Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments

Release 10.2.x
Issue 10
March 2026

Notices

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

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

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third Party Components

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

Service Provider

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to deploy the Avaya Aura® Application Enablement Services *Software-Only ISO image* on a:

- Customer-provided hardware
- Infrastructure as a Service environment

This document is intended for people who deploy and configure Application Enablement Services *ISO image* at a customer site.

The *Software-Only* offer is for customers who want to deploy the Avaya Aura® applications on their own standard Red Hat Enterprise Linux operating system. Avaya Aura® applications support third party applications only on the *Software-Only* deployments.

Note:

A virtualized environment is required for the software-only deployment.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Prerequisites

Before deploying the Avaya Aura® Application Enablement Services on Infrastructure as a Service, ensure that you have the following knowledge and tools.

Knowledge

- Infrastructure as a Service platform that you use
- Linux® Operating System

Tools

For information about tools and utilities, see Configuration tools and utilities on page 36.

Change history

Issue	Date	Summary of changes
10	March 2026	Added the section: Changes to platform support on page 8
9	December 2025	Updated the following section: • Third-party software requirements on page 20
8	August 2025	Updated the following section: • Unsupported features of Avaya Aura application on Infrastructure as a Service on page 17
7	April 2025	Updated the following section: • Appendix A: List of required RPMs on RHEL 8.4 on page 83
6	January 2025	Updated the following sections: • Appendix A: List of required RPMs on RHEL 8.4 on page 83 • Appendix B: List of required RPMs on RHEL 8.10 on page 88

Table continues…

Issue	Date	Summary of changes
5	December 2024	Added the following chapters for Release 10.2.1: • Appendix B: List of required RPMs on RHEL 8.10 • Appendix I: Creating RHEL virtual machine on Nutanix Updated the following sections for Release 10.2.1: • Third-party software requirements • Operating system requirements • Installing the Red Hat Enterprise Linux software for AE Services • Preparing for Software-Only deployment on AWS • Creating RHEL instance on Microsoft Azure • Preparing for Software-Only deployment on Microsoft Azure • Preparing for Software-Only deployment on Google Cloud Platform • Software-only environment overview-Supported platforms • Disk Partitioning
4	August 2024	Updated the following section: • Appendix A: AE Services RPMs
3	May 2024	Updated the following sections: • Software-only environment overview on page 11 • Creating RHEL instance on Amazon Web Services on page 42 • Creating RHEL instance on Microsoft Azure on page 48 • Creating RHEL instance on Google Cloud Platform on page 52
2	April 2024	Updated the following sections: • AE Services resource requirements and the supported footprints. • Deploying Avaya Aura Software-Only ISO image on on-premise, AWS, Microsoft Azure, and Google Cloud Platform.
1	December 2023	Release 10.2

Chapter 2: Overview

Software-only environment overview

In a software-only installation, the customer owns the operating system and must provide and configure the operating system for use with Avaya Aura® application. With the software-only offer, the customer can install and customize the operating system to meet the requirements to install the Avaya Aura® application.

You must run the software-only offer on the supported environments to enable the use of Avaya approved third-party applications for anti-virus, backup, and monitoring.

Avaya Aura® Application Enablement Services (AE Services) runs on a Linux server and is tightly integrated with Avaya Aura® Communication Manager and Avaya Contact Center solutions.

Customers and/or Service Providers must procure a server or virtual machine that meets the recommended hardware requirements and the appropriate version of Red Hat Enterprise Linux® Operating System.

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system and get more control on the system. For the list of supported third-party software applications in Release 10.1 and later, see the Avaya Product Support Notice at PSN020360u.

Avaya Aura® Software-Only environment RPMs

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

For information about RPM updates for the Red Hat Enterprise Linux operating system and required changes to operating system files on Software only installation, see *Avaya Aura® Software Only White paper* on the Avaya Support website.

With Release 10.1 and later, there are no separate Kernel Service Packs (KSP), and Linux Security Update (LSU).

Supported platforms

You can deploy the Avaya Aura® application software-only *ISO image* on the following:

- On-premise platforms:
  - VMware
  - Kernel-based Virtual Machine (KVM)
  - Hyper-V

    Note:

    From Release 8.0.1, Avaya Aura® applications support Hyper-V.
  - Nutanix 6.5 and later
- Cloud platforms:
  - Amazon Web Services
  - Google Cloud Platform
  - Microsoft Azure
  - IBM Cloud for VMware Solutions

    Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

    For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Infrastructure as a Service environment overview

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services

  Note:

  With Release 10.1.x and later, Avaya Aura® will no longer have the Amazon Web Services OVA. Deployment on Amazon Web Services is supported through the software only offer.
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud for VMware Solutions

  For information about IBM Cloud for VMware Solutions, see IBM Cloud for VMware Solutions product documentation.

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- 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.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.
- Allows you to stay current with latest security updates provided by the service provider.

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

- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway and G450 Branch Gateway

Software security updates

Avaya Security Service Packs (SSP) are built for customers who do not use the software-only distribution. In a software-only deployment, the customer provides the operating system. The customer is responsible for installing the appropriate operating system and applying the relevant security patches from Red Hat.

For more details, see *Avaya Aura® Release Notes* on the Avaya Support website.

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system and get more control on the system. For the list of supported third-party software applications in Release 10.1 and later, see the Avaya Product Support Notice at PSN020360u.

Supported applications in Infrastructure as a Service Environment

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Avaya Aura® System Manager	Release 10.2.x	Y	Y	Y
Avaya WebLM	Release 10.1.3.x	Y	Y	Y
Avaya Aura® Session Manager	Release 10.2.x	Y	Y	Y

Table continues…

Application	Release	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Avaya Aura® Communication Manager	Release 10.2.x	Y	Y	Y
Avaya Aura® Application Enablement Services (Software only)	Release 10.2.x	Y	Y	Y
Presence Services using Avaya Breeze® platform	Release 10.1.x	Y	—	—
Avaya Aura® Media Server (Software only)	Release 10.2.x	Y	Y	Y

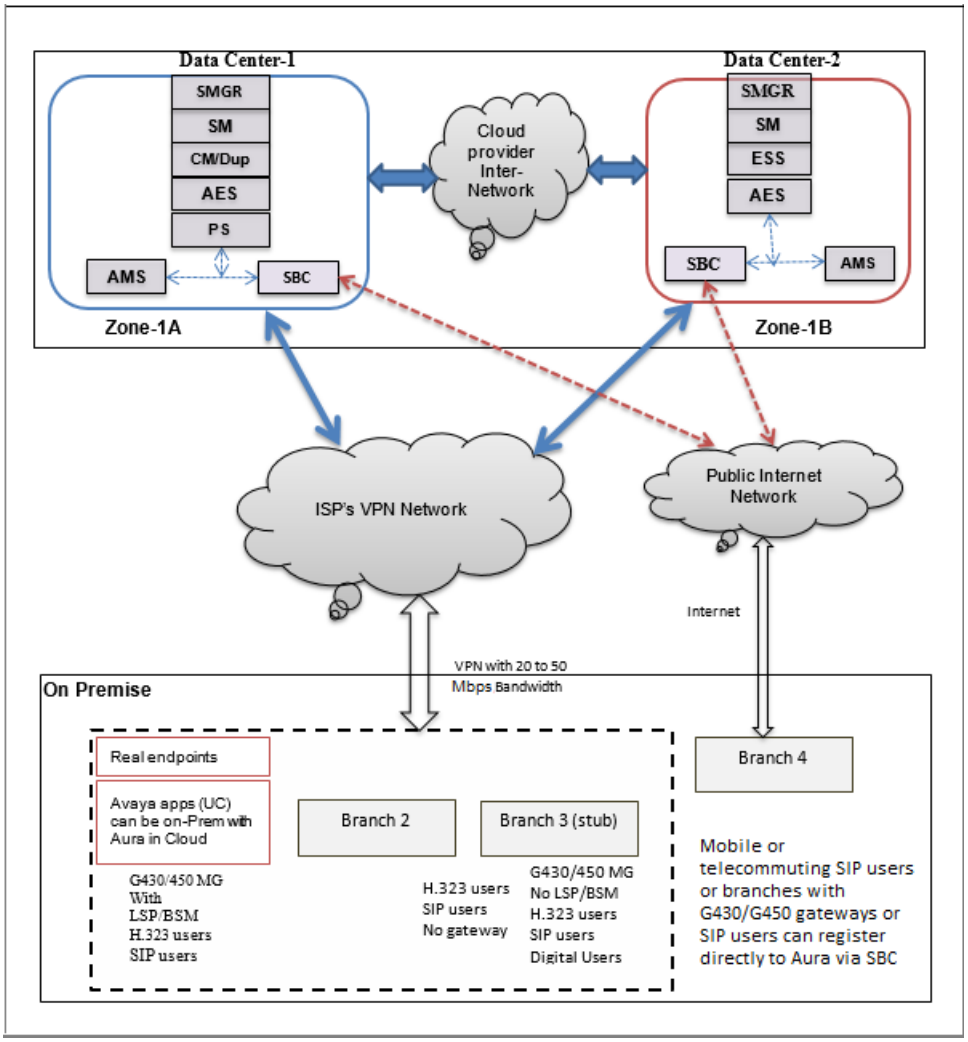
For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.

Important:

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.



Connection types for Infrastructure as a Service

Amazon Web Services

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

Connection type	Resource
VPN connection	For more information, go to https://docs.aws.amazon.com/VPC/ and search for “VPN connections” section.
Direct connection	For more information, see https://aws.amazon.com/directconnect/ section.

Microsoft Azure

You can connect applications in a hybrid network on the Virtual Networks (VNet) in the following ways:

Connection type	Resource
VPN connection	For more information, go to https://docs.microsoft.com/en-us/ and search for “Create a Site-to-Site connection in the Azure portal” section. For more information, go to https://docs.microsoft.com/en-us/ and search for “Azure networking” section.
Direct connection	For more information, go to https://docs.microsoft.com/en-us/ and search for “ExpressRoute overview” section.

Google Cloud Platform

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

Connection type	Resource
VPN connection	For more information, go to https://cloud.google.com/vpn/docs/ and search for “Cloud VPN overview” section.
GCN Direct	For more information, go to https://cloud.google.com/interconnect/docs/ and search for “Dedicated Interconnect Overview” section.

Networking considerations

When you deploy an Avaya application at main location or at a branch location on Infrastructure as a Service, 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 Infrastructure as a Service networking rules.

Infrastructure as a Service has some limitations for establishing public internet VPNs and direct connections.

For more information about Amazon VPC Limits, see the Amazon Web Services documentation at https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.

For more information about Microsoft Azure VPN connection limits and VPN Gateway, see the Microsoft Azure documentation at https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways.

Important:

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

Avaya is not responsible for network connections between Infrastructure as a Service and customer premises.

Unsupported features of Avaya Aura® application on Infrastructure as a Service

The following features are unsupported on the Software-Only Environment.

For more information on Out of Band Management (OOBM) feature support matrix for Avaya Aura® components, refer to section Out of Band Management Support Matrix for Avaya Aura Components on page 18.

Amazon Web Services

The Avaya Aura® application does not support the following features on Amazon Web Services:

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Virtual IP for Geo Redundant High Availability (GRHA) for Avaya Aura® Application Enablement Services

Microsoft Azure

The Avaya Aura® application does not support the following features on Microsoft Azure:

- IPv6 addresses
- Data Encryption
- Security Hardening modes

Google Cloud Platform

The Avaya Aura® application does not support the following features on Google Cloud Platform:

- IPv6 addresses
- Data Encryption
- Security Hardening modes
- Virtual IP for GRHA for Avaya Aura® Application Enablement Services

Note:

For more information about configuring GRHA without Virtual IP on Avaya Aura® Application Enablement Services, see the *Effect of a controlled/uncontrolled failover on AE Services clients*. This white paper is available with the AE Services customer documents on the Avaya Support website: http://www.avaya.com/support.

Out of Band Management Support Matrix for Avaya Aura® Components

The following table provides the information on OOBM support matrix for Avaya Aura® components.

Product	On-Premise (OVA)	IAAS (SW-Only)	Support OOBM
Communication Manager	Yes	Yes	Supported
Session Manager	Yes	Yes	Management only runs OOBM.
Media Server	Yes	Yes	Supported
Session Border Controller	Yes	No	Not Supported
System Manager	No	No	Needs VPC Peering with Voice Network in GCP for communicating with AADS.
WebLM	No	No	Needs VPC Peering with Voice Network in GCP if independently installed from SMGR to license AADS or AES.
Application Enablement Services	Yes	No	Needs to be on Voice Network only.
Avaya Aura® Device Services	No	No	Needs to be on Voice Network and needs VPC Peering in GCP with Voice Network.

Chapter 3: Planning

Downloading software from PLDS

When you order for an Avaya Product Licensing and Delivery System (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 https://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

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

Note:

The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

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

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

Required software

Application Enablement Services Software-Only installation requires that you install the AE Services Software-only template.

Download the AE Services software from the Product Licensing and Delivery System (PLDS) web site, then verify the ISO image. For new installations you must write the ISO image to a CD. For upgrade installations, download the .bin file to the AE Services server.

Latest software updates and patch information

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

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

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

Third-party software requirements

You can deploy the Avaya Aura® application ISO file on a Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 virtual machine by using the operating system command line interface or by using Solution Deployment Manager.

Operating system requirements

For the AE Services 10.2.x Software-only server you must obtain Linux® Operating System RHEL 8.4 or RHEL 8.10 Security Enhanced Linux® Operating System features are disabled on the software-only server. The AE Services Software-Only server supports only the English version of the Linux® Operating System. AE Services is not localized to other languages at this time.

Note:

- The AE Services Release 10.2.x Software-only server supports the 64-bit Linux® Operating System version of RHEL 8.4 or RHEL 8.10.
- For the base virtual machine of the AE Services Release 10.2.x Software-only server, the Boot firmware must be set to UEFI with the Secure Boot enabled.

Tip:

Check the latest AE Services release notes to find the latest supported update. For a copy of the release notes, see the AE Services customer documents on the Avaya Support web site: http://www.avaya.com/support.

Required tools for installation

This section is intended for customers performing installation and Avaya service technicians who are installing or upgrading AE Services Software-Only server for a customer with a maintenance contract.

- You can download the AE Services Software-Only ISO image and files for Release 10.2.x. Visit the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com. If you are performing an installation or upgrade from an earlier release, you need the AE Services Software-Only ISO image.

  Note:

  If you do not have the Software-Only ISO image, see Required software on page 20.
- USB keyboard, USB mouse, video monitor, and cables or laptop computer with an Ethernet crossover cable.
- Blank CDs or DVDs.
- A web browser. For more information about the supported browser versions, see *Administering Avaya Aura® Application Enablement Services*.
- A computer with a CD burner or a DVD burner.
- The customer order number applies to Avaya service technicians who are installing or upgrading AE Services Software-Only server for a customer with a maintenance contract.
- The AE Services license file. For information about getting the license file, see license requirements on page 65.

AE Services resource requirements and the supported footprints on VMware

The following tables show the resource requirements and the supported footprints for deploying AE Services using the following platforms:

Note:

Avaya Aura® Application Enablement Services supports VMware hosts with Hyperthreading enabled at the BIOS level.

To improve the performance of the GRHA, use profiles 2 and 3.

- ISO:
  - On-premise - VMware, KVM, Hyper-V
  - On cloud - Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud for VMware Solutions

Note:

AE Services supports the following footprint matrix for deploying AE Services except for Software-Only installation using customer's own hardware:

Footprints	Profile 1	Profile 2	Profile 3
vCPUs	1	2	4
CPU MHz Reservation **Note:** Reservations are applicable to VMware only.	2190 MHz	4380 MHz	8760 MHz
RAM	4 GiB	4 GiB	6 GiB
HDD	55 GiB	55 GiB	55 GiB
NICs	1 to 3*	1 to 3*	1 to 3*

Note:

* Depending on the network topology, you can configure the following types of networks:

1. Public network (Mandatory)
2. Private network (Optional)
3. Out of Band Management (Optional)

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

		DMCC, WTI — Third party call control: Avaya Aura® Contact Center		DMCC — First Party call control		TSAPI, DLG, CVLAN
Profile	**Footprint**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum number of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Profile 1	**1 CPU and 4 GiB RAM**	1K 10K	20K BHCC 6K BHCC	1K	9K BHCC	1K MPS
Profile 2	**2 CPU and 4 GiB RAM**	2.5K 12K	50K BHCC 12K BHCC	2.4K	18K BHCC	1K MPS
Profile 3	**4 CPU and 6 GiB RAM**	5K 20K	100K BHCC 24K BHCC	8K	36K BHCC	2K MPS

Supported footprints for AE Services on Amazon Web Services

AES Deployment Type	Footprint	AWS ISO instance type	HDD (GiB)	NICs
AES (Software only)	Profile 1	m3.medium or higher	55 GiB	2
AES (Software only)	Profile 2	c4.large or higher, c5a.large, or c5.large	55 GiB	2
AES (Software only)	Profile 3	c3.xlarge or higher, c5a.xlarge, or c5.xlarge	55 GiB	2

Note:

A gibibyte = 1024^3 and gigabyte = 1000^3

Supported footprints for AE Services on Microsoft Azure

AES Deployment Type	Footprint	Azure instance type	HDD (GiB)	NICs
AES (Software only)	Profile 1	Standard B2s (2 vcpus, 4 GiB memory)	55 GiB	2
AES (Software only)	Profile 2	Standard B2s (2 vcpus, 4 GiB memory)	55 GiB	2

Table continues…

AES Deployment Type	Footprint	Azure instance type	HDD (GiB)	NICs
AES (Software only)	Profile 3	Standard F4s v2 (4 vcpus, 8 GiB memory)	55 GiB	2

A gibibyte = 1024^3 and gigabyte = 1000^3

Supported footprints for AE Services on Google Cloud Platform

AES Deployment Type	Footprint	GCP instance type	HDD (GiB)	NICs
AES (Software only)	Profile 1	n1-custom-1-4096 (1 vcpus, 4 GiB memory)	55 GiB	2
AES (Software only)	Profile 2	n2-custom-2-4096 (2 vcpus, 4 GiB memory)	55 GiB	2
AES (Software only)	Profile 3	n2-custom-4-6144 (4 vcpus, 6 GiB memory)	55 GiB	2

A gibibyte = 1024^3 and gigabyte = 1000^3

Virtualized Environment footprint flexibility

Virtualized applications provide a fixed profile based on maximum capacity requirements. However, many customers require only a fraction of the maximum capacity.

Certain virtualized applications offer a flexible footprint profile based on the number of users that are supported. The customer can configure VMware CPU and RAM of a virtual machine according to a particular capacity line size requirement.

The applications that currently support Virtualized Environment footprint flexibility are:

- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

Related links

Configuring hardware resources to support AE Services footprint flexibility on page 25

Configuring hardware resources to support AE Services footprint flexibility

About this task

Use the following procedure only if you have installed Software-only server on VMware:

Procedure

1. Connect to the host or cluster using the VMware vSphere Web client.
2. Log in using the **admin** login and password.
3. Power off the virtual machine:
   a. Right-click on the virtual machine name.
   b. Select **Power** > **Shut Down Guest**.
   c. Click **Yes** in the **Shutdown Confirmation** dialog box.
4. Right-click on the virtual machine name and select **Edit Settings**.
5. Change the Memory Configuration:
   a. Click on the **Hardware** tab.
   b. Click **Memory**.
   c. Change the **Memory Size** to the appropriate limit.
   d. (Optional) Click on the **Resources** tab.
   e. (Optional) Select **Memory**,
   f. (Optional) Verify the **Reservation** is set correctly.
   g. (Optional) clear the **Unlimited** checkbox.
   h. (Optional) Verify the **Limit** slide is set to the same value as the **Reservation**.
6. Change the CPU configuration:
   a. Click the **Hardware** tab.
   b. Select **CPUs**.
   c. Change the **Number of virtual sockets** according to the limit requirement.
   d. (Optional) Click on the **Resources** tab.
   e. (Optional) Select **CPU**.
   f. (Recommended) Verify the **Reservation** is set correctly.

      Avaya recommends the **Reservation** be set to the value of multiplying the number of CPUs by 2190. For example, if the number of CPUs is 4, the **Reservation** should be set to 8760. One CPU should be equal to 2190.
   g. (Optional) Uncheck the **Unlimited** checkbox.

h. (Optional) Verify the **Limit** slide is set to the same value as the **Reservation**.

7. Click **OK**.
8. Wait until the virtual machine finishes the reconfiguration procedure.
9. Power on the virtual machine.

Related links

Virtualized Environment footprint flexibility on page 24

Hardware requirements for the Software-Only server

You must obtain a server that meets the following minimum requirements:

- 2190 MHz Multi-core processor

  Note:

  AE Services 5.2.*x* and later software supports Symmetrical Multiprocessing. AE Services, however, is a network-centric application and not a processor-intensive application. Adding more processors will not necessarily increase the capacity or performance of the platform.

