Deploying Avaya Aura® Application Enablement Services in Virtualized Environment

Release 10.2.x
Issue 7
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 6
Purpose 6
Change history 6
Chapter 2: Overview 8
Virtualized Environment overview 8
Virtualized Environment components for VMware 8
Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) 9
Chapter 3: Planning and preconfiguration 10
Planning checklist for VMware® 10
Planning checklist for ASP R6.0.x (KVM on RHEL 8.10) 10
Deployment guidelines 11
Downloading software from PLDS 12
Customer configuration data 13
AE Services resource requirements and the supported footprints on VMware 14
AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10) 15
Configuration tools and utilities 16
Software details of Application Enablement Services 16
Supported hardware for VMware 17
Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) 17
Supported ESXi version 17
Supported ASP R6.0.x (KVM on RHEL 8.10) version 18
Software requirements 19
Communication Manager and media server requirements 20
Downloading AE Services OVA 20
Registering for PLDS 20
Downloading software from PLDS 20
Verifying the downloaded OVA 22
Network requirements 23
Network interfaces for the server 23
Network latency requirements 25
AE Services security guidelines 26
SAL Gateway 26
Chapter 4: Deploying Application Enablement Services on VMware® 27
Deploying Application Enablement Services on vCenter by using vSphere Client (HTML5) 27
Deploying the application OVA by accessing the ESXi host directly 29
Deploying the AE Services OVA file by using Solution Deployment Manager 31
Application Deployment field descriptions 33
Cloned and copied OVAs are not supported 37

Changing the Virtual Machine properties for the Virtualized Environment 37
Chapter 5: Deploying Application Enablement Services on ASP R6.0.x (KVM on RHEL 8.10) 38
Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit 38
Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using Script 42
Updating the CPU resources for KVM Cockpit 46
Chapter 6: Configuring 48
Configuration checklist 48
Starting the Application Enablement Services virtual machine using vSphere Web client 48
Configuring the virtual machine automatic startup settings on VMware 49
Configuring the network settings in a deployment 49
Out of Band Management 50
Changing the time zone setting 52
Logging on to the AE Services Management web console 52
Virtualized Environment footprint flexibility 53
Configuring hardware resources to support AE Services footprint flexibility 53
Chapter 7: AE Services Licensing 55
AE Services licensing 55
Application Enablement Services license requirements 55
Licensing overview 55
Embedded Avaya WebLM server 55
HTTPS, WebLM, and AE Services 56
Connecting to Avaya WebLM server 57
Logging in to WebLM and creating a WebLM password 58
Installing the AE Services license 59
Restarting AE Services from the Linux command line 60
Restarting AE Services from the AE Services Management web console 60
Troubleshooting licensing error messages 61
Obtaining the AE Services license file 61
Identifying the Host ID using WebLM 61
Uninstalling the AE Services license 62
Chapter 8: Post-installation and verification 63
Verifying the software version 63
Verifying the license 63
Verifying the AE Service IP (Local IP) settings 63
Verifying the Network Configuration settings 64
Verifying the time zone and NTP server settings 64
Editing the NIC configuration 64
Chapter 9: Resources 66
Application Enablement Services documentation 66
Finding documents on the Avaya Support website 67
Accessing the port matrix document 67
Avaya Documentation Center navigation 68

Training ... 69
Viewing Avaya Mentor videos ... 70
Support ... 70
Using the Avaya InSite Knowledge Base ... 71
Appendix A: AE Services administrative user accounts ... 72
The root account ... 72
Changing the password for the root account ... 72
AE Services administrative roles and access privileges (role based access control - RBAC) ... 73
Default accounts and AE Services Management Console access privileges ... 75
Default AE Services accounts ... 77
Modifying reservations on Application Enablement Services ... 78
Appendix B: Managing license entitlements from PLDS ... 80
Activating license entitlements ... 80
Searching for license entitlements ... 81
Moving activated license entitlements ... 83
Regenerating a license file ... 84
Appendix C: Best Practices for VMware performance and features ... 86
BIOS ... 86
Intel Virtualization Technology ... 87
Dell PowerEdge Server ... 87
VMware Tools ... 88
Timekeeping ... 88
VMware networking best practices ... 89
Storage ... 92
Thin vs. thick deployments ... 93
Best Practices for VMware features ... 93
VMware snapshots ... 93
Cloned and copied OVAs are not supported ... 95
VMware High Availability ... 95
VMware vMotion ... 95
VMware features supported by Avaya Aura® ... 96
Appendix D: PCN and PSN notifications ... 99
PCN and PSN notifications ... 99
Viewing PCNs and PSNs ... 99
Signing up for PCNs and PSNs ... 100

Chapter 1: Introduction

Purpose

This document provides procedures for deploying:

- Avaya Aura® Application Enablement Services application on VMware® in a customer-provided Virtualized Environment and Avaya Solutions Platform 130 (Dell PowerEdge R640) in a Avaya-Supplied VMware ESXi 7.0. It includes installation, configuration, installation verification, troubleshooting, and basic maintenance checklists and procedures.
- Avaya Aura® Application Enablement Services application on Kernel-Based Virtual Machine (KVM) Avaya Solution Platform 130 (Dell Power Edge R640, R660xs) in the Avaya-Supplied KVM on Red Hat Enterprise Linux (RHEL) R8.10 or Avaya Solution Platform S8300 in the Avaya-supplied KVM on RHEL R8.10.

The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers themselves. This document does not include optional or customized aspects of a configuration.

Change history

Issue	Date	Summary of changes
7	March 2026	Updated the following sections: • Purpose on page 6 • Virtualized Environment overview on page 8 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 18 • Software requirements on page 19
6	September 2025	Updated the following section: • Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 42

Table continues…

Issue	Date	Summary of changes
5	April 2025	Updated the following sections: • Supported ESXi version on page 17 • Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 42
4	December 2024	Added the Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 42
3	December 2024	Added the following sections for Release 10.2.1: • Planning checklist for KVM • Supported hardware for KVM • Supported KVM version • Supported ESXi version • Supported footprints of AE Services OVA on KVM • Deploying Avaya Aura® Application Enablement Services using KVM Cockpit • Updating the CPU resources for KVM Cockpit Updated the following sections for Release 10.2.1: • Purpose • Virtualized Environment overview • Virtualized Environment components • Software requirements
2	March 2024	Updated VMware features supported by Avaya Aura on page 96 section.
1	December 2023	Release 10.2

Chapter 2: Overview

Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.2.x applications in one of the following Virtualized Environments:

- Avaya Solutions Platform 130 Release 5.1 (Dell PowerEdge R640) is a single host server with a preinstalled ESXi 7.0 Standard VMware License.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- VMware in a customer-provided Virtualized Environment.

Note:

For more information about deploying applications, see the product-specific Software-Only and Infrastructure as a Service guide.

Virtualized Environment components for VMware

Virtualized component	Description
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.
Customer-provided VMware or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0)	
ESXi	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
ESXi Embedded Host Client	The ESXi Embedded Host Client is a native HTML and JavaScript application and is served directly from the ESXi host.
vSphere Client (HTML5)	Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.

Table continues…

Virtualized component	Description
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion. This is not applicable for Avaya Solutions Platform 130.

Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10)

Virtualized component	Description
Avaya Solutions Platform 130 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 (Avaya-Supplied KVM on RHEL R8.10).	
KVM Cockpit	Cockpit is a system administration tool that provides a user interface to monitor and administer servers through a web browser. Cockpit administrators can create and manage KVM-based virtual machines on the host system.

Chapter 3: Planning and preconfiguration

Planning checklist for VMware®

Perform the following procedures before deploying the Application Enablement Services OVA.

#	Action	Link/Notes	✔
1	Gather customer configuration data.	See Customer configuration data on page 13.	
2	Identify configuration tools and utilities.	See Required tools for installation on page 16.	
3	Register for PLDS.	See Registering for PLDS on page 20.	
4	Download the software from PLDS.	See Downloading the software from PLDS on page 12.	
5	Verify the downloaded OVA.	If you are using a Linux-based computer, see Verifying the OVA on a Linux-based computer on page 22. If you are using a Windows-based computer, see Verifying the OVA on a Windows-based computer on page 22.	
6	Download the Avaya Aura® Release 10.2.x release notes.	See Downloading the release notes on page 22.	

Planning checklist for ASP R6.0.x (KVM on RHEL 8.10)

Perform the following procedures before deploying the Application Enablement Services OVA.

#	Action	Link/Notes	✔
1	Gather customer configuration data.	See Customer configuration data on page 13.	
2	Identify configuration tools and utilities.	See Required tools for installation on page 16.	

Table continues…

#	Action	Link/Notes	✔
3	Register for PLDS.	See Registering for PLDS on page 20.	
4	Download the software from PLDS.	See Downloading the software from PLDS on page 12.	
5	Verify the downloaded OVA.	If you are using a Linux-based computer, see Verifying the OVA on a Linux-based computer on page 22. If you are using a Windows-based computer, see Verifying the OVA on a Windows-based computer on page 22.	
6	Download the Avaya Aura® Release 10.1.x release notes.	See Downloading the release notes on page 22.	

Note:

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL images for a virtualized environment.

With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Deployment guidelines

- Deploy maximum number of virtualized environments on the same host.
- Deploy the virtualized environment on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not oversubscribe network resources, oversubscribing affects performance. To ensure consistent and predictable behavior, latency-sensitive traffic such as A1, B1, A2, and B2 must be strictly isolated from any contention-prone VMs shared on the same host. Implement hard isolation mechanisms and enforce guaranteed minimum bandwidth, along with traffic prioritization to protect these flows from performance impact.
- Monitor the server, host, and virtualized environment performance.

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.

