Deploying Avaya Aura® Application Enablement Services in Virtualized Environment

Release 7.1.3
Issue 5
July 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® Application Enablement AE Services virtual application in the Avaya Aura® virtualization offer.

The Avaya Aura® virtualization offer is presented in two variants:

- Avaya Aura® Virtualized Environment (VE) - customer-provided VMware infrastructure, and
- Avaya Aura Virtualized Appliance (VA) - Avaya provided server and VMware hypervisor, also known as Appliance Virtualization Platform.

The information provided in this document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying AE Services on the Avaya Aura Virtualized Environment offer or the Avaya Aura Virtualized Appliance offer. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Change history

Issue	Date	Summary of changes
5	July 2021	Updated the section: AE Services Virtual Machine resource requirements on page 25
4	April 2019	Updated Dual NIC configuration on page 32.
3	May 2018	• Updated the checklist for upgrading AE Services to Release 7.1.3. • Updated the procedure to upgrade to Release 7.1.3.
2	December 2017	• Updated the checklist for upgrading AE Services to Release 7.1.2. • Updated the procedure to upgrade to Release 7.1.2.
1	May 2017	Release 7.1.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 193

Using the Avaya InSite Knowledge Base on page 193

Chapter 2: Avaya Aura Virtualized Appliance Overview

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized offers

Avaya Aura® Release 7.0 and later supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.0.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

The virtualization offers provide the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks which reduces the footprint.
- Lowers power consumption and cooling requirements.
- Enables capital equipment cost savings.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
- Business can scale rapidly to accommodate growth and to respond to changing business requirements.

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized Appliance is a turnkey solution. Avaya provides the hardware, all the software including the VMware hypervisor and might also offer the customer support of the setup. Virtualized Appliance offer is different from Avaya Aura® Virtualized Environment, where Avaya provides the Avaya Aura® application software and the customer provides and supports the VMware hypervisor and the hardware on which the hypervisor runs.

Deployment considerations

- Deployment on the Appliance Virtualization Platform server is performed from the System Manager Solution Deployment Manager or the Solution Deployment Manager standalone Windows client.
- Avaya provides the servers, Appliance Virtualization Platform, which includes the VMware ESXi hypervisor.

Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- S8300D and S8300E

Note:

With WebLM Release 7.x, you cannot deploy WebLM on S8300D Server or S8300E Server running on Appliance Virtualization Platform.

Note:

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for Communication Manager LSP and Branch Session Manager with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

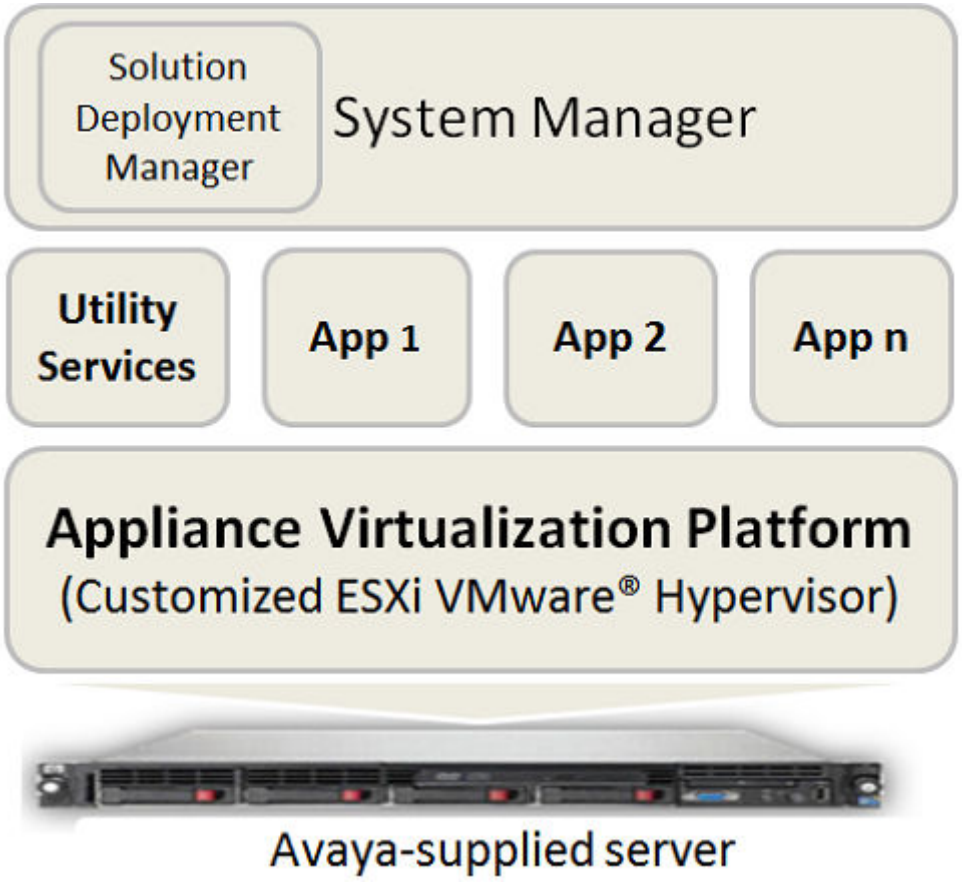
Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to the Release 7.1.3.

Consider the following options if the higher capacity is required from the S8300D:

- Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before.
- Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.



From Avaya Aura® Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.

You can deploy the following applications on Appliance Virtualization Platform:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8

- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

Note:

For deploying Avaya Aura® applications on Appliance Virtualization Platform only use Solution Deployment Manager.

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

Note:

This document uses the following terms, and at times, uses the terms interchangeably.

- server and host
- reservations and configuration values

Deployment considerations

Avaya Pod Fx for Enterprise Communications

Avaya Pod Fx for Enterprise Communications is an alternative deployment option for Avaya Aura® Virtualized Environment applications.

Avaya Pod Fx is a full-stack turnkey solution that combines storage arrays from EMC, virtualization software from VMware, and networking, management, and real-time applications from Avaya.

Avaya Pod Fx accelerates deployment of Avaya Aura® applications and simplifies IT operations.

Documentation

The following table lists the Avaya Pod Fx for Enterprise Communications documents. These documents are available on the Avaya support website at http://support.avaya.com.

Title	Description
Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide	Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.
Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide	Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Avaya Pod Fx. This guide explains how to access and use the applications in the POS management suite.
Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation	Identifies the Avaya Pod Fx customer documentation. Also includes the documentation for the Avaya and non-Avaya products that are included in the Avaya Pod Fx solution.
Avaya Pod Fx for Enterprise Communications – Release Notes	Describes fixed and known issues for Avaya Pod Fx. This document does not describe issues associated with each component in the Avaya Pod Fx. For information on the specific components, see the component Release Notes.

Solution Deployment Manager

The Solution Deployment Manager capability simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8

- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  Note:

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.

- Hardware-based Session Manager 6.x
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

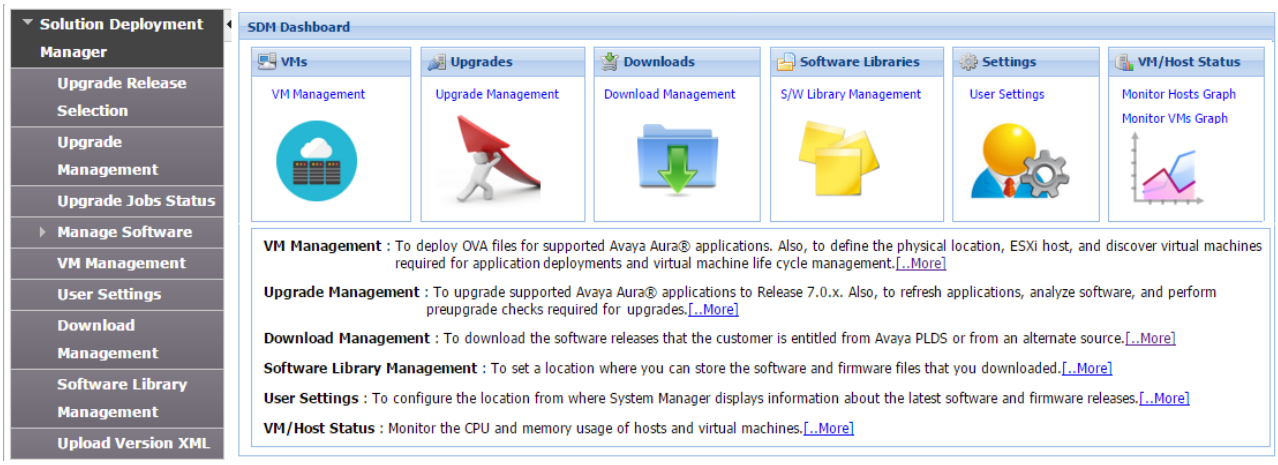
Note:

However, you must manually migrate Services virtual machine that is part of the template.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.1.3. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.0** or **6.3.8** as the target upgrade. Release 7.1.3 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module (UCM) and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Kickstart file.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, WebLM to Release 7.1.3.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the `version.xml` file to perform upgrades.

Virtualized components

Software component	Description
ESXi Host	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.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface. The installable vSphere Client is not available in vSphere 6.5 and later releases.
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available in vSphere 6.5. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
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.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the technician computer on the following operating systems:
  - Windows 7, 64-bit Professional or Enterprise
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.

- Supports deploying the System Manager OVA. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of the Avaya Aura® applications.
- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.
- Configures application and networking parameters required for application deployments.
- Supports the local computer or an HTTP URL to select the application OVA file for deployment. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as, IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  Note:

  To install the patch on a System Manager virtual machine, the Solution Deployment Manager client must be on the same version as of patch. For example, if you are deploying the patch for System Manager Release 7.1.1, you must use the Solution Deployment Manager client Release 7.1.1.

  Avaya Aura® applications must use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs or the application Command Line Interface or Web pages.
- Configure Remote Syslog Profile.
- Create Appliance Virtualization Platform Kickstart file.

Avaya Aura® virtualized software

Software delivery

The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS) and the Avaya support site. Each OVA contains the following components:

- The application software and operating system.
- Preinstalled VMware tools.
- Preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Note:

The customer provides the servers and the VMware® infrastructure, that includes VMware® licenses.

Patches and upgrades

A minimum patch level can be required for each supported application. For more information about the application patch requirements, see the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Important:

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

Performance and capacities

The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

Modifying configuration values might have a direct impact on the performance, capacity, and stability of the virtual machine. Customer must understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) might not be able to assist in fully resolving a problem if the virtual hardware or resource allocation has been changed to unsupported values for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

Chapter 3: Planning and configuration

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 23.	
2	Identify configuration tools and utilities.	See Required tools for installation on page 24.	
3	Register for PLDS.	See Registering for PLDS on page 27.	
4	Download the software for PLDS.	See *Downloading software from PLDS*.	
5	Verify the downloaded OVA.	If you are using a Linux-based computer, see Verifying the OVA on a Linux-based computer on page 29. If you are using a Windows-based computer, see Verifying the OVA on a Windows-based computer on page 29.	
6	Download the Avaya Aura® Release 8.0 release notes.	See Downloading the release notes on page 30.	

Customer configuration data

The following table identifies the key customer configuration information that will be required throughout the deployment and configuration process for AE Services.

Required Data for AE Services	Example Value
Hostname or fully-qualified domain name for the AE Services VM.	aesserver1

Table continues…

Required Data for AE Services	Example Value
DNS search path. **Note:** If you leave this value blank, modify or add the line `search` *<dns search path>* in the file `etc/resolv.conf` after you deploy the AE Services VM successfully.	example.com
Default gateway address for the AE Services VM.	123.45.67.254
Domain name servers for the AE Services VM.	123.45.1.2
IP address for the AE Services VM interface for eth0 (Public interface).	123.45.67.89
Netmask or prefix for the AE Services VM interface for eth0 (Public interface).	255.255.255.0
IP address for the AE Services VM interface for eth1 (Private interface) (optional).	123.45.67.90
Enter the Netmask or prefix for the AE Services VM interface for eth1 (Private interface) (optional).	255.255.255.0
IP address for the AE Services VM interface for eth2 (Out of Band Management interface) (optional).	
Netmask or prefix for the AE Services VM interface for eth2 (Out of Band Management interface) (optional).	
Network Time Protocol (NTP) hostname or IP address (optional).	

