AVAYA

Deploying Avaya Aura® applications on Amazon Web Services

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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 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

Contents

Chapter 1: Introduction

Purpose

This document describes how to convert the Avaya Aura® OVAs to Amazon Machine Image (AMI). It also explains how to deploy the Avaya Aura® application AMIs by using the Amazon Web Services Management console.

This document covers the generic procedures for Avaya Aura® applications. For application-specific configurations, see the product-specific document.

This document is intended for people who install and configure Avaya Aura® application AMIs at a customer site.

Prerequisites

Before deploying Avaya Aura® applications, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Amazon Web Services setup
- Linux® Operating System
- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya Aura® Presence Services
- Avaya Breeze™
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Application Enablement Services
- Avaya Aura® Media Server
- Avaya Diagnostic Server

Skills

How to administer the AWS Management console and Avaya Aura® applications.

Tools

The required tools and utilities, as listed in "Configuration tools and utilities".

Chapter 2: Avaya Aura® on Amazon Web Services overview

Amazon Web Services (AWS) is a cloud services platform that enables the enterprises to securely run the 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
- 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.
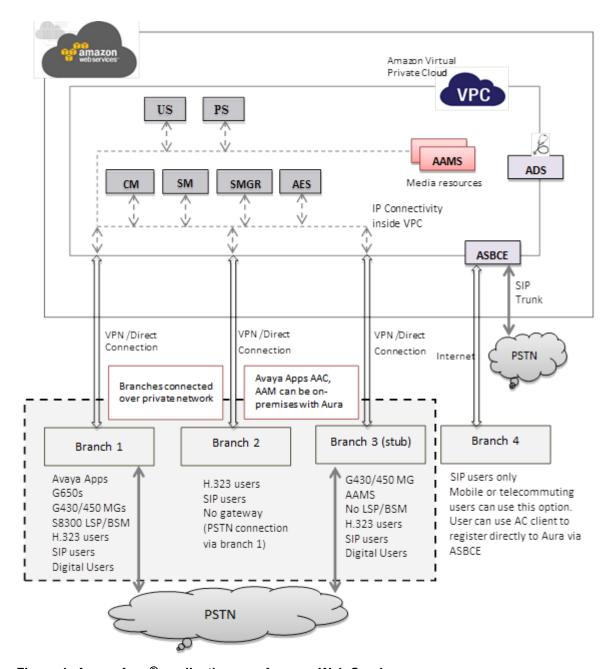
Figure 1: Avaya Aura® applications on Amazon Web Services

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.

Types of network connection

You can connect applications in a hybrid network on Virtual Private cloud (VPC) in 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/.

License management

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 3: Planning and configuration

Planning checklist

Complete the following tasks before deploying the Avaya Aura® applications on Amazon Web Services Management console:

No.	Task	Link/Notes	✔
1.	Download the required software.	Configuration tools and utilities on page 17	
2.	Purchase and obtain the required licenses.	—	
3.	Register for PLDS, and activate license entitlements.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4.	Download the required OVAs.	Downloading software from Avaya PLDS on page 17	
5.	Log on to the Amazon Web Services Management console.	Logging on to the Amazon Web Services Management console on page 18	
6.	Create a key pair.	Creating a key pair on page 19	

Release details of Avaya Aura® application OVAs

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

Product name	Material code	Release version	AWS OVA
System Manager Profiles 2 and 3	392035	7.1	• **Profile 2:** SMGR-7.1.0.0.1125193-aws-50.ova • **Profile 3:** SMGR-PROFILE3-7.1.0.0.1125193-aws-50.ova

Table continues…

Product name	Material code	Release version	AWS OVA
			• **Data Migration Utility:** `datamigration-144.bin` • **Patch:** `System_Manager_R7.1.0.0_S11_710006654.bin`
Session Manager Profiles 1, 2, 3, 4, and 5	392033	7.1	`SM-7.1.0.0.710028-aws-01.ova`
Communication Manager Simplex	392030	7.1	`CM-Simplex-07.1.0.0.531-aws-001.ova`
Utility Services	—	7.1	`US-7.1.0.0.0.16-aws-34_OVF10.ova`
Presence Services with Avaya Breeze™ Profiles 2, 3, 4, and 5	700513331	• Presence Services 7.1 • Avaya Breeze™ 3.3	`Breeze-3.3.0.0.330019-aws-001.ova`
Avaya Aura® Media Server 250, 1000, and 1900 MPUs	392039	7.8	`MediaServer_7.8.0.xxx_2017.xx.xx.bin`
Application Enablement Services Profile 1, 2, and 3	392037	7.1	`swonly-7.1.0.0.0.xx-2017xxxx.iso`
Avaya Diagnostic Server	392038	3.0	`ADS-Installer-3.0.0.0-xxx.tar.gz`
SAL Policy Manager with SSH Proxy (Software only)	—	3.0	`ADS-Proxy-Installer-3.0.0.0-xxx.tar.gz`