- 4 GiB RAM, minimal requirement:
  - 4 GiB RAM for customers who support 10,000 simultaneous MOC/LCS users or a sustained processing rate of 720 TSAPI messages per second.
  - 6 GiB RAM for customers who support 20,000 simultaneous MOC/LCS users or a sustained processing rate of 1,000 TSAPI messages per second.
- 55 GiB free disk space, after installing Linux

  Note:
  - A gibibyte = 1024^3 and gigabyte = 1000^3
  - If you choose to set up the /var directory as a file system to improve reliability, Avaya recommends at least another 9.5 GiB for the /var partition. For more information, see Installing the Red Hat Enterprise Linux software for AE Services on page 38.
  - AE Services does not support vFAT type partition.
- Hard disk drive with at least 7200 rpm rating
- 512 KB L2 cache
- For Communication Manager over CLAN, 100 BaseT Ethernet NIC, which can either be locked to 100M / full, choose Auto–Negotiation to achieve 100M / full.
- For Communication Manager connection over Processor Ethernet 1000 Mbps BaseT Ethernet NIC, choose Auto–Negotiation to achieve 1000 Mbps/ full.
- DVD/CD-ROM drive

For more information about hardware resources capacity footprints for AE Services, see Hardware resources configuration matrix in the *Avaya Aura® Application Enablement Services Overview and Specification*, 02-300360.

Required RPMs

A complete list of required RPMs is packaged in the `Dependencies.txt` file of the ISO.

To see the complete list of required RPMs, see “AE Services RPMs”.

Related links

List of required RPMs on RHEL 8.4 on page 83

Disk partitioning

Use the following table to refer to the minimum recommended values for disk size and partition:

Note:

- A gibibyte = 1024^3 and gigabyte = 1000^3

Partition	Size
/	10 GiB
/boot	1 GiB
/boot/efi	0.5 GiB
/home	1 GiB
/var	9.5 GiB
/var/log	18.5 GiB
/var/log/audit	0.5 GiB
/var/mvap/database	1 GiB
/var/lib/ldap	0.5 GiB
/var/tmp	0.5 GiB
/tmp	3 GiB
/usr/share/tomcat	1 GiB
swap	8 GiB
Total	55 GiB

Client workstation provisioning

Although client workstations are not a requirement for installing the AE Services software, you will need to provide workstations for the AE Services client applications.

- Device, Media, and Call Control (DMCC) clients: You can develop and run DMCC applications on any computer that is capable of running the Java Platform, Standard Edition (Java SE) 1.8 or openJDK 8 client, a .NET client API for Windows, and an XML client API.
- Telephony Server Application Programming Interface (TSAPI) and Call Visor Local Area Network (CVLAN) clients: See the *Avaya Aura®Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide* (02-300543) for hardware and software requirements.
- Java Telephony Application Programming Interface (JTAPI) clients: See the *Avaya Aura®Application Enablement Services JTAPI Programmer's Guide* (02-603488) for hardware and software requirements.

Communication Manager and media server requirements

To use AE Services 10.2.x, you must have the Communication Manager Release 7.1.3.x, 8.0.x, 8.1.x, 10.1.x, or 10.2 software.

Note:

Communication Manager 6.3.x or later provides link bounce resiliency for the Application Enablement Protocol (AEP) transport links that AE Services uses.

- AE Services supports all media servers and gateways that support Communication Manager Release 7.1.3.x, 8.0.x, 8.1.x, 10.1.x, or 10.2.
- AE Services 7.1.3 and later supports both, Control Local Area Network (CLAN) interfaces and Processor Ethernet connections when implementing Survivable Core Server (Enterprise Survivable Server) and Survivable Remote Server (Local Survivable Processor) configurations.
- AE Services DMCC applications that use the High Availability Failover feature require the Communication Manager H.323 Time-to-Service registration feature. These features are available only on Communication Manager 5.2.1 or later.

Network addresses required for installation

Refer to the System Specifications List in the Linux® Operating System Installation Guide and follow the recommendations to record your system requirements and settings. For example:

- Network card
- IP address

- Domain name
- hostname - the name of the AE Services computer.

Important:

When you are assigning a hostname to the AE Services server, make sure you specify a hostname of 15 or fewer characters.

Network interface configurations

Depending on the network infrastructure, to can configure the AE Services server, you can use one NIC that can be extended up to 3 NICs. Use the configuration that best suits your network topology and other characteristics of your network.

Provide the NIC addressing information when you install the Linux software. See Network addresses required for installation on page 28.

To configure the network interface settings after installation, always use the AE Services Management Console. See Editing the NIC configuration (optional) on page 75.

Single NIC configuration

In a single NIC configuration, you use one network interface. The AE Services server uses one NIC for the client, switch, media, OAM connectivity. The AE Services server, Communication Manager, and the client application computer must reside on a private LAN, a virtual LAN (VLAN), or a WAN.

In a single NIC configuration, you must configure the IP interface for the AE Services server to be accessible over the public Internet to register IP endpoints.

Note:

- For NIC configuration, you must use the static IPv4 or static dual stack (IPv6 and IPv4) address (if applicable).

  Caution:

  If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

  Only IPv6 is not supported.

- From Release 10.1 and later, AE Services checks the NICs configuration, where the number of NICs should not be more than three, and the name of the NICs must be eth0 to eth2 (eth0, eth1 or eth2) depending on the number of NICs configured.

Important:

When you install the AE Services software, always use eth0 for a single NIC configuration.

See Required network interface (NIC) settings on page 30 for more information.

Dual or Triple NIC configuration

In a dual or triple NIC configuration, you use two network interfaces for connectivity to two separate network segments. One network segment is used for switch connectivity to Communication Manager, and the other network segment for is used for client and media connectivity (LAN, VLAN, or WAN). The NICs must be on separate networks or network segments. In a dual or triple NIC configuration, the client network is referred to as the production (or public) network, and the Communication Manager segment is referred to as the private network segment.

The private network segment should contain one subnet; this is the only supported configuration. You can configure any default gateway for public and private network segments. However, Avaya recommends using a public gateway as the default gateway to enable access to AE Services through both public and private network segments. After deployment, you must add static routes through CLI to make AE Services accessible from the private network segment.

Note:

- For NIC configuration, you must use the static IPv4 or static dual stack (IPv6 and IPv4) address (if applicable).

  Caution:

  If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

  Only IPv6 is not supported.

- From Release 10.1 and later, AE Services checks the NICs configuration, where the number of NICs should not be more than three, and the name of the NICs must be eth0 to eth2 (eth0, eth1 or eth2) depending on the number of NICs configured.

Important:

When you install the AE Services software, always use the following settings for a dual NIC configuration:

- Use eth0 for the IP address of the AE Services server (production network).
- Use eth1 for the IP address of the private network.

See Required network interface (NIC) settings on page 30 for more information.

Network interface (NIC) settings

The NIC choices for all network interfaces are as follows:

- Auto-Negotiate:
  - Gigabit interfaces: Auto-negotiation (auto-neg) - on

    In this case, you must administer 1000-Mbps / full / auto-neg at each end of the Ethernet link.
  - 100-Mbps interfaces: Auto-negotiation (auto-neg) - on

In this case, you must administer 100-Mbps / full / auto-neg at each end of the Ethernet link.

- Lockdown: 100-Mbps interfaces

  100-Mbps interfaces: Lockdown (auto-neg) - off

  In this case, you must administer 100-Mbps / full / Lockdown at each end of the Ethernet link.

Important:

AE Services defaults to auto-negotiation mode; it negotiates the network speed and duplex mode with the Ethernet switch. Both ends of the Ethernet link must be set to the same mode. Otherwise, a duplex mismatch will occur. Verify that both ends of the Ethernet link operate at the same desired speed and duplex settings.

Keep in mind the following:

- Auto-neg is highly desired for Gigabit links.
- Auto-neg or Lockdown is acceptable for 100-Megabit links.
- Lockdown for Gigabit links is highly discouraged.
- 10-Megabit and/or half-duplex operation is never acceptable and should be corrected.

For detailed information about using auto-negotiation and Lockdown, see Ethernet Link Guidelines at https://support.avaya.com/css/P8/documents/100121639.

See “Editing the NIC configuration (optional)” in the *Administering and Maintaining Avaya Aura® Application Enablement Services*, to set up the NICs with the recommended settings.See Editing the NIC configuration (optional) on page 75 to set up the NICs with the recommended settings.

Note:

The NIC speed 1000, full duplex with auto-negotiate is supported if AE Services is connected to Communication Manager Processor Ethernet that has the same NIC settings.

Network latency requirements

Regardless of the type of network used (LAN, VLAN or WAN), set up the TCP/IP links (CTI links) between the AE Services server and Communication Manager with the following network latency characteristics:

- No more than a 200 ms average round-trip packet delivery time, as measured with **`ping`** over every one-hour time period
- Periodic spiked delays of no more than 2 seconds while maintaining the 200 ms average round-trip delivery time, as measured with **`ping`** over every one-hour time period

These requirements are necessary to maintain the AE Services communication channel with each Communication Manager C-LAN over a LAN/VLAN or WAN. Considerations include:

- If the CTI application issues route requests, the associated vector “wait” step must have a value greater than the largest “periodic spiked delay”. With a maximum delay of 2 seconds, the wait step must be greater than 2 seconds. If you can guarantee “periodic spiked delays” of less than 2 seconds, you can reduce the wait step time-out accordingly.
- If the switch receives no response to a route select, the call will follow the remaining steps in this specific vector, so you must program the vector to deal with this condition. If you encounter “periodic spiked delays” greater than 2 seconds, messages are either:
  - Stored and retransmitted after recovering from a short network outage, or
  - Dropped during a long network outage

  Note:

  The communication channel between the AE Services server and the Communication Manager requires a hub or data switch. Avaya does not support the use of a crossover cable.

AE Services security guidelines

For information about the security features available on the AE Services server and security guidelines for the AE Services server, see the *Whitepaper on Security in Avaya Aura® Application Enablement Services* and Port Matrix for Avaya Aura® Application Enablement Services 10.2. The Whitepaper and Port Matrix are available with the AE Services customer documents on the Avaya Support website at http://www.avaya.com/support.

Related links

List of required RPMs on RHEL 8.4 on page 83

DVD requirements

Use high-quality, write-once, blank DVDs. Do not use multiple rewrite DVDs which are prone to error.

When writing the data to the DVD, use a slower write speed of 4X or a maximum 8X. Attempting to write to the DVD at higher or the maximum speed rated on the disc is likely to result in write errors.

Note:

If the software files you are writing on media are less than 680 MB in size, you can use a CD instead of a DVD.

Writing the ISO image to DVD or CD

Before you begin

1. Download any required software from PLDS.
2. Verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

About this task

If you are writing to a DVD, this procedure requires a computer or server that has a DVD writer and software that can write ISO images to DVD. If you are writing to a CD, this procedure requires a computer or server that has a CD writer and software that can write ISO images to CD.

Important:

When the ISO image is writing to the DVD, do not run other resource-intensive applications on the computer. Any application that uses the hard disk intensively can cause a buffer underrun or other errors, which can render the DVD useless.

Procedure

Write the ISO image of the installer to a DVD or CD.

Other requirements

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

- Hostname check: The hostname must not be the **localhost**.
- DNS check: IP address of the DNS server must be resolvable.

Planning checklist

Use the following checklist to track your installation:

#	Task	Comments	✔
1	Obtain the required hardware for the AE Services Software-Only Server.	See Hardware requirements for the Software-Only server on page 26.	
2	Set up a computer or laptop to access the computer on which you will be installing AE Services.	See Required tools for installation on page 21.	

Table continues…

#	Task	Comments	✔
3	(Optional) Provision for client workstations.	Although client workstations are not required for installing AE Services, you will need them when you are ready to set up your applications. See Client workstation provisioning on page 28.	
4	Make sure the Communication Manager and the media server are compatible with AE Services.	To ensure that your planned installation meets the Communication Manager compatibility requirements, see Communication Manager and media server requirements.	
5	Obtain the required version of Linux® Operating System.	See Operating system requirements on page 21.	
6	(Optional) If you plan to obtain and install the required third-party software components, make sure you have the correct versions.	**Note:** The AE Services installation program installs and configures all of the required third-party packages. Avaya strongly recommends you accept this option when you install the AE Services server software.	
7	(Optional) Set up AE Services server for remote access.	Applies only to customers who have an Avaya maintenance or service contract for their AE Services server.	
8	Review the network interface requirements, and configure the server to match the needs your network configuration.	See Network interface configurations on page 29.	
9	Determine your security requirements.	See AE Services security guidelines on page 32. This section provides you with a link to the White Paper on Security in Application Enablement Services for Software Only Solution.	
10	Install Linux® Operating System.	See Installing the Linux software for on page 38.	
11	Install the AE Services Release 10.2.x Software Only offer.	**Warning:** Configurations made after applying the Super Patch (if available during deployment) are not retained when the Super Patch is removed. The AE Services server data will reflect the configuration of the server immediately before the patch was installed. Apply 10.2.x patches as applicable.	
12	Install the AE Services license.	See license requirements on page 65.	

Table continues…

#	Task	Comments	✔
13	Verify your installation.	See AE Services post-installation administration on page 72.	

Planning for deploying Software-Only ISO on Amazon Web Services

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application ISO on Amazon Web Services:

No.	Task	Description	✔
1.	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/.	
2.	Download the required software.	See Downloading software from PLDS on page 19.	
3	Verify that you have a valid Red Hat subscription.	Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.	

Planning for deploying ISO on Microsoft Azure

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application on Microsoft Azure:

No.	Task	Link/Notes	✔
1.	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/.	
2.	Download the required Avaya Aura® application ISO.	See Downloading software from PLDS on page 19.	

Planning for deploying ISO on Google Cloud Platform

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application on Google Cloud Platform:

No.	Task	Link/Notes	✔
1.	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/.	
2.	Download the required Avaya Aura® application ISO.	See Downloading software from PLDS on page 19.	

Configuration tools and utilities

To deploy and configure the applications, you need the following tools and utilities:

- A browser for accessing the Amazon Web Services Management Console.
- A browser for accessing the AE Services web interface.

Note:

For more information about the supported browser versions, see *Administering Avaya Aura® Application Enablement Services*.

- PuTTY, PuTTYgen, WinSCP, and WinZip.

Chapter 4: Pre-deployment configuration

Installing the Red Hat Enterprise Linux software for AE Services

Before you begin

- You must install the Red Hat Enterprise Linux (RHEL) *before* you install the AE Services software because the AE Services installation script also configures RHEL for AE Services.

  Note:

  Avaya does not provide RHEL installation media with the AE Services Software-Only offer. This document assumes that you have obtained Linux® Operating System RHEL 8.4 or RHEL 8.10 (64-bit) with all security updates applied.

  Refer to the RHEL Installation Guide when you install RHEL. The following steps provide a high-level summary of the installation with a few specific instructions for installing AE Services.

- Perform the installation using the graphical user interface (GUI) installation program. In general, you can use the default options. However, when you install the Software Packages, Avaya recommends that you customize the software selection instead of installing the default packages, as described in this procedure.

Procedure

1. Boot to your RHEL installation media. Follow the instructions of the installation utility.
2. In the RHEL installation program, follow these steps to set up a `/var` partition.

   Note:

   Although you can use the RHEL default partitioning, Avaya recommends that you set up the `/var` directory as a file system (partition) to improve system reliability. This change prevents the AE Services root directory from becoming filled with log messages.

   a. On the **Disk Partition Setup** screen, select the partition method you prefer, such as **Automatically partition**.

   b. On the next screen, click **New**.

   c. Name the partition `/var` and complete the screen.

d. Allocate about 40 percent of the disk drive space to create the `/var` partition if available.

- The `/var` partition must be at least 9.5 GiB in size.
- On the Firewall Configuration screen, the Security Enhanced Linux (SELinux) features are active by default. You must disable SELinux or AE Services will not work correctly.
- Avaya recommends separating `/var/log/` partition to avoid system instability in case the partition fills up due to large log files.
- The `/var/log/` partition must be at least 18.5 GiB in size.

3. On the Software Selection page, in the Base Environment and Add-Ons for Selected Environment sections, keep the default selections.

   In the Base Environment section, the Minimal Install option is selected by default and in the Add-Ons for Selected Environment section, all the options are cleared by default.

4. Complete the RHEL installation and reboot the server.

   The time required for the software installation depends on the options you selected and the server processing power. Allow several minutes.

   Note:

   See Configuring Linux OS on page 39 before installing AE Services Software-Only offer.

5. For security purposes, enable only the specific ports you require.

   Include all the ports that the AE Services software uses. For a list of required ports, see the Port Matrix for Avaya Aura® Application Enablement Services 10.2 and *Whitepaper on Security in Avaya Aura® Application Enablement Services*. The Port Matrix and Whitepaper are available with the AE Services customer documents on the Avaya Support website at http://www.avaya.com/support.

Configuring the Linux operating system for AE Services *Software-Only* installation on on-premise

About this task

Use this procedure to configure the Linux operating system for software-only installation on on-premise.

Before you begin

- Log in to Linux using the root credentials.

- Back up the following files and folders (if present), before installing AE Services:
  - `/etc/openldap`
  - `/etc/sssd`
  - `/etc/ssh`
  - `/etc/pam.d`
  - `/etc/ldap.conf`
  - `/etc/nslcd.conf`
  - `/etc/resolv.conf`
  - `/etc/hosts`

Procedure

1. In the `/etc/sysconfig/network-scripts/ifcfg-ensXXX` or `/etc/sysconfig/network-scripts/ifcfg-eth0`, set the `ONBOOT` file attribute to `Yes`.
2. If the network interface is not currently set to eth0, use **`GRUB Changes`** to rename network interface to `eth0`.
   a. Type `vi /etc/default/grub`.
   b. Look for the line `GRUB_CMDLINE_LINUX` and add the following:

   ```
   net.ifnames=0 biosdevname=0 (with example)
   (GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/
   swap rhgb quiet net.ifnames=0 biosdevname=0")
   ```

   c. Click **Save**.
   d. Type `grub2-mkconfig -o /boot/grub2/grub.cfg`.
   e. If you have not specified names for the interface files during the installation, rename **`/etc/sysconfig/network-scripts/ifcfg-*`** to **`/etc/sysconfig/network-scripts/ifcfg-eth0`** using the below command:

   ```
   mv /etc/sysconfig/network-scripts/ifcfg-ens  /etc/sysconfig/network-scripts/
   ifcfg-eth0
   ```

   - Open `/etc/sysconfig/network-scripts/ifcfg-eth0`.
   - Update *DEVICE* and *NAME* value from esn* to `eth0`.
3. Disable the firewall by entering the command:

   ```
   systemctl disable firewalld
   ```

   Warning:

   This is a slow process and affects system performance when logging is enabled.
4. Disable journaling for *systemd* as follows:

   ```
   systemctl disable systemd-journald.service
   systemctl disable systemd-journald.socket
   ```

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

5. Do the following to create entries in the `/etc/hosts` file and edit the **`/etc/hosts`** command:
   a. Make sure IPv4 and IPv6 loopback entries are added in the `/etc/hosts` file. The loopback entries must be in the following formats:
      - **`127.0.0.1 localhost.localdomain localhost`**
      - **`::1 localhost6.localdomain6 localhost6`**

      Caution:

      If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

      Only IPv6 is not supported.
   b. Edit **`/etc/hosts`** and add an entry for your server. For example: `ipAddress fqdn hostname`.
6. In `/etc/resolv.conf` edit **`nameserver`**. If **`nameserver`** is not present, add it.
7. Run `hostname <hostname>`, where <hostname> is the host name entry you added.
8. Run `shutdown –r now`

Related links

Deploying Avaya Aura Software-Only ISO image on on-premise, AWS, Microsoft Azure, and Google Cloud Platform on page 59

Predeployment tasks for deploying ISO on Amazon Web Services

Predeployment checklist for Amazon Web Services

Perform the following tasks to deploy Avaya Aura® application ISO on Amazon Web Services.

No.	Task	Link/Notes	✔
1	Create a virtual machine.	See Creating RHEL instance on Amazon Web Services on page 42	
2	Assign the required resources to the virtual machine.	See Disk partitioning on page 27	
3	Copy the ISO to the virtual machine.	See Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services on page 43	

Table continues…

No.	Task	Link/Notes	✔
4	Create security groups.	See Creating security groups on page 44	

Creating RHEL instance on Amazon Web Services

About this task

Use this procedure to create RHEL virtual machine on Amazon Web Services.

Note:

Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Also, note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Amazon Web Services documentation.

Procedure

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

   The system displays the EC2 Management Console page.
3. Click **Launch an Instance**.
4. Under **Name and tags**, for Name, enter a descriptive name for your instance.

   Note:

   Remember the name entered for the tag. The name entered for the tag is used to identify the RHEL instance after the instance is created.
5. Under **Application and OS Images (Amazon Machine Image)**, search for the supported RHEL version in **Community AMIs**, and click **Select**.

   For the supported RHEL version, see “Third party software requirements” section.
6. Under **Instance type**, select the instance type according to your required footprints.
7. Under **Key pair (login)**, select an existing key pair or create a new key pair dialog box using the following options:
   - **Choose an existing key pair**.
   - **Create a new key pair**.
8. If you select the **Choose an existing key pair** option, from the **Select a key pair** drop-down list, and select a key pair.