Customer configuration data

The following table identifies the key customer configuration information required during the deployment and configuration process for Application Enablement Services:

Required data for Application Enablement Services	Example value
Hostname or fully qualified domain name for the Application Enablement Services virtual machine.	aesserver1
DNS search path. **Note:** If you leave this value blank, you must modify or add `search` *<dns search path>* in the file `etc/resolv.conf` after you deploy the Application Enablement Services virtual machine successfully.	example.com
Default gateway address of the Application Enablement Services virtual machine.	123.45.67.254
Domain name servers for the Application Enablement Services virtual machine.	123.45.1.2
IP address of the Application Enablement Services virtual machine interface for eth0, the public interface.	123.45.67.89
Netmask or prefix for the Application Enablement Services virtual machine interface for eth0 (Public interface).	255.255.255.0
IP address of the Application Enablement Services virtual machine interface for eth1 (Private interface).	123.45.67.90
Enter the Netmask or prefix for the Application Enablement Services virtual machine interface for eth1 (Private interface).	255.255.255.0
IP address of the Application Enablement Services virtual machine interface for eth2 (Out of Band Management interface).	
Netmask or prefix for the Application Enablement Services virtual machine interface for eth2 (Out of Band Management interface).	
Network Time Protocol (NTP) hostname or IP address.	

Note:

- DHCP is activated only after you configure it from the command line after initial deployment.
- DHCP does not start when you start Application Enablement Services for the first time.
- Avaya recommends that you should not use DHCP with Application Enablement Services.

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.

- OVA: VMware or Avaya Solutions Platform

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

AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10)

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 KVM hosts with Hyperthreading enabled at the BIOS level.

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

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 = 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

Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring the application:

- 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*.

- USB keyboard, USB mouse, video monitor, and cables or laptop computer with Ethernet crossover cable.
- An SFTP client for Windows, for example WinSCP.
- An SSH client, for example, PuTTY and PuTTYgen.

Software details of Application Enablement Services

For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at https://support.avaya.com/.

Supported hardware for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see the Broadcom website (formerly VMware).

Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x and Avaya Solutions Platform S8300 Release 6.0.x.

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

Note:

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

  Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).

- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

Supported ASP R6.0.x (KVM on RHEL 8.10) version

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Y	Y

Note:

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell R660xs or Dell R640. The Dell R660xs only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.
- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660xs server only supports KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.

- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660xs, S8300E) is a single host server with preinstalled KVM on RHEL R8.10 software.
- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Solutions Platform 130 (Avaya-supplied KVM on RHEL 8.10): Dell PowerEdge R660xs or R640.
- Avaya Solutions Platform S8300 (Avaya-supplied KVM on RHEL 8.10): S8300E.

  Note:

  Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 7.0 or 8.0
  - VMware® vCenter Server 7.0 or 8.0

  To view compatibility with other solution releases, see Broadcom website (formerly VMware) and search for VMware Product Interoperability Matrix.
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.

Note:

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
- Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
- Avaya Aura® Release 8.1.x and later supports ASP R6.0.x (KVM on RHEL 8.10) hypervisor.

  For more information about upgrading from RHEL 8.4 to RHEL 8.10, see *Upgrading Avaya Aura® Application Enablement Services*

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.

Downloading AE Services OVA

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in to SSO with your SSO ID and password.
3. On the PLDS registration page, register as:
   - An Avaya Partner: Enter the Partner Link ID. To know your Partner Link ID, send an email to prmadmin@avaya.com.
   - A customer: Enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)
4. Click **Submit**.

   Avaya sends the PLDS access confirmation within one business day.

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.

Verifying the downloaded OVA

Verifying the OVA on a Linux-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded OVA matches the md5 checksum that is displayed for the OVA on the PLDS website.

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

Procedure

1. Enter `md5sum filename`, where *filename* is the name of the OVA. Include the .ova file extension in the filename.
2. Compare the md5 checksum of the OVA to be used for installation with the md5 checksum that is displayed for the OVA on the PLDS website.
3. Ensure that both checksums are the same.
4. If the numbers are different, download the OVA again and reverify the md5 checksum.

Verifying the OVA on a Windows-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded OVA matches the md5 checksum that is displayed for the OVA on the PLDS website.

Use this procedure if you downloaded OVA files to a Windows-based computer.

Procedure

1. Download a tool to compute md5 checksums from one of the following websites:
   - https://sourceforge.net/projects/filechecksumutility/
   - http://www.richherrick.com/software/hash/index.html

   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 OVA and note the md5 checksum.
3. Compare the md5 checksum of the OVA to be used for installation with the md5 checksum that is displayed for the OVA on the PLDS website.
4. Ensure that both numbers are the same.
5. If the numbers are different, download the OVA again and reverify the md5 checksum.

Downloading the Avaya Aura® release notes

About this task

Use this procedure to download Avaya Aura® release notes.

Make sure you read the AE Services section in the Avaya Aura® release notes before you install the software.

Note:

The release notes are in .PDF format. Make sure you have Adobe Acrobat Reader or a similar PDF document reading application installed on your computer.

Procedure

1. Using your web browser, go to `https://support.avaya.com`.
2. Click **Support by Product** > **Documents**.
3. In the Enter Your Product Here box on the Documents page, start typing Application Enablement Services, and select Application Enablement Services from the drop-down list.
4. From the **Choose Release** box, select 10.2.x.
5. In the Filters area, click **Release & Software Update Notes** and click **Enter**.
6. Click the title of the release notes.

   Your browser displays the release notes as a .PDF document.
7. Optionally, save the .PDF document to your computer.

Network requirements

Network interfaces for the server

AE Services uses network interfaces, referred to as NICs (network interface cards). The NICs use standard IEEE 802.3 Ethernet connections.

AE Services runs on VMware as a guest virtual machine. As a guest virtual machine, AE Services is responsible for configuring its virtual Ethernet interfaces. When you install the Application Enablement Services software, provide the network configuration for the virtual Ethernet.

- If your configuration uses only one network interface (referred to as a single NIC configuration), you only need to provide an IP address for eth0.
- If your configuration uses multiple network interfaces, you will need to provide an IP address for eth0 and an IP address for eth2.

Keep in mind that these “eth” settings refer to virtual Ethernet interfaces. The installation program maps these virtual ethernet IP addresses to physical Ethernet interface ports, which are designated in the software as eth0 and eth2.

Important:

Due to the nature of the virtual network interface card configured on the AE Services VM, you are unable to manually change the link speed of this virtual network interface card.

Caution:

Avaya Global Support Services (GSS) may not be able to assist in fully resolving a problem if an Avaya Application issue occurs and the reservations have been modified by the customer. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

Related links

Single NIC configuration on page 24
Dual NIC configuration on page 24
Network interface (NIC) settings on page 25

Single NIC configuration

In a single NIC configuration, you use one network interface. That is, AE Services uses one NIC for client, switch, and media 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 for the registration of 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.

AE Services recommends a single NIC configuration for connectivity to most Communication Manager media servers. For information about upgrading to AE Services Release 10.2.x, see *Upgrading Avaya Aura® Application Enablement Services*.

Related links

Network interfaces for the server on page 23

Dual NIC configuration

In a dual 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 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.

Related links

Network interfaces for the server on page 23

Network interface (NIC) settings

Important:

Due to the nature of the virtual network interface card configured on the AE Services VM, you are unable to manually change the link speed of this virtual network interface card.

Related links

Network interfaces for the server on page 23

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.

SAL Gateway

You require a Secure Access Link (SAL) Gateway for remote access and alarming.

Through SAL, support personnel or tools can gain remote access to managed devices to troubleshoot and debug problems.

A SAL Gateway:

1. Receives alarms from Avaya products in the customer network.
2. Reformats the alarms.
3. Forwards the alarms to the Avaya support center or a customer-managed Network Management System.

For more information about SAL Gateway and its deployment, see the Secure Access Link documentation on the Avaya Support website at https://support.avaya.com.

Chapter 4: Deploying Application Enablement Services on VMware®

Deploying Application Enablement Services on vCenter by using vSphere Client (HTML5)

About this task

Use this procedure to use vSphere Client (HTML5) and deploy Application Enablement Services on vCenter.

Before you begin

- Use vSphere Client (HTML5) to access vCenter Server.
- Download the Client Integration Plug-in.

Procedure

1. To access the vCenter Server, do the following:
   a. On the web browser, type the vCenter FQDN or IP Address.
   b. Select vSphere Client (HTML5) and type the vCenter Server credentials.
2. Select the Cluster or ESXi host, right-click, and then click **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.
3. On the Select an OVF template page, do one of the following:
   - To download the application OVA from a web location, select **URL**, and provide the complete path of the OVA file.
   - To access the application OVA from the local computer, select **Locate file**, click **Browse**, and navigate to the OVA file.
4. Click **Next**.
5. On the Select a name and folder page, do the following:
   a. In **Virtual machine name**, type a name for the virtual machine.
   b. In **Select a location for the virtual machine**, select a location for the virtual machine.

6. Click **Next**.
7. On the Select a compute resource page, select a host, and click **Next**.
8. On the Review details page, verify the OVA details, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I accept all license agreements**.
10. Click **Next**.
11. Select the AE Services profile in the **Deployment Configuration** section.
12. On the Select storage page, in **Select virtual disk format**, click the required disk format.
13. Click **Next**.
14. On the Select networks page, select the destination network for each source network.
15. In **IP protocol**, keep **IPv4**. Do not select **IPv6**.

    Caution:

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

    Only IPv6 is not supported.

    Note:

    Enable dual stack from AE Services Management Console after installation is complete.
16. Click **Next**.
17. On the Customize template page, enter the configuration and network parameters.

    For more information about the configuration and network parameters, see “Application Deployment field descriptions”.
18. Click **Next**.
19. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
20. To start the AE Services virtual machine, perform one of the following options:
    - Right-click the virtual machine and click **Power** > **Power On**.
    - Navigate to **Host** > **Virtual Machines**, select the virtual machine, and click **Actions** > **Power** > **Power On**.

      The system starts the AE Services virtual machine. When the system starts for the first time, configure the parameters for AE Services.
21. Click the **Console** tab and verify that the system startup is successful.

Deploying the application OVA by accessing the ESXi host directly

About this task

Use this procedure to deploy the application OVA on Avaya Solutions Platform 130 and equivalent server.

Before you begin

When you deploy or upgrade Avaya Aura® applications on Avaya Solutions Platform 130 ensure to:

- Update the Dell R640 BIOS and firmware to the latest release.
- Enable the iDRAC and connect it to an ethernet switch.

Note:

After deploying OVA directly from host, you must check that HDD size matches your profile.