Note:

- DHCP will not take effect until you configure it from the command line after initial deployment.
- Do not expect AE Services to initiate DHCP on first boot.
- Avaya recommends that you do not use DHCP with AE Services.

Configuration tools and utilities

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

Note:

AE Services 7.1.3 deployment via System Manager Solution Deployment Manager client on Dell™ PowerEdge™ R610 Appliance Virtualization Platform server with 4 GB or 6 GB RAM is insufficient. The recommended RAM is at least 12 GB. Upgrade your system RAM accordingly before deploying AE Services 7.1.3.

The following are the general hardware and software requirements to deploy AE Services 7.1.3:

- You can download the AE Services VMware OVA for Release 7.1.3, from the Avaya Product Licensing and Delivery System (PLDS) website.
- USB keyboard, USB mouse, video monitor, and cables or laptop computer with an Ethernet crossover cable.
- A computer that can route to the VMware server that has a web browser. AE Services supports the following browsers:
  - Microsoft Internet Explorer version 11.

    Note:

    For web pages to display components correctly on Microsoft Internet Explorer, use the **Compatibility View** setting on some AE Services Web pages. **Compatibility View Settings** can be found from **Internet Explorer > Tools**. Then select **Compatibility View Settings**, and add the AE Services server IP address to the list.
  - Google Chrome version 47
  - Mozilla Firefox version 43.
  - Microsoft Edge browser.
- The customer order number applies to Avaya service technicians who are installing or upgrading the AE Services server for a customer with a maintenance contract.

For information about getting the AE Services license file, see the AE Services license requirements section.

Site preparation

Hardware and resource requirement

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 http://www.vmware.com/resources/guides.html.

AE Services Virtual Machine resource requirements

The Avaya Aura® AE Services VM requires minimum following set of resources to be available on the VMware ESXi based host or Appliance Virtualization Platform before deployment.

VMware Resource	Value
Supported profiles: Profile 1 Profile 2 Profile 3	Supported Virtual CPUs/CPU Total Hertz/Memory 1CPU/2190 MHz Reservation/4 GB memory/30 GB HDD 2CPU/4380 MHz Reservation/4 GB memory/30 GB HDD 4CPU/8760 MHz Reservation/6 GB memory/30 GB HDD **Tip:** 7200 MHz on Dell R610 and HP G7, the CSR1 server types.
Storage requirement	30 GB
Shared network-interface cards	1
IOPS	6
Network usage	75 Kbps

Note:

See *Avaya Aura® Application Enablement Services Overview and Specification* to find the supported AE Services capacities per Profile.

Note:

AE Services has been tested using a SAN-based datastore only. All other disk configurations are untested.

Solution Deployment Manager will check and verify the available resources on the host server based on the selected AE Services flexible footprint profile before deploying the OVA. If the necessary, resources can not be allocated, Solution Deployment Manager will not initiate deployment. Using VMware vSphere, the AE Services VM can be deployed on a host that does not have the available resources to allocate to the AE Services VM, however, the VM will not be allowed to power up. There are CPU reservations assigned to the AE Services VM, built into the OVA, that are specified for a specific profile. For more information about hardware resources to support the AE Services footprint flexibility, see Reconfiguring hardware resources to support VE flexible footprint. on page 188

Software requirements

Software requirements

Avaya Aura® AE Services uses the current software release 7.1.3 as its standard release.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 7.1.2 and later on a customized version of VMware® ESXi 6.0.

- Customer-provided Virtualized Environment offer: Supports the following software versions:
  - VMware® vSphere ESXi 5.5
  - VMware® vSphere ESXi 6.0
  - VMware® vSphere ESXi 6.5
  - VMware® vSphere ESXi 6.7
  - VMware® vCenter Server 5.5
  - VMware® vCenter Server 6.0
  - VMware® vCenter Server 6.5
  - VMware® vCenter Server 6.7

  To view compatibility with other solution releases, see VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

Note:

- vSphere ESXi 6.7 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.7.
- vSphere ESXi 6.5 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.
- Avaya Aura® Release 7.1 and later does not support vSphere ESXi 5.0 and 5.1.

Communication Manager and media server requirements

To use AE Services 7.1.3, you must have the Communication Manager official Release 6.0.x, 6.2, 6.3.x, 7.0, 7.0.1, 7.1, 7.1.1, 7.1.2, or 7.1.3 software running on an IP-enabled media server.

Note:

Communication Manager 6.0 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 6.3.x, 7.0, 7.0.1, 7.1, 7.1.1, 7.1.2, or 7.1.3.
- AE Services 7.1.3 supports both, Control Local Area Network (CLAN) interfaces and Processor Ethernet connections when implementing Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP) 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 place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com 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. Enter http://plds.avaya.com in your Web browser 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 on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. 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.

13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

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-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 AE Services release notes

About this task

Make sure you read the AE Services release notes before you install the software.

Note:

AE Services provides release notes as .PDF documents. 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 7.1.3.
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

VMware and AE Services use network interfaces, sometimes 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

Supported servers on page 31
Single NIC configuration on page 31
Dual NIC configuration on page 32
Network interface (NIC) settings on page 32

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 7.0 and later:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9

For fresh installations, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9.

Related links

Network interfaces for the server on page 30

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.

AE Services recommends a single NIC configuration for connectivity to most Communication Manager media servers. See *Supported Servers* for more information about deployments and upgrades to AE Services Release 7.1.3.

Related links

Network interfaces for the server on page 30

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.

Related links

Network interfaces for the server on page 30

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 30

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*. This white paper is 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.

You can deploy SAL Gateway OVA:

- On Avaya Aura® Virtualized Appliance by using Solution Deployment Manager
- In the Avaya Aura® Virtualized Environment by using vCenter, vSphere or Solution Deployment Manager

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

Chapter 4: Initial setup and connectivity

Deployment of cloned and copied OVAs

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 on the virtual machine. At this time, Avaya only supports the deployment of new OVAs.

Related links

Best Practices for VMware performance and features on page 209

Deployment guidelines

- Deploy as many virtual appliances on the same host as possible.
- Deploy the virtual appliances 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 resources. Oversubscribing affects performance.
- Monitor the server, host, and virtual appliance performance.

Important:

The values for performance, occupancy, and usage can vary greatly. The blade server might run at 5% occupancy, but a virtual machine might run at 50% occupancy. Note that a virtual machine behaves differently when the CPU usage is higher.

Deployment checklist

Use the following checklist to deploy AE Services Release 7.1.3 virtual application by using the following checklist:

#	Action	✔
1	Using the Avaya Support website at http://support.avaya.com, download the following: • For a Virtualized Environment new installation: - AE Services 7.1.3 OVA. • For a Virtualized Environment upgrade from 6.3.x or 7.0.x to 7.1.3: - AE Services 7.1.3 OVA.	
2	Install the supported server.	
3	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation. Ensure that the license file copies are accessible.	
6	AE Services 7.1.3 can be deployed as follows: • Direct OVA deployment: - Install the AE Services 7.1.3 OVA in the Virtualized Environment using vCenter, vSphere. • Upgrading from previous AE Services versions to AE Services Release 8.0	

Accessing Solution Deployment Manager

About this task

You require to start Solution Deployment Manager to deploy and upgrade virtual machines, and install service packs or patches.

Procedure

Perform one of the following:

- If System Manager is not already deployed, double-click the Solution Deployment Manager client.
- If System Manager is available, on the web console, click **Services** > **Solution Deployment Manager**.

Installing the Solution Deployment Manager client on your computer

About this task

In Avaya Aura® Virtualized Appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches and hypervisor patches.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

From Avaya Aura® Appliance Virtualization Platform Release 7.0, Solution Deployment Manager is mandatory to upgrade or deploy the Avaya Aura® applications.

Procedure

1. Download the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products** > **Downloads**, and type the product name as **System Manager**, and Release as **7.1.x**.
3. Click the **Avaya Aura® System Manager Release 7.1.x SDM Client Downloads, 7.1.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.

8. Click **Next**.
9. On the Pre-Installation Summary page, review the information, and click **Next**.
10. On the User Input page, perform the following:
    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
    b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

       The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

       You can save the artifacts in the specified directory.
    c. In **Data Port No**, select the appropriate data port.

       The default data port is 1527. The data port range is from 1527 through 1627.
    d. In **Application Port No**, select the appropriate application port.

       The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

       Note:

       After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
    e. **(Optional)** Click **Reset All to Default**.
11. Click **Next**.
12. On the Summary and Validation page, verify the product information and the system requirements.

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.
13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.
15. To start the client, click the Solution Deployment Manager client icon, .

Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

Deploying AE Services in the Virtualized Appliance

Deploying AE Services OVA using System Manager Solution Deployment Manager or Solution Deployment Manager client

Procedure

1. To deploy AE Services:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager** and then click,**VM Management**.
   - For Solution Deployment Manager Client, on the desktop, click the Solution Deployment Manager icon and then click **VM Management**.
2. Click on **Location > Host > Virtual Machines**
3. Click on **New** to create Virtual Machine
4. On the **VM** Name Field, enter the Host Name of AE Services.

   Note:

   Make sure you are installing AE Services on the correct Location and Host.
5. Select the Data Store.
6. On the Deploy OVA section, deploy AE Services OVA.

   Important:

   Before deploying AE Services OVA, see *Upgrading Avaya Aura® applications to Release 7.1* for the following:
   - Downloading the AE Services OVA.
   - Deploying the AE Services OVA.
7. Select the software library.
8. Select the OVA File.
9. Select the **Footprint**.
10. In the Configuration Parameters Section, enter the AE Services Network Configuration information.
11. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