Supported footprints for the Avaya Aura® applications on AWS

Product name	Footprint	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
System Manager	Profile 2	m4.2xlarge	8	32	105	1
System Manager	Profile 3	m4.2xlarge	8	32	250	1
Session Manager	Profile 1	c4.xlarge	4	7.5	90 • **Disk 1:** 50	2

Table continues…

Product name	Footprint	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
					• **Disk 2:** 10 • **Disk 3:** 30	
Session Manager	Profile 2	c4.2xlarge	8	15	90 • **Disk 1:** 50 • **Disk 2:** 10 • **Disk 3:** 30	2
Session Manager	Profile 3	c4.2xlarge	8	15	125 • **Disk 1:** 60 • **Disk 2:** 25 • **Disk 3:** 40	2
Session Manager	Profile 4	c4.4xlarge	16	30	125 • **Disk 1:** 60 • **Disk 2:** 25 • **Disk 3:** 40	2
Session Manager	Profile 5	c4.8xlarge	36	60	175 • **Disk 1:** 85 • **Disk 2:** 25 • **Disk 3:** 65	2
Communication Manager Simplex	Max users 36000	m4.large	2	8	64	2
Utility Services	-	t2.micro	1	1	20	1
Presence Services with Avaya Breeze™	Avaya Breeze™ Profile 2	m4.xlarge	4	16	80	2

Table continues…

Product name	Footprint	AWS instance type	AWS vCPU	AWS RAM (GB)	HDD (GB)	NICs
Presence Services with Avaya Breeze™	Avaya Breeze™ Profile 3	c4.2xlarge	8	15	80	2
Presence Services with Avaya Breeze™	Avaya Breeze™ Profile 4	m4.2xlarge	8	32	150	2
Presence Services with Avaya Breeze™	Avaya Breeze™ Profile 5	c4.4xlarge	16	30	300	2
Avaya Aura® MS (Software only)	250 MPU	c4.xlarge	4	7.5	50	2
Avaya Aura® MS (Software only)	1000 MPU	c4.2xlarge	8	15	50	2
Avaya Aura® MS (Software only)	1900 MPU	c4.4xlarge	16	30	50	2
AE Services (Software only)	Profile 1	m3.medium	1	4 (3.75)	30	2
AE Services (Software only)	Profile 2	c4.large	2	4 (3.75)	30	2
AE Services (Software only)	Profile 3	c3.xlarge	4	6 (7.5)	30	2
Avaya Diagnostic Server (Software only)	-	m4.xlarge	4	8	Free Space 230	2
SAL Policy Manager with SSH Proxy (Software only)	-	m4.large	2	4		1

System capacities for applications

For information about the system capacities, such as number of users, gateways, and endpoints, see the product-specific documentation on the Avaya Support website at http://support.avaya.com.

For software only deployment of Avaya Aura® Media Server, the existing capacity planning tools require a benchmark score as indicated in the following table:

Deployment type	Instance family	Instance type	AWS vCPUs	AWS RAM (GB)	Disk (GB)	Operating System	MPU rating	Bench mark score
Software only (PVI)	Compute Optimized - C4	c4.xlarge	4	7.5	50	Red Hat or CentOS 6.x	250	1325

Table continues…

Deployment type	Instance family	Instance type	AWS vCPUs	AWS RAM (GB)	Disk (GB)	Operating System	MPU rating	Bench mark score
Software only (PVI)	Compute Optimized - C4	c4.2xlarge	8	15	50	Red Hat or CentOS 6.x	1000	5300
Software only (PVI)	Compute Optimized - C4	c4.4xlarge	16	30	50	Red Hat or CentOS 6.x	1900	10600

Configuration tools and utilities

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

- Avaya Aura® application OVAs, see "Release version of Avaya Aura® application 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.