Procedure

1. To access the ESXi host, do the following:
   a. On the web browser, type the ESXi host FQDN or IP address.
   b. In **User name**, type the username of the ESXi host.
   c. In **Password**, type the password of the ESXi host.
   d. Click **Log in**.
2. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.
3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK file page, do the following:
   a. Type a name for the virtual machine.
   b. Click to select files or drag and drop the OVA file from your local computer.
6. Click **Next**.
7. On the Select storage page, select a datastore, and click **Next**.
8. On the License agreements page, to accept the End User License Agreement, click **I Agree** and to accept the Root Access Acceptance Statement, click **I Agree**.
9. Click **Next**.

10. On the Deployment options page, perform the following:
    a. From **Network mappings**, select the required network.
    b. From **Disk provisioning**, select **Thick provision lazy zeroed**.
    c. From **Deployment type**, select profile.
    d. Clear **Power on automatically**.
11. Click **Next**.
12. On the Additional settings page, click **Next**.
13. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
14. To edit the virtual machine settings, click the VM radio option and perform the following:
    - Click **Actions** > **Edit Settings** to edit the required parameters.

      Note:
    - Click **Save** to save the reservation changes.

    Note:

    Ensure that the virtual machine is powered down to edit the settings.
15. To ensure that the virtual machine automatically starts after a hypervisor reboot, click the VM radio option, and click **Actions** > **Autostart** > **Enable**.

    Note:

    If you do not enable autostart, manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.
16. To start the virtual machine, if application is not already powered on, perform one of the following steps:
    - Click the VM radio option and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine and click **Power** > **Power On**.
    - Navigate to **Host** > **Virtual Machines**, select the virtual machine and click **Actions** > **Power** > **Power On**.

    The system starts the application virtual machine. When the system starts for the first time, configure the parameters for the application.
17. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the application configuration parameters.

Deploying the AE Services OVA file by using Solution Deployment Manager

About this task

Use this procedure to use Solution Deployment Manager and deploy AE Services.

Before you begin

- Add a location.
- Add the ESXi, vCenter, or Avaya Solutions Platform 130 host.

  For more information about adding the host, see “Managing the ESXi host by using SDM”.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ().
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

   Solution Deployment Manager displays the Applications Deployment window.
4. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      Solution Deployment Manager displays the host name in the **Platform FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The Capacity Details section displays the capacity details.
6. Click **Next**.
7. To get the OVA file, select the **OVA** tab, and click one of the following:
   - **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the application OVA file.
   - **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the following message: `Invalid file content. Avaya Certificate not found or invalid`
8. In **Flexi Footprint**, select the footprint size that the application supports.

9. **(Optional)** To install the patch file, click **Service or Feature Pack**, and enter the appropriate parameters.
   - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
   - **S/W Library**, and select the latest service or feature pack from the drop-down list.
   - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

   You can install the patch file now or after completing the AE Services OVA deployment.
10. Click **Next**.

    In Configuration Parameters and Network Parameters sections, Solution Deployment Manager displays the fields that are specific to the application that you deploy.
11. In the Configuration Parameters section, complete the fields.

    For more information, see “Application Deployment field descriptions”.
12. In the Network Parameters section:

    For the ESXi host or Avaya Solutions Platform 130, select the required port groups.
13. For private interface configuration, on the **Network Parameters** tab, perform one of the following:
    - For Appliance Virtualization Platform, in the Select a Network Mapping for Additional VM Network Interfaces section, select the required network connection or network adapter in **Private**.
    - For VMware, in the Select a Network Mapping for VM Network Interfaces section, select the required values in the **Private** field.
14. Click **Deploy**.
15. On Eula Acceptence page, to accept AVAYA GLOBAL SOFWARE LICENSE TERMS, click **Accept** and to accept ROOT ACCESS ACCEPTANCE STATEMENT, click **Accept**.

    In the Platforms for Selected Location <location name> section, Solution Deployment Manager displays the deployment status in the **Current Action Status** column.

    Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.
16. To view details, click the **Status Details** link.
17. Log in to the AE Services as a root user.
18. To reconfigure AIDE, run the following command:

    ```
    /opt/mvap/bin/setAIDE configure
    ```

Next steps

If required, you can install the patch file after completing the AE Services OVA deployment.

For more information, see “Installing software patches” in *Upgrading Avaya Aura® Application Enablement Services*.

Application Deployment field descriptions

Select Location and Platform

Name	Description
Select Location	The location name.
Select Platform	The platform name that you must select.
Platform FQDN	The platform FQDN.
Data Store	The data store for the application. The page populates the capacity details in the Capacity Details section.

Capacity Details

The system displays the CPU and memory details of the ESXi host. The fields are read-only.

Note:

If the host is in a cluster, the system does not display the capacity details of CPU and memory. Ensure that the host resource requirements are met before you deploy the virtual machine.

Name	Description
Name	The resource name.
Full Capacity	The maximum capacity.
Free Capacity	The available capacity.
Reserved Capacity	The reserved capacity.
Status	The configuration status.

Provide admin and root Credentials

The system displays the Provide admin and root Credentials section for OS.

Name	Description
Platform IP	The platform IP.
Platform FQDN	The platform FQDN.
Admin User of OS	The admin username of OS.
Admin Password of OS	The admin password of OS.
Root User of OS	The root user of OS.

OVA Details

Name	Description
Application Name	The name of the application.

Table continues…

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.
URL	The option to specify the URL or absolute path from where you can get the OVA or ISO file.
OVA from software library	The option to specify the software library where the OVA or ISO file is saved.
Select Software Library	The default path provided during the installation of the Solution Deployment Manager client. The default path is `C:\Program Files\Avaya\SDMClient\Default_Artifacts`. The field is available only when you click **OVA from software library**.
Browse	The option to specify the location from where you can get the OVA or ISO file.
Select OVA	The URL or absolute path to the OVA or ISO file of the application that you must provide. For example, `C:\Program Files\SDM\<Application OVA_10.2.x.ova>` The field is available only when you click **Browse**. **Note:** System Manager validates any file that you upload during deployment and accepts only the OVA or ISO file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file. When you select **OVA from software library**, you can select the OVA or ISO file of the application that you want to deploy.
Submit File	The field is available only when you click **Browse**. Selects the OVA or ISO file of the application that you want to deploy.
Flexi Footprint	The footprint size supported for the selected application. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description

Table continues…

Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends that you enable EASG. You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.

Data Encryption

Note:

Data Encryption is supported only for Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware Virtualized Environment.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled. • **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase. • **On vCenter or ESXi:** When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields. • **On vCenter base deployments:** If the passphrase field is left blank during deployment, the user is prompted to set the encryption boot passphrase on first login via CLI. The system restricts operations on OAM until the time the boot passphrase is set.

Table continues…

Name	Description
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Network Parameters

When you deploy the application on VMware, the system displays the Select a Network Mapping for VM Network Interfaces section.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Private	The field is available only when you deploy Application Enablement Services.
Out of Band Management	The port number that is mapped to the out of band management port group.

Button	Description
Deploy	Displays the EULA acceptance screen. To accept EULA and start the deployment process, click **Accept**.

Cloned and copied OVAs are not supported

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA. At this time, Avaya only supports the deployment of new OVAs.

Related links

Best Practices for VMware performance and features on page 86

Changing the Virtual Machine properties for the Virtualized Environment

About this task

Use this procedure to adjust the Virtual Machine properties of the server to meet the requirements of the AE Services template.

Important:

Any modification to the Virtual Machine resource settings (for example, removal of resources all together) is not recommended. Modifying these allocated resources could have a direct impact on the performance/capacity of the AE Services Virtual Machine. For the AE Services Virtual Machine to run at full capacity, these resource size requirements must be met. Removing or downsizing reservations significantly could put this requirement at risk. For more information, see AE Services resource requirements and the supported footprints on VMware on page 14.

Procedure

1. In the vSphere Client window, select **Host** > **Virtual Machines**.
2. Right-click the Virtual Machine, and select **Edit Settings**.
3. In the Virtual Machine Properties window, click the **Resources** tab.
4. In the Settings list, click **CPU**.
5. In the Resources Allocation area, perform one of the following steps:
   - Move the Reservation slider to specify the appropriate number.
   - Enter the appropriate number in the Reservation box.

   Note:

   Since the AE Services Virtual Machine requires four virtual CPUs, multiply by four the CPU speed displayed under the host's summary tab.
6. Click **OK**.

Chapter 5: Deploying Application Enablement Services on ASP R6.0.x (KVM on RHEL 8.10)

Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit

About this task

Application Enablement Services requires two network interfaces.

AE Services provides an OVA that contains qcow2 file.

Before you begin

- Install ASP R6.0.x (KVM on RHEL 8.10).

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the image from AE Services KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **`custadm`** credentials.
- Check if `/var/lib/libvirt/staging` exists.

  ```
  sudo ls -ld /var/lib/libvirt/images
  ```
- Ensure to remove the older images from the staging folder.

  Ensure sufficient space is available in the staging folder to copy the KVM image.
- If the staging folder does not exist, create it using the following commands:

  `sudo mkdir /var/lib/libvirt/staging`

  `sudo chown custadm:wheel /var/lib/libvirt/staging`
- Verify file permissions. The above chown command allows the custadm write into this directory with sudo. The permissions must appear as seen below:

  ```
  drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
  ```
- Copy the AE Services KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **`custadm`** credentials.
- If not still in the CLI, login again to the ASP R6.0.x CLI with **`custadm`** credentials.