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 Avaya Logins you are preventing Avaya access to your
system.
This is not recommended, as it impacts Avaya’s ability to provide
support for the product. Unless the customer is well versed in
managing the product themselves, Avaya Logins should not be
disabled.
```

a. 1: To enable EASG.

   Avaya recommends to enable EASG.

   You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

b. 2: To disable EASG.

12. In the Network Parameters field, assign the NICs to the private port.
13. Accept the EULA Acceptance.
14. Verify the AE Services Deployment Status steps by clicking the **Status Details Link** in the AE Services Entry of the Virtual Machine list.
15. AE Services OVA deployment is successful. Verify the AE Services deployment status clicking the status link.

    For more information, see *Deploying Avaya Aura® applications from System Manager*.

    Install the latest Avaya Aura® Application Enablement Services 7.1.3 Super Patch (if available), and other release patches as applicable.

    For more information, see Avaya Aura® 7.1.3 Release Notes.

Deploying AE Services in the Virtualized Environment

Deploying Application Enablement Services OVA using the vSphere client connected to Vcenter

About this task

Use this procedure if the vSphere Client is connected to vCenter.

Procedure

1. Using the vSphere Client, log into the target vCenter.
2. In the vSphere Client window, select **File > Deploy OVF Template**.
3. On the Source section, click **Browse**.
4. In the Open dialog box, select the OVA you want to deploy.
5. Click **Open**.
6. On the Source section, click **Next**.
7. On the OVF Template Details section, click **Next**.
8. On the End User License Agreement section, read the license agreement.
9. Click **Accept** to accept the terms of the license agreement, then click **Next**.
10. In the **Name** box on the Name and Location section, enter the name for the AE Services VM, for example AES-7–1–3. The default is `Application Enablement Services`.
11. Click **Next**.
12. Select the AE Services profile under the Deployment Configuration section. Click **Next**.
13. On the Host/Cluster section, select the host or cluster on which you want to run the AE Services template.

    Note:

    If you selected the host before performing Step 2, the Disk Format section appears. Go to Step 19.
14. Click **Next**.
15. On the Specify a Specific Host section, select the specific host within the cluster on which you want to run the AE Services template.
16. Click **Next**.

    If the host has more than one datastore, the Storage section appears. Go to Step 17.

    If the host has only one datastore, the Disk Format section appears. Go to Step 19.

17. On the Storage section, select the appropriate datastore to deploy the AE Services Virtual Machine.
18. Click **Next**.

    The Disk Format section appears.
19. On the Disk Format section, select **Thick Provision Lazy Zeroed**.
20. Click **Next**.

    The Network Mapping section appears.
21. On the Network Mapping section, select the appropriate network.
22. Click **Next**.
23. On the Properties section, perform the following steps:
    a. Under Application settings, enter the hostname or fully-qualified domain name for the AE Services VM in the **Hostname** box.

       Note:

       - The hostname may contain only the ASCII letters `a` through `z` (case sensitive), the digits `0` through `9`, and the hyphen (`-`).
       - The hostname cannot begin with or end with a hyphen (`-`).
       - The entire hostname (including the delimiting dots) may consist of up to 255 characters.
       - The hostname cannot exceed 15 characters.

    b. In the **DNS Search Path** box, enter the domain name of the AE Services VM.

       Note:

       If you leave the DNS Search Path box blank, you must modify the file `/etc/resolv.conf` after you power up the system.

    c. Under System Time settings, select the **Timezone** and **NTP server(s)** as applicable.
    d. In the Configuration Parameters Section, enter a selection to enable (recommended) or disable Avaya Login access for Enhanced Access Security Gateway (EASG). For additional information about how to enable or disable EASG after initial deployment or mange the EASG site certificate, see Administering and Maintaining Avaya Aura® Application Enablement Services 7.1.

       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 Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Enter 1 to Enable EASG (Recommended), or 2 to Disable EASG.

e. Under Networking Properties settings, enter the default gateway address for the VM. in the **Default Gateway** box.

Note:

If you leave the **Default Gateway** box blank, you must configure this setting after deployment.

f. In the **DNS** box, enter the domain name servers for this VM. Use a comma to separate multiple servers.

Note:

If you leave the **DNS** box blank, you must configure this setting after completing the deployment.

g. In the **Public IP Address** box, enter the IP Address. Enter the Public Netmask in the **Public Netmask** box.

h. In the **Private IP Address** box, enter the IP Address. Enter the Private Netmask in the **Private Netmask** box. This substep is optional.

i. In the **Out of Band Management IP Address** box, enter the Out of Band Management IP Address. Enter the Out of Band Management Netmask in the **Out of Band Management Netmask** box. This substep is optional.

Note:

Out of Band Management cannot be enabled after AE Services deployment.

24. Click **Next**.
25. On the Ready to Complete section, verify the settings displayed. If you need to modify any of the settings, click **Back**.
26. Click **Finish** to deploy the OVF.

    The `Deploying Application Enablement Services` message box appears showing the status of the deployment.

When deployment is complete, the `Deployment Completed Successfully` message box appears.

27. On the `Deployment Completed Successfully` message box, click **Close**.
28. Power on the AE Services VM

Note:

Install the latest Avaya Aura® Application Enablement Services 7.1.3 Super Patch (if available), and other release patches as applicable.

For more information, see Avaya Aura® 7.1.3 Release Notes.

Deploying the application OVA using vSphere Web Client by accessing the host directly

About this task

Use this procedure for deploying application OVA on ACP 130. This same procedure is applicable for ESXi 6.5 u2 onwards.

Before you begin

- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.

Procedure

1. On the Web browser, type the host URL: `https://<Host FQDN or IP Address>/ui`.
2. Enter login and password.
3. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.
4. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
5. Click **Next**.
6. 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.
7. Click **Next**.
8. On the Select storage page, select a datastore, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I Agree**.
10. Click **Next**.

11. 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.

       For more information about supported footprints, see “Supported footprints of Communication Manager on VMware”.
    d. Uncheck **Power on automatically**.
12. Click **Next**.
13. On the Additional settings page, click **Next**.
14. On the Ready to complete page, review the settings, and click **Finish**.

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

    Note:

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

    Note:

    If you do not enable autostart you must manually start the virtual machine after the hypervisor reboot.
17. To start the virtual machine, if application is not already powered on perform one of the following steps:
    - Click VM radio option, and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the application virtual machine.

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

Deploying Application Enablement Services OVA using vSphere Client connected to host

About this task

Use this procedure if the vSphere Client is connected directly to the host (that is, without vCenter).

Procedure

1. Using the vSphere Client, log into the ESXi host server.
2. In the vSphere Client window, select **File > Deploy OVF Template**.
3. On the Source page, click **Browse**.
4. In the Open dialog box, select the OVA you want to deploy.
5. Click **Open**.
6. On the Source page, click **Next**.
7. On the OVF Template Details page, verify the information, and then click **Next**.
8. On the End User License Agreement page, read the license agreement.
9. Click **Accept** to accept the terms of the license agreement.
10. Click **Next**.
11. In the Name box on the Name and Location page, enter the name for the AE Services VM (for example, AES-7–1). The default is Application Enablement Services.
12. Click **Next**.

    If the host has more than one datastore, the Storage page appears. Go to Step 13.

    If the host has only one datastore, the Disk Format page appears. Go to Step 15.
13. On the Storage page, select the appropriate datastore to deploy the AES Virtual Machine.
14. Click **Next**.

    The Disk Format page appears.
15. On the Disk Format page, select **Thick Provision Lazy Zeroed**.
16. Click **Next**.

    The Network Mapping page appears.
17. On the Network Mapping page, select the appropriate network.
18. Click **Next**.
19. On the Ready to Complete page, verify the settings displayed. If you need to modify any of the settings, use the **Back** button.
20. When you are ready to deploy the OVF, click **Finish**.

The `Deploying Application Enablement Services` message box appears showing the status of the deployment.

When the deployment is complete, the `Deployment Completed Successfully` message box appears.

21. In the Deployment Completed Successfully message box, click **Close**.
22. Using the vSphere interface, power on the AE Services VM
23. Using the vSphere interface, open a console window for the AE Services VM
24. In the console window during the first boot phase, an interactive session will be started to allow a user to enter the AE Services VM network information. When prompted, please read and answer each question.

Note:

Install the latest Avaya Aura® Application Enablement Services 7.1.3 Super Patch (if applicable), and other release patches as applicable.

For more information, see Avaya Aura® 7.1.3 Release Notes.

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 Virtual Machine resource requirements on page 25.

Procedure

1. In the vSphere Client window, select **View > Inventory > Virtual Machines and Templates**.
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: Virtual machine management

Virtual machine management

The VM Management link from Solution Deployment Manager provides the virtual machine management.

VM Management provides the following capabilities:

- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change and patch installation of the Appliance Virtualization Platform host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environments.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA file on the host by using the System Manager Solution Deployment Manager or the Solution Deployment Manager client.

Related links

Certification validation on page 84

Managing the location

Viewing a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Locations tab.

   The Locations section lists all locations.

Adding a location

About this task

You can define the physical location of the host and configure the location specific information. You can update the information later.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

   The system displays the new location in the VM Management Tree section.

Related links

New and Edit location field descriptions on page 56

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the **Location** tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.

4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 56

Deleting a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation dialog box, click **Yes**.

   The system does not delete the virtual machines that are running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**.

VM Management field descriptions

Name	Description
Auto-Reload VM Management Tree	The option to automatically reload the VM Management Tree after the completion of operations, such as, refreshing virtual machines.

Locations

Name	Description
Location Name	The location name.
City	The city where the host is located.
Country	The country where the host is located.

Button	Description
New	Displays the New Location section where you can provide the details of the location that you want to add.
Edit	Displays the Edit Location section where you can change the details of an existing location.
Delete	Deletes the locations that you select. The system moves the hosts associated with the deleted locations to unknown location.

Hosts

Name	Description
Host Name	The name of the host.
Host IP	The IP address of the host.
Host FQDN	FQDN of the host.
IPv6	The IPv6 address of the host. If the IP address of the ESXi host is an IPv4 address, the column does not display any value.
vCenter FQDN	FQDN of vCentre.
Current Action	The operation that is currently being performed on the host.
Last Action	The last completed operation on the host.
License Status	The status of the license.
Host Version	The host version.
Offer Type	The host type. The options are: • **AVP**: Appliance Virtualization Platform host • **Customer VE**: customer-provided VMware ESXi host
SSH Status	The SSH service status. The values are enabled and disabled.
Host Certificate	The certificate status of the Appliance Virtualization Platform host. The values are: • : The certificate is added in Solution Deployment Manager and correct. • : The certificate is not accepted or invalid. You can click **View** for details of the certificate status.
vCenter Certificate	The certificate status of the ESXi host. The values are: • : The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • : The certificate is not accepted or invalid. You can click **View** for details of the certificate status.

Note:

Depending on the Appliance Virtualization Platform host and vCenter certificate status, the system enables the options in **More Actions**.

Button	Description
Auto Refresh	The option to automatically refresh the page with the latest changes. For example, the page updates: • The VM state when a virtual machine changes • The license status or certificate status of host when host changes The system refreshes the data every minute.
Add	Displays the New Host section where you can provide the details of the host that you want to add.
Edit	Displays the Host Information section where you can change the details of an existing host.
Remove	Removes the hosts that you select only from the Solution Deployment Manager client. The system moves the hosts associated with the deleted locations to unknown location.
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.
More Actions > **AVP Update/Upgrade Management**	Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **SSH** > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays `SSH enabled successfully`.
More Actions > **SSH** > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.

Table continues…

Button	Description
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the virtual machine host. Also Syslog is only for Appliance Virtualization Platform. You can select multiple Hosts and Push syslog configuration on selected hosts.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view syslog profiles of selected the Appliance Virtualization Platform host.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
More Actions > **Lifecycle Actions** > **Host Restart**	Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Lifecycle Actions** > **Host Shutdown**	Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **AVP Cert. Management** > **Generate/Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the host. Depending on the host type, the options are: • **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only. • **Accept Certificate**: To accept a valid certificate for the host or vCenter. • **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate.
More Actions > **AVP Cert. Management** > **Manage Certificate**	Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected host.
More Actions > **AVP Cert. Management** > **Generic CSR**	Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.
More Actions > **Snapshot Manager**	Displays the Snapshot Manager dialog box from where you can view and delete the virtual machine snapshot.
More Actions > **WebLM Configuration**	Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.

Table continues…

Button	Description
More Actions > **Set Login Banner**	Displays the Message of the Day dialog box from where you can push the login banner text to the selected host. **Note:** This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support **Set Login Banner**.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM IPv6	The IPv6 address of the virtual machine, if any.
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.1.
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the VMware host or Appliance Virtualization Platform host on which the virtual machine resides.

Table continues…

Name	Description
Trust Status	The status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store name.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machine from host and Solution Deployment Manager Client.
Start	Starts the selected virtual machines.
Stop	Stops the selected virtual machines.
Show Selected	Displays only the selected virtual machines.
More Actions > **Restart**	Starts the selected virtual machines that were stopped earlier.
More Actions > **Refresh VM**	Updates the status of the virtual machines.
More Actions > **Re-establish connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected virtual machine.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number. Administrators use the field to check entitlements.
Address	The address where the host is located.
City	The city where the host is located.
State/Province/Region	The state, province, or region where the host is located.
Zip/Postal Code	The zip code of the host location.
Country	The country where the host is located.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnetwork mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).

Button	Description
Save	Saves the location information and returns to the Locations section.
Edit	Updates the location information and returns to the Locations section.
Delete	Deletes the location information, and moves the host to the Unknown location section.
Cancel	Cancels the add or edit operation, and returns to the Locations section.

Managing the host

Adding an Appliance Virtualization Platform or ESXi host

About this task

Use the procedure to add an Appliance Virtualization Platform or ESXi host. You can associate an ESXi host with an existing location.

If you are adding an standalone ESXi host to System Manager Solution Deployment Manager or to the Solution Deployment Manager client, add the standalone ESXi host using its FQDN only.

Solution Deployment Manager only supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add a host other than the Appliance Virtualization Platform and VMware ESXi hosts, the system displays the following error message:

```
Retrieving host certificate info is failed: Unable to communicate with
host. Connection timed out: connect. Solution Deploymnet Manager only
supports host management of VMware-based hosts and Avaya Appliance
Virtualization Platform (AVP).
```

Before you begin

A location must be available.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, click **Add**.
4. In the New Host section, provide the Host name, IP address or FQDN, user name, and password.
5. Click **Save**.
6. On the Certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can only accept the certificate. If the certificate is invalid, to generate certificate, see the VMware documentation.

   In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. On the **Virtual Machines** tab, in the VMs for Selected Location <location name> section, select the required virtual machine.
   b. Click **More Actions** > **Re-establish connection**.

For more information, see “Re-establishing trust for Solution Deployment Manager elements”.

c. Click **More Actions** > **Refresh VM**.

Important:

When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.

8. On the **Hosts** tab, select the required host and click **Refresh**.

Next steps

After adding a new host under VM Management Tree, the refresh host operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. Under VM Management Tree, establish trust for all the virtual machines that are deployed on the host.
2. Ensure that the system populates the **Application Name** and **Application Version** for each virtual machine.
3. Once you have performed a trust establishment and refresh host operation on all virtual machines, you can perform refresh operation on the host.

Related links

New and Edit host field descriptions on page 80
Generating and accepting certificates on page 86

Editing an ESXi host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host that you want to update.
4. Change the ESXi host information.
5. Click **Save**.

   The system updates the ESXi host information.

Related links

New and Edit host field descriptions on page 80

Upgrading Appliance Virtualization Platform from Solution Deployment Manager

About this task

Upgrade Appliance Virtualization Platform from Release 7.0.x or 7.1.x to Release 7.1.3 by using upgrade bundle from the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Note:

- From System Manager Solution Deployment Manager, you cannot update Appliance Virtualization Platform that hosts this System Manager.
- When you update Appliance Virtualization Platform, the system shuts down all the associated virtual machines and restarts the Appliance Virtualization Platform host. During the update process, the virtual machines will be out of service. Once Appliance Virtualization Platform update is complete, the system restarts the virtual machines.
- If you are upgrading or updating the Appliance Virtualization Platform host, then you must not restart, shutdown, upgrade, or install the patch on the virtual machine that is hosted on the same Appliance Virtualization Platform host.

  If you are deploying or upgrading a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.

  If you are installing a patch on a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.
- If you are using services port to update or upgrade Appliance Virtualization Platform, connect the system directly with the Appliance Virtualization Platform services port (Gateway 192.168.13.1). If you connect the system using the Utility Services services port (Gateway 192.11.13.1), the Appliance Virtualization Platform update or upgrade fails.

Before you begin

1. Add a location.
2. Add a host.
3. Enable the SSH service on the Appliance Virtualization Platform host.

Note:

Install only Avaya-approved service packs or software patches on Appliance Virtualization Platform. Do not install the software patches that are downloaded directly from VMware®.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.

3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **AVP Update/Upgrade Management**.
4. On the Update Host page, click **Select Patch from Local SMGR**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.

   For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-7.1.2.0.0.xx.zip`.

   In the Hosts for Selected Location <location name> section, the system displays the update status in the **Current Action** column.
6. On the AVP Update/Upgrade - Enhanced Access Security Gateway (EASG) User Access page, read the following messages, and do one of the following:

   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 Avaya Logins you are preventing Avaya access to your
   system.
   This is not recommended, as it impacts Avaya's ability to provide
   support for the product. Unless the customer is well versed in
   managing the product themselves, Avaya Logins should not be
   disabled.
   ```

   a. To enable EASG, click **Enable EASG**.

      Avaya recommends to enable EASG.

      You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

   b. To disable EASG, click **Disable EASG**.
7. On the EULA Acceptance page, read the EULA, and do one of the following:

   a. To accept the EULA, click **Accept**.

   b. To decline the EULA, click **Decline**.
8. To view the details, in the **Current Action** column, click **Status Details**.

Host Create/Update Status window displays the details. The patch installation takes some time. When the patch installation is complete, the **Current Action** column displays the status.

Next steps

If virtual machines that were running on the Appliance Virtualization Platform host does not automatically start, manually start the machines.

Related links

Update Host field descriptions on page 84

Changing the network parameters for an Appliance Virtualization Platform host

About this task

Use this procedure to change the network parameters of Appliance Virtualization Platform after deployment. You can change network parameters only for the Appliance Virtualization Platform host.

Note:

If you are connecting to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. Therefore, after the IP address changes, close Solution Deployment Manager, and restart Solution Deployment Manager by using the new IP address to reconnect.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnetmask, and other parameters as appropriate.

   Note:

   An Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

   If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:

   - Public or signaling traffic, Appliance Virtualization Platform, and all virtual machines public traffic.

- Management, Appliance Virtualization Platform, and all virtual machine management ports.

5. To change the gateway IP address, perform the following:
   a. Click **Change Gateway**.

      The **Gateway** field becomes available for providing the IP address.

   b. In **Gateway**, change the IP address.
   c. Click **Save Gateway**.
6. Click **Save**.

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 81

Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager

About this task

With Appliance Virtualization Platform, you can team NICs together to provide a backup connection when the server NIC or the Ethernet switch fails. You can also perform NIC teaming from the command line on Appliance Virtualization Platform.

Appliance Virtualization Platform supports Active-Standby and Active-Active modes of NIC teaming. For more information, see “NIC teaming modes”.

Note:

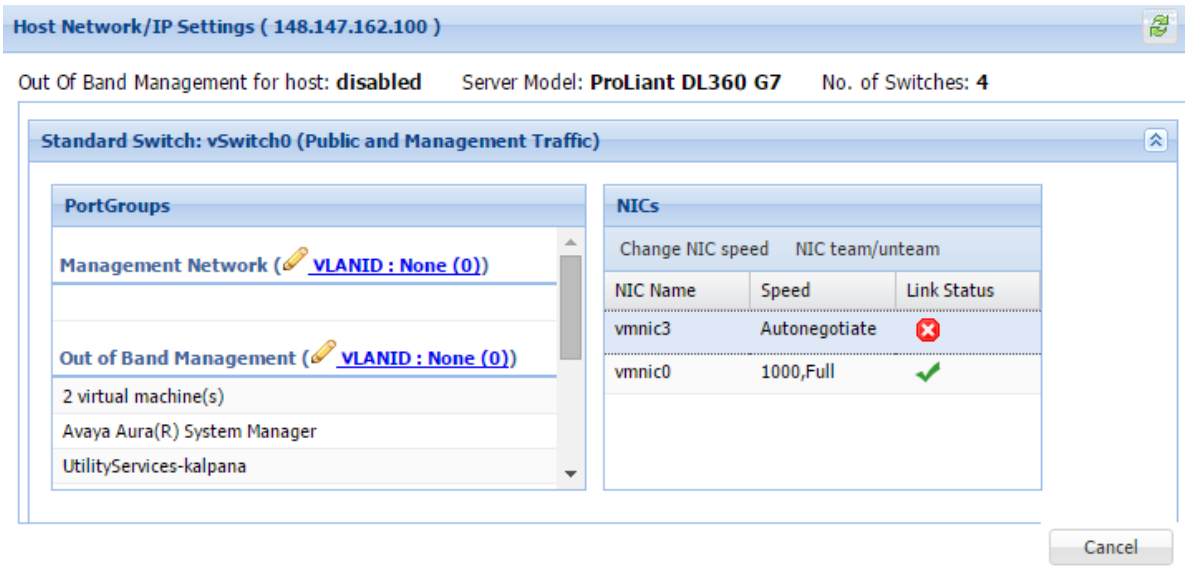
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fails because public IP address cannot be reached with the service port. To avoid this error, edit the host with the service port IP address again.
- If FQDN of the Appliance Virtualization Platform host is updated by using Host Network/IP setting for domain name, refresh the host to get the FQDN changes reflect in Solution Deployment Manager.

Use this procedure to change network settings, such as changing VLAN ID, NIC speed, and NIC team and unteaming for an Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params** > **Change Network Settings**.



The Host Network/ IP Settings page displays the number of switches as 4.

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.
- **vSwitch3**. No reservations.

5. To change VLAN ID, perform the following:
   a. To expand the Standard Switch: vSwitch<n> section, click .

      The section displays the vSwitch details.

   b. Click on the VLANID link or the edit icon ( ).

      The system displays the Port Group Properties page where you can edit the VLAN ID port group property.

   c. In **VLAN ID**, select an ID from the available values.

      For more information about the value, see NIC teaming.

   d. Click **OK**.

The system displays the new VLAN ID.

Note:

You can change the services port VLAN ID for S8300D servers only through Solution Deployment Manager.

6. To change the NIC speed, perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.

      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.

      For more information, see VLAN ID assignment.

   The system displays the updated NIC speed in the **Speed** column.

   If the NIC is connected, the system displays ✔ in **Link Status**.

   Note:

   You can change the speed only for common servers. You cannot change the speed for S8300D and S8300E servers.
7. To change the NIC teaming, perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.

      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or unteaming, select the vmnic and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.

      For more information, see NIC teaming modes.
   d. Click **OK**.

      The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.
   e. To check the status of the vmnic, click **NIC team/ unteam**.
8. To get the latest data on host network IP settings, click **Refresh**.

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for S8300D and S8300E servers.

Related links

Host Network / IP Settings field descriptions on page 82

Changing the password for an Appliance Virtualization Platform host

About this task

You can change the password for the Appliance Virtualization Platform host. This is the password for the administrator that you provide when installing the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **More Actions** > **Change Password**.
4. In the Change Password section, type the current password and the new password.

   For more information about password rules, see “Password policy”.
5. Click **Change Password**.

   The system updates the password of the Appliance Virtualization Platform host.

Related links

Password policy on page 65
Change Password field descriptions on page 83

Password policy

The password must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.
- Must not contain an uppercase letter at the beginning and a digit or a special character at the end.

Examples of invalid passwords:

- Password1: Invalid. Uppercase in the beginning and a digit at the end.
- Password1!: Uppercase in the beginning and a special character at the end.

Example of a valid password: myPassword!1ok

If the password does not meet the requirements, the system prompts you to enter a new password. Enter the existing password and the new password in the correct fields.

Ensure that you keep the admin password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.

Related links

Changing the password for an Appliance Virtualization Platform host on page 65

Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Generate AVP Kickstart**.
3. On **Create AVP Kickstart**, enter the appropriate information, and click **Generate Kickstart File**.

   The system prompts you to save the generated kickstart file on your local computer.

Related links

Create AVP Kickstart field descriptions on page 66

Create AVP Kickstart field descriptions

Name	Description
Choose AVP Version	The field to select the release version of Appliance Virtualization Platform.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. The options are: • **yes**: To enable the IPv6 format. • **no**: To disable the IPv6 format.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters

Table continues…

Name	Description
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300D and E only)	VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on S8300D and S8300E servers.
Out of Band Management Setup	The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • **yes**: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • **no**: To disable Out of Band Management. The default option.
OOBM vLAN ID (Used on S8300D and E only)	Out of Band Management VLAN ID for S8300D. Use **OOBM VLAN ID** only on the S8300D server. • For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.

Table continues…

Name	Description
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Confirm Password	Admin password for Appliance Virtualization Platform.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain 14 characters.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Generate Kickstart File	Generates the Appliance Virtualization Platform kickstart file and the system prompts you to save the file on your local computer.