The Avaya Aura® OVAs for AWS have aws-001 or aws-'xxx' in the version string and only these OVAs must be converted and deployed on AWS. You cannot correctly convert or deploy the standard application OVAs on AWS.

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.

Logging on to the Amazon Web Services Management console

Before you begin

You must create an Amazon 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 login information, for example, the password. The private key is used to decrypt the encrypted data. This key pair can be used when you deploy an Avaya Aura® application AMI.

Procedure

1. Log on 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, you must save it. If you lose the key, you cannot retrieve the key and be unable to access the instance.

Unsupported features for Avaya Aura® AWS instances

The Avaya Aura® AWS instances do not support the following features:

- Solution Deployment Manager deployments

- Standalone Avaya WebLM

- High Availability of Avaya SBCE, Communication Manager, and Avaya Aura® MS

- Communication Manager Duplex configurations

- Network configuration changes, such as IP Address, Gateway, and FQDN. NAT in the IP link is not supported in the following cases:
  - H.323 Station on Communication Manager
  - SIP station that connects directly to Session Manager
  - G450, G430, and G650 Gateways connecting to Amazon Web Services
- Cloning of AWS instances
- IPv6 addresses and configuration
- Out of Band Management configuration

Uptime of Avaya Aura® applications

The Avaya Aura® applications availability is based on the Amazon Web Services availability, which is a best effort 99.95%, but Amazon Web Services specific uptime instance values must be confirmed with Amazon Web Services.

License management

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 4: Converting OVA to AMI

Checklist for converting Avaya Aura® application OVA to an Amazon Machine Image

No.	Task	Link/Notes	✔
1.	Create a bucket for uploading the OVAs.	Creating a bucket for uploading the OVAs for AMI conversion on page 21	
2.	Upload the Avaya Aura® application OVA.	Uploading Avaya Aura OVAs to the Amazon Web Services console on page 22	
3.	Create an Amazon EC2 virtual server instance.	Creating a Linux Amazon EC2 virtual server instance on page 22	
4.	Create an access key.	Creating a user access key on page 24	
5.	Obtain the virtual server instance user ID.	Obtaining the virtual server instance user id on page 24	
6.	Import the OVA for AMI conversion.	Importing the OVA for AMI conversion on page 25	

Creating a bucket for uploading the OVAs for AMI conversion

Procedure

1. Log on 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.

The name must be all in lowercase.

5. In the **Region** field, click a region for your bucket.

   For more information about creating a bucket and selecting an appropriate region, see [Amazon S3 Documentation]().

6. Click **Create**.

Uploading Avaya Aura® OVAs to the Amazon Web Services console

Procedure

1. Log on to the Amazon Web Services Management console.

2. Go to **Services** > **Storage**, and click **S3**.

   The system displays the S3 Management Console page.

3. In the All Buckets, click a bucket name.

4. Click **Upload**.

   The system displays the Upload - Select Files and Folders dialog box.

5. Click **Add Files**.

6. In the Choose File to Upload dialog box, select one or more OVA files from your local system, and click **Open**.

7. Click **Upload**.

Creating a Linux Amazon EC2 virtual server instance

Procedure

1. Log on 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. Log on 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. Log on 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>`.

7. To allow importing files into the EC2 instance, create a vmimport role, and associate the following trust policies:

   - AmazonEC2FullAccess
   - IAMFullAccess
   - AmazonS3FullAccess
   - AWSConfigRole
   - AWSOpsWorksInstanceRegistration

   a. Create a file `role-policy.json` with the following content and run the command: `aws iam create-role --role-name vmimport --assume-role-policy-document file://role-policy.json`.

      For example:

      ```
      {
      "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":"*"
}
]
}
```

b. Create a file called `trust-policy.json` with the following content and run the command: `aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json`.

For example:

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

8. To import the ova for conversion, run the 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>\" } } ]}"`

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

In the following example, when the system converts the CM Simplex OVA, **ImportTaskId** is `import-ami-ffmanv5x`.