9. If you select the **Create a new key pair** 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 **Create key pair**. The key pair will automatically download to the system after clicking on **Create key pair**.
   c. Save the file in a secure and accessible location.

      Note:

      You will not be able to download the file again.
10. Under **Network settings**, choose **Edit**. For Security group name, select **Create security group** for creating a new security group or **Select existing security group** to select an existing security group.

    If you select an existing security group, from **Common security groups** dropdown, choose your security group from the list of existing security groups.
11. Click **Configure storage**.
12. Review the details of each configuration in the **Summary** panel.
13. Click **Launch Instances**.

    The system creates the RHEL instance.
14. Click on the hyperlink of the instance ID to view the details of your instance.

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

Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Amazon Web Services

Create a ppk file

Procedure

1. Open WinSCP.
2. From the advance section, choose the authentication and browse to the .ppk file, and click login.
3. Enter the login credentials.
4. Upload the .iso to the virtual machine instance by using the IP address of the virtual machine.

Creating security groups

About this task

AWS uses security groups to control inbound and outbound traffic.

Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Security group**.
2. Click **Create Security Group**.
3. In **Security group** name, type a name of your choice.
4. In **Description**, type a description for the group.
5. From **VPC**, select the Virtual Private Cloud that you plan to use for AE Services.
6. Configure the inbound and outbound traffic rules for the group.

   For more information on supported ports, refer the port matrix document available on https://support.avaya.com.
7. Repeat steps 2 to 6 to create the additional required security groups.

Preparing for *Software-Only* deployment on AWS

About this task

Use this procedure to prepare the setup to deploy the Avaya Aura® Software-Only ISO image on AWS.

Procedure

1. From Release 10.1 and later, AE Services checks the NICs configuration, where the number of NICs should not be more than three, and the name of the NICs must be eth0 to eth2 (eth0, eth1, or eth2) depending on the number of NICs configured.

   If there are NICs other than eth0, eth1, or eth2, they must be removed.

   For example: `mv /etc/sysconfig/network-scripts/ifcfg-ens3 /tmp`
2. Configure the LDAP server. For more information, see "Configuring the LDAP server".
3. Disable the firewall by entering the command:

   ```
   systemctl disable firewalld
   ```

   Warning:

   This is a slow process and affects system performance when logging is enabled.
4. Disable journaling for *systemd* as follows:

   ```
   systemctl disable systemd-journald.service
   systemctl disable systemd-journald.socket
   ```

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

5. Do the following to create entries in the `/etc/hosts` file and edit the **`/etc/hosts`** command:
   a. Make sure IPv4 and IPv6 loopback entries are added in the `/etc/hosts` file. The loopback entries must be in the following formats:
      - **`127.0.0.1 localhost.localdomain localhost`**
      - **`::1 localhost6.localdomain6 localhost6`**

      Caution:

      If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

      Only IPv6 is not supported.
   b. Edit **`/etc/hosts`** and add an entry for your server. For example: `ipAddress fqdn hostname`.
6. Add the full DNS hostname to `/etc/hosts` file.
7. Change the hostname in the `/etc/hostname` file.
8. Append the following line to the file `network` at `/etc/sysconfig/`:

   ```
   HOSTNAME=<hostname>
   ```
9. Replace `<hostname>` with the host name of the AES.
10. Append the following line to the file `cloud.cfg` at `/etc/cloud/`:

    ```
    preserve_hostname: true
    ```

    Caution:

    To use your existing LDAP directory with AE Services, you must manually configure your LDAP implementation for compatibility with AE Services User Management.
11. Upload the AES ISO to the RHEL 8.4 or RHEL 8.10 instance.

Related links

List of required RPMs on RHEL 8.4 on page 83
Deploying Avaya Aura Software-Only ISO image on on-premise, AWS, Microsoft Azure, and Google Cloud Platform on page 59
Configuring the LDAP server on page 132

Managing AWS instances

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

Note:

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

Starting an AWS instance

About this task

For more information on starting an AWS instance, see the following website:

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

Procedure

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

   The system displays the EC2 Management Console page.
3. In the left navigation pane, click **Instances**.
4. To select one or more instances, use the following methods:
   a. To act on **Instance State** dropdown: Click **Instance State** > **Start Instance**.
   b. To act on the **Actions** dropdown: Click **Actions** > **Manage instance State** > **Start instance**.

   The system displays the **Manage instance state** page. Select the **Start** radio button, and click **Change state**. The system displays a message to start the instances.
5. Click **Start**.

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

Stopping an AWS instance

About this task

For more information on stopping an AWS instance, see the following website:

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

Procedure

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

   The system displays the EC2 Management Console page.
3. In the left navigation pane, click **Instances**.
4. To select one or more instances, use the following methods:
   a. To act on the **Instance State** dropdown: Click **Instance State** > **Stop Instance** .
   b. To act on the **Actions** dropdown: Click **Actions** > **Manage instance State** > **Stop instance**.

   The system displays the **Manage instance state** page. Select the **Stop** radio button, and click **Change state**. The system displays a message to stop the instances.

5. Click **Stop**.

   When the system stops the instance, the **Instance State** column displays the state as `stopped`.

Rebooting an AWS instance

Procedure

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

   The system displays the EC2 Management Console page.
3. In the left navigation pane, click **Instances**.
4. To select one or more instances, use the following methods:
   a. To act on the **Instance State** dropdown: Click **Instance State** > **Reboot Instance**.
   b. To act on the **Actions** dropdown: Click **Actions** > **Manage instance State** > **Reboot instance**.

   The system displays the **Manage instance state** page. Select the **Reboot** radio button, and click **Change state**. The system displays a message to reboot the instances.
5. Click **Reboot**.

Predeployment tasks for deploying ISO on Microsoft Azure

Predeployment checklist for Microsoft Azure

Perform the following tasks to deploy Avaya Aura® application ISO on Microsoft Azure.

No.	Task	Link/Notes	✔
1	Create a virtual machine.	See Creating RHEL instance on Microsoft Azure on page 48	
2	Assign the required resources to the virtual machine.	See Disk partitioning on page 27	
3	Copy the ISO to the virtual machine.	See Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure on page 49	

Creating RHEL instance on Microsoft Azure

Before you begin

Create an account on Microsoft Azure.

Important:

Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

Please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Microsoft Azure documentation.

Procedure

1. Log on to the Azure portal.
2. In the search box, type virtual machine, and click **Virtual machines**.
3. On the Virtual machines page, click on the **+ Create** link and select **+ Virtual machine**.

   The system displays the Create a virtual machine page.
4. In the **Basics** tab, do the following:
   a. In **Project details**, select the **Resource group**.
   b. In **Instance details**, provide the **Virtual machine name** and select the **Region**.
   c. In **Image**, select **Red Hat Enterprise Linux 8.4 or Red Hat Enterprise Linux 8.10** from the images list.
   d. In **Size**, select the required details.
   e. From **Administrator account**, in **Authentication type**, select **Password**, and enter the required credentials.

      Ensure that you select authentication type as **password** instead of **SSH public key**.
   f. Optional: Select the required **Inbound port rules**.
   g. Click **Next: Disks**.
5. In the **Disks** tab, do the following:
   a. From **Disk options**, select the required **OS disk type** and **Encryption type**.

      Caution:

      Do not use temporary disk for application configuration. It might lead to loss of data.
   b. In **Data disks for 'undefined'**, click **Create and attach a new disk**.

c. On Create a new disk page, click **Change size** and select **55 GiB** from the list.

d. Click **OK**.

A new disk of size 55 GiB is created.

e. Click **Next: Networking**.

6. In the **Networking** tab, from **Network interface** select the required **Virtual network**, **Subnet**, and **Public inbound ports**.

Select other fields on that page, if required.

7. In the **Management**, **Advanced**, and **Tags** tabs, fill the details, if required.
8. In the **Review + create** tab, review the details and click **Create**.

The deployment begins. Wait till the deployment is complete.

9. Ensure that the hard disk size is 55 GiB.

Next steps

Uploading the ISO on to the RHEL virtual machine instance on Microsoft Azure.

Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure

Before you begin

Create RHEL virtual machine instance on Microsoft Azure.

Procedure

1. Open WinSCP session with your RHEL machine on Microsoft Azure by using the user ID and password that you provided at the time of creating the virtual machine.
2. From the advance section, choose the authentication and browse to the .ppk file, and click **login**.
3. Enter the login credentials.
4. Upload the .iso file to the virtual machine instance.

Preparing for *Software-Only* deployment on Microsoft Azure

About this task

Use this procedure to prepare the setup to deploy the Avaya Aura® Software-Only ISO image on Microsoft Azure.

Procedure

1. From Release 10.1 and later, AE Services checks the NICs configuration, where the number of NICs should not be more than three, and the name of the NICs must be eth0 to eth2 (eth0, eth1, or eth2) depending on the number of NICs configured.

If there are NICs other than eth0, eth1, or eth2, they must be removed.

For example: `mv /etc/sysconfig/network-scripts/ifcfg-ens3 /tmp`

2. Configure the LDAP server. For more information, see "Configuring the LDAP server".
3. Disable the firewall by entering the command:

```
systemctl disable firewalld
```

Warning:

This is a slow process and affects system performance when logging is enabled.

4. Disable journaling for *systemd* as follows:

```
systemctl disable systemd-journald.service
systemctl disable systemd-journald.socket
```

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

5. Do the following to create entries in the `/etc/hosts` file and edit the **`/etc/hosts`** command:
   a. Make sure IPv4 and IPv6 loopback entries are added in the `/etc/hosts` file. The loopback entries must be in the following formats:
      - **`127.0.0.1 localhost.localdomain localhost`**
      - **`::1 localhost6.localdomain6 localhost6`**

      Caution:

      If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

      Only IPv6 is not supported.

   b. Edit **`/etc/hosts`** and add an entry for your server. For example: `ipAddress fqdn hostname`.
6. Add the full DNS hostname to `/etc/hosts` file.
7. Change the hostname in the `/etc/hostname` file.
8. Append the following line to the file `network` at `/etc/sysconfig/`:

```
HOSTNAME=<hostname>
```

9. Replace `<hostname>` with the host name of the AES.
10. Append the following line to the file `cloud.cfg` at `/etc/cloud/`:

```
preserve_hostname: true
```

Caution:

To use your existing LDAP directory with AE Services, you must manually configure your LDAP implementation for compatibility with AE Services User Management.

11. Upload the AES ISO to the RHEL 8.4 or RHEL 8.10 instance.

Related links

Deploying Avaya Aura Software-Only ISO image on on-premise, AWS, Microsoft Azure, and Google Cloud Platform on page 59
Configuring the LDAP server on page 132
List of required RPMs on RHEL 8.4 on page 83

Predeployment tasks for deploying ISO on Google Cloud Platform

Predeployment checklist for Google Cloud Platform

Perform the following tasks to deploy Avaya Aura® application ISO on Google Cloud Platform.

No.	Task	Link/Notes	✔
1	Create a PPK file	See Creating a PPK file on page 51.	
2	Create RHEL virtual machine instance	See Creating RHEL instance on Google Cloud Platform on page 52.	
3	Assign the required resources to the RHEL virtual machine instance	See Disk partitioning on page 27.	
4	Copy the ISO to the RHEL virtual machine instance	See Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform on page 53	

Creating a PPK file

Procedure

1. Open puttygen file, and click **Load**.
2. Under the **Parameters** section, select SSH-2 RSA.
3. Under **Actions** section, click **Generate**.

   You will be instructed to move the mouse cursor around within the PuTTY Key Generator window as a randomizer to generate the private key.
4. Enter a value in the **Key passphrase** and enter the same value in the **Confirm passphrase** field to protect the private key.
5. Click **Save private key**, and save the file to your local computer.
6. The box under **Public key for pasting into OpenSSH authorized_keys file:** contains the public key.
7. Copy the public key.

8. Open a text editor and paste the public key into the text editor and save the file.

Creating RHEL instance on Google Cloud Platform

Before you begin

- Create an account on the Google Cloud Platform
- Create a ppk file.

Important:

Installing only the required RPMs to the system for security and stability. Do not install a complete Red Hat system.

In a software-only installation, the customer installs the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, check the list of tested RPMs and follow the instructions in the PSN020617u that Avaya publishes periodically on the Avaya Support website.

Note:

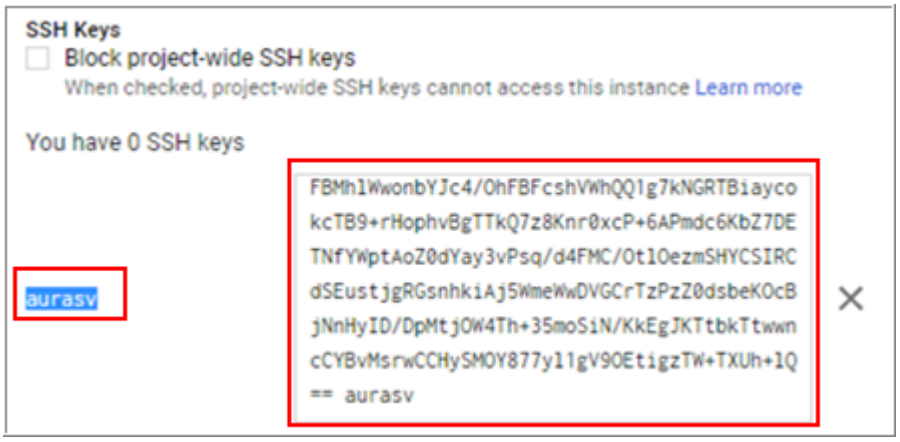
Please note that the steps provided in this section are for reference. For the most up-to-date information, see the Google Cloud Platform documentation.

Procedure

1. Log on to the Google Cloud Platform.
2. Go to **Compute Engine** > **VM Instances**.
3. On the VM Instances page, click **CREATE INSTANCE**
4. On the **Create an instance** page, update the following fields:
   a. In **Name**, enter your product name.
   b. In **Region**, select the required region.
   c. In **Zone**, select the required zone.
   d. Under **Machine configuration**, in **Series**, select **E2**.
   e. In **Machine type**, select the number of vCPUs and memory needed for your deployment.
5. Under the **Boot disk** section, click **Change** and do the following:
   a. Select the appropriate RHEL image. For the supported RHEL version, see the “Third party software requirements” section.
   b. In **Size (GiB)**, enter the required disk size and click **Select**.
6. Click **Networking** > **Networking interfaces**, and update the following fields:
   a. In **Network**, select the VPC network.
   b. In **Subnetwork**, select an appropriate subnet.
   c. In **Primary Internal IP**, select Ephemeral Custom.
   d. In **Custom ephemeral IP address**, enter an IP address that is within the range of your network.

e. In **External IP**, select an appropriate option.

7. Click **Done**.
8. Click **Security**.
9. Under the **SSH Keys** section, in the **Enter entire key data** section, copy your private key details.



When you paste the key, a user login is also created.

10. Click **Create**.

A Virtual machine instance is deployed and it appears under the VM instances page.

Next steps

Uploading the ISO to the RHEL virtual machine instance.

Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform

About this task

You can upload the ISO file using WinSCP.

Before you begin

Create a virtual machine instance on Google Cloud Platform.

Reuse the PPK file that was created earlier.

Procedure

1. Open WinSCP and enter the login credentials.
2. Click **Advanced**, and select **Advanced**.
3. In the left pane of the Advanced Site Settings window, click **Authentication**.
4. In the right pane, click the browse icon under the **Private key file** field and browse to the .ppk file.

5. Click **OK**, and click **Login**.
6. Upload the .iso to the virtual machine instance.

Preparing for *Software-Only* deployment on Google Cloud Platform

About this task

Use this procedure to prepare the setup to deploy the Avaya Aura® Software-Only ISO image on Google Cloud Platform.

Procedure

1. From Release 10.1 and later, AE Services checks the NICs configuration, where the number of NICs should not be more than three, and the name of the NICs must be eth0 to eth2 (eth0, eth1, or eth2) depending on the number of NICs configured.

   If there are NICs other than eth0, eth1, or eth2, they must be removed.

   For example: `mv /etc/sysconfig/network-scripts/ifcfg-ens3 /tmp`
2. Configure the LDAP server. For more information, see "Configuring the LDAP server".
3. Disable the firewall by entering the command:

   ```
   systemctl disable firewalld
   ```

   Warning:

   This is a slow process and affects system performance when logging is enabled.
4. Disable journaling for *systemd* as follows:

   ```
   systemctl disable systemd-journald.service
   systemctl disable systemd-journald.socket
   ```

   Make sure you see the line `SELINUX=disabled` in the `/etc/selinux/config` file.
5. Do the following to create entries in the `/etc/hosts` file and edit the **`/etc/hosts`** command:
   a. Make sure IPv4 and IPv6 loopback entries are added in the `/etc/hosts` file. The loopback entries must be in the following formats:

      - **`127.0.0.1 localhost.localdomain localhost`**
      - **`::1 localhost6.localdomain6 localhost6`**

      Caution:

      If you need to use the IPv6 architecture, it must be dual stack (IPv6 and IPv4).

      Only IPv6 is not supported.

   b. Edit **`/etc/hosts`** and add an entry for your server. For example: `ipAddress fqdn hostname`.

6. Add the full DNS hostname to `/etc/hosts` file.
7. Change the hostname in the `/etc/hostname` file.
8. Append the following line to the file `network` at `/etc/sysconfig/`:

   ```
   HOSTNAME=<hostname>
   ```

9. Replace `<hostname>` with the host name of the AES.
10. Append the following line to the file `cloud.cfg` at `/etc/cloud/`:

    ```
    preserve_hostname: true
    ```

    Caution:

    To use your existing LDAP directory with AE Services, you must manually configure your LDAP implementation for compatibility with AE Services User Management.

11. Upload the AES ISO to the RHEL 8.4 or RHEL 8.10 instance.

Related links

List of required RPMs on RHEL 8.4 on page 83
Deploying Avaya Aura Software-Only ISO image on on-premise, AWS, Microsoft Azure, and Google Cloud Platform on page 59
Configuring the LDAP server on page 132

Verifying the status of SELinux

About this task

Use this procedure to verify the status of SELinux.

Caution:

If you fail to disable SELinux before you install the AE Services software, some AE Services will not start and you might encounter other problems.

If the Linux operating system is already installed, use these steps to determine if the SELinux is disabled.

Procedure

1. Log in to the server as a user with root privileges.
2. From the command line interface, run the following command and press **Enter**:

   ```
   /usr/sbin/sestatus
   ```

3. If SELinux is enabled, you must disable SELinux and then reboot the server.

   You can specify the SELinux mode using the configuration file `/etc/sysconfig/selinux`. Change the value of SELINUX to disabled as shown in the following example:

   # This file controls the state of SELinux on the system.

```
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
# targeted - Only targeted network daemons are protected.
# mls - Multi Level security protection.
SELINUXTYPE=targeted
```

Verifying the umask settings

About this task

A umask setting of 022 is required for installing the AE Services Software-only offer.

Procedure

1. Log in to the server as root.
2. To determine the umask settings, from the command line interface, type **umask**. The output of the command should be 022. If it is not 022, follow the next steps to change the umask setting.
3. Open `/etc/init.d/functions` file and search for umask. Change the line containing umask to: **umask 022**. Follow the same step for `/etc/profile` file and `/etc/bashrc` file
4. Once the changes are complete, source the file using **source /etc/bashrc /etc/profile /etc/init.d/functions**.

Verifying that you have assigned a hostname

About this task

The hostname of the AE Services server must be 15 or fewer characters.

Procedure

1. Log in to the server as a user with root privileges.

2. To determine the hostname associated with an AE Services server, from the command line interface, type `uname -n`.

Verifying the ISO image on a Linux-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Linux-based computer.

Procedure

1. Enter `md5sum file name`, where *file name* is the name of the ISO image. Include the .iso file name extension.
2. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
3. Ensure that both numbers are the same.
4. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Verifying the ISO image on a Windows-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Windows-computer.

Procedure

1. Download a tool to compute md5 checksums from one of the following Web sites:
   - http://www.md5summer.org/
   - http://code.kliu.org/hashcheck/

   Note:

   Avaya has no control over the content published on these external sites. Use the content only as reference.
2. Run the tool on the downloaded ISO image and note the md5 checksum.
3. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.

4. Ensure that both numbers are the same.
5. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Chapter 5: Deploying AE Services

Deploying Avaya Aura® *Software-Only ISO image* on on-premise, AWS, Microsoft Azure, and Google Cloud Platform

About this task

Use this procedure to deploy the Avaya Aura® *ISO image* in a *Software-Only* environment.

For more information about the supported platforms, see the **Supported platforms** topic under Software-only environment overview on page 11.

Note:

The deployment of Avaya Aura® applications as software only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as software only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Before you begin

- If you are installing Avaya Aura® *Software-Only ISO image* on on-premise, see “Configuring the Linux operating system for AE Services Software-only installation on on-premise”.
- If you are installing Avaya Aura® *Software-Only ISO image* on AWS, see “Preparing for *Software-Only* deployment on AWS”.
- If you are installing Avaya Aura® *Software-Only ISO image* on Microsoft Azure, see “Preparing for *Software-Only* deployment on Microsoft Azure”.
- If you are installing Avaya Aura® *Software-Only ISO image* on Google Cloud Platform, see “Preparing for *Software-Only* deployment on Google Cloud Platform”.