Related links

Generating the Appliance Virtualization Platform kickstart file on page 66

Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, click **More Actions** > **SSH** > **Enable SSH**.
5. On the Confirm dialog box, in the **Time (in minutes)** field, type the time after which the system times out the SSH connection.

   The value range is from 10 minutes through 120 minutes.
6. Click **Ok**.

   The system displays `enabled` in the **SSH status** column.

7. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

   The system displays `disabled` in the **SSH status** column.

Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform.

You can enable SSH, disable SSH, and check the SSH status on the Appliance Virtualization Platform host.

Before you begin

Start an SSH session.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Navigate to the `$MGMT_HOME/infra/bin/avpSSHUtility` location.
3. Type `./enableDisableSSHOnAVP.sh`.

   The system displays the following options:

   - Enable SSH on the Appliance Virtualization Platform host.
   - Disable SSH on the Appliance Virtualization Platform host.
   - Check the SSH status on the Appliance Virtualization Platform host.
4. To enable SSH, perform the following:
   a. At the prompt, type `1` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.
   c. Type the time in minutes.

      The time is the duration after which the system blocks any new SSH connections. The valid range 10 to 120 minutes.

      The system displays the message and enables SSH on Appliance Virtualization Platform host.

   For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.
5. To disable SSH, perform the following:
   a. At the prompt, type `2` and press `Enter`.

b. Type the IP address of the Appliance Virtualization Platform host.

If SSH is already disabled, the system displays `False` and the message `SSH is already disabled. No operation performed. Exiting`.

6. **(Optional)** To view the status of SSH, perform the following:
   a. At the prompt, type `3` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is enabled, the system displays `Is SSH enable — false`.

   If SSH is disabled, the system displays `Is SSH disable — true`.

Changing the IP address and default gateway of the host

About this task

When you change the default gateway and IP address from the vSphere, the change might be unsuccessful.

You cannot remotely change the IP address of the Appliance Virtualization Platform host to a different network. You can change the IP address remotely only within the same network.

To change the Appliance Virtualization Platform host to a different network, perform Step 2 or Step 3.

Before you begin

Connect the computer to the services port.

Procedure

1. Using an SSH client, log in to the Appliance Virtualization Platform host.
2. Connect the Solution Deployment Manager client to services port on the Appliance Virtualization Platform host, and do the following:
   a. To change the IP address, at the command prompt of the host, type the following:

   ```
   esxcli network ip interface ipv4 set -i vmk0 -I <old IP address of the host>
   -N <new IP address of the host> -t static
   ```

   For example:

   ```
   esxcli network ip interface ipv4 set -i vmk0 -I 135.27.162.121 -N 255.255.25
   5.0 -t static
   ```

   b. To change the default gateway, type `esxcfg-route <new gateway IP address>`.

   For example:

   ```
   esxcfg-route 135.27.162.1
   ```

3. Enable SSH on the Appliance Virtualization Platform host and run the **`./serverInitialNetworkConfig`** command.

For more information, see Configuring servers preinstalled with Appliance Virtualization Platform.

Appliance Virtualization Platform license

From Appliance Virtualization Platform Release 7.1.2, you must install an applicable Appliance Virtualization Platform host license file on an associated Avaya WebLM server and configure Appliance Virtualization Platform to obtain its license from the WebLM server. WebLM Server can be either embedded System Manager WebLM Server or standalone WebLM Server. Appliance Virtualization Platform licenses are according to the supported server types. The following table describes the applicable Appliance Virtualization Platform license type according to the supported server types.

Server type	Appliance Virtualization Platform license feature keyword	Appliance Virtualization Platform license feature display name
• Avaya S8300D • Avaya S8300E	VALUE_AVP_1CPU_EMBD_SRVR	Maximum AVP single CPU Embedded Servers
Common Server Release 1 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R610 Common Server Release 2 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R620 Common Server Release 3 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9	• VALUE_AVP_1CPU_CMN_SRVR • VALUE_AVP_2CPU_CMN_SRVR	• Maximum AVP single CPU Common Servers • Maximum AVP dual CPU Common Servers
Common Server Release 3 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9	VALUE_AVP_XL_SRVR	Maximum AVP XL Server

To configure the Appliance Virtualization Platform license file:

1. Obtain the applicable license file from the Avaya PLDS website.
2. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

Note:

The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance

Virtualization Platform license file contains all the necessary licenses for the complete solution.

3. Configure the applicable **WebLM IP Address/FQDN** field for each Appliance Virtualization Platform host by using either System Manager Solution Deployment Manager, Solution Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

You can view the license status of the Appliance Virtualization Platform host on the **Hosts** tab of the System Manager Solution Deployment Manager or Solution Deployment Manager Client interfaces. The Appliance Virtualization Platform license statuses on the **Hosts** tab are:

- **Normal:** If the Appliance Virtualization Platform host has acquired a license, the **License Status** column displays **Normal**.
- **Error:** If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The **License Status** column displays **Error - Grace period expires: <DD/MM/YY> <HH:MM>**.
- **Restricted:** If the 30-day grace period of the Appliance Virtualization Platform license expires, Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The **License Status** column displays **Restricted**. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

  on the configured WebLM Server, full administrative functionality will be restored.

  Note:

  Restricted administrative actions for:

  - **AVP Host: AVP Update/Upgrade Management**, **Change Password**, **Host Shutdown**, and **AVP Cert. Management**.
  - **Virtual Machine: New**, **Delete**, **Start**, **Stop**, and **Update**.

Appliance Virtualization Platform licensing alarms

If the Appliance Virtualization Platform license enters either License Error Mode or License Restricted Mode, the system generates a corresponding Appliance Virtualization Platform licensing alarm. You must configure the Appliance Virtualization Platform alarming. For information about how to configure the Appliance Virtualization Platform alarming feature, see *Accessing and Managing Avaya Aura® Utility Services*.

Configuring WebLM Server for an Appliance Virtualization Platform host

Before you begin

1. Add an Appliance Virtualization Platform host.

   For information about adding a host, see “Adding an Appliance Virtualization Platform or ESXi host”.

2. Obtain the license file from the Avaya PLDS website.

3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions** > **WebLM Configuration**.

      The system displays the WebLM Configuration dialog box.
4. In **WebLM IP Address/FQDN**, type the IP address or FQDN of WebLM Server.

   For WebLM configuration, if you select:

   - Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.
   - Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.
5. In **Port Number**, type the port number of WebLM Server.

   Embedded System Manager WebLM Server supports both 443 and 52233 ports.
6. Click **Submit**.

   The system displays the status in the **Current Action** column.

   The system takes approximately 9 minutes to acquire the Appliance Virtualization Platform host license file from the configured WebLM Server. On the **Hosts** tab, you can click the **Refresh** icon.

   When the Appliance Virtualization Platform host acquires the license, on the **Hosts** tab, the **License Status** column displays **Normal**.

WebLM Configuration field descriptions

Name	Description
WebLM IP Address/FQDN	The IP Address or FQDN of WebLM Server.
Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Submit	Saves the WebLM Server configuration.

Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager

Procedure

1. Perform one of the following:
   - On the System Manager Web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - On the desktop, click the SDM icon (), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Shutting down the Appliance Virtualization Platform host

About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Lifecyle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Client or through the Solution Deployment Manager client.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.
4. Click **More Actions** > **Lifecyle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

   The system restarts the host and virtual machines running on the host.

Removing an ESXi host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Host tab, in the Hosts for Selected Location <location name> section, select one or more hosts that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

Configuring the login banner for the Appliance Virtualization Platform host

About this task

You can configure a login banner message on one or more Appliance Virtualization Platform hosts at a time.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in Hosts for Selected Location <location name>, select one or more Appliance Virtualization Platform hosts on which you want to configure the message.
4. Click **More Actions** > **Push Login Banner**.

   You can change the login banner text only on the Security Settings page from **Security** > **Policies** on System Manager.
5. On the Message of the Day window, click **Push Message**.

   The system updates the login banner on the selected Appliance Virtualization Platform hosts.

Mapping the ESXi host to an unknown location

About this task

When you delete a location, the system does not delete the virtual machines running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**. You can configure the location of an ESXi host again.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the left navigation pane, click the **Unknown location host mapping** link.
3. In the Host Location Mapping section, select an ESXi host and click **Edit**.

   The system displays the Host Information page.
4. Select a location to which you want to map the ESXi host.
5. Click **Submit**.

   The system displays the ESXi host in the selected location.

Applying third-party AVP certificates

Applying third-party Appliance Virtualization Platform certificates

About this task

Use this procedure to create, download, upload, and push third-party Appliance Virtualization Platform certificates, and push the certificates to Appliance Virtualization Platform hosts.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.
- Ensure that the certificate is valid on the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. To generate CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.

b. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

c. Click **View/Generate CSR**.

The system displays the View/Generate CSR dialog box.

d. Add or edit the details of the generic CSR.

For more information, see “Creating or editing generic CSR”.

e. Click **Generate CSR**.

The system generates CSR for the Appliance Virtualization Platform host.

f. To view the status, in the **Upgrade Status** column, click **Status Details**.

The time required for the complete process varies depending on the data on System Manager.

5. To download CSR, do the following:

a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.

b. Click **Download CSR**.

c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

d. To view the status, in the **Upgrade Status** column, click **Status Details**.

The time required for the complete process varies depending on the data on System Manager.

e. When the system displays a prompt, save the file.

6. Extract the downloaded certificates, and ensure that the third-party signs them.

7. To upload and push the signed certificate from third-party CA, do the following:

a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.

b. Click **Browse** and select the required certificates for one or more Appliance Virtualization Platform hosts.

c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

d. Agree to add the same certificate on Solution Deployment Manager.

e. Click **Push Certificate**.

f. To view the status, in the **Upgrade Status** column, click **Status Details**.

The time required for the complete process varies depending on the data on System Manager.

Creating or editing generic CSR

About this task

Use this procedure to create or edit a generic CSR for third-party Appliance Virtualization Platform certificates. With a generic CSR, you can apply the same set of data for more than one Appliance Virtualization Platform host.

Procedure

1. In VM Management Tree, select a location.
2. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions** > **AVP Cert. Management** > **Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

Next steps

Complete the CSR generation, download, third-party signing and push the certificates to the Appliance Virtualization Platform hosts.

Load AVP host certificate field descriptions

Name	Description
Host IP	The IP address of the Appliance Virtualization Platform host.
Host FQDN	The FQDN of the Appliance Virtualization Platform host.
Certificate	The option to select the signed certificate for the Appliance Virtualization Platform host.
I agree to accept to add the same certificate in SDM.	The option to accept the certificate in Solution Deployment Manager.

Button	Description
Browse	Displays the dialog box where you can choose the signed certificate file. The accepted certificate file formats are: • `.crt` • `.pki`
Retrieve Certificate	Displays the Certificate dialog box with the details of the uploaded signed certificate.
Push Certificate	Pushes the uploaded signed certificate to the selected Appliance Virtualization Platform host.
Cancel	Cancels the push operation.

Create or edit CSR field descriptions

Name	Description
Organization	The organization name of the CSR.
Organization Unit	The organization unit of the CSR.
Locality	The locality of the organization associated with the CSR.
State	The state of the organization associate with the CSR.
Country	The country of the organization associate with the CSR. In the Edit mode, you can specify only two letters for the country name.
Email	The email address associate with the CSR.

Button	Description
Create/Edit CSR	Saves or edits the information entered associated to the CSR.
Cancel	Cancels the add or edit operation of the CSR.

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

Use this procedure to delete the virtual machine snapshots that reside on the Appliance Virtualization Platform host by using Solution Deployment Manager.

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 VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host.
4. Click **More Actions** > **Snapshot Manager**.

   The system displays the Snapshot Manager dialog box.
5. Select one or more snapshots, and click **Delete**.

   The system deletes the selected snapshots.