```
[ec2-user@ip-10-10-11-23 ~]$ aws ec2 import-image --cli-input-json "{ \"Description
\": \"CM-Simplex-07.1.0.0.xxx-aws-001.ova\", \"DiskContainers\": [ { \"Description
\": \"<First CLI task>\", \"UserBucket\": { \"S3Bucket\": \"avayabucket\", \"S3Key
\" : \"CM-Simplex-07.1.0.0.xxx-aws-001.ova\" } } ]}"
CM-Simplex-07.1.0.0.xxx-aws-001.ova import-ami-ffmanv5x 2 active pending
SNAPSHOTDETAILS 0.0
USERBUCKET avayadevbucket CM-Simplex-07.1.0.0.xxx-aws-001.ova
```

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 13. 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. Log on 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. Log on 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 Avaya Aura® applications

Deploying the Avaya Aura® application AMI

Before you begin

Convert the Avaya Aura® application AWS OVA to AMI. For more information, see "Checklist for converting OVA to an Amazon Machine Image".

Procedure

1. Log on 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**.

   The system displays the list of AMIs.

4. Select the Avaya Aura® application 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. Selecting an incorrect instance type might affect the usability of the system . For information about the instance type, see "Supported footprints for the Avaya Aura® applications on AWS".

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.

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

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

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

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

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

    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/.

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

    - **Choose an existing key pair**: If you select this option, perform the following:

        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.

12. Click **Launch Instances**.

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

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

Managing instances

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. Log on 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. Log on 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. Log on 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: Deploying Software only applications

Deploying Application Enablement Services

Before you begin

- Ensure that you have deployed RHEL 7.2 64–bit AMI on AWS.
- Download the AES ISO from Avaya PLDS.
- Check `/etc/sysconfig/network-scripts/ifcfg-eth0` if ONBOOT is set to `Yes`

Procedure

1. Complete GRUB Changes and rename the network interface to `eth0`.

    a. Type vi /etc/default/grub

    b. Look for the words **GRUB_CMDLINE_LINUX** and add the following: `net.ifnames=0 biosdevname=0` and save the file.

    c. Enter `grub2-mkconfig -o /boot/grub2/grub.cfg`.

2. Enter `systemctl disable firewalld`

    This will disable the firewall.

    ⚠ **Warning:**

    The following is a very slow process and might affect system performance when logging is enabled.

3. Disable journaling for *systemd*. Enter the following:

    a. `systemctl disable systemd-journald.service`

    b. `systemctl disable systemd-journald.socket`

    Make sure you see the line `SELINUX=disabled` in the `/etc/selinux/config` file.

4. Edit `/etc/hosts` and add an entry for your server, for example `ipAddress fqdn hostname`

5. Edit `/etc/resolve`, nameserver and search entries

6. Run `hostname <hostname>`, where <hostname> is the host name entry you added.

7. Run `shutdown -r now`

Deploying Avaya Aura® Media Server

Before you begin

- Create a virtual server instance. Use the latest 64-bit Red Hat Enterprise Linux Server 6.x AMI, or equivalent 64-bit CentOS 6.x AMI. For information about creating an EC2 virtual server instance, see "Creating an Amazon EC2 virtual server instance".
- Ensure that the correct instance type is used.
- Configure and install YUM to use a Red Hat repository or CentOS repository.
- Disable Linux firewall correct open ports per the Avaya Aura® MS documentation.
- Check that unzip is installed, and if not, install it.
- Check that sufficient space is available to deploy Avaya Aura® MS. Many Amazon OS images have a small OS partition and might not automatically resize. If a second storage partition is required, be sure to use that partition location when deploying Avaya Aura® MS.
- Open correct ports on the EC2 security group as per the Avaya Aura® MS documentation.
- Download the Avaya Aura® MS binary installer for softwareonly installations.

Procedure

1. Connect using SSH to the virtual server instance.

2. Transfer the Media Server binary installer to the instance.

3. Log in with an account with root privileges, and run the following to perform the YUM update on the system:

   ```
   [root@ec2 ~]# yum update
   ```

4. Run the following to ensure that the binary installer is owned by root and has executable permissions:

   ```
   [root@ec2 ~]# chown root:root MediaServer_7.8.0.xxx_2017.xx.xx.bin