Note:

All the following commands *MUST* be prefaced with "**sudo**":

- Run the following command to verify the AE Services KVM image available in the staging folder: **sudo ls -lr /var/lib/libvirt/staging**
- Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: **sudo tar -xvf AES-10.2.0.0.0.198.20231107-e70-00-kvm.ova**
- KVM OVA file extracts the following files:
- AES-10.2.0.0.0.198.20231107-e70-00-kvm.cert
  - AES-10.2.0.0.0.198.20231107-e70-00-kvm.mf
  - AES-10.2.0.0.0.198.20231107-e70-00-kvm.ovf
  - AES-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
- The extracted qcow2 images are in thin provision format. The qcow2 images MUST be converted to thick provision. When running the commands to convert to thick provision, a unique identifier can be added to the new qcow2 image. Avaya recommends to use VM name as a unique identifier. For example:

  AES-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2

  To

  AES[Unique Identifier]-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
- Ensure you are in the `/var/lib/libvirt/staging` directory before you proceed to convert `AES-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2 (thin)` to `AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2(thick).`

  ```
  sudo qemu-img convert -O qcow2 -o
  preallocation=full AES-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
  AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
  ```
- To verify that the conversion is successful and verify the disk size, run the following commands:
  - sudo qemu-img info AES-10.2.0.0.0.198.20231107-e70-00-kvm.qcow

    Disk size must display as 2.97 GiB
  - sudo qemu-img info AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2

    Disk size must display as 55 GB
- Copy the `AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2` to the `/var/lib/libvirt/images` directory. Ensure you are in the /`var/lib/libvirt/staging` directory before performing these steps:
  - cd /var/lib/libvirt/staging
  - sudo cp AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2 /var/lib/libvirt/images
- Ensure the images are present in the `/var/lib/libvirt/images` directory.
  - cd /var/lib/libvirt/images

- sudo ls -lr

- From the `/var/lib/libvirt/images` directory, run the following command to change the owner and permissions to 640 on the files:
  - sudo chown qemu:qemu AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
  - sudo chmod 640 AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2
- Go to `/var/lib/libvirt/staging` directory and remove all the extracted images and converted images. This is important to ensure that there is sufficient space for future deployments of KVM images. Do NOT remove files from the “images” directory.
  - cd /var/lib/libvirt/staging

    sudo ls -lr

    sudo rm *AES*

Procedure

1. Login to the KVM Cockpit web console as **`custadm`** in the following format: https://*<IP address or FQDN of KVM host>*:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

   Note:

   VMs are not visible when in Limited access mode!
3. In the Switch to administrative access window, enter the password for **`custadm`**.

   The **Limited access** button on the top-right of the window changes to **Administrative access**.
4. Navigate to **System** > **Virtual Machines** > **Import VM**.
5. In the Import a virtual machine window, do the following:
   a. In the **Name** field, enter a name for the AE Services virtual machine.
   b. In the **Disk Image** field, select the `AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2` image of the Application Enablement Services on the KVM Cockpit host under `/var/lib/libvirt/images/` dictionary.
   c. In the **Operating System** field, select **RHEL 8 Unknonwn** version.
   d. In the **Memory** field, select the required memory in MiB format.

      Note:

      Based on the required footprint, enter a value in the **Memory** field.

      For more information on footprints, see AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10) on page 15.
   e. Click **Import and edit**.

      Virtual Machine details page appears.

f. Under the Disks section, verify the `AESThick-10.2.0.0.0.198.20231107-e70-00-kvm.qcow2` image disk image size is correctly displayed in the **Capacity** field. By default, **virtio** is selected under the **Bus** field, and this needs to be modified.

6. Under the Disks section, click **Edit**.
7. In the Edit <attributes name> window, do the following:
   a. in the **Bus** field, select **scsi**.
   b. In the **Cache** field, select **directsync**.
   c. click **Save**.

   In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.
8. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
9. In the Overview section, in the **CPU** field, click **edit**.

   CPU Details window opens.
10. In the CPU details window, based on the required footprint, enter a value in the **vCPU Maximum** and **vCPU Count** fields.
11. Select the default **host-model** mode.
12. Enter values in the **vCPU Maximum** and **vCPU Count** fields, based on the required footprint.

    For more information on footprints, see AE Services resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10) on page 15
13. Click **Apply**.
14. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.

    AE Services requires two NICs:

    - NIC1 for Public IP address
    - NIC2 is for Out of Band Management
15. To add more network interfaces, under the Network interfaces section, click **Add network interface** and do the following:
    a. In the **Interface type** field, select **Bridge to LAN**.
    b. From the **Source** field, select the required network bridge.
    c. Click **Add**.
16. On the virtual machine, click **Run** to start the AE Services virtual machine.

Next steps

On first boot of tAE Services configure the virtual machine, follow the AE Services deployment guide.

Deploying AE Services on ASP R6.0.x (KVM on RHEL 8.10) using Script

About this task

AE Services provides a KVM OVA that contains one `qcow2` file:

AES-*-kvm.qcow2

Note:

- Disk encryption is possible using the script-based deployment.
- Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.
- Deployment of applications *MUST* be performed one at a time and delete the artifacts prior to deploying the next application.

  Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

Before you begin

- Install ASP R6.0.x (KVM on RHEL 8.10).

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the AE Services KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **`custadm`** credentials.
- Ensure that the staging folder exist:

  `sudo ls -ld /var/lib/libvirt/staging`
- Ensure to remove the older images from the staging folder.
- Ensure sufficient space is available in the staging folder to copy the KVM image.
- If the staging folder does not exist, create it using the following commands:

  - `sudo mkdir /var/lib/libvirt/staging`

  - `sudo chown custadm:wheel /var/lib/libvirt/staging`
- The chown command now allows **`custadm`** to write into the staging directory with **`sudo`**. For example, the permissions should look as follows:

```
drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
```

- Copy the AE Services KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **`custadm`** credentials.
- Run the following command to verify the AE Services KVM image is available in the staging folder:

  `sudo ls -lr /var/lib/libvirt/staging`

Procedure

1. Log in to the ASP R6.0.x CLI as a **custadm** user and verify the ASP version using the following command: **swversion**
2. Go to the staging folder;

   sudo cd /var/lib/libvirt/staging
3. Do the following:

ASP is on R6.0.0.0	ASP is on R6.0.0.1

a. Run the following command to extract the OVA file: **sudo tar -xvf AES-*-kvm.ova**
 	
KVM OVA extracts the following files:
• AES-*-kvm.ovf
• AES-*-kvm.qcow2
• AES-*-kvm.mf
• AES-*-kvm.cert
• ovf.py
• install_vm.py
b. Run the following script to deploy AE Services:
 	
sudo python3 install_vm.py
	Run the following script to deploy AE Services: **installVM AES-*.ova**
	
	ASP completes the auto-verification to ensure the following files are available:
	
	`AES-*-KVM.ovf`
	`AES-*-kvm.qcow2`
	`ovf.py`
	`install_vm.py`
	`AES-*-kvm.mf`
	`AES-*-KVM.cert`
	`AES-*-KVM.cert: OK`
	`Verified OK`
	`AES-*-kvm.qcow2: OK`
	`AES-*-KVM.ovf: OK`
	`install_vm.py: OK`
	`ovf.py: OK`

4. Press **ENTER** to read the **EULA**.
5. Press **Y** to accept the **EULA**.
6. Enter a name for the AE Services virtual machine. For example, `AES_VM`.
7. Select the required AE Services profile.

   For more information, see AES resource requirements and the supported footprints on ASP R6.0.x (KVM on RHEL 8.10) on page 15
8. Select the network interfaces.

   ASP 6.0.x CLI displays the currently available network interface bridges and select the required bridge for AE Services.

   Note:

   AE Services requires two NICs:

   • NIC1 for Public IP address

   • NIC2 is for Out of Band Management (Optional)

ASP 6.0.x CLI displays the currently available disk space and the required disk space to deploy AE Services.

9. To configure the VM properties, enter `Y` in the **Would you like to configure the VM properties? [y/n]:** field, and continue providing the property details.
10. In the **AES Hostname** field, enter a valid host name or a FQDN.

    If a FQDN is entered, FQDN also administers the local domain name. Valid characters are, a - z, A - Z, 0 - 9, and hyphen (-). The maximum length for the hostname is 15 characters.
11. In the **DNS Search Path** field, enter a domain name of the AE Services virtual machine. For example, mydomain.com
12. In the **Password for cust** field, enter the password for cust user. If this field is left blank, default password will be used. Reenter the password for cust user in the **Confirm Password for cust** field.

    The password length is a minimum of 14 characters and a maximum of 20 characters.
13. In the **Password for root** field, enter the root password. If this field is left blank, default password will be used. Reenter the root password in the **Confirm Password for root** field.

    The password length is a minimum of 14 characters and a maximum of 20 characters.
14. **(Optional)** In the **NTP Server** field, enter a valid NTP address or a hostname.

    You can type up to three NTP servers separated by a comma.
15. Enable or disable Enhanced Avaya Security Gateway (EASG).

    Important:

    Avaya recommends to enable **EASG**.

    Note:

    Enable: (Recommended)

    By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

    In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

    Disable:

    By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

    - Enter `1` to enable EASG.

- Enter `2` to disable EASG.

16. Enable or disable Data Encryption.

    By enabling Data Encryption, your Communication Product's Operational data and Log Files will be encrypted. You will be prompted to enter a pass-phrase that will be used to create/access an encryption key. Secondly, you will be asked to configure the option for local key storage.

    It is important to note that the encryption of the disk may have a performance impact. For further information, contact the Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

    By disabling Data Encryption, your Communication Product's Operational data and Log Files will be left unencrypted.

    Enter 1 to Enable Encryption or enter 2 to Disable Encryption.

    a. In the **Data Encryption** field, if `1` is entered, do the following

       - In the **Enter Encryption Passphrase** field, enter the passphrase.
       - In the **Confirm Enter Encryption Passphrase** field, reenter the passphrase.
       - In the **Require Encryption Passphrase at Boot-Time: (yes/no)**, enter the required value.

       If **`1`** is entered, you must enter the encryption passphrase whenever the AE Services reboots.

       If **`2`** is entered, there is no need to enter the encryption passphrase whenever the AE Services reboots.

       Important:

       You *MUST* remember the data encryption passphrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA.

    b. In the **Data Encryption Active** field, if `2` is entered, no action is required.

17. In the **Default Gateway** field, enter the default gateway address for the AE Services virtual machine.
18. In the **DNS** field, enter the domain name servers for the AE Services virtual machine.
19. In the **Public IP Address** field, enter the IP address for the AE Services interface.
20. In the **Public Netmask** field, enter the netmask or prefix for the AE Services interface.
21. In the **`Power on VM automatically after deploy?: [y/n]`** field, enter one of the following:

    - **`y`**: Indicates AE Services virtual machine is automatically powered-on after deployment.
    - **`n`**: Indicates user has to manually power on the AE Services virtual machine on KVM cockpit.

22. In the **Proceed?[y/n]** field, enter one of the following:
    - **y**: AE Services deployment begins.
    - **n**: AE Services deployment cancels.