Related links

Snapshot Manager field descriptions on page 80

Snapshot Manager field descriptions

Name	Description
VM ID	The ID of the virtual machine.
Snapshot Age	The duration of snapshot creation. For example: 75 days 19 hours
VM Name	The name of the virtual machine.
Snapshot Name	The name of the snapshot.
Snapshot Description	The description of the snapshot.
SDM Snapshot	The snapshot taken from Solution Deployment Manager. The options are **Yes** and **No**.

Button	Description
Cancel	Exits from the Snapshot Manager dialog box.
Delete	Deletes the selected snapshot.

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 79

New and Edit host field descriptions

Name	Description
Location	The location where the host is available. The field is read only.
Host Name	The hostname of Appliance Virtualization Platform or the ESXi host.
Host FQDN or IP	The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.
User Name	The user name to log in to Appliance Virtualization Platform or the ESXi host. **Note:** For Appliance Virtualization Platform, provide the admin credentials that you configured while generating the Kickstart file.
Password	The password to log in to Appliance Virtualization Platform or the ESXi host.

Button	Description
Save	Saves the host information and returns to the Hosts for Selected Location <location name> section.

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IPv4	The IPv4 address of the Appliance Virtualization Platform host.
Subnet Mask	The subnet mask the Appliance Virtualization Platform host.
IPv6	The IPv6 address of the Appliance Virtualization Platform host (if any).
Host Name	The host name the Appliance Virtualization Platform host
Domain Name	The domain name the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
NTP Server1 IP/FQDN	The NTP Server1 IP address of the Appliance Virtualization Platform host.
NTP Server2 IP/FQDN	The NTP Server2 IP address of the Appliance Virtualization Platform host.
IPv4 Gateway	The gateway IPv4 address. The field is available only when you click **Change IPv4 Gateway**.
IPv6 Default Gateway	The default gateway IPv6 address (if any). The field is available only when you IPv6 has been configured for the system. The user, also needs to click **Change IPv6 Gateway**.

Button	Description
Change IPv4 Gateway	Makes the **IPv4 Gateway** field available, and displays **Save IPv4 Gateway** and **Cancel IPv4 Gateway Change** buttons.

Table continues…

Button	Description
Change IPv6 Gateway	Makes the **IPv6 Default Gateway** field available, and displays **Save IPv6 Default Gateway** and **Cancel IPv6 Default Gateway Change** buttons.
Save IPv4 Gateway	Saves the gateway IPv4 address value that you provide.
Cancel IPv4 Gateway Change	Cancels the changes made to the IPv4 gateway.
Save IPv6 Default Gateway	Saves the default IPv6 gateway address value that you provide.
Cancel IPv6 Default Gateway Change	Cancels the changes made to the IPv6 default gateway.

Button	Description
Save	Saves the changes that you made to network parameters.

Host Network / IP Settings field descriptions

Port Groups

Standard Switch vSwitch <n> displays the Port Groups and NICs sections.

Name	Description
or **VLAN ID** link	Displays the Port Group Properties page where you configure VLAN ID.
VLAN ID	Displays the VLAN ID. The options are: • **None (0)** • **1 to 4093** The field displays only unused IDs.
OK	Saves the changes.

NIC speed

Button	Description
Change NIC speed	Displays the vmnic<n> dialog box.

Name	Description
Configured speed, Duplex	Displays the NIC speed. The options are: • **Autonegotiate** • **10,Half** • **10,Full** • **100,Half** • **100,Full** • **1000,Full**
OK	Saves the changes.

NIC teaming

Button	Description
NIC team/unteam	Displays the Out of Band Management Properties vSwitch<n> dialog box.

Button	Description
Move Up	Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.
Move Down	Moves the VMNIC from active to standby adapter or from standby to unused adapter.
Refresh	Refreshes the page.
OK	Saves the changes.

Change Password field descriptions

Name	Description
Current Password	The password for the user you input when adding the host.
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Update Host field descriptions

Name	Description
Patch location	The location where the Appliance Virtualization Platform patch is available. The options are: • **Select Patch from Local SMGR**: To use the Appliance Virtualization Platform patch that is available on the local System Manager. • **Select Patch from software library**: To use the Appliance Virtualization Platform patch that is available in the software library.
Ignore Signature Validation	Ignores the signature validation for the patch. **Note:** If the Appliance Virtualization Platform patch is unsigned, you must select the **Ignore signature validation** check box.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Installs the patch on the Appliance Virtualization Platform host.

Certificate validation

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

You can check the following with certificate-based TLS sessions:

- Certificate valid dates

- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state

Note:

Only System Manager Release 7.1 and later supports **OCSP**. Other elements of Avaya Aura® Suite do not support **OCSP**.

- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Validates the certificates when a virtual machine is deployed or upgraded on vCenter managed hosts

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can open the web page of the host. The system displays the existing certificate and you can match the details.

Generating and accepting certificates

About this task

With Solution Deployment Manager, you can generate certificates only for Appliance Virtualization Platform hosts.

For the VMware ESXi hosts, if the certificate is invalid:

- Get a correct certificate for the host and add the certificate.
- Regenerate a self-signed certificate on the host.

  For more information, see “Generating new self-signed certificates for the ESXi host”.

Before you begin

Require permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **AVP Cert. Management** > **Generate/Accept Certificate**.
5. On the Certificate window, do the following:
   a. Click **Generate Certificate**.

      Note:

      You can generate certificate only for the Appliance Virtualization Platform host.

   b. Click **Accept Certificate**.

   In the Hosts for Selected Location <location name> section, the **Host Certificate** column must display ✔.

Next steps

If the system displays an SSL verification error when you gain access to the Appliance Virtualization Platform host from the vSphere client, restart the Appliance Virtualization Platform host.

Related links

Adding an Appliance Virtualization Platform or ESXi host on page 57
Generating new self-signed certificates for the ESXi host on page 89

Updating the certificate on the ESXi host from VMware

About this task

Use the procedure to update the ESXi host certificate.

For information about updating vCenter certificates, see the VMware documentation.

Before you begin

Start an SSH session on the ESXi host.

Procedure

1. Start vSphere Web Client, and log in to the ESXi host as admin or root user.
2. Ensure that the domain name and the hostname of the ESXi host is set correctly and matches the FQDN that is present on the DNS servers, correct the entries to match if required.

   For security reason, the common name in the certificate must match the hostname to which you connect.
3. To generate new certificates, type `/sbin/generate-certificates`.

   The system generates and installs the certificate.
4. Restart the ESXi host.
5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. From the Direct Console User Interface (DCUI), restart management agents.

      Note:

      The host certificate must now match the fully qualified domain name of the host.

      VMware places only FQDN in certificates that are generated on the host. Therefore, use a fully qualified domain name to connect to ESXi hosts and vCenter from Solution Deployment Manager.

      Appliance Virtualization Platform places an IP address and FQDN in generated certificates. Therefore, from Solution Deployment Manager, you can connect to Appliance Virtualization Platform hosts through IP address or FQDN.

      The connection from Solution Deployment Manager 7.1 to a vCenter or ESXi host by using an IP address fails because the IP address is absent in the certificate and the connection is not sufficiently secure.

Related links

Generating new self-signed certificates for the ESXi host on page 89

Managing certificates for existing hosts

About this task

By default, the certificate status of the host or vCenter that is migrated from earlier release is invalid. To perform any operation on the host from Solution Deployment Manager, you require a valid certificate. Therefore, you must get the valid certificate and accept the certificate.

Depending on the host type and the validity of the certificate, use appropriate steps to generate the certificate, and then accept the certificate.

Before you begin

Require permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.
4. **(Optional)** On an Appliance Virtualization Platform host, click **More Actions** > **Generate/ Accept Certificate**, and on the Certificate dialog box, do one of the following:
   - If the certificate is valid, click **Accept Certificate**.
   - If the certificate is invalid, click **Generate Certificate**, and then click **Accept Certificate**.
5. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions** > **Generate/ Accept Certificate**, and click **Accept Certificate**.
   - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

     For more information, see “Generating new self-signed certificates for the ESXi host”.
6. For vCenter, do the following:
   a. Click **Map vCenter**, select the vCenter server, and click **Edit**.
   b. In the Certificate dialog box, accept certificate, and click **Save**.

Related links

Generating new self-signed certificates for the ESXi host on page 89
Generating and accepting certificates on page 86

Generating new self-signed certificates for the ESXi host

About this task

Generate new certificates only if you change the host name or accidentally delete the certificate. Under certain circumstances, you must force the host to generate new certificates.

To receive the full benefit of certificate checking, particularly if you want to use encrypted remote connections externally, do not use a self-signed certificate. Instead, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

Before you begin

Start an SSH session on the ESXi host.

Procedure

1. Log in to the ESXi host as an admin user.
2. To create a backup of any existing certificates, in the `/etc/vmware/ssl` directory, rename the certificates by using the following commands:

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```

   Note:

   Do not perform the step if you are regenerating certificates because you deleted the certificates.
3. To generate new certificates, type `/sbin/generate-certificates`.
4. Restart the ESXi host.

   The generation process places the certificates places in the correct location.
5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. Restart management agents from Direct Console User Interface (DCUI).
6. Do the following to confirm that the host successfully generated new certificates:
   a. Type `ls -la`.
   b. Compare the time stamps of the new certificate files with `orig.rui.crt` and `orig.rui.key`.

Next steps

Replace the self-signed certificate and the key with a trusted certificate and key.

Managing the virtual machine

Deploying the Utility Services OVA file through System Manager Solution Deployment Manager

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy Utility Services OVA on the Avaya-provided server.

To deploy Utility Services, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable. First deploy the Utility Services OVA and then deploy all other applications one at a time.

Before you begin

- Complete the deployment checklist.

  For information about the deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.
- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.

      The system displays the host name in the **Host FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The page displays the capacity details.
6. Click **Next**.
7. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.

b. In **Select OVAs**, select the OVA file that you want to deploy.

c. In **Flexi Footprint**, select the footprint size that the application supports.

- **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
- **Default**: For all other server platforms.

8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

9. In the Network Parameters section, ensure that the following fields are preconfigured:

   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled

   For more information, see “VM Deployment field descriptions”.

10. In the Configuration Parameters section, complete the fields.

    For more information about Configuration Parameters, see Network Parameters and Configuration Parameters field descriptions.

11. Click **Deploy**.

12. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.

13. To view details, click the **Status Details** link.

    For information about VM Management field descriptions, see *Deploying Avaya Aura® applications from System Manager*.

14. Reboot the Utility Services virtual machine.

Next steps

1. To activate the serviceability agent registration, reset the Utility Services virtual machine.
2. Deploy all other Avaya Aura® applications one at a time.

Related links

VM Deployment field descriptions on page 102
Network Parameters and Configuration Parameters field descriptions

Deploying an OVA file for an Avaya Aura® application

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy OVA for an Avaya Aura® application on the virtual machine.

To deploy an Avaya Aura® application, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client if System Manager is unavailable.

Deploy Utility Services first, and then deploy all other applications one at a time.

Before you begin

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Ensure that the certificate is valid on the Appliance Virtualization Platform host or vCenter managed hosts.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.

      The system displays the host name in the **Host FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The page displays the capacity details.
6. Click **Next**.
7. To get the OVA file, select the **OVA** tab, and do one of the following:
   - Click **URL**, in **OVA File**, type the absolute path to the OVA file, and click **Submit**.
   - Click **S/W Library**, in **File Name**, select the OVA file.
   - Click **Browse**, select the required 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 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 for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
   - Click **URL**, and provide the absolute path to the latest service or feature pack.
   - Click **S/W Library**, and select the latest service or feature pack.
   - Click **Browse**, and select the latest service or feature pack.

   You can install the patch file for the Avaya Aura® application now or after completing the Avaya Aura® application OVA deployment.
10. Click **Next**.