   [root@ec2 ~]# chmod 700 MediaServer_7.8.0.xxx_2017.xx.xx.bin
   ```

5. Install the Avaya Aura® MS software as root and specify the AWS deployment mode by running:

   ```
   [root@server5088-vm07 ~]# ./MediaServer_7.8.0.xxx_2017.xx.xx.bin -
   DDEPLOY_PROFILE=aws
   ```

   The Avaya Aura® MS installer checks for any missing required packages and uses YUM to install any missing packages.

6. If YUM displays a list of packages to download, press y, and then press **Enter**

7. Read the installation overview, and press **Enter** to continue.

8. Read through all the pages of the license agreement, and press **Enter**.

9. To accept the terms of the license agreement, type y and press **Enter**.

10. Install Element Manager by clicking **Enter period missing**

11. Accept the default Linux group name by clicking **Enter**.

12. Accept the default install folder `/opt/Avaya/mediaserver` or select a folder mounted on a specific volume, and press **Enter**.

    Note: `/opt` can be mounted on a small OS partition that is not easily resizable. Validate that sufficient space is available and choose the best location.

13. When the system displays the installation summary, press **Enter**.

14. When the system completes the installation, press **Enter**.

Next steps

Access the Avaya Aura® MS Element Manager interface on a web browser, `https://<ip_address>:8443/emlogin` by using the administrator credentials.

Deploying Avaya Diagnostic Server

Before you begin

- Create a virtual server instance. Use the existing the Red Hat Enterprise Linux Server release 6.5 with 32-bit or 64-bit AMI. For information about creating EC2 virtual server instance, see "Creating an Amazon EC2 virtual server instance".

- Obtain the JRE, Oracle 1.8 or later 32-bit or 64-bit.

    JRE must match the system type of the OS. If the OS is 32-bit, then JRE must be of 32-bit.

    ✳ Note:

    For deploying Avaya Diagnostic Server, the system requires approximately 230–GB storage space. When you launch the RHEL, ensure that you have the minimum storage space.

- Set the JAVA_HOME environment variable.

- Disable **SELINUX**.

- Install the 32 glibc package.

- Install the perl, unzip, lsof, and iptables-services packages.

- Assign a static hostname to the instance. For information, see the AWS documentation at https://aws.amazon.com/premiumsupport/knowledge-center/linux-static-hostname-rhel7-centos7/

- Download the installer.

About this task

You can deploy Avaya Diagnostic Server in two modes, attended, and unattended.

To deploy Avaya Diagnostic Server in attended mode, start the installation in the Linux GUI mode. Ensure that X Windows capabilities are installed and configured on Linux.

Procedure

For information about deploying ADS in attended and unattended modes, see *Deploying Avaya Diagnostic Server* for Release 3.0 on the Avaya Support website at http://support.avaya.com.

Chapter 7: Configuring Avaya Aura® instances

For information about configuring Avaya Aura® instances, see the product-specific Amazon Web Services deployment guide on the Avaya Support website at http://support.avaya.com.

Related links

Dual data center configuration on page 36

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).

Related links

Configuring Avaya Aura instances on page 36

Chapter 8: Resources

Documentation

See the following related documents on the Avaya Support website at http://support.avaya.com.

Title	Use this document to:	Audience
Implementing		
Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment	To deploy AE Services in a Software-Only environment.	System administrators and IT personnel
Implementing and Administering Avaya Aura® Media Server	To deploy Avaya Aura® MS.	System administrators and IT personnel
Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS	To deploy Avaya Aura® MS.	System administrators and IT personnel
Deploying Avaya Diagnostic Server for Release 3.0	To deploy Avaya Diagnostic Server in a Software-Only environment.	System administrators and IT personnel
Administering		
Accessing and Managing Avaya Aura® Utility Services	Describes the procedures for administering Utility Services.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Communication Manager	Describes the procedures and screens used for administering Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® System Manager	Describes the procedures for configuring System Manager Release 7.1 and the Avaya Aura® applications and systems managed by System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Aura® Session Manager	Describes the procedures for administering Session Manager.	Solution Architects, Implementation Engineers, Sales

Table continues…

Title	Use this document to:	Audience
		Engineers, Support Personnel
Avaya Aura® Presence Services Snap-in Reference	Describes the steps to deploy and configure Presence Services.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administering Avaya Session Border Controller for Enterprise	Describes the procedures for administering Avaya SBCE.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Related links

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**.

Related links

Amazon Web Services documentation

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

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.

Related links

Using the Avaya InSite Knowledge Base on page 39

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

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

Related links

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**.

Logging on 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 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