    Note:

    Once the AE Services virtual machine is successfully deployed, ASP R6.0.x displays the following message: `Domain creation completed`. Otherwise, repeat step 3 on page 43 onwards.
23. Log in to the KVM Cockpit web console as **custadm** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
24. If Web console is in **Limited access** mode, click on **Turn on administrative access** button.

    Note:

    VMs are not visible when in **Limited access** mode.
25. For administration actions, on the top-right of the window, click on the **Limited access** or **Turn on administrative access** button.
26. Navigate to **System** > **Virtual Machines**.

    Verify that the AE Services virtual machine is deployed.
27. Click on the AE Services virtual machine.
28. If the **Power on VM automatically after deploy?: [y/n]** field is set to **n**, then click **Run** to power on the virtual machine.

    If the **Power on VM automatically after deploy?: [y/n]** field is set to **y**, AE Services virtual machine starts automatically.
29. On the AE Services virtual machine Console, accept **EULA**.
30. Login to AE Services virtual machine using cust user credentials.
31. **(Optional)** In the Overview section, enable **AutoStart** to automatically start the virtual machine whenever the host reboots.

Updating the CPU resources for KVM Cockpit

Procedure

1. Log in to the KVM Cockpit web console as **custadm** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

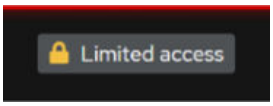


Figure 1: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

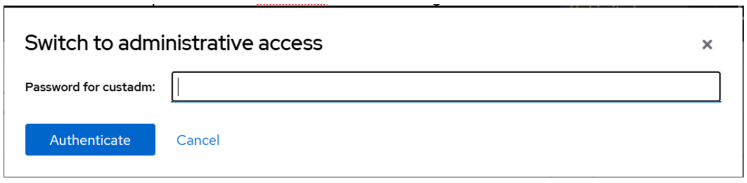


Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

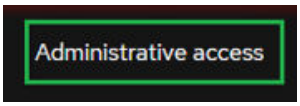


Figure 3: Administrative access button

4. Navigate to **System** > **Virtual Machines**.
5. If the virtual machine is running, right-click on the virtual machine to update and select **Shut Down**.
6. Right-click on the virtual machine and choose **Open/Edit**, and go to Overivew section.

   KVM Cockpit displays the CPU details window.
7. Update the CPU reservation details such as vCPU maximum, vCPU count, Sockets, Core per socket, and Threads per core.
8. Click **Apply**.
9. Click **Run** to start the virtual machine.

Chapter 6: Configuring

Configuration checklist

Use the following checklist for configuring the AE Services virtual appliance.

#	Action	Link/Notes	✔
1	Start the AE Services VM.	See Starting the Application Enablement Services virtual machine using vSphere Web client on page 48.	
2	Configure the AE Services VM to start automatically after a power failure.	See Configuring the virtual machine automatic startup settings on VMware on page 49.	
3	Configure the network settings.	See Configuring the network settings in a deployment on page 49.	
4	Configure the time zone and time configuration.	Once you have configured the network correctly, you can update the time and time zone settings for the AE Services VM from the AE Services Management Console. See Changing the time zone setting on page 52.	
5	Connect to a remote WebLM and license the AE Services system.	See Application Enablement Services license requirements on page 55.	

Starting the Application Enablement Services virtual machine using vSphere Web client

Procedure

1. In the vSphere Web client window, select **Host** > **Virtual Machines**.
2. Right-click the AE Services VM, and select **Power On**.
3. Right-click the AE Services VM, and select **Open Console**.
4. Wait for the AE Services VM to boot up.

   Once the AE Services VM boots up, configure the AE Services VM (if necessary).

Configuring the virtual machine automatic startup settings on VMware

About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software does not use the startup selections.

Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Manage**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Edit**.

   The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Configuring the network settings in a deployment

About this task

Use this procedure to initially configure the network settings for a deployment.

Note:

After you initially configure the network settings for a deployment, you can change the network information from the AE Services Management Console. For more information, see *Administering and Maintaining Avaya Aura® Application Enablement Services*. This configuration is initially needed for AE Services deployed through vSphere Web client only, and not for AE Services deployed through vCenter or SDM.

Note:

The `netconfig` command does not support IPv6.

Caution:

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

Only IPv6 is not supported.

Procedure

1. In the vSphere Client window, select **Host** > **Virtual Machines**.
2. Right-click the AE Services VM, and select **Open Console**.
3. Using the Open Console window, log into AE Services as `cust`.
4. Change to `root` user.
5. At the command prompt, type `netconfig` and press the ENTER key.
6. On the Properties page, perform the following steps:
   a. In the Hostname box, enter the hostname or fully-qualified domain name for the AE Services VM.

      Keep in mind the following information:

      - The hostname may contain only the ASCII letters a through z (case insensitive), the digits 0 through 9, and the hyphen (-).
      - The hostname cannot begin with or end with a hyphen (-).
      - The hostname cannot exceed 15 characters.
      - The hostname if given in upper-case will automatically get converted to lower-case.

   b. In the **DNS Search Path** box, enter the domain name of the AE Services VM.
   c. In the **Default Gateway** box, enter the default gateway address for the VM.
   d. In the **DNS** box, enter the domain name servers for this VM. Use a comma to separate multiple servers.
   e. In the **Network 1 IP Address** box, enter the IP address for this interface.
   f. In the **Network 1 Netmask** box, enter the netmask or prefix for this interface.
   g. In the **Network 2 IP Address** box, enter the IP address for this interface (optional).
   h. In the **Network 2 Netmask** box, enter the netmask or prefix for this interface (optional).
7. When finished, select **OK** and press the ENTER key.
8. At the command prompt, type reboot and press the ENTER key to reboot the AE Services VM.

Out of Band Management

Out of Band Management provides the ability to move the AE Services Management Console Web-based management and configuration traffic of the server to a dedicated subnetwork.

Table 1: Application Enablement Services Out of Band Management

Component	Interface	Description
DMCC Service	Eth0 (public IP)	The Device, Media, and Call Control (DMCC) service provides both, first-party and third-party call control features using a Java API. It also provides XML and .NET interfaces. TCP/IP, TLS and SIP protocols may be used to connect a DMCC Client to DMCC.
DLG Service	Eth0 (public IP)	The DEFINITY LAN Gateway (DLG) service tunnels messages over TCP/IP. That is, the DLG service supports a set of TCP/IP connections for the communications channel between Avaya Aura® Communication Manager and AE Services. The DLG service is also used for transporting ASAI/Q.931 messages.
CVLAN Service	Eth0 (public IP)	The CallVisor LAN (CVLAN) service is a C/C++ based API that enables applications to exchange ASAI messages with the AE Services server. CVLAN provides a full complement of third-party call control capabilities such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking features, and querying Avaya Aura® Communication Manager for information.
TSAPI Service	Eth0 (public IP)	The Telephony Services API (TSAPI) is a C/C++ based API that provides a full complement of third party call control capabilities. The Java Telephony API (JTAPI) is a client side interface to the TSAPI service. It provides third party call control.
Transport Service	Eth0 (public IP) Eth1 (private IP)	The Transport link is a secure TCP/IP connection between the AE Services server and Avaya Aura® Communication Manager. The default interface is eth0
System Management Service	Eth0 (public IP), or Eth2 (Out of Band Management IP	Listens on port 443 for HTTPS connection to provide users a web interface to enable SOAP-based access to Avaya Aura® Communication Manager administration functions. The default interface is eth0, unless Out-of-Band Management has been configured.
Telephony Web Service	Eth0 (public IP), or Eth2 (Out of Band Management IP)	Listens on port 8443 and 443 for HTTPS connection to provide users a web interface that enables high level call control functionality over standard web services interfaces (SOAP/ XML). The default interface is “eth0”, unless Out-of-Band Management has been configured.
AES Management Console	Eth0 (public IP) or Eth2 (Out of Band Mgmt IP)	The Application Enablement Services Management Console listens on port 443 for HTTPS connections, and provides an Operations, Administration and Management interface for maintenance of the AE Services server. The default interface is eth0, unless Out-of-Band Management has been configured.

Changing the time zone setting

Procedure

1. From your browser, log in to AE Services Management Console. See Logging into the Management Console on page 52.
2. From the main menu, select **Maintenance > Date Time/NTP Server**.
3. Make your changes, and then click **Apply**.

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.

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.

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

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.

Chapter 7: AE Services Licensing

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 overview

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

- Obtain the license from the Avaya Product Licensing and Delivery System (PLDS) website.
- After you install the AE Services software, log in to the AE Services Management Console to access the Avaya Web License Manager (WebLM).
- Use WebLM to install the license.
- After you install the license file, you must reboot the AE Services server.
- When the license file is installed, you will have access to the AE Services software.

Embedded Avaya WebLM server

Embedded Avaya WebLM Server and AE Services

This feature is supported on all AE Services offers. The license file is deployed inside a AE Services server running on Tomcat.

The license file installed on the embedded Avaya WebLM server uses the AE Services host ID.

Note:

If the eth0 IP address is changed, you must obtain a new license file.

Embedded Avaya WebLM Server and Geographic Redundancy

Obtain the Avaya WebLM host ID from both AE Services servers prior to configuring Geographic Redundancy.

- For the Geographic Redundancy feature to be activated, the license file generated for embedded Avaya WebLM server requires host IDs of both AE Services servers within the license file.

- If Geographic Redundancy is already configured, disable HA to get the Avaya WebLM host ID from each AE Services server.

Embedded Avaya WebLM support by release

Embedded Avaya WebLM is supported on all AE Services Software-Only offers.

From Release 7.0.1 and later, AE Services VMware offer supports Embedded Avaya WebLM.

Extended Avaya WebLM service feature

Extended Avaya WebLM service supports Avaya WebLM service deployed on System Manager or standalone Avaya WebLM server.

Enterprise Wide Licensing

In pooled mode, multiple AE Services servers share a pool of licenses installed on an external master Avaya WebLM server.

In allocation mode, a pool of licenses are subdivided and distributed to a local (or embedded) Avaya WebLM server from a master Avaya WebLM.

For a more responsive AE Services server, use allocation mode with embedded Avaya WebLM servers.

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 Avaya WebLM server

About this task

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

From the AE Services Release 7.1.3, do not enter Avaya WebLM credentials to log in to the Embedded Avaya WebLM interface. The change password link on the Avaya WebLM user interface does not work. if you changed the password, log out and log in again to Avaya WebLM. The Avaya WebLM login credentials are required only to log in to the external WebLM.