    In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
11. In the Network Parameters section, ensure that the following fields are preconfigured:
    - **Public**
    - **Services**: Only for Utility Services
    - **Out of Band Management**: Only if Out of Band Management is enabled

    For more information, see “VM Deployment field descriptions”.
12. In the Configuration Parameters section, complete the fields.

    For each application that you deploy, fill the appropriate fields. For more information, see “VM Deployment field descriptions”.
13. Click **Deploy**.
14. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.
15. To view details, click **Status Details**.

Next steps

Related links

Installing software patches on page 94
VM Deployment field descriptions on page 102

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with a virtual machine using the Solution Deployment Manager client.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> area, select a virtual machine.
4. Click **More Actions** > **Re-establish connection**.
5. Select the release version of the product deployed on the virtual machine.
6. Enter the user name and password for virtual machines with the following versions:
   - **7.0**
   - **others**
7. Click **Reestablish Connection**.

Installing software patches

About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Note:

When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions** > **Installed Patches** on the Upgrade Management page, then perform the following:

1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
2. Refresh the element.

Before you begin

- Perform the preupgrade check.

- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. To view the update status, click .

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display .

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Editing a virtual machine

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
  - Utility Services must be available and must be discovered.
  - If Utility Services is discovered, the system must display Utility Services in the **VM App Name** column. If the application name in **VM App Name** is empty, perform the following to establish trust between the application and System Manager:
    - Click **More Actions** > **Re-establish connection**.
    - Click **More Actions** > **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.

The system displays the Edit VMs section.

4. **(Optional)** Click **Change Flexi Footprint** and do the following:
   a. Click **Change flexi foot print value**.
   b. In **Flexi Footprint**, select a foot print that the application supports.

   Important:

   Each application must ensure that only the supported flexible footprint is selected.
5. To update the IP address and FQDN of the virtual machine, perform the following:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for Utility Services, establish trust on all virtual machines that are running on the host on which Utility Services resides.
   b. Click **More Actions** > **Refresh VM**.

      Note:

      To update IP address or FQDN for Utility Services, refresh all virtual machines that are running on the host on which Utility Services resides.
   c. Click **Update IP/FQDN in Local Inventory**.
   d. Click **Update VM IP/FQDN**.
   e. Provide the IP address and FQDN of the virtual machine.

      Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.
6. Click **Save**.

Deleting a virtual machine

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the right navigation pane, click **Virtual Machines**.
4. On the Virtual Machines page, select one or more virtual machines.
5. On the Delete page, click **Delete**, and click **Yes** to confirm the deletion.

   The system turns off the virtual machines, and deletes the selected virtual machines from the host.

Changing the network parameters of Appliance Virtualization Platform and Avaya Aura® applications

About this task

Change the network parameters for Appliance Virtualization Platform and each Avaya Aura® application from the application, and then change the IP address and FQDN of Avaya Aura® applications and Appliance Virtualization Platform from Solution Deployment Manager.

Before you begin

- Connect the system on which Solution Deployment Manager is running to the new network for changing network parameters.
- When many Avaya Aura® applications are running on an Appliance Virtualization Platform host, ensure that you change the network parameter in the following order:
  1. Appliance Virtualization Platform
  2. Avaya Aura® applications that are running on the host except Utility Services.
  3. Utility Services

Note:

If you fail to follow the order, Utility Services network parameter update might fail.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Network Parameters section, change the following as appropriate, and click **Save**:
   - IP address, subnetmask, and other parameters
   - Gateway IP address

   For more information, see “Change Network Parameters field descriptions”.
5. Change the network parameters first for each Avaya Aura® application on the host, and then for Utility Services.

   For more information, see *Administering Avaya Aura® application* available for each application. Also, see “Network Parameters for Avaya Aura® applications”.
6. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services:
   a. In the Edit VMs section, select a virtual machine and click **Edit**.

b. Click **Update IP/FQDN in Local Inventory**.

c. Click **Update VM IP/FQDN**.

d. Provide the IP address and FQDN of the virtual machine.

Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.

7. Click **Save**.
8. Do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services :

a. Click **More Actions** > **Re-establish connection**.

Note:

To update IP address or FQDN for Utility Services , establish trust on all virtual machines that are running on the host on which Utility Services resides.

b. Click **More Actions** > **Refresh VM**.

Note:

To update IP address or FQDN for Utility Services, refresh all virtual machines that are running on the host where Utility Services resides.

When you update the IP address and FQDN for Utility Services, the system also updates the Services Port static route for each application.

Related links

Change Network Parameters field descriptions on page 81
Changing the network parameters for an Appliance Virtualization Platform host on page 61
Network parameter update for Avaya Aura applications on page 113

Updating Services Port Static Routing on an Avaya Aura® application

About this task

You might have to change the static routing if the Avaya Aura® application that is running on the Appliance Virtualization Platform host is:

- Deployed by using the vSphere client and does not have the route.
- Non-operational or unreachable when you start the Avaya Aura® application update.

Before you begin

- Update network parameters of Utility Services if applicable.

- Ensure that the Avaya Aura® application resides on the same subnetwork as Utility Services.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select an Avaya Aura® application.
3. Click **More Actions** > **Update Static Routing**.

   The VM Update Static Routing page displays the details of Avaya Aura® application and Utility Services. The fields are read-only.
4. Click **Update**.
5. On the Success dialog box, click **OK**.

   The system updates the Avaya Aura® application with the new IP address of Utility Services for Services Port static routing.

Related links

Update Static Routing field descriptions on page 111

Starting a virtual machine from Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to start.
4. Click **Start**.

   In **VM State**, the system displays `Started`.

Stopping a virtual machine from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.

3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.
4. Click **Stop**.

   In **VM State**, the system displays `Stopped`.

Restarting a virtual machine from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.
- Virtual machines must be in the running state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to restart.
4. Click **Restart**.

   In **VM State**, the system displays `Stopped` and then `Started`.

Common causes for VM deployment failure

If the virtual machine is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the VM to not work properly
- Chosen a private virtual network

Following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as `0.0.0.0`.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the **Current Action Status** column on the **Virtual Machine** tab.

VM Deployment field descriptions

Select Location and Host

Name	Description
Select Location	The location name. The field is display-only.
Select Host	The hostname of the ESXi host. For example, smgrdev. The field is display-only.
Host FQDN	FQDN of the ESXi host.
Data Store	The data store for the virtual machine. The page populates the capacity details in the Capacity Details section.
Next	Displays the Deploy OVA section in the Location & Host Details screen where you provide the details required for deployment.

Capacity Details

The system displays the CPU and memory details of the 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 name
Full Capacity	The maximum capacity
Free Capacity	The available capacity
Reserved Capacity	The reserved capacity
Status	The configuration status

Deploy OVA on System Manager Solution Deployment Manager

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment.
Enable enhanced security	The option to enable JITC mode deployment.
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy. **Note:** System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.

Table continues…

Name	Description
Flexi Footprint	The footprint size supported for the selected host. **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.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA on the Solution Deployment Manager client

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment.
Enable enhanced security	The option to enable JITC mode deployment.

The system displays the following options for deployment by providing OVA path.

Name	Description
Browse	The option to enter the full/absolute path of the `.ova` file to install it as a virtual machine on the system that hosts the Solution Deployment Manager client.
OVA File	The absolute path to the `.ova` file on the system that hosts the Solution Deployment Manager client. The field is available only when you click **Provide OVA Path**.
Submit File	Selects the `.ova` file of System Manager that you want to deploy.

With the **S/W Library** option you can select a `.ova` file that is available in the local software library of the system that hosts the Solution Deployment Manager client.

The system displays the following options for deployment using local software library.

Name	Description
File Name	The file name of the `.ova` file that is to be installed on the system that hosts the Solution Deployment Manager client. The field is available only when you click **S/W Library**.

With the **URL** option, you can type the URL of the `.ova` file. The system displays the following options.

Name	Description
URL	The URL of the `.ova` file that is to be installed on the system that hosts the Solution Deployment Manager client. The field is available only when you click **URL**.
Submit	Selects the `.ova` file to be deployed that is extracted from the URL.

The system displays the following common fields.

Name	Description
Flexi Footprint	The footprint size supported for the selected host. The field is available is common for all three types of deployment. **Important:** Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.
Next	Displays the **Configuration Parameters** tab in the OVA Details section where you provide the OVA details.

Configuration Parameters

The system populates most of the fields depending on the OVA file.

Note:

For configuration parameter fields, for Communication Manager Messaging and Utility Services, see VM Deployment Configuration and Network Parameters field descriptions on page 107.

Name	Description
VM Name	The name of the virtual machine.
Product	The name of the Avaya Aura® application that is being deployed. The field is read-only.
Version	Release number of the Avaya Aura® application that is being deployed. The field is read-only.
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Table 1: Configuration Parameters for Communication Manager simplex OVA deployment

Name	Description
CM IPv4 Address	The IPv4 address of the Communication Manager virtual machine.
CM IPv4 Netmask	The IPv4 network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The IPv4 default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine. The field is optional.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine. The field is optional.
CM IPv6 Gateway	The IPv6 gateway of the Communication Manager virtual machine. The field is optional.
Out of Band Management IPv4 Address	The IPv4 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv4 Netmask	The IPv4 subnetwork mask of the Communication Manager virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv4 subnetwork mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Server(s)	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). You can type up to three NTP servers.
DNS Server(s)	The DNS IP address of the Communication Manager virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IPv4 address of WebLM. The field is mandatory.

Table continues…

Name	Description
EASG User Access	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 to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.
Confirm Password	The password required to be confirmed. The field is mandatory.

Network Parameters

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.
Services	The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
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 where you must click **Accept** to start the deployment process.

Related links

VM Deployment Configuration and Network Parameters field descriptions on page 107

VM Deployment Configuration and Network Parameters field descriptions

Table 2: Configuration Parameters for Communication Manager Messaging deployment

Name	Description
Messaging IPv4 address	The IP address of the Communication Manager Messaging virtual machine.
Messaging IPv4 Netmask	The network mask of the Communication Manager Messaging virtual machine.
Messaging IPv4 Gateway	The default gateway of the Communication Manager Messaging virtual machine. For example, 172.16.1.1.
Out of Band Management IPv4 Address	The IP address of the Communication Manager Messaging virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Out of Band Management IPv4 Netmask	The subnetwork mask of the Communication Manager Messaging virtual machine for out of band management.
Messaging Hostname	The hostname of the Communication Manager Messaging virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). The field is optional.
DNS Server(s)	The DNS IP address of the Communication Manager Messaging virtual machine. Separate the IP addresses with commas(,). The field is optional.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
Messaging Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
Messaging Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Confirm Password	The password required to be confirmed.

Configuration and Network Parameters for Utility Services deployment

Name	Description
Networking Properties	

Table continues…

Name	Description
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine. **Note:** The host name is regardless of the interface that is used to access. The Public interface is the default interface.
Public IP address	The IP address for this interface. Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Public Default Gateway	The IP address of the default gateway. Required field unless you use DHCP. **Note:** The default gateway should be configured for the Public network. You can use the `ovf_set_static` command to allow a static route to be assigned to the OOBM network, enabling OOBM network to reach a second subnet.
Public IPv6 address	The IP address for this interface. Required field unless you use DHCP.
Public IPv6 Prefix	The netmask for this interface. Required field unless you use DHCP.
Default IPv6 Gateway	The IP address of the default gateway. Required field unless you use DHCP.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.
Out of Band Management IPv6 Address	The IPv6 address for this interface. This field is optional.
Out of Band Management IPv6 Prefix	The IPv6 prefix for this interface. This field is optional.
Network Time Protocol IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
TImezone setting	The selected timezone setting for the Utility Services virtual machine.

Table continues…

Name	Description
DNS	The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP. You can specify up to three DNS Servers.
Name	Primary WebLM IP address for Licensing. A valid Utility Services license is required for all deployment types and modes other than deployment on Appliance Virtualization Platform.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirm Password	The confirmation password.
Application Properties	
Communication Manager IP	IP address of Communication Manager. **Note:** A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.

