes**.
5. Select a volume, click **Actions** > **Attach Volume**.

6. In the **Attach Volume** dialog box, type the name of the instance to attach the instance to the volume.
7. Click **Attach**.

Next steps

Troubleshoot the machine.

Chapter 9: License Management

License management and Licensing requirements

Avaya SBCE uses WebLM for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the System Management page. 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. To install a license file on a newly installed or upgraded EMS, you have a 30-day grace period from the day of installation or upgrade.

Important:

Virtual EMS cannot run a local WebLM.You must use **External WebLM Server URL** option for licensing configurations of AWS. **Use Local WebLM Server** option is only applicable for hardware deployments.

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

For mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use an ova WebLM or System Manager WebLM.

Following are the use cases for managing licenses when an AWS supported application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 7.1, AWS supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, but

only the AWS supported applications move to AWS, then you do not have to regenerate the license for those applications that move to AWS.

- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to AWS, then all the licenses need to migrate to the centralized System Manager Release 7.1 with integrated WebLM in AWS and the supported AWS applications that move need to regenerate the license files.

Chapter 10: 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
Implementation		
Deploying Avaya Session Border Controller for Enterprise	Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Virtual installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 7.2.	Implementation engineers
Maintenance and Troubleshooting		
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers, Administrators
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures.	Implementation engineers, and Sales engineers
Reference		
Avaya Port Matrix: ASBCE 7.2	Port information.	Implementation engineers, Administrators, and Sales engineers

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from the selected category.
7. Click **Enter**.

Amazon Web Services documentation

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

Training

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

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller
5U00160E	Knowledge Collection Access: Avaya Unified Communications Core Support

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.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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: 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**.

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

S

T

U

V