Procedure

1. Open an ssh session to the AE Services server and open an account with root privileges.
2. List the contents of `/etc/fstab` to find out the name of the media directory.

   The media directory is the mount point for this procedure.
3. To install from a CD or DVD, insert the disk into the DVD or CD drive on the AE Services server.

   If you have installed and configured the Autorun RPM on the server, the installation program starts automatically.

4. Do the following steps if the installation program does not start automatically:
   a. To ensure that the media directory is properly mounted, type the command `mount mountpoint`
   b. To start the installation program manually, type the command `mountpoint/install-10.2.x.x.x.x-x`

   The installation wizard displays the Navigating the dialog boxes screen. Go to step 5.
5. To install the AE Services server software from an ISO image, download the ISO image to the `/tmp` directory of the AE Services server, and then do one of the following:
   - Mount the image using the **mount** command. For example `mount -t iso9660 -o loop /tmp/swonly-<build-number>.iso mountpoint`.
   - Validate that the operating system fulfills all the prerequisites by typing the command: `/mountpoint/install-10.2.x.x.x.x.x -c`

     Note:

     If the RPM check fails, install the missing RPMs.

     To view the complete list of all the required RPMs, see “AE Services RPMs”.
   - Start the installation program manually, by typing the command: `/mountpoint/install-10.2.x.x.x.x-x`.

   The installation wizard displays the Navigating the dialog boxes screen.
6. Press `Enter` to continue with the installation.

   The installation wizard displays the Select Installation Media screen
7. Select the media and press `Enter`.
8. In the Enter RPM URL screen, type the path name.

   For example, `/media/cdrom/Releases`.
9. Highlight **OK** and press `Enter`.

   The installation wizard displays the Select Release Version screen with the latest version selected by default.
10. Press `Enter`.
11. In the Co-residency warning screen, highlight **Yes** and press `Enter`.
12. In the Choose Installation Method screen, verify that **Install/Update** is selected.
13. Highlight **OK** and press `Enter`.

    The installation wizard displays the Choose Installation Packages screen with the following packages selected:
    - MVAP-Avaya AE Services
    - Third Party-Third_Party_Packages

14. Highlight **OK** and press `Enter`.

    The installation wizard displays the Optional Package screen with the **aesvcs-linuxconfig** package selected by default.

15. Select the Optional Package.

    Caution:

    If you use your own implementation of LDAP, cs-cusldap will overwrite your existing LDAP directory. To use the existing LDAP directory with AE Services, manually configure your LDAP implementation for compatibility with AE Services User Management.

    Avaya recommends that you accept the default configuration package **aesvcs-linuxconfig**, which is the Linux configuration package for AE Services.

    The installation wizard displays the Enable and Disable Enhanced Access Security Gateway Options screen.

16. Select the appropriate Security Gateway Option.

    Note:

    Enhanced Access Security Gateway option enables or disables Avaya Services logins to access your system. Register your product using Avaya Global Registration Tool to enable Avaya Remote Connectivity. You can also enable this feature after deploying the application by using the command **`EASGManage`**.

    The installation wizard displays the Last chance to abort -- Ready to Proceed? screen.

17. Select **Yes** to continue.

18. Verify the installation command. If all options are correct, press `Enter` to select **Yes**.

    The time required to install the software depends on the packages and the server processing power. Allow 5 to 10 minutes for the installation. When the installation is complete, the program displays the following message:

    ```
    Success, Installation/Update completed
    ```

19. During the installation, press `Enter` to Exit.

    - If the installation is successful, the wizard displays the following message:

      ```
      Installation Successful — Install/Upgrade log file is in /var/
      disk/avaya
      ```

    - If the installation is unsuccessful, the wizard displays the following message:

      ```
      Installation/Update failed
      ```

20. Press `Enter` to select **OK**.

21. Please remove the DVD or CD if you used it for the AE Services installation

22. Reboot the server.

Next steps

Install the AE Services license. See license requirements on page 65.

After installing AE Services server, if you face any discrepancy with LDAP, see Configuring an LDAP server for User Management on page 131

Related links

List of required RPMs on RHEL 8.4 on page 83
Configuring the Linux operating system for AE Services Software-Only installation on on-premise on page 39
Preparing for Software-Only deployment on AWS on page 44
Preparing for Software-Only deployment on Microsoft Azure on page 49
Preparing for Software-Only deployment on Google Cloud Platform on page 54
Configuring the LDAP server on page 132

Installing the AE Services patch using CLI

Procedure

1. Log in to the AE Services command line interface.
2. Copy the patch file on the AE Services server.
3. To provide executable permission, run the command: **`chmod +x <patch_file_name>`**.
4. Switch to the root user.
5. To install the patch, run the command: **`./<patch file_name>`**.
6. To accept the license terms, read the End User License Agreement, and type `Y`.
7. Run the command: **`swversion`** to verify the AE Services version.

Accounts installed during the installation of AE Services server

The installation program sets up the AE Services server with avaya and cust accounts by default. It also adds service accounts, such as craft and sroot, for Avaya service technicians.

Using installation logs to check up on an installation

About this task

You can use the installation logs to verify the success of an installation or upgrade, or to troubleshoot errors.

Procedure

1. Change directories to the /var/disk/avaya directory.
2. Use a text editor to view the log files.

   Log files for an installation or upgrade are named as follows: installation-status.log.

Using the Linux shell to locate files installed by AE Services

About this task

Follow this procedure to find out where a particular RPM installs its files:

Procedure

1. From the command line, log in as root.
2. Type `rpm -ql packagename` where *packagename* is the name of the RPM without the version number. For example `aesvcs-platform`.

   Linux displays the directories created and the files installed by the RPM.

Configuring load balancer on Microsoft Azure

About this task

You must configure a load balancer to use Virtual IP with Geo Redundant High Availability (GRHA) configuration onMicrosoft Azure.

Before you begin

Before installing the load balancer, install AE Services on respective virtual machines to be included in the load balancer rule.

Note:

If you install AE Services on virtual machines after installing the load balancer, the installation fails as the AE Services installer cannot reach repository servers because of load balancer rule.

Procedure

1. Create a load balancer of Type=Internal and SKU=standard with a static front-end IP address that matches the AE Services alias IP address.
2. Create a back-end pool with the two AE Services virtual machines. Use the eth0 IP address on each machine.
3. Create a TCP health probe using port 450 (Unencrypted) or port 453 (Encrypted) according to the selected port under **Networking** > **Ports** > **TSAPI Ports** on OAM page. Use the minimum values of 5 seconds interval and 2 probes.
4. Create a load balancing rule using the Front-end, back-end and probes defined above and select HA ports and Floating IP enabled.
5. On the AE Services Management Console main menu, click **Networking** > **AE Services IP (Local IP)**.
6. In the **Client Connectivity** field, select **Any**.

Chapter 6: AE Services licensing

Application Enablement Services license requirements

To get the full functionality for Application Enablement Services, you must install the Application Enablement Services product license. The product license specifies the features you are permitted to use. For more information about licensed features, see *Avaya Aura® Application Enablement Services Overview and Specification*.

Licensing lifecycle overview

About this task

Use this overview to learn about the licensing cycle and when licensing events take place.

Procedure

1. Obtain the license from the Avaya Product Licensing and Delivery System (PLDS) website. For more information, see Downloading software from PLDS on page 19.
2. After you install the software, log in to the Management Console to access the Avaya Web License Manager (WebLM).
3. After installing AE Services software, log in to the AE Services Management Console to access the Avaya Web License Manager (WebLM).
4. Use WebLM to install the license.
5. After you install the license file, restart the AE Services server.
6. When the license file is installed, you have access to the AE Services software.

HTTPS, WebLM, and AE Services

HTTPS is used for connecting a Master Avaya WebLM server and the AE Services Avaya WebLM client or embedded Local Avaya WebLM. The Master Avaya WebLM server can operate in an allocation mode or a pooled mode or both. For the allocation mode, the Master Avaya WebLM server acts as a client of the AE Services embedded Avaya WebLM to establish an HTTPS session and push a license file down to the AE Services embedded Local Avaya WebLM. For the

pooled mode, the AE Services C++ and Java Avaya WebLM clients establish an HTTPS session to the Master Avaya WebLM server or the AE Services embedded Local Avaya WebLM to acquire a license.

During the TLS handshake, for an HTTPS client-server session, the server must send its identity certificate to the client and the client must validate the server's identity certificate. For example, the Not Before date and the Not After date timeframe is valid, and the server identity certificate was signed by a trusted Certificate Authority (CA) known by the client. If the client is unable to validate the server's identity certificate, the handshake connection is terminated.

Note:

- For the pooled mode, the Master Avaya WebLM CA certificates must be imported into the AE Services Trusted Certificate store using the AE Services Management Console.
- For the allocation mode, the AE Services Apache Web server CA certificates must be imported into the Master Avaya WebLM trust store.

While attempting to connect to Avaya WebLM from the AE Services server or from a Master Avaya WebLM to the AE Services embedded Local Avaya WebLM, the connection might not get established. The following are some troubleshooting suggestions:

- Pooled mode: Using the Management Console, verify that the CA certificate used to sign the Master Avaya WebLM server's identity certificate is in the AE Services Trusted Certificate store. For a default System Manager installation where the Master Avaya WebLM is also embedded, the System Manager's embedded CA is used to sign the System Manager server identity certificate. Each System Manager deployment creates its own unique CA certificate with the same Common Name. Therefore, when validating whether the System Manager CA certificate is installed on the AE Services server, ensure that the System Manager CA certificate Serial ID matches the Serial ID of the System Manager CA certificate in the AE Services trust store.
- Allocation mode: Verify that the CA certificate used to sign the AE Services server identity certificate is in the Master Avaya WebLM trust store.
- Verify that the port is not blocked by a firewall.
- Verify that the Avaya WebLM server identity certificate has not expired.
- Check the AE Services log files for a TLS/SSL connection error, for example, using an unknown certificate.

Connecting to a WebLM server

About this task

Use this procedure to specify the IP address and port number of the WebLM server that Application Enablement Services uses for licensing.

Procedure

1. Log in to AE Services Management Console. See Logging on to the AE Services Management web console on page 73.

2. On the main menu, click **Licensing** > **WebLM Server Address**.
3. In the **WebLM IP Address** field, type the IP address of the WebLM server in the format `1.2.3.4`.

   If you use a remote WebLM server, enter the IPv4 address of the remote WebLM server.
4. Select the **SSL** check box to specify the appropriate setting for SSL.
5. In the **WebLM Port** field, type the port number of the WebLM server.

   The default port is `8443`.

Installing the AE Services license

About this task

To get the full functionality for AE Services you must install the AE Services license. Avaya sends the AE Services license file in an email message. If you did not receive a license file from Avaya, see Obtaining the AE Services license file on page 70. If you are upgrading from AE Services 6.x and you already have a license on a remote WebLM server (for example, the license was installed on a standalone WebLM server or System Manager), you need another license file. Uninstall the license file if you are upgrading from a major release to another release.

All earlier AE Services releases require a new license file when upgrading to AE Services.

Note:

By default, the AE Services server has a 30-days grace period. If a license file is not installed, the AE Services server enters in License Error mode. In License Error mode, you have 30-days in which to install a valid license file for AE Services. Error mode may also occur if an invalid (expired or incorrect) license file has been installed.

Procedure

1. Log on to the AE Services Management Console and click **Licensing** > **WebLM Server Access**.
2. On the Web License Manager Logon page, type your WebLM user name and password, and click the arrow.
3. On the WebLM Install License page, click **Browse**.
4. Locate the AE Services license file, and select it.
5. With the license file name displaying in the text box, click **Install**.

   WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message **License file installed successfully**.

   Note:

   If you do not receive this message, see Troubleshooting licensing error messages on page 69.

6. Verify that the license settings.
   a. Click **Licensed Products** > **Application_Enablement**.
   b. Verify that the correct license settings are enabled.
7. Click **Logout**.
8. Restart AE Services.

   See Restarting AE Services from the AE Services Management Console on page 69 or Restarting AE Services from the Linux command line on page 68.

Restarting AE Services from the Linux command line

About this task

You must restart AE Services to use the capabilities of the license. You can restart AE Services from the command line or through the Application Enablement Services Management Console, the web-based administrative interface.

Follow this procedure to restart AE Services from the command line.

Note:

This procedure is available only if you installed the Avaya Services package.

Procedure

1. Open an ssh session to the AE Services server, using either of the following methods.
   - Customers using the Avaya Services package: Log in as cust, and access the root account by using the **`su - root`** command.
   - Avaya service technicians: Log in as craft, and access the root account by using the **`su - sroot`** command.
2. Restart AE Services using the following command: **`systemctl restart aesvcs.service`**.

Result

The **`restart`** command stops AE Services, configures them, and then starts the services. The restart process takes from 3 to 10 minutes.

Restarting AE Services from the AE Services Management web console

About this task

Use this procedure to restart AE Services through the AE Services Management console to use the capabilities of the new license. You can also restart AE Services from the command line interface.

Procedure

1. Log in to the AE Services Management web console.
2. On the AE Services Management web console, click **Maintenance** > **Service Controller**.
3. On the Service Controller page, click **Restart AE Server**.
4. On the Restart AE Server page, click **Restart**.

   After a pause, the AE Services server returns to the Service Controller page. A restart can take several minutes.
5. Verify that all the correct licensed services are running.

Troubleshooting licensing error messages

If your browser displays an error message, try to resolve the problem as shown in the following table. If you cannot resolve the problem, contact your Avaya representative.

Error message	Explanation
`License file is invalid or not created for this server. License file was NOT installed.`	The file is corrupt or the Host ID in the license file does not match the Host ID in the server. For more information, see Identifying the Host ID using WebLM on page 70.
`Attempting to install a license file that is currently installed. License file was NOT installed`	This license is already active.
`More than one license exists, the AE Server will not be started. Please have only one valid license and delete other licenses.`	A valid license already exists due to an upgrade from an earlier release. You must remove the old license before you install the new license for the latest major release. See Uninstalling the AE Services license on page 71.

Table continues…

Error message	Explanation
`No valid license file found`	WebLM might display this message on the main page after AE Services reports "`License file installed successfully`". To resolve this problem: 1. Verify you are using the AE Services server host name, and not the IP address. 2. If the host name is correct, contact your Avaya representative.

Obtaining the AE Services license file

Procedure

1. Determine the Host ID of the first NIC on the server.

   See Identifying the Host ID using WebLM on page 70.

2. Log in to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
3. Provision the license file.
4. Download the license file.

Identifying the Host ID using WebLM

About this task

If AE Services software is already installed, you can use WebLM to identify the Host ID.

Procedure

1. Navigate to WebLM.
2. On the WebLM Home page, click **Server properties**.
3. On the Server Properties page, locate the value for Primary Host ID.

   Note:

   If the NIC you used to generate the Host ID changes after initial installation, contact your local Avaya distributor. If you have a technical support agreement with Avaya, call 1-800-344-9670.

Identifying the MAC address using ifconfig

About this task

If you have not installed AE Services or you cannot access WebLM, use the Linux **`ifconfig`** command to identify the MAC address of the NIC.

If the server has a dual NIC or multiple NICs, provide the MAC address of the first Ethernet interface on the first NIC.

If remote WEBLM server is used, the MAC ID of the remote server should be used for license generation.

Procedure

1. From the Linux command prompt, type `ifconfig eth0`.
2. In the ifconfig command output, the MAC address corresponds to the hexadecimal value for HWaddr.

   In the following example it is expressed as `00:B0:D0:44:9F:A1`.

   ```
   eth0 Link encap:Ethernet HWaddr 00:B0:D0:44:9F:A1
   inet addr:10.10.10.1 Bcast:10.255.255.255 Mask:255.0.0.0
   ```

   Note:

   If the NIC you used to generate the MAC address changes after initial installation, contact your local Avaya distributor. If you have a technical support agreement with Avaya, call 1-800-344-9670.

Uninstalling the AE Services license

Procedure

1. Navigate to WebLM.
2. From the main menu, click **Uninstall License**.
3. From the Uninstall License page, select the check box for the Application_Enablement license, and click **Uninstall**.

   Your browser displays a message asking if you want to continue.
4. Click **OK**.

Chapter 7: AE Services post-installation administration

AE Services post-installation administration

Use the information in this chapter to perform post-installation administrative tasks. For all other administrative tasks, see the *Administering Avaya Aura® Application Enablement Services*.

Opening an ssh session to AE Services

About this task

This procedure assumes that you have a secure shell (ssh) client, such as PuTTY or PuTTYtel running on your administrative workstation.

Procedure

1. Start your ssh client, and complete the information in the dialog box that it presents to open a session. For example, specify the following information to open a session to the AE Services server.
   - Host Name (or IP address) - enter the host name or IP address of your AE Services server, for example, `aeserver.example.com`.
   - Port - enter `22`.
   - Connection type - enter `SSH`.
   - Click **Open**.

     Note:

     The server displays the PuTTY Security Alert window the first time you connect to the SAMP. If you see this window, click **Yes** to accept the server's host key.

   The system displays the PuTTY window.
2. If you are an Avaya service technician or Business Partner, log in as follows:
   a. At the login as: prompt, type `craft`.
   b. At the prompt, type the challenge/password.
   c. At the command prompt, type `su - sroot`.
   d. At the prompt, type the challenge/password.

3. If you are a customer and the Avaya services package is installed, log in as follows:
   a. At the login as: prompt, type `cust`.
   b. At the password prompt, type the password for the cust account.
   c. At the command prompt, type `su - root`.
   d. At the password prompt, type the password for the root account.
4. If you are a customer and the Avaya services package is not installed, log in as `root`.

Logging on to the AE Services Management web console

About this task

Important:

You cannot log in to the AE Services Management web console with root credentials. If you installed the Avaya Services package (cs-services), log in as either craft or cust.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name/IP address>`, the AE Services URL.

   For example: `https://aserver.example.com`

   If you are accessing the AE Services server for the first time, the browser displays a security alert for an SSL certificate.

   If the SSL certificate is not presented, verify that the address bar on your browser displays https and the fully qualified domain name or IP address of the AE Services server.
2. On the Security alert window, click **Yes** to accept the certificate.
3. On the Application Enablement Services welcome page, click **Continue To Login**.
4. On the Application Enablement Services Management web console login page, in **Username** , type the login ID.
5. Click **Continue**.
6. In **Password**, type the password.

   When logged in as a service technician, and if the Enhanced Access Security Gateway (EASG) is present, your login ID is challenged by EASG. You must enter a proper response in the **Response** field to log in successfully.

   For customer user login credentials, these options are not presented.
7. Click **Login**.

   The browser displays the Application Enablement Services Management web console. The main menu is in the left pane and the welcome page is in the right pane.

Note:

If you are logging in for the first time, AE Services displays the End User License Agreement page.

Verifying the software version

About this task

You can see the software version in the upper-right corner of the AE Services Management Console window. If not, you can run the **swversion** command.

Procedure

1. Log in to the AE Services command line interface.
2. At the prompt, type the **swversion** command.
3. Verify the version number and build number.

Verifying the license

Procedure

1. Log in to AE Services Management Console.
2. On the main menu, click **Licensing** > **WebLM Server Access**.
3. On the Web License Manager main menu, click **Licensed Products** > **Application_Enablement**.
4. On the Application Enablement (Standard License file) page, verify the Licensed Features settings.

Verifying the AE Service IP (Local IP) settings

Procedure

1. Log in to AE Services Management Console.
2. From the main menu, select **Networking > AE Service IP (Local IP)**.

   The settings on the AE Services IP (Local IP) page should match the settings you specified during initial deployment.

   - If you set up a single NIC configuration, the IP settings in the Client Connectivity, Switch Connectivity, and Media Connectivity fields should be the same.
   - If you set up a dual NIC configuration, the IP settings should match the settings you specified during initial deployment.

     Note:

     The private network segment should contain one subnet; this is the only supported configuration. You can configure any default gateway for public and private network segments. However, Avaya recommends using a public gateway as the default

gateway to enable access to AE Services through both public and private network segments. After deployment, you must add static routes through CLI to make AE Services accessible from the private network segment.

Verifying the Network Configuration settings

Procedure

1. Log in to AE Services Management Console.
2. On the main menu, click **Networking** > **Network Configure**.
3. On the Network Configure page, verify the settings that you configured on the AE Services server.

Verifying the time zone and NTP server settings

Procedure

1. From your browser, log in to AE Services Management Console.
2. From the main menu, select **Maintenance** > **Date Time/NTP Server**.

   The settings for the time zone and NTP server should match the settings you typed on the Date/Time Initialization screen when you installed the software.

Editing the NIC configuration

About this task

Network interfaces are configured during the AE Services installation process on the Configure Network Information page.

Use this procedure only if you need to change the NIC settings from Auto-Negotiate to Lockdown (100M links only).

The values that are initially displayed on the Network Configure page reflect the negotiated values between the NICs on the AE Services server and the Ethernet switch on your network.

Important:

AE Services has been tested at 1000BaseT full duplex and 100BaseT full duplex. These are the required speed and duplex mode settings for both network interfaces eth0 and eth1.