Procedure

1. On your web browser, log in to AE Services Management Console.
2. On the AE Services Management Console main menu, click **Licensing** > **WebLM Server Address**.
3. In the **WebLM IP Address** field, enter the IPv4 address of the remote Avaya WebLM server to point your AE Services server to the Avaya WebLM server.

   If AE Services requires to use the embedded Avaya WebLM server, enter the IP address `127.0.0.1`.
4. Select the **SSL** check box to specify the appropriate setting for SSL.

   By default the **SSL** check box is selected.
5. In the **WebLM Port** field, enter the port number of the WebLM server.

   Note:

   If System Manager WebLM server is used, import the System Manager CA certificate.

   The configuration for Secondary WebLM is optional.

   AE Services uses secondary WebLM server for licensing only if the primary WebLM server is not available and you have configured the **Secondary WebLM IP Address**.
6. In the **Secondary WebLM IP Address** field, enter the IPv4 address of the secondary WebLM server to point your AE Services server to the WebLM server.

7. Select the **Secondary SSL** check box to specify the appropriate setting for SSL.
8. In the **Secondary WebLM Port** field, enter the port number of the secondary WebLM server.

Logging in to WebLM and creating a WebLM password

About this task

The Web License Manager (WebLM) provides you with the ability to install and manage Avaya product licenses. The first time you run a WebLM session, you must create a new WebLM password.

Note:

Before you start this procedure, make sure your browser allows pop-up windows from avaya.com.

Note:

This procedure is not applicable for Embedded WebLM as no password is required to login in Embedded WebLM.

Follow this procedure to access WebLM from the Application Enablement Services Management Console.

Procedure

1. In the address bar of your browser, type `https://`*`fully-qualified domain name or IP address of the AE Services server`* and press ENTER.
2. From the Application Enablement Services welcome page, click **Continue to Login**.
3. From the Application Enablement Services Management Console log in page, type your user name and password, and click **Login**.

   Important:

   You cannot log in to the Application Enablement Services Management Console as the root user. Avaya service technicians should log in as craft. Customers should log in as cust.

   Your browser displays the Application Enablement Services Management Console. The main menu is in the left pane and the welcome page is in the right pane.
4. From the main menu, select **Licensing > WebLM Server Access**.
5. Follow these steps to complete the Web License Manager Logon screen.
   a. In the User Name field, type `admin`, the default WebLM User name.
   b. In the Password field, type `weblmadmin`, the default WebLM password.
   c. Click the arrow.

      The first time you log in to WebLM, the server displays the **Change Password** page.
6. Complete the fields on the Change Password page and click **Submit**.

Your browser displays the login page again.

7. Log in as `admin` with the password you just created.

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 61. 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 61.

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 60 or Restarting AE Services from the Linux command line on page 60.

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.

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 61.
`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 62.
`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 61.

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.

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 8: Post-installation and verification

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 9: 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 67
Accessing the port matrix document on page 67
Avaya Documentation Center navigation on page 68

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 66

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 66

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 66

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 71

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 70

Appendix A: 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**

Default AE Services accounts

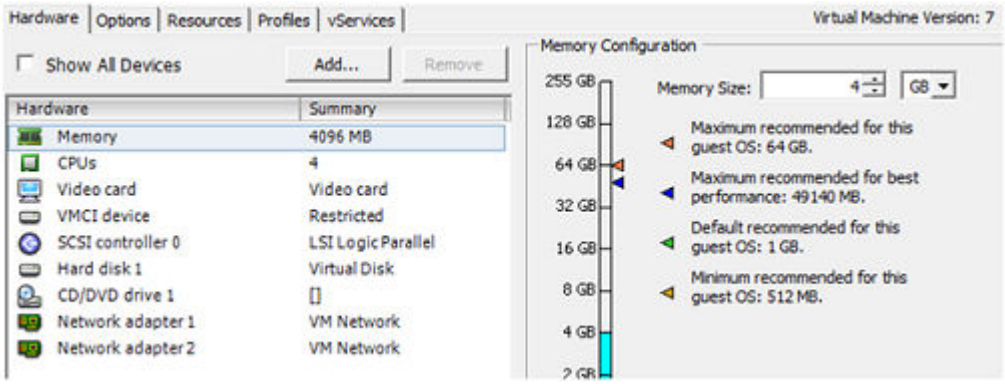
Account name (log-in identifier)	Linux Group	Access privileges
craft Available on AE Services Software-Only Server only if you enabled EASG at the time of installation.	susers securityadmin	Intended for Avaya services technicians. Provides local or remote access to the Linux shell. • Local - Log in from 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.

Modifying reservations on Application Enablement Services

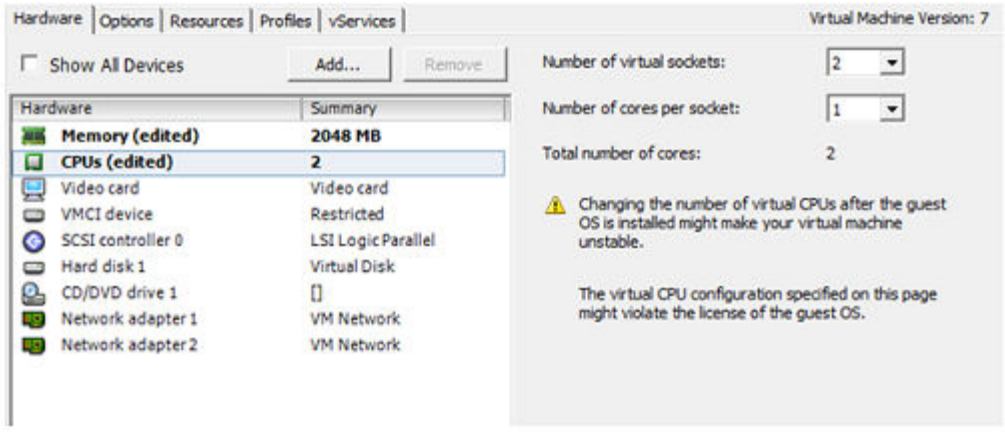
The following procedure modifies reservations on Application Enablement Services.

Procedure

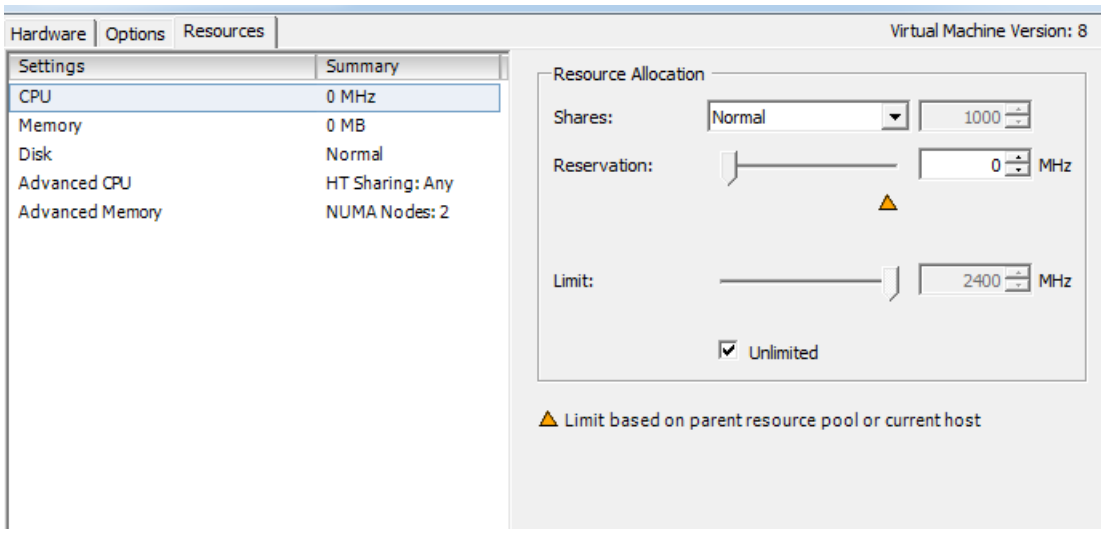
1. Deploy the Application Enablement Services OVA.
2. Before booting the virtual machine, reduce reservations:
   a. Right-click the Application Enablement Services virtual machine and select **Edit Settings**.
   b. In the **Settings** window, select the **Hardware** tab.
   c. In the left pane, under **Hardware**, select **Memory**.



   d. In the right pane, change the **Memory Size** value from the existing value to the required value.
   e. In the left pane, select **CPUs**.
   f. In the right pane, adjust the **Number of virtual sockets** from the existing value to the required value.



g. At the top of the **Settings** window, select the **Resources** tab.

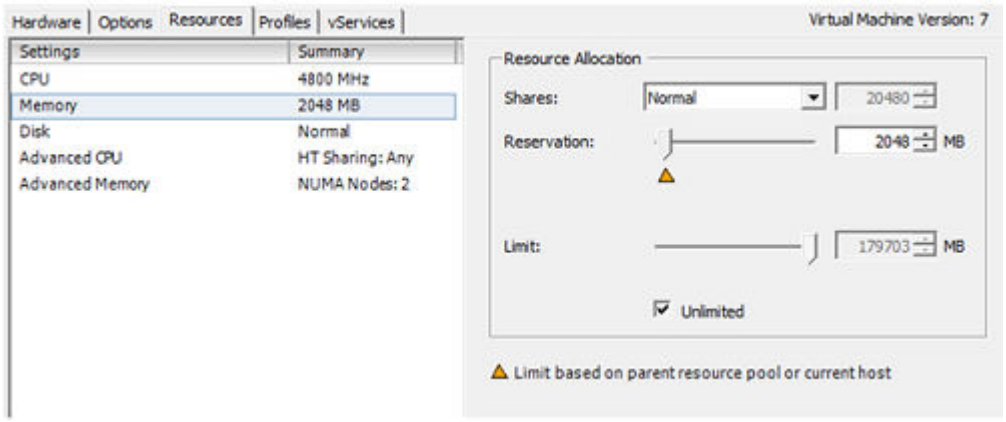


h. In the left pane, select **CPU**.

i. In the right pane, click in the **MHz** box and change the number from the existing value to the required value.

j. in the left pane, select **Memory**.

k. In the right pane, click in the **MB** box and change the number from the existing value to the required value.



l. Click **OK** to exit the window.