Procedure

1. On the AE Services Management Console, click **Networking** > **Network Configure**.
2. On the Network Configure page, edit any of the settings that you want to change, and click **Apply Changes**.

Note:

Changing the settings for a NIC will cause the NIC to restart. Once you change the settings, they remain in effect until you reset them. Rebooting the AE Services server will not reset any of the values.

Chapter 8: Resources

Application Enablement Services documentation

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

Title	Description	Audience
Design		
Avaya Aura® Application Enablement Services Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide	Installing TSAPI and CVLAN Client and SDK	Customers and sales, services, and support personnel
Using		
Upgrading Avaya Aura® Application Enablement Services	Upgrading Application Enablement Services applications.	System administrators and IT personnel
Administering Avaya Aura® Application Enablement Services	Administering Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel
Avaya Aura® Application Enablement Services Data Privacy Guidelines	Describes how to administer Application Enablement Services to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation		
Deploying Avaya Aura® Application Enablement Services in Virtualized Environment	Deploy Application Enablement Services applications in Virtualized Environment	Implementation personnel
Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments	Deploy Application Enablement Services applications in Software-Only and Infrastructure as a Service Environments	Implementation personnel
Maintenance and Troubleshooting		

Table continues…

Title	Description	Audience
Maintaining Avaya Aura® Application Enablement Services	Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 78
Accessing the port matrix document on page 78
Avaya Documentation Center navigation on page 79

Finding documents on the Avaya Support website

Procedure

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

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

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

Related links

Application Enablement Services documentation on page 77

Accessing the port matrix document

Procedure

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

   This field is not available if there is only one release for the product.

5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Related links

Application Enablement Services documentation on page 77

Avaya Documentation Center navigation

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

Important:

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

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

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

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

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.

- Send feedback for a topic.

Related links

Application Enablement Services documentation on page 77

Training

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

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 82

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

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

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

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

Related links

Support on page 81

Appendix A: List of required RPMs on RHEL 8.4

The following are lists of required RPMs on RHEL 8.4 for Application Enablement Services Software-Only environment:

A

audit-libs-3.0-0.17.20191104git1c2f876.el8.i686

B

brotli-1.0.6-3.el8.i686	bzip2-libs-1.0.6-26.el8.i686

C

cyrus-sasl-lib-2.1.27-6.el8_5.i686

E

elfutils-libelf-0.185-1.el8.i686	expat-2.2.5-4.el8_5.3.i686

G

gdk-pixbuf2-2.36.12-5.el8.i686	glib2-2.56.4-156.el8.i686
glibc-2.28-164.el8_5.3.i686	gmp-6.1.2-10.el8.i686
gnutls-3.6.16-4.el8.i686	

I

iputils-20180629-7.el8.x86_64	irqbalance-1.4.0-6.el8.x86_64

J

jansson-2.11-3.el8.x86_64	jbigkit-libs-2.1-14.el8.i686
json-c-0.13.1-0.4.el8.x86_64	

K

kbd-2.0.4-10.el8.x86_64	kbd-legacy-2.0.4-10.el8.noarch

Table continues…

kbd-misc-2.0.4-10.el8.noarch	kernel-4.18.0-305.19.1.el8_4.x86_64
kernel-tools-4.18.0-305.19.1.el8_4.x86_64	kernel-tools-libs-4.18.0-305.19.1.el8_4.x86_64
kexec-tools-2.0.20-46.el8.x86_64	keyutils-libs-1.5.10-6.el8.i686
keyutils-libs-1.5.10-9.el8.x86_64	kmod-25-17.el8.x86_64
kmod-libs-25-17.el8.x86_64	kpartx-0.8.4-10.el8.x86_64
krb5-libs-1.18.2-8.3.el8_4.i686	krb5-libs-1.18.2-8.3.el8_4.x86_64

L

less-530-1.el8.x86_64	libacl-2.2.53-1.el8.i686
libacl-2.2.53-1.el8.x86_64	libaio-0.3.112-1.el8.x86_64
libassuan-2.5.1-3.el8.x86_64	libattr-2.4.48-3.el8.i686
libattr-2.4.48-3.el8.x86_64	libblkid-2.32.1-27.el8.x86_64
libblkid-2.32.1-28.el8.i686	libcap-2.26-4.el8.x86_64
libcap-2.26-5.el8.i686	libcap-ng-0.7.11-1.el8.i686
libcap-ng-0.7.9-5.el8.x86_64	libcom_err-1.45.6-1.el8.x86_64
libcom_err-1.45.6-2.el8.i686	libcroco-0.6.12-4.el8_2.1.x86_64
libcurl-7.61.1-18.el8_4.1.x86_64	libcurl-7.61.1-22.el8.i686
libdaemon-0.14-15.el8.x86_64	libdb-5.3.28-40.el8.x86_64
libdb-5.3.28-42.el8_4.i686	libdb-utils-5.3.28-40.el8.x86_64
libdrm-2.4.103-1.el8.x86_64	libdrm-2.4.106-2.el8.i686
libedit-3.1-23.20170329cvs.el8.x86_64	libestr-0.1.10-1.el8.x86_64
libfastjson-0.99.8-2.el8.x86_64	libffi-3.1-22.el8.i686
libffi-3.1-22.el8.x86_64	libgcc-8.4.1-1.el8.x86_64
libgcc-8.5.0-4.el8_5.i686	libgcrypt-1.8.5-4.el8.x86_64
libgomp-8.4.1-1.el8.x86_64	libgpg-error-1.31-1.el8.x86_64
libidn2-2.2.0-1.el8.i686	libjpeg-turbo-1.5.3-12.el8.i686
libmnl-1.0.4-6.el8.x86_64	libmount-2.32.1-27.el8.x86_64
libmount-2.32.1-28.el8.i686	libmspack-0.7-0.3.alpha.el8.4.x86_64
libndp-1.7-5.el8.x86_64	libnfnetlink-1.0.1-13.el8.x86_64
libnghttp2-1.33.0-3.el8_2.1.i686	libnl3-3.5.0-1.el8.x86_64
libnl3-cli-3.5.0-1.el8.x86_64	libpciaccess-0.14-1.el8.i686
libpciaccess-0.14-1.el8.x86_64	libpipeline-1.5.0-2.el8.x86_64
libpng-1.6.34-5.el8.i686	libpng-1.6.34-5.el8.x86_64
libpsl-0.20.2-6.el8.i686	libpwquality-1.4.4-3.el8.x86_64
libseccomp-2.5.1-1.el8.x86_64	libselinux-2.9-5.el8.i686
libselinux-2.9-5.el8.x86_64	libselinux-utils-2.9-5.el8.x86_64

Table continues…

libsemanage-2.9-6.el8.x86_64	libsepol-2.9-2.el8.i686
libsepol-2.9-2.el8.x86_64	libsmartcols-2.32.1-27.el8.x86_64
libss-1.45.6-1.el8.x86_64	libssh-0.9.4-3.el8.i686
libssh2-1.8.0-8.module+el8.0.0+4084+cceb9f44.1.x86_64	libstdc++-8.4.1-1.el8.x86_64
libstdc++-8.5.0-4.el8_5.i686	libsysfs-2.1.0-24.el8.x86_64
libtasn1-4.13-3.el8.i686	libtasn1-4.13-3.el8.x86_64
libteam-1.31-2.el8.x86_64	libtiff-4.0.9-20.el8.i686
libtool-ltdl-2.4.6-25.el8.x86_64	libunistring-0.9.9-3.el8.i686
libunistring-0.9.9-3.el8.x86_64	libuser-0.62-23.el8.x86_64
libutempter-1.1.6-14.el8.x86_64	libuuid-2.32.1-27.el8.x86_64
libuuid-2.32.1-28.el8.i686	libverto-0.3.0-5.el8.i686
libverto-0.3.0-5.el8.x86_64	libwayland-server-1.19.0-1.el8.i686
libxcrypt-4.1.1-6.el8.i686	libxml2-2.9.7-9.el8_4.2.x86_64
libxslt-1.1.32-6.el8.x86_64	libzstd-1.4.4-1.el8.i686
linux-firmware-20201218-102.git05789708.el8.noarch	lm_sensors-libs-3.4.0-23.20180522git70f7e08.el8.i686
logrotate-3.14.0-4.el8.x86_64	lshw-B.02.19.2-2.el8.x86_64
lsscsi-0.32-2.el8.x86_64	lua-5.3.4-11.el8.x86_64
lua-libs-5.3.4-12.el8.i686	lvm2-2.03.11-5.el8.x86_64
lvm2-libs-2.03.11-5.el8.x86_64	lzo-2.08-14.el8.x86_64

M

make-4.2.1-10.el8.x86_64	man-db-2.7.6.1-17.el8.x86_64
mariadb-connector-c-3.1.11-2.el8_3.i686	mesa-libgbm-21.1.5-1.el8.i686
microcode_ctl-20210216-1.20210608.1.el8_4.x86_64	

N

ncurses-6.1-7.20180224.el8.x86_64	ncurses-base-6.1-7.20180224.el8.noarch
ncurses-libs-6.1-7.20180224.el8.x86_64	net-snmp-agent-libs-5.8-22.el8.i686
net-snmp-libs-5.8-22.el8.i686	nettle-3.4.1-7.el8.i686
NetworkManager-1.30.0-7.el8.x86_64	NetworkManager-libnm-1.30.0-7.el8.x86_64
NetworkManager-team-1.30.0-7.el8.x86_64	NetworkManager-tui-1.30.0-7.el8.x86_64
network-scripts-10.00.15-1.el8.x86_64	newt-0.52.20-11.el8.x86_64
nftables-0.9.3-18.el8.x86_64	nspr-4.32.0-1.el8_4.x86_64
nss-3.67.0-6.el8_4.x86_64	nss-softokn-3.67.0-6.el8_4.x86_64

Table continues…

nss-softokn-freebl-3.67.0-6.el8_4.x86_64	nss-util-3.67.0-6.el8_4.x86_64
numactl-libs-2.0.12-11.el8.x86_64	

O

openldap-2.4.46-15.el8.x86_64	openssh-8.0p1-5.el8.x86_64
openssh-clients-8.0p1-5.el8.x86_64	openssh-server-8.0p1-5.el8.x86_64
openssl-1.1.1g-15.el8_3.x86_64	openssl-libs-1.1.1g-15.el8_3.i686
openssl-libs-1.1.1g-15.el8_3.x86_64	openssl-pkcs11-0.4.10-2.el8.i686
open-vm-tools-11.2.0-2.el8.x86_64	os-prober-1.74-6.el8.x86_64

P

p11-kit-0.23.22-1.el8.i686	p11-kit-0.23.22-1.el8.x86_64
p11-kit-trust-0.23.22-1.el8.x86_64	pam-1.3.1-14.el8.x86_64
parted-3.2-38.el8.x86_64	passwd-0.80-3.el8.x86_64
pciutils-3.7.0-1.el8.x86_64	pciutils-libs-3.7.0-1.el8.x86_64
pcre2-10.32-2.el8.i686	pcre-8.42-4.el8.x86_64
pcre-8.42-6.el8.i686	pcsc-lite-libs-1.8.23-4.1.el8_4.i686
perl-libs-5.26.3-420.el8.i686	pinentry-1.1.0-2.el8.x86_64
plymouth-0.9.4-9.20200615git1e36e30.el8.x86_64	plymouth-core-libs-0.9.4-9.20200615git1e36e30.el8.x86_64
plymouth-scripts-0.9.4-9.20200615git1e36e30.el8.x86_64	policycoreutils-2.9-14.el8.x86_64
polkit-0.115-11.el8_4.1.x86_64	polkit-pkla-compat-0.1-12.el8.x86_64
popt-1.18-1.el8.i686	popt-1.18-1.el8.x86_64
procps-ng-3.3.15-6.el8.x86_64	

R

readline-7.0-10.el8.x86_64	rootfiles-8.1-22.el8.noarch
rpm-4.14.3-14.el8_4.x86_64	rpm-build-libs-4.14.3-14.el8_4.x86_64
rpm-libs-4.14.3-19.el8_4.x86_64	rpm-libs-4.14.3-19.el8_5.2.i686
rsyslog-8.1911.0-6.el8.x86_64	

S

sed-4.5-2.el8.x86_64	selinux-policy-3.14.3-67.el8.noarch
selinux-policy-targeted-3.14.3-67.el8.noarch	setup-2.12.2-6.el8.noarch
sg3_utils-1.44-5.el8.x86_64	sg3_utils-libs-1.44-5.el8.x86_64
shadow-utils-4.6-12.el8.x86_64	shared-mime-info-1.9-3.el8.x86_64
slang-2.3.2-3.el8.x86_64	snappy-1.1.8-3.el8.x86_64

Table continues…

sqlite-3.26.0-13.el8.x86_64	subscription-manager-1.28.13-2.el8.x86_64
subscription-manager-rhsm-certificates-1.28.13-2.el8.x86_64	sudo-1.8.29-7.el8.x86_64
systemd-239-45.el8_4.2.x86_64	systemd-libs-239-45.el8_4.2.x86_64

T

tar-1.30-5.el8.x86_64	tcl-8.6.8-2.el8.i686
teamd-1.31-2.el8.x86_64	tuned-2.15.0-2.el8.noarch
tzdata-2021a-1.el8.noarch	

U

usermode-1.113-1.el8.x86_64	util-linux-2.32.1-27.el8.x86_64

V

vim-minimal-8.0.1763-15.el8.x86_64	virt-what-1.18-6.el8.x86_64

W

which-2.21-12.el8.x86_64

X

xfsprogs-5.0.0-8.el8.x86_64	xmlsec1-1.2.25-4.el8.x86_64
xmlsec1-openssl-1.2.25-4.el8.x86_64	xz-5.2.4-3.el8.x86_64
xz-libs-5.2.4-3.el8.i686	xz-libs-5.2.4-3.el8.x86_64

Y

yum-4.4.2-11.el8.noarch

Z

zlib-1.2.11-17.el8.i686	zlib-1.2.11-17.el8.x86_64

Appendix B: List of required RPMs on RHEL 8.10

The following are lists of required RPMs on RHEL 8.10 for Application Enablement Services Software-Only environment:

A

acl	adcli	aesvcs-alarmService-config	aesvcs-avaya-license
aesvcs-callcontrol	aesvcs-certMgmt-config	aesvcs-cmapi	aesvcs-common-utils
aesvcs-config-security	aesvcs-hmdc	aesvcs-install-scripts-hooks	aesvcs-linux-config
aesvcs-mvap-snmp	aesvcs-platform	aesvcs-services	aesvcs-sms
aesvcs-snmp	aesvcs-telephonysvc	aesvcs-telrestsvc	aesvcs-tomcat-config
aesvcs-userService-config	aesvcs-vmware-config	aesvcs-vmware-hooks	aide
alsa-lib	annobin	apache-commons-collections	apache-commons-daemon
apache-commons-dbcp	apache-commons-pool	apr	apr-util
apr-util-bdb	apr-util-openssl	atk	audit
audit-libs	augeas-libs	auracommon	authselect
authselect-libs	autogen	autogen-libopts	avahi
avahi-libs	avaya-os-tools	AvayaProductRootCA	axis

B

basesystem	bash	bash-completion	bc
bind-export-libs	bind-libs	bind-libs-lite	bind-license
bind-utils	binutils	biosdevname	brotli
bubblewrap	bzip2	bzip2-libs	

C

ca-certificates	cairo	c-ares	cert_tool

Table continues…

checkpolicy	chkconfig	chrony	clamav
clamav-data	clamav-filesystem	clamav-lib	clamav-update
clamd	clevis	clevis-dracut	clevis-luks
clevis-systemd	compat-openssl10	copy-jdk-configs	coreutils
coreutils-common	cpio	cpp	cracklib
cracklib-dicts	cronie	cronie-anacron	crontabs
crypto-policies	crypto-policies-scripts	cryptsetup	cryptsetup-libs
cs_configuration	cs-cusldap	cs-userservice	cs-verifysig
cups-libs	curl	cyrus-sasl	cyrus-sasl-gssapi
cyrus-sasl-lib			

D

dbus	dbus-common	dbus-daemon	dbus-glib
dbus-libs	dbus-tools	dejavu-fonts-common	dejavu-sans-fonts
device-mapper	device-mapper-event	device-mapper-event-libs	device-mapper-libs
device-mapper-persistent-data	dhcp-client	dhcp-common	dhcp-libs
dialog	diffutils	dmidecode	dnf
dnf-data	dnf-plugins-core	dnf-plugin-subscription-manager	dos2unix
dosfstools	dracut	dracut-config-rescue	dracut-network
dracut-squash	dwz		

E

e2fsprogs	e2fsprogs-devel	e2fsprogs-libs	ecj
efibootmgr	efi-filesystem	efi-srpm-macros	efivar
efivar-libs	elfutils-debuginfod-client	elfutils-default-yama-scope	elfutils-libelf
elfutils-libs	elinks	ethtool	execstack
expat	expect		

F

fapolicyd	fapolicyd-selinux	file	file-libs
filesystem	findutils	fipscheck	fipscheck-lib
firewalld	firewalld-filesystem	fontconfig	fontpackages-filesystem
freetype	fribidi	fstrm	fuse
fuse-common	fuse-libs	fwupd	

G

gawk	gc	gcc	gcc-gdb-plugin
gcc-plugin-annobin	gdb	gdb-headless	gdbm
gdbm-libs	gdisk	gdk-pixbuf2	gdk-pixbuf2-modules
geolite2-city	geolite2-country	gettext	gettext-libs
ghc-srpm-macros	giflib	glib2	glibc
glibc-all-langpacks	glibc-common	glibc-devel	glibc-gconv-extra
glibc-headers	glibc-langpack-en	gmp	gnupg2
gnupg2-smime	gnutls	gobject-introspection	go-srpm-macros
gpgme	gpg-pubkey	gpm-libs	graphite2
grep	groff-base	grub2-common	grub2-efi-x64
grub2-tools	grub2-tools-efi	grub2-tools-extra	grub2-tools-minimal
grubby	gtk2	gtk-update-icon-cache	guile
gzip			

H

hardlink	harfbuzz	haveged	hdparm
hicolor-icon-theme	hostname	httpd	httpd-filesystem
httpd-tools	http-parser	hwdata	

I

ima-evm-utils	info	initscripts	iotop
ipcalc	iproute	iprutils	ipset
ipset-libs	iptables	iptables-ebtables	iptables-libs
iputils	irqbalance	isl	

J

jansson	jasper-libs	java-1.8.0-openjdk	java-1.8.0-openjdk-devel
java-1.8.0-openjdk-headless	javapackages-filesystem	javapackages-tools	jbigkit-libs
jose	jq	json-c	json-glib

K

kbd	kbd-legacy	kbd-misc	kernel
kernel-core	kernel-headers	kernel-modules	kernel-tools
kernel-tools-libs	kexec-tools	keyutils-libs	kmod
kmod-libs	kpartx	krb5-libs	krb5-workstation

L

langpacks-en	less	libacl	libaio
libarchive	libassuan	libatasmart	libatomic_ops
libattr	libbabeltrace	libbasicobjects	libblkid
libblockdev	libblockdev-crypto	libblockdev-fs	libblockdev-loop
libblockdev-mdraid	libblockdev-part	libblockdev-swap	libblockdev-utils
libbpf	libbsd	libbytesize	libcap
libcap-ng	libcollection	libcom_err	libcom_err-devel
libcomps	libcroco	libcurl	libdaemon
libdatrie	libdb	libdb-utils	libdhash
libdnet	libdnf	libdrm	libedit
libestr	libevent	libfastjson	libfdisk
libffi	libfontenc	libgcab1	libgcc
libgcrypt	libglvnd	libglvnd-egl	libglvnd-glx
libgomp	libgpg-error	libgudev	libgusb
libibverbs	libICE	libicu	libidn2
libini_config	libipa_hbac	libipt	libjose
libjpeg-turbo	libkadm5	libkcapi	libkcapi-hmaccalc
libksba	libldb	libluksmeta	libmaxminddb
libmd	libmetalink	libmnl	libmodulemd
libmount	libmpc	libmspack	libndp
libnetfilter_conntrack	libnfnetlink	libnfsidmap	libnftnl
libnghttp2	libnl3	libnl3-cli	libnsl2
libpath_utils	libpcap	libpciaccess	libpipeline
libpkgconf	libpng	libpq	libprelude
libpsl	libpwquality	librdkafka1	libref_array
librepo	libreport-filesystem	libretls	librhsm
libseccomp	libsecret	libselinux	libselinux-utils
libsemanage	libsepol	libsigsegv	libSM
libsmartcols	libsmbclient	libsmbios	libsmi
libsolv	libss	libssh	libssh2
libssh-config	libsss_autofs	libsss_certmap	libsss_idmap
libsss_nss_idmap	libsss_sudo	libstdc++	libsysfs
libtalloc	libtasn1	libtdb	libteam
libtevent	libthai	libtiff	libtirpc
libtool-ltdl	libudisks2	libunistring	libusbx

Table continues…

libuser	libutempter	libuuid	libverto
libwayland-client	libwayland-server	libwbclient	libX11
libX11-common	libX11-xcb	libXau	libxcb
libXcomposite	libxcrypt	libxcrypt-devel	libXcursor
libXdamage	libXext	libXfixes	libXft
libXi	libXinerama	libxkbcommon	libxml2
libxmlb	libXrandr	libXrender	libxshmfence
libxslt	libXtst	libXxf86vm	libyaml
libzip	libzstd	linux-firmware	lksctp-tools
lm_sensors	lm_sensors-libs	lmdb-libs	logrotate
lshw	lsof	lsscsi	lua
lua-libs	luksmeta	lvm2	lvm2-libs
lz4-libs	lzo		

M

make	man-db	mariadb-connector-c	mariadb-connector-c-config
mdadm	memstrack	mesa-libEGL	mesa-libgbm
mesa-libGL	mesa-libglapi	microcode_ctl	mod_http2
mod_session	mod_ssl	mokutil	mozjs60
mpfr			

N

ncurses	ncurses-base	ncurses-libs	net-snmp
net-snmp-agent-libs	net-snmp-libs	net-snmp-utils	nettle
net-tools	NetworkManager	NetworkManager-libnm	NetworkManager-team
NetworkManager-tui	network-scripts	network-scripts-team	newt
nftables	nginx-filesystem	npth	nscd
nspr	nss	nss-pam-ldapd	nss-softokn
nss-softokn-freebl	nss-sysinit	nss-util	numactl-libs

O

ocaml-srpm-macros	ongres-scram	ongres-scram-client	oniguruma
openblas-srpm-macros	openldap	openldap-clients	openldap-servers
openssh	openssh-clients	openssh-server	openssl
openssl-libs	openssl-pkcs11	open-vm-tools	os-prober

P

p11-kit	p11-kit-trust	pam	pango
parted	passwd	pciutils	pciutils-libs
pcre	pcre2	pcsc-lite-devel	pcsc-lite-libs
perl	perl-Algorithm-Diff	perl-Archive-Tar	perl-Archive-Zip
perl-Attribute-Handlers	perl-autodie	perl-B-Debug	perl-bignum
perl-Carp	perl-Compress-Bzip2	perl-Compress-Raw-Bzip2	perl-Compress-Raw-Zlib
perl-Config-Perl-V	perl-constant	perl-CPAN	perl-CPAN-Meta
perl-CPAN-Meta-Requirements	perl-CPAN-Meta-YAML	perl-Data-Dumper	perl-Data-OptList
perl-Data-Section	perl-DB_File	perl-devel	perl-Devel-Peek
perl-Devel-PPPort	perl-Devel-SelfStubber	perl-Devel-Size	perl-Digest
perl-Digest-MD5	perl-Digest-SHA	perl-Encode	perl-Encode-devel
perl-Encode-Locale	perl-encoding	perl-Env	perl-Errno
perl-experimental	perl-Exporter	perl-ExtUtils-CBuilder	perl-ExtUtils-Command
perl-ExtUtils-Embed	perl-ExtUtils-Install	perl-ExtUtils-MakeMaker	perl-ExtUtils-Manifest
perl-ExtUtils-Miniperl	perl-ExtUtils-MM-Utils	perl-ExtUtils-ParseXS	perl-File-Fetch
perl-File-HomeDir	perl-File-Path	perl-File-Temp	perl-File-Which
perl-Filter	perl-Filter-Simple	perl-Getopt-Long	perl-HTTP-Tiny
perl-inc-latest	perl-interpreter	perl-IO	perl-IO-Compress
perl-IO-Socket-IP	perl-IO-Socket-SSL	perl-IO-Zlib	perl-IPC-Cmd
perl-IPC-System-Simple	perl-IPC-SysV	perl-JSON-PP	perl-libnet
perl-libnetcfg	perl-libs	perl-Locale-Codes	perl-Locale-Maketext
perl-Locale-Maketext-Simple	perl-local-lib	perl-macros	perl-Math-BigInt
perl-Math-BigInt-FastCalc	perl-Math-BigRat	perl-Math-Complex	perl-Memoize
perl-MIME-Base64	perl-Module-Build	perl-Module-CoreList	perl-Module-CoreList-tools
perl-Module-Load	perl-Module-Load-Conditional	perl-Module-Loaded	perl-Module-Metadata
perl-Mozilla-CA	perl-MRO-Compat	perl-Net-Ping	perl-Net-SSLeay
perl-open	perl-Package-Generator	perl-Params-Check	perl-Params-Util
perl-parent	perl-PathTools	perl-perlfaq	perl-PerlIO-via-QuotedPrint
perl-Perl-OSType	perl-Pod-Checker	perl-Pod-Escapes	perl-Pod-Html
perl-podlators	perl-Pod-Parser	perl-Pod-Perldoc	perl-Pod-Simple

Table continues…

perl-Pod-Usage	perl-Scalar-List-Utils	perl-SelfLoader	perl-Socket
perl-Software-License	perl-srpm-macros	perl-Storable	perl-Sub-Exporter
perl-Sub-Install	perl-Sys-Syslog	perl-Term-ANSIColor	perl-Term-Cap
perl-TermReadKey	perl-Test	perl-Test-Harness	perl-Test-Simple
perl-Text-Balanced	perl-Text-Diff	perl-Text-Glob	perl-Text-ParseWords
perl-Text-Tabs+Wrap	perl-Text-Template	perl-Thread-Queue	perl-threads
perl-threads-shared	perl-Time-HiRes	perl-Time-Local	perl-Time-Piece
perl-Unicode-Collate	perl-Unicode-Normalize	perl-URI	perl-utils
perl-version	php	php-cli	php-common
php-fpm	php-mbstring	php-soap	php-xml
pigz	pinentry	pixman	pkgconf
pkgconf-m4	pkgconf-pkg-config	platform-python	platform-python-pip
platform-python-setuptools	plymouth	plymouth-core-libs	plymouth-scripts
policycoreutils	policycoreutils-python-utils	polkit	polkit-libs
polkit-pkla-compat	popt	postgresql	postgresql-jdbc
postgresql-server	prefixdevname	procps-ng	protobuf-c
psmisc	publicsuffix-list-dafsa	python36	python3-audit
python3-augeas	python3-beautifulsoup4	python3-bind	python3-chardet
python3-cloud-what	python3-configobj	python3-cssselect	python3-dateutil
python3-dbus	python3-decorator	python3-dmidecode	python3-dnf
python3-dnf-plugins-core	python3-ethtool	python3-firewall	python3-gobject-base
python3-gpg	python3-hawkey	python3-html5lib	python3-idna
python3-iniparse	python3-inotify	python3-libcomps	python3-libdnf
python3-librepo	python3-libs	python3-libselinux	python3-libsemanage
python3-libxml2	python3-linux-procfs	python3-lxml	python3-nftables
python3-perf	python3-pip	python3-pip-wheel	python3-ply
python3-policycoreutils	python3-pwquality	python3-pycurl	python3-pyparsing
python3-pysocks	python3-pyudev	python3-requests	python3-rpm
python3-rpm-macros	python3-schedutils	python3-setools	python3-setuptools
python3-setuptools-wheel	python3-six	python3-slip	python3-slip-dbus
python3-sssdconfig	python3-subscription-manager-rhsm	python3-syspurpose	python3-systemd
python3-unbound	python3-urllib3	python3-webencodings	python-rpm-macros
python-srpm-macros			

Q

qemu-guest-agent	qt5-srpm-macros		

R

readline	redhat-logos-httpd	redhat-release	redhat-release-eula
redhat-rpm-config	rng-tools	rootfiles	rpm
rpm-build-libs	rpm-libs	rpm-plugin-fapolicyd	rpm-plugin-selinux
rpm-plugin-systemd-inhibit	rsync	rsyslog	rsyslog-gnutls
rust-srpm-macros			

S

samba-client-libs	samba-common	samba-common-libs	sed
selinux-policy	selinux-policy-targeted	setup	sg3_utils
sg3_utils-libs	shadow-utils	shared-mime-info	shim-x64
slang	snappy	sohd	spiritAgentrpm
sqlite	sqlite-libs	squashfs-tools	sscg
sssd	sssd-ad	sssd-client	sssd-common
sssd-common-pac	sssd-ipa	sssd-kcm	sssd-krb5
sssd-krb5-common	sssd-ldap	sssd-nfs-idmap	sssd-proxy
subscription-manager	subscription-manager-rhsm-certificates	sudo	sysstat
systemd	systemd-libs	systemd-pam	systemd-udev
systemtap-sdt-devel			

T

tar	tcl	teamd	timedatex
tmux	tomcat	tomcat-el-3.0-api	tomcat-jsp-2.3-api
tomcat-lib	tomcat-servlet-3.1-api	tpm2-abrmd	tpm2-abrmd-selinux
tpm2-tools	tpm2-tss	traceroute	trousers
trousers-lib	tsapi-client-linux	ttmkfdir	tuned
tzdata	tzdata-java		

U

unzip	usermode	util-linux	

V

volume_key-libs

W

wget	which		

X

xfsprogs	xkeyboard-config	xmlsec1	xmlsec1-openssl
xorg-x11-fonts-Type1	xorg-x11-font-utils	xz	xz-libs

Y

yum

Z

zip	zlib		

Appendix C: AE Services administrative user accounts

The root account

The Linux root account (or user name) has complete administrative authority of the Linux system. The root user has access to all files and commands on the Linux operating system. However, the root user cannot log in to the AE Services Management console.

Changing the password for the root account

About this task

After the service technician has provided you with the password for the root account, follow this procedure to change the password for the root account.

Procedure

1. Open an ssh session to AE Services.
2. As the root user, type `passwd root` and press the ENTER key.
3. At the prompt, type the new password you are assigning.

   The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 14 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.
4. Press the ENTER key.
5. At the prompt, type the new password again and press the ENTER key.

AE Services administrative roles and access privileges (role based access control - RBAC)

AE Services provides role-based access control (RBAC), which establishes the following roles for AE Services administrators (AE Services Management Console access and ssh access). The AE Services server uses the reserved Linux user ID range 500-599 and the reserved Linux group ID range 500-599 for the default AE Services server users and groups.

Role	Linux group	Linux group ID	AE Services Management Console access
System_Administrator	susers	555	Read and write access to the following menus: • AE Services • Communication Manager Interface • Licensing • Maintenance • Networking • Security (the System_Administrator does not have access to Account Management, PAM, and AIDE Properties) • Status • Utilities • Help **Note:** The System_Administrator role does not have access to User Management.
Security_Administrator	securityadmin	505	Read and write access to the following menus in the AE Services Management Console: • Security (the Security_Administrator does not have access to Enterprise Directory, Host AA, and Standard Reserved Ports) • Status • Help

Table continues…

Role	Linux group	Linux group ID	AE Services Management Console access
UserSvc_Admin	usrsvc_admin	508	Read and write access to the following menus: • User Management **Note:** To acquire the Administrative role for User Management, a user must have an administered account in User Admin (the local LDAP data store) with the Avaya role set to userservice.useradmin.
Auditor	users	100	Limited, read-only access to the following menus: • Security — access is limited to: - Audit - Certificate Management - Security Database > CTI Users • Status - Alarm Viewer - Logs -- access is limited to: • Audit Logs • Error Logs • Install Logs • User Management Service Logs • Status > Status and Control — access is limited to: - CVLAN Service Summary - DLG Service Summary - DMCC Service Summary - Switch Conn Summary - TSAPI Service Summary • Help

Table continues…

Role	Linux group	Linux group ID	AE Services Management Console access
Backup_Restore	backuprestore	507	Limited, read and write access to the following to the following menus: • Maintenance — access is limited to: - Server Data > Backup - Server Data > Restore • Help
Avaya_Maintenance	avayamaint	506	Limited, read and write access to the following menus in the AE Services Management Console: • Maintenance - Security Database - Service Controller - Server Data • Status - Logs • Utilities - Diagnostics • Help
EASG Administrator	easg	510	Read and write access of the EASG option on the PAM Password Manager.

Default accounts and AE Services Management Console access privileges

Security alert:

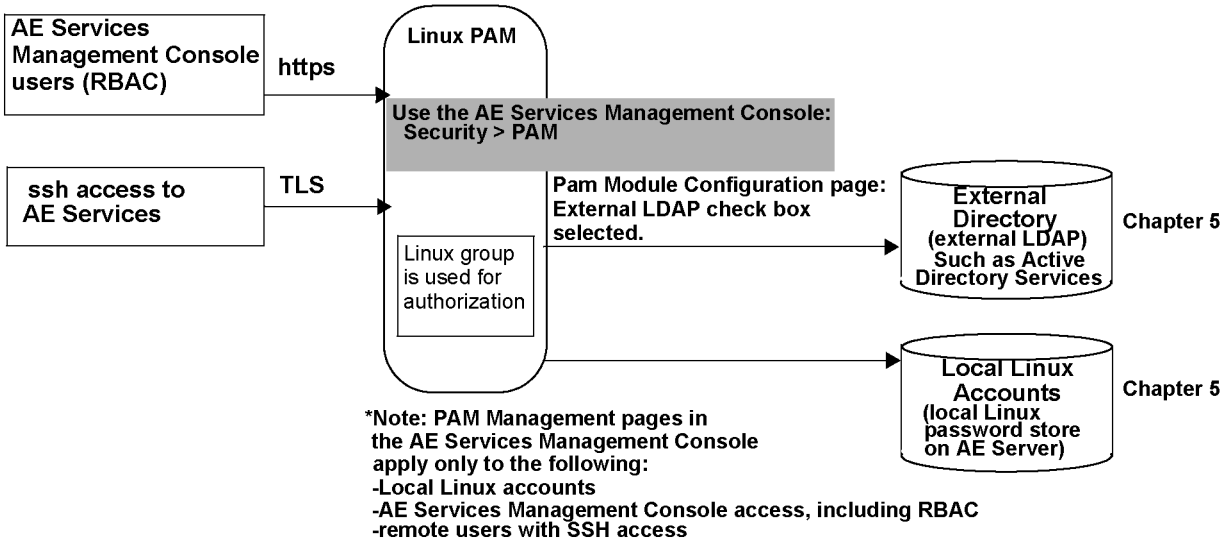
You must change the password for the **cust** account after initially using it.

Account name (log-in identifier)	Linux Group	AE Services Management Console access privileges
craft (Avaya services account) Available on: • AE Services Software - Only Server only if you enabled EASG at the time of installation. • AE Services using VMware® in the Virtualized Environment	susers securityadmin	Read and write access to the following menus: • AE Services • Communication Manager Interface • Licensing (you have access to this menu) • Maintenance • Networking • Security (AE Services sets up the craft account with access to Security) • Status • Utilities • User Management (AE Services sets up the craft account with access to Security) • Help
cust (customer account) Available on: • AE Services Software-Only Server • AE Services using VMware® in the Virtualized Environment	susers securityadmin usrsvc_admin easg datacontroller	Read and write access to the following menus: • AE Services • Communication Manager Interface • Licensing (you have access to this menu) • Maintenance • Networking • Security (AE Services sets up the cust account with access to Security) • Status • User Management (AE Services sets up the cust account with access to Security) • Utilities • Help
avaya (customer account) Available on: • AE Services Software-Only Server • AE Services using VMware® in the Virtualized Environment	Not applicable	Read and write access to the following menus: • User Management • Help • **Status** > **Logs** > **User Management Service**

Table continues…

Account name (log-in identifier)	Linux Group	AE Services Management Console access privileges
datacontroller (customer account) • AE Services Software-Only Server • AE Services using VMware® in the Virtualized Environment	datacontroller	Read and write access to the following menus: • Help • **Status** > **Log Manager**

Authenticating and authorizing administrators for AE Services Management Console and ssh access



Default AE Services accounts

Account name (log-in identifier)	Linux Group	Access privileges
craft Available on AE Services Software-Only Server only if you enabled EASG at the time of installation.	susers securityadmin	Intended for Avaya services technicians. Provides local or remote access to the Linux shell. • Local - Log in from a local console as craft, and then access the root account (**`su - sroot`**) • Remote - Log in from a remote console with a secure shell client (ssh), as craft, and then access the root account (**`su - sroot`**)
cust Available on AE Services Software-Only Server.	susers securityadmin usrsvc_admin easg datacontroller	Intended for customers. Provides local or remote access to the Linux shell. • Local - Log in from a local console as cust, and then access the root account (**`su - root`**) • Remote - Log in from a remote console with a secure shell client (ssh), as cust, and then access the root account (**`su - root`**)
avaya Available on AE Services Software-Only Server.	Not applicable	User Management administration only. You do not have access to any other administrative menus.
datacontroller Available on AE Services Software-Only Server.	datacontroller	Log and trace retention and clearing logs and traces only. You do not have access to any other administrative menus.

Accounts installed during the installation of AE Services server

The installation program sets up the AE Services server with avaya and cust accounts by default. It also adds service accounts, such as craft and sroot, for Avaya service technicians.

The cust account

The installation program sets up the AE Services server with the cust account by default.

Security alert:

The customer is responsible for changing the password for the cust account after initially using it. See Changing the default password for the cust account on local Linux on page 106 and Changing the default password for the cust account in User Management on page 106 for more information.

AE Services installs the cust account in two places: in the local Linux password store and in the local LDAP directory (User Management Service).

- The local User Management Service cust account provides access to all the User Management Service administrative tasks in the Application Enablement Services Management Console.
- The Linux cust account provides access to all other administrative tasks not available with the User Management Service cust account.

The craft account

When you enable EASG, the installation program sets up the AE Services server with the craft account by default. The craft account provides Avaya service technicians with read-write access to all administrative functions using either the Linux command line or the AE Services Management Console.

Adding a System Administrator account

Procedure

1. From the command line, log in as **root**.
2. Type `useradd -g susers -G securityadmin username` to add a user name that has System Administrator access privileges.

   Tip:

   The **useradd** and **adduser** commands are equivalent. You can use either command, and both commands accept the same arguments.
3. Type `passwd username` to display the password prompt.
4. At the password prompt, type a password, and press **Enter**.
5. At the prompt to re-enter your password, type the password you just created, and press **Enter**.
6. Log out.

7. From your web browser, log in to the AE Services Management Console with the new user name and password, as follows:
   a. In the address bar of your browser, type the fully qualified domain name or IP address of the AE Services server, for example `aeserver.example.com`.
   b. On the initial welcome screen, select **Continue to Login**.
   c. Complete the log in screen with the new user name and password, and click **Login**.

      Your browser displays the Application Enablement Services Management Console home page, and you have access to all operations in the AE Services Management Console.

Changing the default password for the User Management administrator (the avaya account)

About this task

By default, AE Services installs the avaya account for all installations. The avaya account provides you with administrative access to User Management. The default password for this account is set to avayapassword.

Procedure

1. Log in to the AE Services Management Console as avaya with the default password.
2. On the main menu, select **User Management** > **User Admin** > **List All Users**.
3. On the List All Users page, click **avaya**, and click **Edit**.
4. In the **New Password** field, enter a new password.

   The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.

   Note:

   If you want the avaya user to be able to access all administrative domains, the password for the avaya account must be identical to the password for the Linux user.
5. In the **Confirm New Password** field, re-enter the new password.
6. Click **Apply**.

Changing the password for the cust account on local Linux

About this task

Use this procedure to change the password for the cust account in local Linux. The local Linux cust account provides remote access to the Linux shell.

Note:

If you require a greater level of security for this account, see Creating a new User Management administrator account and removing the default cust account from User Management on page 107.

Procedure

1. Log in to the AE Services Management Console as a cust user.
2. On the main menu, click **Security** > **Account Management** > **Modify Login**.
3. On the Modify Login page, do the following:
   - In the **Login ID** field, type `cust`, and click **Continue**.
   - In the **Enter password** field, type a new password.

   The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 14 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.
4. In the **Re-enter password** field, type the new password again.
5. Click **Apply**.

Changing the password for the cust account in User Management

About this task

AE Services installs the cust account in two places: in the local Linux password store and in the User Management service (local LDAP directory). This topic describes changing the password for the cust account in User Management (the local LDAP directory). The User Management cust account provides access to the User Management features in the AE Services Management Console.

Note:

If you change the Linux cust account password, you do not have to change the User Management password. The next time you log in to the AE Services Management Console, the User Management password will automatically be changed to the new password. However, if you remove the Linux cust account password and create a new account, you must change the User Management password to match the new Linux cust account password. AE Services Management Console will not automatically update the User Management password when a new Linux cust account is created.

Note:

If you require a greater level of security for this account, see Creating a new User Management administrator account and removing the default cust account from User Management on page 107.

Procedure

1. Log in to the AE Services Management Console.).
2. From the main menu, select **User Management > User Admin > List All Users**.
3. From the List All Users page, select the option button for **cust** and click **Edit**.
4. In the Password field, enter a new password.

   The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.
5. In the Confirm Password field, re-enter the new password.
6. Click **Apply Changes**.

Creating a new User Management administrator account and removing the default cust account from User Management

About this task

If you do not want to use the User Management cust account, you can create a new User Management account that is equivalent to cust, and then remove the cust account from User Management.

Follow this procedure to create a new User Management account, with privileges equivalent to cust, and then remove the cust account from User Management.