3. Boot the Application Enablement Services virtual machine.

Appendix B: 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 C: Best Practices for VMware performance and features

The following sections describe the best practices for VMware performance and features.

Related links

BIOS on page 86
VMware Tools on page 88
Timekeeping on page 88
VMware networking best practices on page 89
Storage on page 92
Thin vs. thick deployments on page 93
VMware features supported by Avaya Aura on page 96

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper, “Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs” at https://www.vmware.com/.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers

Related links

Best Practices for VMware performance and features on page 86
Intel Virtualization Technology on page 87
Dell PowerEdge Server on page 87

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

Related links

BIOS on page 86

Dell PowerEdge Server

The following are the BIOS recommendations for Dell PowerEdge Servers supported by Avaya SBC:

When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- In Processor Settings, set:
  - **Turbo Mode** to **enable**.
  - **C States** to **disabled**.

Related links

BIOS on page 86

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Related links

Best Practices for VMware performance and features on page 86

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service

cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the **`chronyc sources -v`** command from a command window. The results from this command:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **chronyd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

Related links

Best Practices for VMware performance and features on page 86

VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

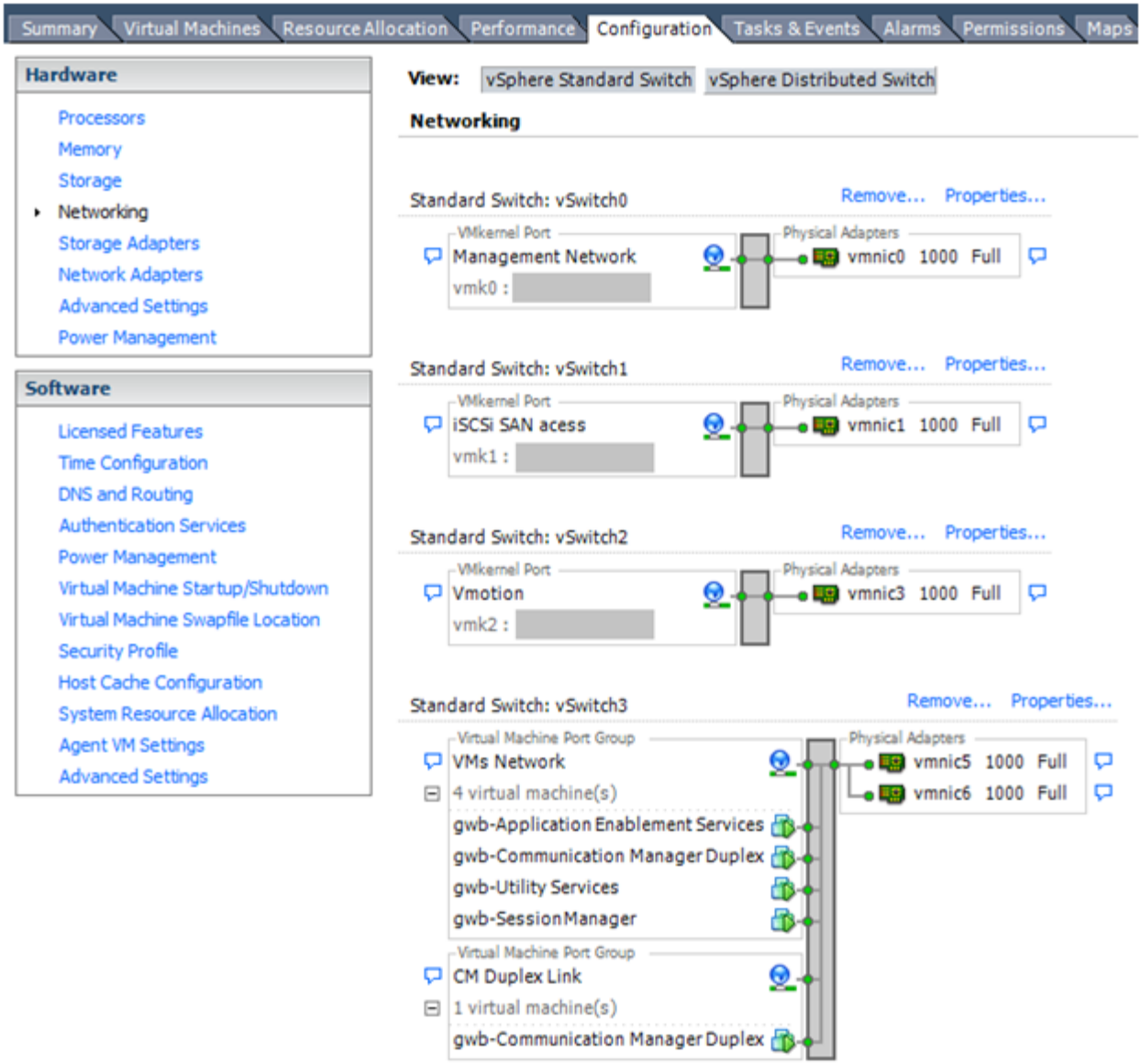
The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.

- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

Disclaimer: The images in this section represent older ESXi versions and may vary for the latest ESXi versions.

Networking Avaya applications on VMware ESXi – Example 1



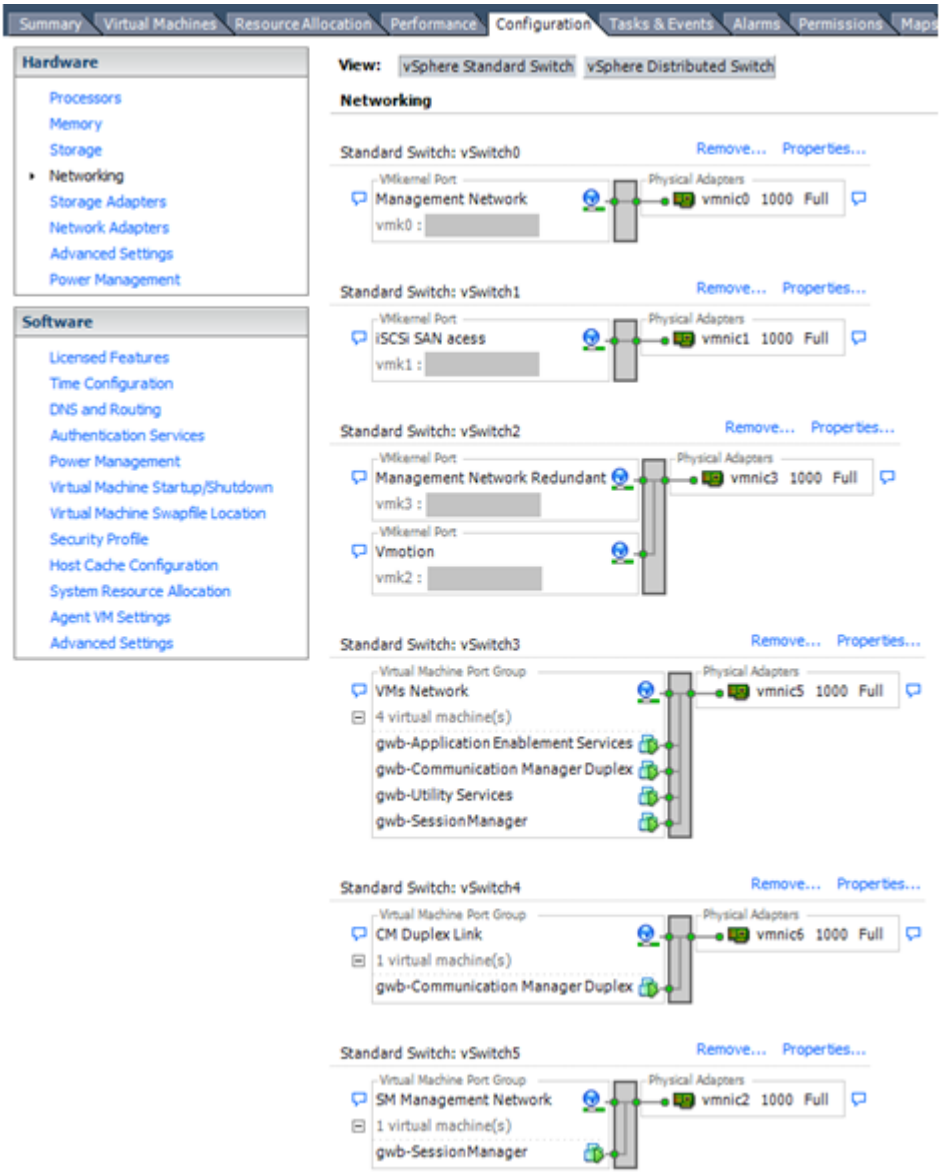
This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the

Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.

- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0,

VMware Management Network operations can continue on this redundant management network.

- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

References

Title	Link
Product Support Notice PSN003556u	Go to https://support.avaya.com and search for PSN003556u.
VMware vSphere 8.0 Documentation	Go to Broadcom website (formerly known as VMware) and search for *VMware vSphere 8.0 Documentation*.
VMware vSphere 7.0 Documentation	Go to Broadcom website (formerly known as VMware) and search for *VMware vSphere 7.0 Documentation*.

Related links

Best Practices for VMware performance and features on page 86

Storage

The Avaya Aura® AE Services virtual machine does not have a large disk footprint, nor is it particularly disk input/output intensive. AE Services generates a fair amount of log information. As a general rule, if a failure occurs at any of the hypervisor, network, or network-attached storage levels, it is possible for AE Services to lose some of its logging information.

When deploying AE Services in a VMware environment, follow these storage recommendations:

- Always deploy AE Services with a thickly provisioned disk. The choice between eager and lazy zeroed makes no difference for the AE Services VM.
- For best performance, use AE Services only on disks local to the ESXi host or SAN storage devices. Do not store AE Services on an NFS storage system.

Related links

Best Practices for VMware performance and features on page 86

Thin vs. thick deployments

VMware ESXi uses a thick virtual disk by default when it creates a virtual disk file.. The thick disk preallocates the entire amount of space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are preallocated for that virtual disk.