Procedure

1. From your browser, log in to the AE Services Management Console as cust with the default password, custpw. See Logging into the Management Console on page 73.
2. From the main menu, select **User Management > User Admin > Add User**.
3. Complete the Add User page as follows:
   a. In the User Id field type a user name, for example `aesuseradmin`.
   b. In the Common Name field, enter the name the user prefers to use, for example `Jan Green`.
   c. In the Surname field, type the user's last name, for example `Green`.
   d. In the User Password field, type a password.

      The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.
   e. In the Confirm Password field, re-enter the password.
   f. In the Avaya Role field, select **userservice.useradmin**.
   g. Click **Apply**.

      Your browser displays the Add User Results page, indicating that the user was created successfully.
4. Log out of the AE Services Management Console (you are logging out as cust).
5. Log in to the AE Services Management Console again with the user name and password you created in Step 3 (aesuseradmin and the password for aesuseradmin).
6. From the main menu, select **User Management > User Admin > List All Users**.
7. From the List All Users page, select **cust**, and click **Delete**.
8. From the Delete User page, click **Delete**.

Creating a new User Management administrator account and removing the default avaya account from User Management

Procedure

1. From your browser, log in to the AE Services Management Console as avaya with the default password, avayapassword. See Logging into the Management Console on page 73.

2. From the main menu, select **User Management > User Admin > Add User**.
3. Complete the Add User page as follows:
   a. In the User Id field type a user name, for example `aesuseradmin`.
   b. In the Common Name field, type the name the user prefers to use, for example `Pat Adams`.
   c. In the Surname field, type the user's last name, for example `Adams`.
   d. In the User Password field, type a password.

      The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.
   e. In the Confirm Password field, re-enter the password.
   f. In the Avaya Role field, select **userservice.useradmin**.
   g. Click **Apply**.

      Your browser displays the Add User Results page, indicating that the user was created successfully.
4. Log out of the AE Services Management Console (you are logging out as avaya).
5. Log in to the AE Services Management Console again with the user name and password you created in Step 3 (`aesuseradmin`, based on this example).
6. From the main menu, select **User Management > User Admin > List All Users**.
7. From the List All Users page, select the option button next to **avaya**, and click **Delete**.
8. From the Delete User page, click **Delete**.

Creating a new Linux System Administrator account and removing the default Linux cust account

Procedure

1. From your browser, log in to the AE Services Management Console as cust with the default password, custpw. (See Logging into the Management Console on page 73.
2. From the main menu, select **Security > Account Management > Add Login**.
3. Complete the Add Login page as follows:

Note:

These settings assume that you want to set up the new system administrator with the same administrative roles that were set up for the cust account.

a. In the Login ID field, enter a new user name for the system administrator, for example `aesadmin`, and click **Continue**.

b. In the Default Login Group field, type `susers` (the susers Linux group maps to the System_Administrator role).

c. In the Additional Login Groups field, type `securityadmin` (the securityadmin Linux group maps to the Security_Administrator role).

(When completing the Default Login Group and Additional Login Groups fields, you must use the group names for RBAC assignments. See administrative roles and access privileges (role based access control - RBAC) on page 98.

d. In the Password authentication fields, enter a password and then re-enter the password to confirm it.

The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 14 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: pound (#), dollar ($), apostrophe (’), double quotes ("), backslash (\), space, and any ASCII control character.

e. In the remaining fields, either accept the defaults, or complete the fields according to your business requirements, and click **Apply**.

AE Services displays the Add Login page with a message indicating that the login was successfully created.

4. From the navigation bar, click **Logout** (you are logging out as cust)
5. Log in to the AE Services Management Console again with the new system administrator account (aesadmin, based on this example).
6. From the main menu, select **Security > Account Management > Remove Login**.
7. From the Remove Login page in the Login ID field, type `cust` and click **Continue**.
8. On the Remove Login page, verify that you are removing the appropriate login (cust), and click **Delete**.

AE Services removes the cust login and displays the Remove Login page with a message indicating that the login was successfully deleted.

Appendix D: Managing license entitlements from PLDS

Activating license entitlements

Before you begin

Obtain the Host ID of WebLM if you are activating license entitlements on a new license host.

About this task

Use License Activation Code (LAC) to activate one or more license entitlements from the available licenses. After successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification email message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification email message.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an email message.

   Note:

   If you do not have an email message with your LAC, see “Searching for entitlements” and make a note of the appropriate LAC from the LAC column.

   Note:

   The Quick Activation automatically activates all license entitlements on LAC. However, you can remove line items or specify the number of licenses to activate from the available licenses.
4. Enter the License Host information.

   You can create a new license host or use an existing license host.
5. Click **Next** to validate the registration detail.
6. Enter the License Host Information.

7. Type the number of licenses that you want to activate.
8. Review the Avaya License Agreement and accept the agreement.
9. Perform the following steps to send an activation notification email message:
    a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
    b. Enter the comments or special instructions in the **Comments** field.
    c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Searching for license entitlements

About this task

Use the functionality to search for an entitlement by using one or all of the following search criteria:

- Company name
- Group name
- Group ID
- License activation code

PLDS also provides other additional advanced search criteria for searching license entitlements.

Note:

Avaya associates or Avaya Partners can search license entitlements only by company name.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Assets** > **View Entitlements**.

   The system displays Search Entitlements page.

4. To search license entitlements by company name, type the company name in the **%Company: field**. To see a complete list of companies before you search for their corresponding entitlements, do the following:

   a. Click the search icon  .

   b. Type the name or several characters of the name and a wildcard (%) character.

   c. Click **Search Companies**.

   d. Select the company name from the list.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter `Av%`, the system searches for all the company names starting with the letter Av. You can enter a wildcard character at any position in the search criteria.

5. To search license entitlements by group name, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard character if you do not know the exact name of the group you are searching for. For example, if you enter `Gr%`, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character at any position in the search criteria.

6. To search license entitlements by LAC, enter the specific LAC in the **%LAC:** field.

   Tip:

   If you do not know the exact LAC that you want to search, use a wildcard character. For example, if you type `AS0%`, the system searches for all LACs starting with AS0. You can enter a wildcard character at any position in the search criteria.

   You will receive LACs in an e-mail if you have provided the email address in the sales order. If you do not have this code, search by using one of the other search criteria.

7. To search license entitlements by application, *product* or license status, select the appropriate application, product, and/or status from the field.

8. Click **Search Entitlements**.

Result

The system displays all corresponding entitlement records at the bottom of the page.

Moving activated license entitlements

Before you begin

Host ID or License Host name of the move from/to License Host.

About this task

Use this functionality to move activated license entitlements from one License Host to another. You can chose to move all or a specified quantity of license entitlements.

Note:

If you move a specified number of activated license entitlements from one host to another by using the Rehost/Move transaction in PLDS, two new license files are generated:

- One license file reduces the number of license entitlements on the License Host from which you are moving license entitlements.
- One license file increases the number of license entitlements on the License Host to which you are moving license entitlements.

Install each of these license files on the appropriate server.

If you move all activated license entitlements, only one license file is generated. Install this new license file on the License Host to which you are moving license entitlements. Remove the license file from the License Host from which you are moving all license entitlements.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Activation** > **Rehost/Move** from the Home page.
4. Click **View Activation Record information** to find and select licenses to rehost or move.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

   Note:

   If you are an Avaya associate or Avaya Partner, enter the search criteria and click **Search Activation Records**.
5. Select **Rehost/Move** for the License Host from which you are moving license entitlements.
6. In the **Search License Hosts** field, enter the License Host to which you are moving license entitlements.

   Alternatively, you can click **Add a License Host** to select an existing License Host.
7. Validate the Registration Detail, and click **Next**.
8. Enter the License Host Information.
9. Enter the number of Licenses to move in the **QTY column** field and click **Next**.

10. Accept the Avaya Legal Agreement.

    You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

11. Perform the following steps to send an activation notification email message:
    a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
    b. Enter the comments or special instructions in the **Comments** field.
    c. Click **Finish**.
12. Click **View Activation Record**.

- The **Overview** tab displays a summary of the license activation information.
- The **Ownership** tab displays the registration information.
- The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Regenerating a license file

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail, and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

9. Perform the following steps to send an activation notification email message:
   a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.

c. Click **Finish**.

10. Click **View Activation Record**.

- The **Overview** tab displays a summary of the license activation information.
- The **Ownership** tab displays the registration information.
- The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Appendix E: Enterprise-wide licensing

Overview of enterprise-wide licensing

Starting with Release 4.2, AE Services supports enterprise-wide licensing. With enterprise-wide licensing, AE Services customers are able to purchase any number of licenses and then allocate those licenses to various AE Services at their own discretion. This means that AE Services customers are able to pool or share all AE Services features and Rights To Use (RTU) among AE Services. This applies only to AE Services features licensed in the AE Services license file and not those licensed in the Communication Manager license file.

Note:

Enterprise-wide licensing is not supported in System Platform High Availability Failover configurations.

- To compare standard licensing with enterprise-wide licensing, see Comparison of standard licensing and enterprise-wide licensing on page 118.
- For examples of licensing configurations, see Licensing configuration examples on page 118.
- For the procedures required to set up an AE Services configuration that uses enterprise-wide licensing, see Setting up a configuration for allocating licenses on page 121.

Comparison of standard licensing and enterprise-wide licensing

Standard licensing	Enterprise-wide licensing
The standard license file continues to be used for standalone AE Services server licensing. A standard license is generated by the Product Licensing and Delivery System (PLDS) from the system record for an AE Services server.	Enterprise-wide licensing includes a master enterprise license file (ELF) and an allocation license file (ALF). • The master enterprise license file (ELF) is generated by the PLDS from the system record from the enterprise. The master license file can reside on an AE Services server or a dedicated WebLM server. • The allocation license file (ALF) is generated by WebLM based on features in the master license file and user allocations on the AE Services server. The ALF or ALFs can reside on one or more AE Services servers.
The standard license file is installed on the AE Services server. In a standard licensing arrangement, AE Services and the WebLM server are normally co-resident.	With enterprise wide licensing, the WebLM server does not have to be co-resident with AE Services, but each local WebLM server is normally co-resident with the AE Services server that it licenses.
With standard licensing, a license cannot be moved from one server to another, and capacities can not be reallocated.	With enterprise-wide licensing, you can reallocate enterprise capacities and features as desired.

Licensing configuration examples

To understand how licensing configurations work, this section provides a description of standard licensing and enterprise-wide licensing.

Standard licensing

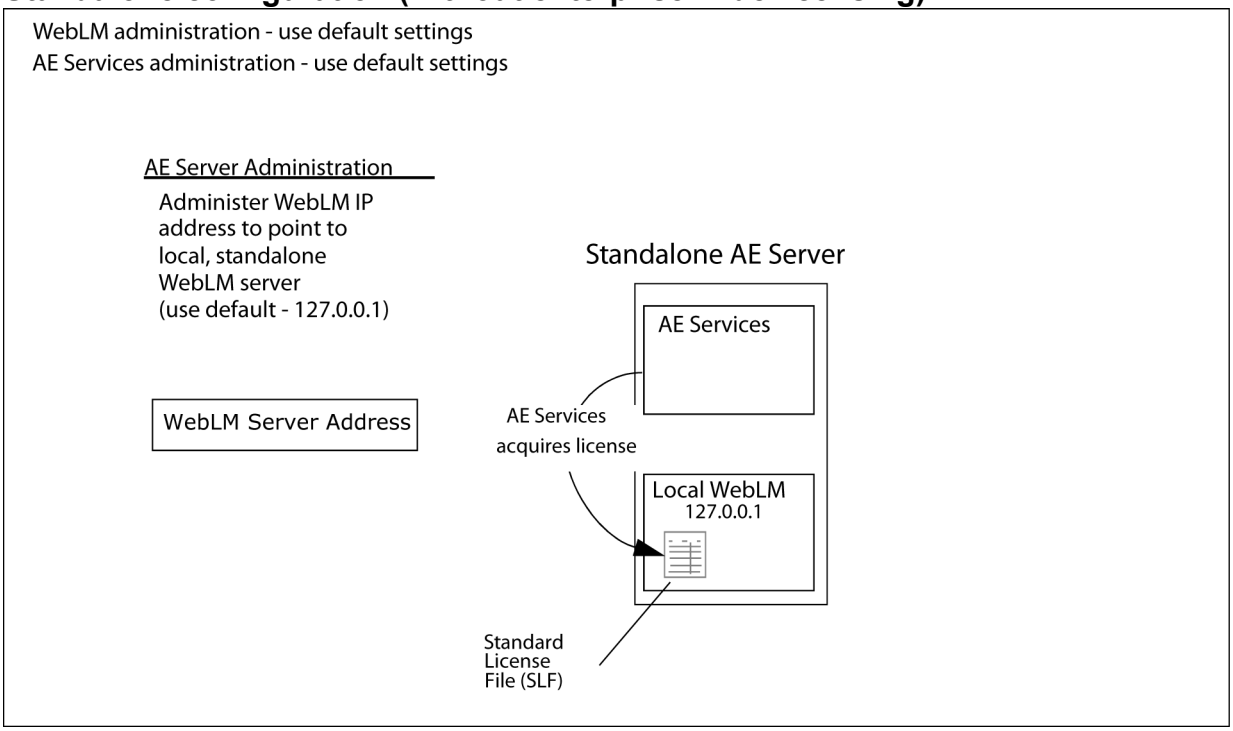
In a standard licensing configuration for Software-only offer, the standard license file (SLF) is installed on the AE Services server and is controlled by the WebLM server running on the AE Services server.

The following figure illustrates the standard licensing configuration.

Note:

If you use the standalone configuration, use the default settings on the WebLM Server Address page in the AE Services Management Console.

Standalone configuration (without enterprise-wide licensing)



Note:

The default IP address, 127.0.0.1, shown in the illustration above is for both, the AE Services Software-only offer and VMware offer.

Enterprise-wide licensing — allocating licenses or features

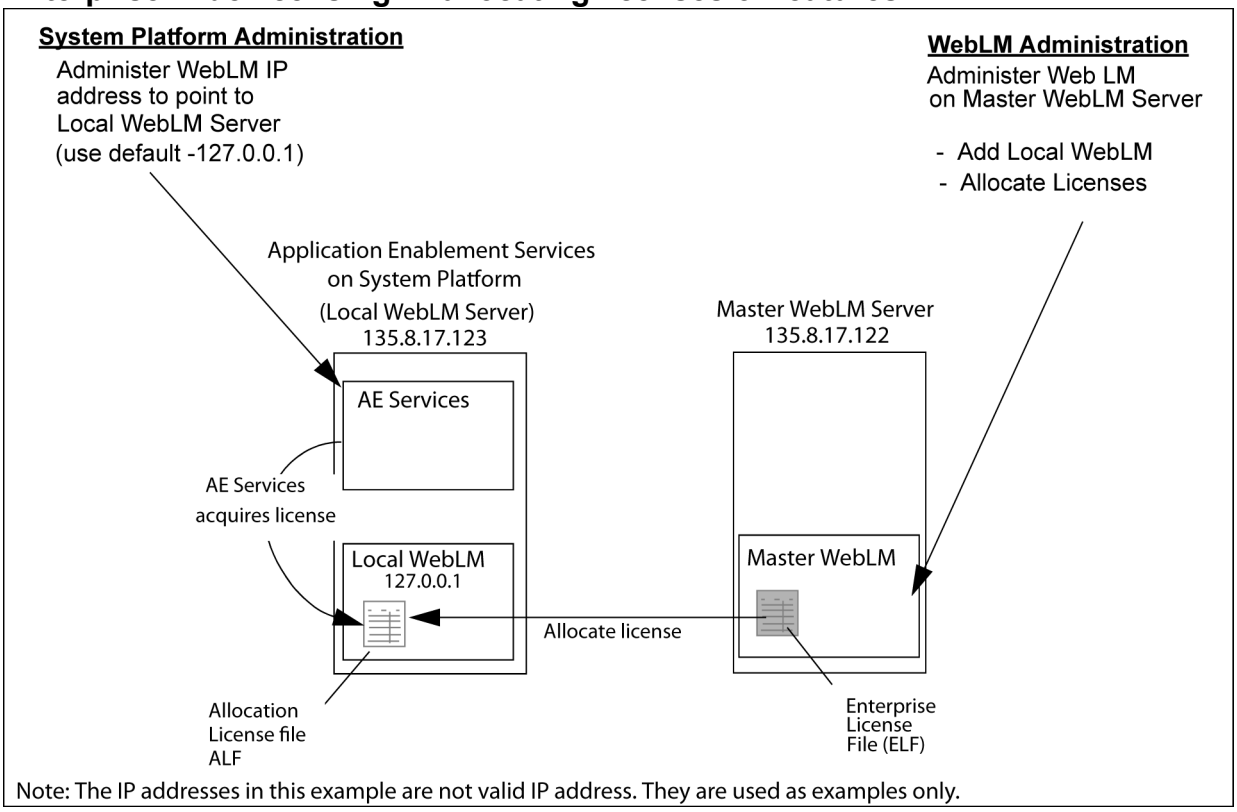
AE Services expanded its licensing capabilities to include enterprise-wide licensing. Enterprise-wide licensing provides the flexibility to move capacities and features from one AE Services server to another. With enterprise-wide licensing, you can move capacities or features from one server to another by using a master WebLM server to allocate license features to different AE Services servers.

Because this configuration relies on a master enterprise license file (ELF), which generates allocation license files (ALF), it is referred to as an ELF/ALF configuration. Each ALF will reside on an AE Services server with a Local WebLM Server. This is the recommended model for AE Services enterprise configurations. If you use the ELF/ALF model, you do not need to change the default settings on the WebLM Server Address page.

For this configuration you must use WebLM Administration to configure the master WebLM server so that it can allocate licenses to each local WebLM server on the AE Services servers. (In the WebLM Administration, select **Licensed Products** > **Application Enablement (CTI)** > **Configure Local WebLMs** > **Add Local WebLM**.)

The following figure illustrates an ELF/ALF configuration:

Enterprise-wide licensing — allocating licenses or features



Note:

Beginning with AE Services 7.0, System Platform is not supported.

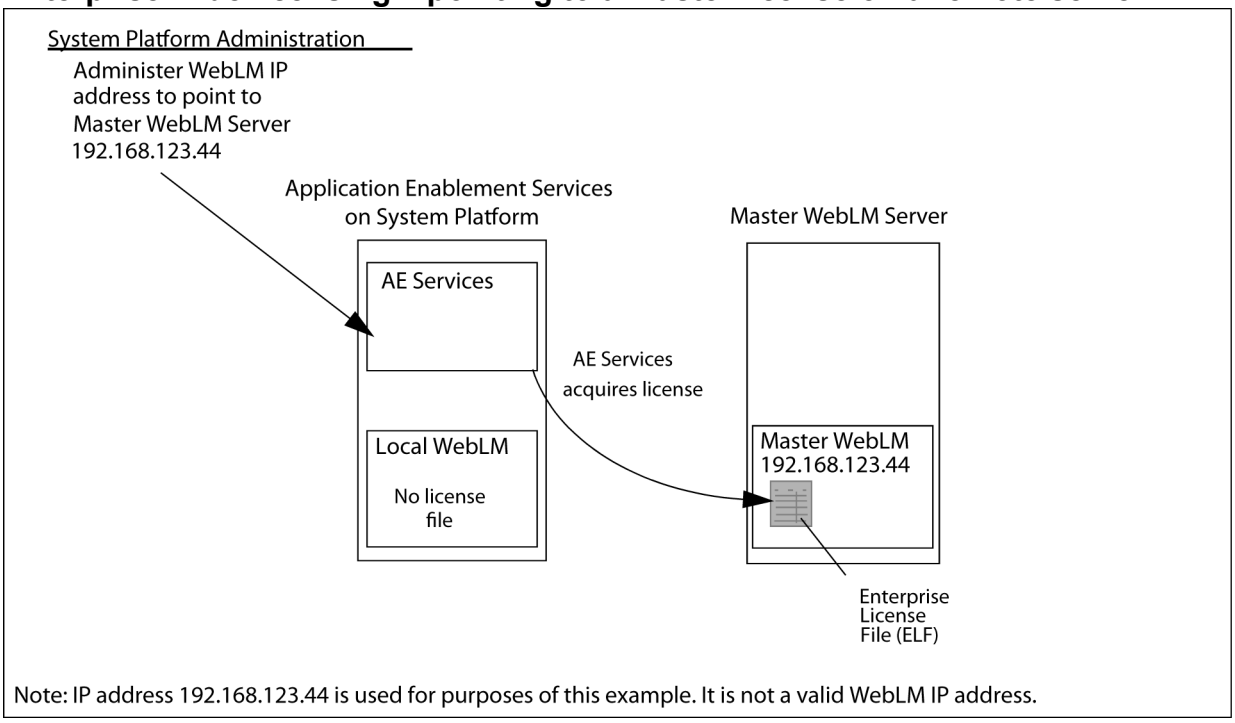
Enterprise-wide licensing — pointing to a master license on a remote server

Another type of enterprise licensing configuration is an enterprise license file (ELF)-only configuration. In an ELF-only configuration, the enterprise license file resides on a master WebLM server, and one or more AE Services servers point to the IP address of the master WebLM server. No allocation license files (ALFs) reside on AE Services servers.

If you use the ELF-only configuration, you must administer the WebLM Server Address page in the AE Services Management Console with the WebLM IP address and WebLM port number for the master WebLM server that hosts the ELF.

The following figure illustrates an ELF-only configuration.

Enterprise-wide licensing – pointing to a master license on a remote server



Note:

Beginning with AE Services 7.0, System Platform is not supported.

Caution:

Using the ELF-only configuration is not recommended because network latency and outages can affect the ability of the AE Services server to acquire licenses, and it creates a single point of failure for licensing.

Setting up a configuration for allocating licenses

About this task

Use the following procedures to set up a configuration for allocating licenses.

Installing the license file and configuring the master WebLM server

About this task

This procedure applies to a configuration where the master WebLM server allocates licenses to local AE Services servers (see Enterprise-wide licensing — allocating licenses or features on page 119). You will need to use this procedure to install the master enterprise license file (ELF) on the master WebLM server.

Follow these steps to install the enterprise license file (ELF) on the server that hosts the enterprise license file (ELF). For Software-only offer, this server can be an AE server or a computer dedicated to WebLM.

Procedure

1. Log in to the computer that has the license file stored on it.
2. From a web browser, type the fully qualified domain name or IP address of the AE Services server, for example `https://aserver.example.com`.

   In terms of this configuration example, the IP address would be 135.8.17.122.
3. Press **Enter**.
4. On the Application Enablement Services welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager Log on screen, enter your WebLM user name and password, and click the arrow.
6. On the WebLM main menu, click **Browse**.
7. Locate the license file and click **Open**.
8. Click **Install**.

   WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message: License file installed successfully. Notice that the WebLM main menu now displays Application_Enablement under Licensed Products.
9. From the WebLM main menu, select **Application_Enablement > Enterprise Configuration**.
10. Complete the Configure Enterprise page as follows:
    a. For the Master WebLM Configuration settings, which are required, accept the defaults.
       - Name: Master WebLM Server
       - Description: leave blank
       - IP Address: <IP address of the local c-dom>.
    b. For the Default Periodic Operation Settings settings, which are required, accept the defaults.
    c. For the SMTP Server Settings, which are optional, provide the name of the SMTP Server (Server Name), the user ID of the administrator (Admin Account), and the password of the administrator (Admin Password).

       These are the authentication settings for the SMTP server that sends email notifications for periodic operation failures.
    d. For the Email Notification Settings for Periodic Operation, complete the settings (Email Notification and Email Addresses) based on your operational requirements.

       By default, email notification is disabled (off).

e. For the Default Periodic License Allocation Schedule, select the day and time, based on your operational requirements.

f. For the Default Period Usage Query Schedule, select the day and time, based on your operational requirements.

g. Click **Submit**.

Next steps

Continue with Adding a local WebLM server on page 123.

Adding a local WebLM server

About this task

From the Master WebLM Server web page, follow this procedure to add a local WebLM server.

Note:

- You can allocate feature licenses only if the connection between the Master WebLM server and the local WebLM server is validated and established.
- The AE Services on VMware offer does not support a local WebLM.

Procedure

1. From the WebLM main menu, select **Application Enablement > Local WebLM Configuration > Add Local WebLM** .
2. Complete the Add Local WebLM page as follows:
   - Local WebLM Settings:
     - Name: the *<name of the local AE Services server>*, for example, lzbundled05. (Although this name is required, it can be any name you choose.)
     - Description: a descriptive term for the local AE Services server (optional)
     - IP Address for Software-only offer is *<IP address of the Local AE Services server>*. For purposes of this example, the IP address is 135.8.17.123.

       Note:

       The AE Services on VMware offer does not support a local WebLM.

     - Port: 8443 (the default)
   - Periodic License Allocation Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.
   - Periodic Usage Query Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.
3. Click **Configure and Validate**.

Next steps

Continue with Setting up the Local WebLM Server in your configuration on page 124.

Note:

Before you can uninstall an Enterprise-Wide License from the master WebLM, you must first de-allocate all of its licenses and delete all local WebLM servers associated with the license.

Setting up the Local WebLM Server in your configuration

About this task

Use the following procedure to change the default WebLM password and to verify the settings on the WebLM Server Address page in the AE Services Management Console.

Procedure

1. From a web browser, type the fully qualified domain name or IP address of the AE Services Server, for example `https://aserver.example.com`.

   In terms of this configuration example, the IP address would be 135.8.17.123.
2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.
4. From the Application Enablement Services Welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager log on screen, log in to WebLM with the default user name and password.

   The default user name is `admin`, and the default password is `weblmadmin`. The first time you log in to WebLM, the WebLM server displays the Change Password page.
6. On the Change Password page, complete the fields and click **Submit**.

   The password must contain 6 to 14 characters. White spaces are not permitted in the password, and the password itself must not be blank.
7. On the Web License Manager log on screen, log in as `admin` with the new password.
8. From the WebLM main menu, select **Logout** to log out of WebLM.
9. Log on to the AE Services server (local WebLM server) again.
10. From the AE Services Management Console main menu, select **Licensing > WebLM Server Address**.
11. Verify that the WebLM Server address page displays the following settings for Software-only offer:
    - WebLM IP Address: 127.0.0.1
    - WebLM Port: 443

Next steps

Continue with Changing the allocations of a license file on page 125.

Changing the allocations of a license file

About this task

Using the master Avaya WebLM server you can change license file allocations for your local Avaya WebLM servers. Use this procedure to change the license allocations using the Master Avaya WebLM server web page

Procedure

1. On the web browser, type the fully qualified domain name or IP address of the Application Enablement Services server, for example `https://aserver.example.com`.

   In terms of this configuration example, the IP address would be 135.8.17.123.
2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.
4. On the Application Enablement Services Welcome page, click **Licensing** > **WebLM Server Access**.
5. On the Web License Manager log in screen, enter your Avaya WebLM user name and password, and click **Log in**.
6. From the Avaya WebLM main menu, click **Application Enablement Services** > **Allocations**.
7. On the Allocations by Features page, click **Change Allocations**.
8. On the Change Allocations page, enter an appropriate value in the **New Allocation** field, and click **Submit Allocations**.

   For example, assume that you want to allocate 20 TSAPI Simultaneous User licenses to the local WebLM server, enter `20` in the **New Allocations** field, and click **Submit Allocations**.

Next steps

Continue with Verifying the license allocations on the Local WebLM Server on page 125.

Verifying the license allocations on the Local WebLM Server

About this task

Follow these steps to verify that the license allocations that you administered are in effect.

Procedure

1. From a web browser, type the fully qualified domain name or IP address of the AE Server, for example `https://aserver.example.com`.

   In terms of this configuration example, the IP address would be 135.8.17.123.
2. Press **Enter**.
3. At the Security Alert, click **Yes** to accept the SSL certificate.

4. From the Application Enablement Services Welcome page, click **Licensing > WebLM Server Access**.
5. On the Web License Manager log on screen, enter your WebLM user name and password, and click the arrow.
6. From the WebLM main menu, select **Licensed Products > Application Enablement**.
7. Verify that the licensed features on the local WebLM server are consistent with the settings you administered on the master WebLM server.

Note:

The Allocation license is valid for up to 30 days. The master WebLM will push the ALF to the local WebLM based on the administered schedule (Periodic License Allocation Schedule).

Appendix F: Setting up the AE Services server for remote access

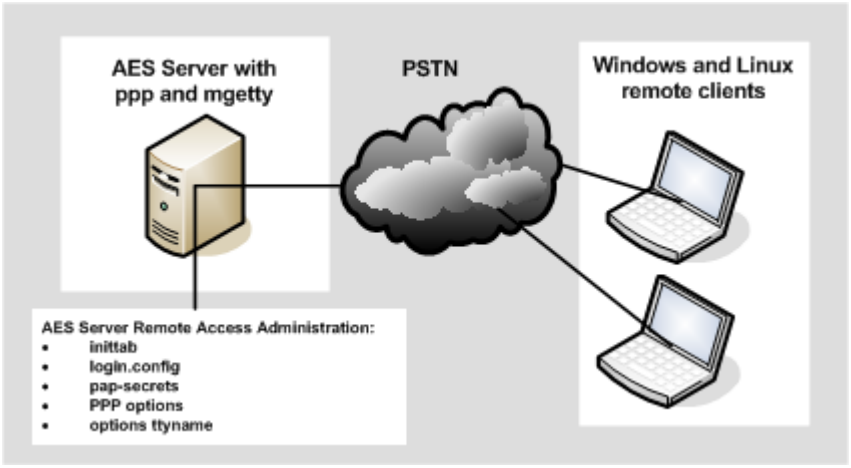
AE Services server remote access configuration

Avaya technical support (Services) personnel must have remote access to the AE Services server to perform administration and maintenance tasks.

Note:

The information in this appendix applies only to customers who have an Avaya maintenance or service contract for their AE Services server.

The following figure illustrates a remote access setup.



AE Services Software-Only server requirements for remote access

- A Software-Only server with the default Linux® Operating System software components already installed. In addition to the default software components, you must install the following packages:
  - The Linux ppp package

- The Linux mgetty package .

- A modem that supports Linux® Operating System.

Configuring the AE Services server for remote access

Procedure

1. From a text editor such as vi or emacs, open the /etc/inittab file.
2. Add one line for each modem you plan to use.

   For example, enter `S0:2345:respawn:/sbin/mgetty -D ttyS0` where `-D` is the parameter for a data modem and `ttySO` is the device identifier.

   The device identifier value varies according to your hardware. For example, ttyS0 is associated with COM1 and ttyS1 is associated with COM2.

   Note:

   ttyS0 identifies a serial modem. Modify these instructions as required if you are using a different type of modem.
3. Save your changes.
4. Open the /etc/mgetty+sendfax/login.config file.
5. Remove the # sign from the AutoPPP line to uncomment it.
6. Edit the line to include a reference to the options file by specifying **`file /etc/ppp/options`**. For example: `/AutoPPP/ - a_ppp /usr/sbin/pppd file /etc/ppp/options`.
7. Save your changes.
8. Open the /etc/ppp/pap-secrets file to set up Password Authentication Protocol (PAP) authentication:
9. Edit the file so it consists of one line containing the following characters: * * “ ” * For example:

```
# Secrets for authentication using PAP
# client        server       secret       IP address
      *                     *                   ""                          *
```

   These settings enable any registered user to log in. Alternatively, you could specify user names, passwords, and IP addresses.
10. Save your changes.
11. Open the appropriate options file for your modem.

For example, if your modem is connected to ttys0, open the /etc/ppp/options.ttyS0 file. Include a *<serverIP>:<clientIP>* entry for each tty. You must separate the server IP address and the client IP address with a colon.

The default *<serverIP>*:*<clientIP>* entry for each tty is **192.168.25.10:192.168.25.20** where **192.168.25.10** is the server IP and **192.168.25.20** is the client IP.

12. Save your changes.
13. Open the /etc/ppp/options file. Verify that the client PPP supports the options listed in the following table. Edit the file, if necessary, and save your changes.

lock	**Creates a lock file that has exclusive access to a specific device.**
-detach	Prohibits the pppd process from forking and becoming a background process. This happens when a serial device is specified.
modem	Sets up the server to use modem control lines. The client waits for a signal from the modem before opening a serial device (default behavior). You can change this handshake if necessary.
crtscts	Specifies hardware flow control.
proxyarp	Let the client appear as if it is on the same LAN as its peers.
asyncmap 0	Prohibits the pppd process from setting up and using escape control sequences.

Recommendations for setting up a Linux client to dial in to the AE Services server

To establish a PPP connection to the AE Services server from a Linux client, use either the GNOME or KDE Dialer. The specific procedure varies depending on the version of Linux you are using.

Setting up a Microsoft Windows client to dial in to the AE Services server

About this task

Use this procedure to configure a dial-up connection in Windows XP.

To establish a PPP connection to the AE Services server from a Microsoft Windows client, use the network connections setup appropriate for your version of Windows.

Procedure

1. Click **Start > Control Panel > Network Connections**.

2. Click **Create a connection to the network at your office**.
3. In the Location Information dialog box, enter the appropriate information, and then click **OK**.
4. Click **OK** to close the Phone and Modem Options dialog box and start the New Connection wizard.
5. In the New Connection Wizard, click **Dial-up connection**, and then click **Next**.
6. When you are done, click **Finish**.
7. Open a newly created connection and click **Properties**
8. On the **Properties** window, click **Security**
9. Select **Show terminal windows** and click **OK** to complete the wizard.

PPP connections checklist

Use this checklist to set up PPP connections.

Item	✔
You must administer a login and password on the AE Services server for the client connection. By default, no login and password are administered to support remote access	
You must administer an IP address for the client connection. The default Client IP address is 192.168.25.20.	

Appendix G: Configuring an LDAP server for User Management

About this task

To use your existing Lightweight Directory Access Protocol (LDAP) directory with AE Services, you need to configure your LDAP implementation for compatibility with AE Services User Management. After installing AE Services server, if you face any discrepancy with LDAP, configure the LDAP server.

Before you begin

- Ensure that you have installed AE Services server software.

  Note:

  - AE Services server software installs the cs-cusldap and cs-userservice packages. To verify whether the packages are installed, run **`rpm -q 'cs-userservice|cs-cusldap'`** command.
  - Back up the files on your system.
- Ensure that your LDAP implementation is an OPEN LDAP of version 2.1.22-28.
- If your security policy doesn't allow multiple users with ID equals to zero, modify the user ID for sroot to an unused ID using the command **`usermod -u new_UID sroot`**.

Procedure

1. Restore `/etc/ldap.conf` file from the backup.
2. Merge `/etc/sssd/sssd.conf` file with your modified `sssd.conf` file.
3. Restart sssd service using the command **`service sssd restart`**.
4. Restart sshd service using the command **`service sshd restart`**.
5. Add admin user to the following groups: securityadmin, usrsvc_admin and susers.
6. Run the following command to access sudo commands and web interface for an LDAP user:

   ```
   usermod -a -G securityadmin,usrsvc_admin,susers admin_username
   ```
7. If required, add root shell permission for cust and sroot user types to `/etc/sudoers`.
8. Reboot the server.

Related links

Configuring the LDAP server on page 132

Configuring the LDAP server

About this task

Use this procedure to manually configure your LDAP server for User Management.

Procedure

1. Copy the mvapus schema file named `mvapus.schema` from `/var/mvap/config/cus` to the LDAP schema directory at `/etc/openldap/schema`.
2. Edit the `core.schema` file at `/etc/openldap/schema/` as follows:
   a. Locate the **userid** attribute specification section.
   b. Type `ORDERING caseIgnoreOrderingMatch` after the line **EQUALITY caseIgnoreMatch**.
   c. Save the schema file.
3. Edit the `slapd.conf` file at `/etc/openldap/` as follows:
   a. Type the following include statement to the already existing set of \include statements: include `/etc/openldap/schema/mvapus.schema`
   b. Note the suffix value used in the current `slapd.conf` file.
   c. Save and close the `slapd.conf` file.
4. Modify the `init.ldif` file to match the chosen **organizationalUnit** for the \users and the existing suffix used by the enterprise as follows:
   a. Delete the first entry in the `init.ldif` file.
   b. Update the second entry to reflect the desired **organizationalUnit**.

      For example, ou=users
   c. Update the **DN** attribute of the next two entries to reflect the chosen **organizationalUnit** and suffix in use in the enterprise.
   d. Save and close the `init.ldif` file.
5. Restart the LDAP server.
6. Use the ldapadd tool or equivalent to add the entries in the `ldif.init` file into the LDAP server.

   For example, `ldapadd -x -D` *`bind credentials DN`* `-W -f init.ldif`

Related links

Configuring an LDAP server for User Management on page 131

Appendix H: Configuring PuTTY

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

Before you begin

Download the PuTTYGen software.

Procedure

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

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

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

Configuring PuTTY for an SSH session

Before you begin

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

Procedure

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

Signing in to the Amazon EC2 virtual server instance

Before you begin

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

Procedure

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

Identifying the SSH user name of the RHEL instance on AWS

About this task

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

Before you begin

Create RHEL instance on Amazon Web Services.

Procedure

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

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

Appendix I: Creating RHEL virtual machine on Nutanix

Uploading the RHEL ISO to Nutanix server

About this task

You can install RHEL on Nutanix 6.5 and later, after uploading the standard RHEL ISO image on the Nutanix server.

Note:

The RHEL ISO must be customer-provided. Avaya is not responsible for the RHEL ISO image.

Procedure

1. Log in to Nutanix server using Nutanix Prism web console.
2. Navigate to **Home** > **Settings** > **Image Configuration**.
3. In the **Image Configuration** screen, click **Upload Image**.

   Nutanix Prism web console displays the **Create Image** window.
4. In the **Name** field, enter a name for the image.
5. In the **Image Type** field, select the ISO image to upload.
6. In the **Storage Container** field, select the required option.
7. Under **Image Source** field, either browse for the ISO image through URL or upload the image file if stored in your local machine.
8. Click **Save**.

   You can view the image upload status from the drop-down list on top of the **Home** page.

Next steps

Installing RHEL on Nutanix 6.5 and later.

Installing RHEL on the Nutanix server

Before you begin

- Upload the RHEL image on Nutanix 6.5 and later.
- Log in to Nutanix 6.5 server using the Nutanix Prism web console.

Procedure

1. Navigate to **Home** > **VM**.
2. In the **VM** page, click **Create VM**.
3. In the **Create VM** window under **General Configurations**, enter appropriate values in the **Name**, **Description**, and **Timezone** fields.
4. In the **vCPUs** field under **Compute Details**, enter the number of CPUs required for the application.

   For more information about the required CPU, see footprint profile on page 22.
5. In the **Number of Cores per vCPU** field, enter the required value.
6. In the **Memory** field, enter appropriate memory in GiB.

   For more information about the required resources, see footprint profile on page 22.
7. Under **Boot Configuration**, select **UEFI**.
8. Under **Disks**, click the Edit icon for the CD-ROM disk type, and do the following:
   a. In the **Type** field, ensure **CD-ROM** is displayed.
   b. In the **Operation** field, select **Clone from Image Service**.
   c. In the **Bus Type** field, Avaya recommends selecting **IDE**.
   d. In the **Image** field, select the RHEL ISO Image.
   e. Click **Update**.

   The CD-ROM and the disk size are displayed.

   AE Services requires 56 GiB of hard disk. For more information, see footprint profile on page 22
9. Click **Add New Disk** next to **Disks**, and do the following:
   a. In the **Type** field, select Disk.
   b. In the **Operations** field, select **Allocate on Storage Container**.
   c. In the **Bus Type** field, select the same bus type which you selected while updating the disk.
   d. In the **Storage Container** field, select the appropriate storage container.
   e. In the **Size** field, enter the required GiB size.
   f. Click **Add**.

10. Under **Network Adapters (NIC)**, do the following:
    a. Click **Add New NIC** to add a Network Interface Card (NIC).
    b. In the **Create NIC** window, select the **Subnet Name**.
    c. In the **Network Connection State** field, select **Connected**.
    d. Click **Add**.
    e. To add multiple NICs, repeat 10.a to 10.d.
11. Under **VM Host Affinity**, click **Set Affinity** and do the following:
    a. In the **Set VM Host Affinity** window, select the hosts.

       Select multiple hosts to ensure one node (virtual machine) runs in case another node fails.
    b. Click **Save**.

    After the successful creation of virtual machine, virtual machine appears in the VM page.
12. Select the newly created VM and click **Power On**.
13. Click **Launch Console**.

    Note:

    The **Launch Console** button is enabled only when the virtual machine is Powered On.

    After the RHEL boots, Red Hat Enterprise Linux 8.10 welcome screen appears.
14. Click **Continue**.
15. In the **Installation Summary** screen, under **LOCALIZATION**, click **Language Support** to select the supported language.
16. Click **Time & Date** to set the required timezone.
17. Under **SOFTWARE**, click **Software Selection**.
18. Select **Minimal Install** and then click **Done**.
19. Under **SYSTEM**, click **Installation Destination** and do the following:
    a. Under **Storage Configuration**, select the **Custom** radio button and click **Done**.
    b. In the **Manual Partitioning** window, set the partitioning as required.

       For information on disk partitions and size, see Disk Partitioning on page 27.
    c. Click the **+** icon to create a new mount point.
    d. Select the available partition from the **Mount Point** drop-down menu. To add custom partitions, type the required partition name. For eg:`/etc/opt/defty`.
    e. Enter the capacity in GiB in the **Desired Capacity** field and then click **Add Mount Point**.
    f. In the **Manual Partitioning** window, click **Done**.

g. In the **Summary of Changes** window, click **Accept Changes**.

h. Click **Done**.

20. Click **Network & Host Name** and do the following:

    a. Enter a name in the **Host Name** field and click **Apply**.

    b. To configure the IP, click **Configure**.

    c. Click **IPV4 Settings** and select the required option from the **Method** drop-down menu.

    d. Click **Done**.

21. Under **USER SETTINGS**, click **Root Password**.

    In the **Root Password** window, set a password for the root user and then click **Done**.

22. Click **User Creation** and in the Create User window, enter the details and click **Done**.

23. Click **Begin Installation**.

    The RHEL virtual machine is installed on the Nutanix 6.5 server and later.

24. Click **Reboot System** to reboot the RHEL virtual machine.

Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W