- Thin-provisioned disks can grow to the full size as specified at the time of virtual disk creation, but they cannot shrink. Once you allocate the blocks, you cannot deallocate them.
- Thin-provisioned disks run the risk of overallocating storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the formatting process may cause the thin-provisioned disk to grow to full size. For example, if you present a thin-provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the format tool in Microsoft Windows writes information to all sectors on the disk, which in turn inflates the thin-provisioned disk to full size.

Related links

Best Practices for VMware performance and features on page 86

Best Practices for VMware features

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

  If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the Take Snapshot window, clear the **Include virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots

Related links

Best Practices for VMware performance and features on page 86

Cloned and copied OVAs are not supported

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA. At this time, Avaya only supports the deployment of new OVAs.

Related links

Best Practices for VMware performance and features on page 86

VMware High Availability

VMware High Availability is a viable method of Avaya Aura® AE Services recovery in the VMware environment. For more information, see VMware's documentation on High Availability.

Important:

When using VMware High Availability with AE Services, all link associations between AE Services and Avaya Aura® Communication Manager will go down in a failure situation. The VM will then be booted again on a standby server and return to working order.

Related links

Best Practices for VMware performance and features on page 86

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.

- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Related links

Best Practices for VMware performance and features on page 86

VMware features supported by Avaya Aura®

This section does not cover Avaya Solutions Platform (ASP) 130 and ASP S83000. Avaya does not support advanced VMware features on its ASP 130 and ASP S8300 hardware. It supports the basic VMware features as listed in the following table. For more information about support and limitations on ASP 130 and ASP S8300, see https://download.avaya.com/css/public/documents/101062774.

Note:

For more information about Avaya Aura® Media Server, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

The following table lists the VMware features supported on customer-provided Virtualized Environment for various Avaya Aura® Release10.2 components.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
ESXi 7.0	Yes	Yes	Yes	Yes	Yes	Yes
ESXi 8.0	Yes	Yes	Yes	Yes	Yes	Yes
vCenter See foot note[1]	Yes	Yes	Yes	Yes	Yes	Yes
vSphere WebClient (HTML5)	Yes	Yes	Yes	Yes	Yes	Yes
VMFS 6	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

[1] Limited to deployment, managing VMs, basic monitoring, and making VMs part of a vCenter cluster.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
VMware vMotion See foot note[2]	Yes	Yes	Yes	Yes	Yes	Yes
Storage vMotion	Yes	Yes	Yes	Yes	Yes	Yes
VMware Snapshot See foot note[3]	Yes	Yes	Yes	Yes	Yes	Yes
VMware Live Snapshot	Not supported	Not supported	Not supported	Not supported	Not supported	No
VMware High Availability	Yes	Yes	Yes	Yes	Yes	Yes
Proactive High Availability	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)
Storage DRS	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading ratio for Virtual CPUs and Physical CPU	2:1	2:1	2:1	2:1	2:1	2:1
VMware DRS (Compute and Memory) See foot note[4]	Yes	Yes	Yes	Yes See foot note[5]	Yes	Yes
Secure boot for virtual machine	Yes	Yes	Yes	Yes	Yes	Yes
Content Library	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

[2] Ensure that vMotion occurs when an Avaya Aura® application virtual machine is in maintenance mode.
[3] Snapshots should be used when patching the products. As per the backup mechanism provided in the product-specific documentation, you should perform daily backups instead of using snapshots of the products. Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.
[4] With two conservative modes - Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.
[5] DRS supports In-cluster migration - Applicable for Avaya SBC for Enterprise.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
VMware Fault Tolerance (FT)	Not supported	Not supported	Not supported	Yes See foot note[6]	Not supported	Yes
vSphere Standard Switch	Yes	Yes	Yes	Yes	Yes	Yes
vSphere Distributed Switch	Yes	Yes	Yes	Yes	Yes	Yes
Hot Pluggable Virtual Hardware	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Reservation Required see foot note[7]	Yes	Yes	Yes	Yes	Yes	Yes
vSAN support See foot note[8]	Yes	Yes	Yes	Yes	Yes	Yes
Thin Provisioning	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

Related links

Best Practices for VMware performance and features on page 86

[6] For more information about the Fault Tolerance for Application Enablement Services, see *Avaya Aura Application Enablement (AE) Services 7.x, 8.x, and 10.x High Availability (HA) White Paper.*

[7] Avaya Aura® does not support reservationless deployments on ASP 130. Avaya recommends always making reservations when choosing a reservationless deployment. It is crucial to strictly adhere to the guidelines outlined in the Application Notes. For more information on reservationless deployment, see the *"Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware"* at https://support.avaya.com .

[8] If you are using vSAN, use Thick Provisioning. Even though VMware supports vSAN with Thin Provisioning, Avaya Aura® does not support it.

Appendix D: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.
2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

Index

A

accessing port matrix 67
activating license entitlements 80
AE Services
    deploy 31
AE Services field descriptions
    Application Deployment 33
AES server
    hostname 61, 62
AES software
    licensed services 59
    restarting 60
Application Deployment
    AE Services field descriptions 33
Application Enablement Services 16
automatic restart
    virtual machine 49
Avaya Aura® application
    ESXi version 17
    KVM version 18
Avaya InSite Knowledge Base 71
Avaya support website 70
Avaya WebLM 55

B

best practices
    performance and features 86
    VMware networking 89
BIOS 86
BIOS settings
    for Dell servers 87

C

change history 6
Change Password page in WebLM 58
changing the Virtual Machine properties 37
checklist
    configuration procedures 48
    planning 10
clones
    deployment 37, 95
collection
    delete 68
    edit 68
    generating PDF 68
    sharing content 68
Communication Manager
    requirements 20, 25
configuration 49
configuration data
configuration data *(continued)*
    customer 13
configuration procedures
    checklist 48
configuration tools and utilities
    deploying or upgrading 16
configure 49
configuring
    virtual machine automatic restart 49
configuring the network settings 49
content
    publishing PDF output 68
    searching 68
    sharing 68
    sort by last updated 68
    watching for updates 68
crossover cable 60
CTI link requirements 25
customer configuration data 13

D

delays on communications channel 25
deploy
    AE Services 31
deploying
    OVA using KVM Cockpit 38
deploying AE Services on vCenter by using vSphere Client (HTML5) 27
deploying copies 37, 95
deployingAES on ASP using Script 42
deployment 49
    thick 93
    thin 93
deployment guidelines 11
document changes 6
documentation
    Application Enablement Services 66
documentation center 68
    finding content 68
    navigation 68
documentation portal 68
downloading software
    using PLDS 12, 20
Dual NIC configuration guidelines 24
duplex settings for AES 25

E

Editing
    CPU resources for KVM 46
Embedded Avaya WebLM server 55
error messages

error messages *(continued)*
WebLM ... 61
ESXi ... 96
ESXi version
Avaya Aura® application ... 17
Ethernet interfaces
on SAMP ... 60

F

features best practices ... 86
finding content on documentation center ... 68
finding port matrix ... 67
flexible footprint ... 53
configuring hardware resources ... 53
footprint flexibility ... 53

G

guidelines
deployment ... 11

H

hardware resources
configuring for flexible footprint ... 53
High Availability ... 95
HTTPS ... 56

I

installation
license file ... 59
Intel Virtualization Technology ... 87
interface speed for AES ... 25

K

KB
Support site ... 71
KVM component
virtualized environment ... 9
KVM version
Avaya Aura® application ... 18

L

laptop computer
connecting to server ... 60
license entitlements
activating ... 80
searching for ... 81
license file for AES
installing ... 59
removing an existing file ... 58
verify settings ... 59
licensed features
specific features ... 55
Licensed Products page for Application Enablement ... 59
licenses
AE Services ... 59
Licensing ... 55
log in
as user with root privileges ... 60
to OAM ... 58
to WebLM ... 61
WebLM ... 62
logging
AE Services Management web console ... 52

M

media server requirements ... 20, 25

N

network
interface speed and duplex settings ... 25
latency requirements ... 25
network configuration settings
verifying ... 64
Network interfaces ... 23
Network interfaces, required settings ... 25
network settings ... 49
NIC
Ethernet interface for technician ... 60
NIC configuration, editing ... 64
NIC, recommended settings ... 25
NTP time source ... 88

O

OAM
home page ... 58
Out of Band Management
Application Enablement Services ... 50
Network interface configurations ... 50
OVA
verifying on Linux-based computer ... 22
verifying on Windows-based computer ... 22
OVA file
deploy ... 29

P

packet delivery time ... 25
Password policy
Linux ... 72
PCN notification ... 99
performance best practices ... 86
periodic spiked delays ... 25
ping, measure round-trip packet delivery time ... 25

planning
checklist 10
PLDS 20
downloading software 12, 20
port matrix 67
PSN notification 99
purposeinstallation in Virtualized Environment 6

R

reducing reservations
Communication Manager 78
regenerating a license file 84
registering 20
rehosting 83
removing an existing license file 58
Removing the AE Services license file 62
requirements
AE Services 14, 15
AE Services footprints 14, 15
license file 59
media server 20, 25
virtual machine storage 92
reservations
reducing for Communication Manager 78
resource requirements 14, 15
resources
server 17
restarting AE Services 60

S

SAL Gateway 26
searching for content 68
searching for license entitlements 81
security guidelines 26
Server Properties page in WebLM 61
settings 49
sharing content 68
signing up
PCNs and PSNs 100
Single NIC configuration guidelines 24
snapshots 93
software details 16
software requirements 19
sort documents 68
starting AES virtual machine 48
storage 92
support 70
supported hardware and resources 17

T

technician
reserved interface 60
thick deployment 93
thin deployment 93
timekeeping 88
training 69

V

verifying
AE Service IP (Local IP) settings 63
license 63
network configuration settings 64
software version 63
videos 70
viewing
PCNs 99
PSNs 99
virtual machine
automatic restart configuration 49
Virtual Machine properties
changing 37
Virtualized Environment 37
virtual machine storage 92
virtualized environment 8
vMotion 95
VMware 95, 96
VMware components
virtualized environment 8
VMware networking
best practices 89
VMware software requirements 19
VMware Tools 88
VMware_Features 96
vSphere 96
VT support 87

W

watchlist 68
WebLM 56
error messages 61
logging in 61, 62
WebLM server
connecting 57