Table continues…

Name	Description
Utility Services Mode	The mode in which you want to deploy Utility Services. The options are: • **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform. You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed. • **Utility Services Only**: Use to disable routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the services port becomes non-operational. • **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services, or when Utility Services are not required. With the services port feature, through a laptop connected to the services port of Appliance Virtualization Platform, you can gain access to Avaya virtual machines and the hypervisor that are deployed. • **Hardened Mode Services Port Only**: Sets up the system for military grade hardening. **Note:** With Utility Services 7.1.2 onwards, you can apply extended security hardening by selecting one of the following modes only: • **Services Port Only** • **Hardened Mode services port only** **Note:** For the Solution Deployment Manager client to connect to the services port features of Utility Services, change the IP address to `192.11.13.5` on the computer of the technician Utility Services can gain access to the hypervisor and all virtual machines through the IP address `192.11.13.6`. Utility Services provides application routing between the physical port and virtual applications.
Admin User Password	The admin user password.
Confirm Password	The confirmation password.

Table continues…

Name	Description
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management. **Note:** **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.

Update Static Routing field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
Utility Services IP	The IP address of Utility Services

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

Button	Description
Action to be performed	The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are: • **All**: Displays all the software patches. • **Commit**: Displays the software patches that you can commit. • **Rollback**: Displays the software patches that you can rollback.
Get Info	Displays software patches, service packs, and feature packs that you installed.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

Name	Description
VM Name	The name of the System Manager virtual machine on which you want to install the patch.
VM IP	The IP address of System Manager on which you want to install the patch.
Patch Name	The software patch name that you want to install.
Patch Type	The patch type. The options are service pack and software patch.
Patch Version	The software patch version.
Patch State	The software patch state. The states are: • Activated • Deactivated • Removed • Installed
Patch Status	The software patch status.

Update VM field descriptions

Name	Description
VM Name	The System Manager virtual machine name
VM IP	The IP address of System Manager
VM FQDN	FQDN of System Manager
Host Name	The host name
Select bin file from Local SMGR	The option to select the software patch or service pack for System Manager. The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager. This option is available only on the Solution Deployment Manager client.
Auto commit the patch	The option to commit the software patch or service pack automatically. If the check box is clear, you must commit the patch from **More Actions** > **Installed Patches**.

Button	Description
Install	Installs the software patch or service pack on System Manager.

Reestablish Connection field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
User Name	The user name
Password	The password

Button	Description
Reestablish Connection	Establishes connection between System Manager and the virtual machine.

Network parameter update for Avaya Aura® applications

You can change the network parameters for Avaya Aura® applications that run on an Appliance Virtualization Platform server.

The commands listed might change. Therefore, from the Avaya Support website at https://support.avaya.com, get the latest command update for an Avaya Aura® application from the appropriate document.

Tip:

On the Avaya Support website navigate to **Support by Product** > **Documents** > **<Avaya Aura application>**, type the release number, click **Installation, Upgrades & Config**, click **Enter**, and search for the updates.

Avaya Aura® application	Command	Interface where you perform the task
Appliance Virtualization Platform	`serverInitialNetworkConfig`	CLI
System Manager	`changeIPFQDN -IP <IPv4 address> -FQDN <FQDN> -GATEWAY <IPv4 Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6 Gateway address> -IPV6PREFIX <IPv6 prefix>`	CLI

Table continues…

Avaya Aura® application	Command	Interface where you perform the task
Communication Manager	-	The Network Configuration page from **Administration** > **server(Maintenance)** > **ServerConfiguration** on Communication Manager SMI.
Session Manager	**SMnetSetup**	CLI
Avaya Breeze™ and all installed snap-ins	**CEnetSetup**	CLI
Utility Services	**VMware_conf.sh**	CLI
Avaya Aura® Messaging	-	See the Avaya support website.
Avaya Aura® Media Server	-	See the Avaya support website.
SAL Gateway	-	Currently, you cannot change Network Parameters for SAL Gateway

Virtual machine report

With System Manager Release 7.1.3 and later, you can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the `/swlibrary/reports/generate_report.sh` folder.

Important:

If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

generate_report.sh command

The **generate_report.sh** generates the virtual machine report.

Syntax

```
sh ./generate_report.sh [-g] [-u Provide SMGR UI user name] [-p Provide SMGR UI password] [-s] [-a]
```

-g	The option to generate the report.
-u, SMGR UI user name	System Manager Web console user name.
-p, SMGR UI password	System Manager Web console password.
-s	The option to view the status of the generated report.
-a	The option to abort the generated report.

Generating a virtual machine report

Before you begin

If the application is of prior to Release 7.1, you must establish the trust with all applications before running the Report Generation utility.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password>` command:

   For example: `./generate_report.sh -g -u admin -p password`

   The system displays the following message: `Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].`
4. To proceed with report generation, type `Y`, and press `Enter`.

   The system generates the report in the `.csv` format in the `/swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv` folder.

   Note:

   If you re-run the report generation script when the report generation process is in progress, the system displays the following message: `Report Generation Process is Already Running, Kindly try after some time.`
5. **(Optional)** To view the logs, go to `/swlibrary/reports/generate_report-YYYYMMDDxxxx.log`.

Viewing the status of the virtual machine report

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -s` command.

   If the virtual machine report generation is in progress, the system displays the following message: `Report Generation Process is Running.`

Aborting the virtual machine report generation

About this task

If the virtual machine report generation process is in progress and you want to abort the report generation process, use the following procedure.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -a` command.

   The system aborts the virtual machine report generation process.

Monitoring a host and virtual machine

Monitoring a host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Monitor Hosts tab.
3. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring a virtual machine

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Monitor VMs tab.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.

b. In **Virtual machines**, click a virtual machine on the host that you selected.

4. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Managing vCenter

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 5.5, 6.0, 6.5, and 6.7. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.

      For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.

   b. In **User Name**, type user name to log in to vCenter.
   c. In **Password**, type password to log in to vCenter.
   d. In **Authentication Type**, select the authentication type.

      If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.

e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

PSC must have a valid certificate.

The system enables **PSC IP or FQDN** and you must provide the IP or FQDN of PSC.

f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.

5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds vCenter.

In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Related links

Editing vCenter on page 118
Map vCenter field descriptions on page 119
New vCenter and Edit vCenter field descriptions on page 120

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from earlier release, on the Certificate page, click **Accept Certificate**, and click **Save**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:

- Select an ESXi host and click the edit icon ( ).
- Select one or more ESXi hosts, select the location, and click **Bulk Update** and click **Update**.

If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables. Click **Commit** to get an updated list of managed and unmanaged hosts.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The values are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.

Table continues…

Button	Description
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept certificate for vCenter. For vCenter, you can only accept certificate. You cannot generate certificate.

Button	Description
Add	Displays the New vCenter page, where you can add a new ESXi host.
Edit	Displays the Edit vCenter page, where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** For Release 7.1, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.

Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Managing syslog profiles

Adding a remote Syslog server profile

About this task

Use this procedure to configure a remote Syslog server details in System Manager such that it receives to receive system logs from Appliance Virtualization Platform hosts.

Before you begin

To view the Syslog data from the Appliance Virtualization Platform host or application, ensure that:

- The firewall on the Syslog server is configured correctly.
- The Syslog service on the server is running.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click **VM Management**.
3. In the lower pane, click **Configure Remote Syslog Profile**.
4. Click **Add**.
5. In the Add Syslog Receiver dialog box, add the details of the Syslog server, such as profile name, IP address or FQDN, and port.
6. In **TCP/UDP**, click **TCP** or **UDP**.
7. If the remote host is TLS based, do the following:
   a. Select **TLS based Remote Host**.
   b. Click **Browse** and select a certificate file that you want to upload.
8. Click **Save**.

Syslog Receiver Configuration field descriptions

Name	Description
Profile Name	The name of the Syslog server configuration.
IP/FQDN	The IP address or host name of the Syslog server configuration.
Port	The port number of the Syslog server configuration.

Table continues…

Name	Description
TCP/UDP	The type of port used for the Syslog server configuration. The options are: • **TCP** • **UDP**
TLS based Remote Host	The option to select if the remote host is TLS based.
Select Certificate	The field to upload a certificate for the TLS based remote host. This option is available only if the **TLS based Remote Host** is selected.

Button	Description
Add	Displays the Add Syslog Receiver dialog box where you can add the Syslog server configuration.
Edit	Displays the Add Syslog Receiver dialog box where you can edit the configuration of the selected Syslog server.
Delete	Deletes the selected Syslog server configuration.
Browse	The field to browse and select a certificate for the TLS based remote host. This option is available only if the **TLS based Remote Host** is selected.

Pushing a system log to Syslog servers

About this task

Use this procedure to a send an Appliance Virtualization Platform host's log files to Syslog servers.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Syslog config** > **Push**.
5. In the Push Syslog Configuration dialog box, select the required Syslog profile, and click **Push**.

   The system sends the system log to the selected Syslog server.

Viewing configured Syslog servers

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Syslog config** > **View**.
5. In the View Syslog Configuration dialog box, select the required Syslog profile to view it.

Deleting configured Syslog servers

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Syslog config** > **Delete**.
5. In the Delete Syslog Configuration dialog box, select the required Syslog profile and click **Delete**.
6. On the confirmation dialog box, click **Yes**.

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

   The page displays the details of jobs that you selected.

Related links

Job History field descriptions on page 125

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Name	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Chapter 6: Configuration

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 on page 126.	
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 127.	
3	Configure the network settings.	See Configuring the network settings in a deployment on page 127.	
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 130.	
5	Connect to a remote WebLM and license the AE Services system.	See AE Services license requirements on page 130.	

Starting the Application Enablement Services virtual machine using vSphere

Procedure

1. In the vSphere Client window, select **View > Inventory > VMs and Templates**.
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 ignores the startup selections.

Before you begin

Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

1. In the Web browser, type the vSphere vCenter host URL.
2. Click **Hosts and Clusters** or **VMs and Templates** icon.
3. In the left pane, select the host where the virtual machine is located.
4. Click **Configure**.
5. Under Virtual Machines, select **VM Startup/Shutdown**, and click **Edit**.

   The system displays the Edit VM Startup and Shutdown window.
6. Select **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 client only, and not for AE Services deployed through VCenter or SDM.

Note:

The `netconfig` command does not support IPv6.

Procedure

1. In the vSphere Client window, select **View > Inventory > VMs and Templates**.
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 sensitive), the digits 0 through 9, and the hyphen (-).
      - The hostname cannot begin with or end with a hyphen (-).
      - The entire hostname (including the delimiting dots) may consist of up to 255 characters.
      - The hostname cannot exceed 15 characters.

   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 3: 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. Additionally, DMCC provides the integration for Microsoft LCS 2005, OCS 2007, LYNC, and Sametime. 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 137.
2. From the main menu, select **Maintenance > Date Time/NTP Server**.
3. Make your changes, and then click **Apply**.

AE Services licensing

AE Services license requirements

To get the full functionality for AE Services you must install the AE Services product license. The product license specifies the features you are permitted to use. For more information about licensed features, see the *Avaya Aura® Application Enablement Services Overview and Specification*, 02-300360.

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. See Downloading software from PLDS on page 28 for more information.
- 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.

Embedded Avaya WebLM is supported on AE Services 6.x System Platform and software-only offers only.

Embedded Avaya WebLM supports on AE Services VMWare offers from the Release 7.0.1.

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 a 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.

Avaya WebLM also supports IPv6.

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.

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.

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 136. If you are upgrading from AE Services 6.1.x, 6.2, or 6.3.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.

To get the full functionality for AE Services you must install the AE Services license. All AE Services 7.1.x offers require a new license to be installed when upgrading from AE Services 6.1.x, 6.2, and 6.3.x. AE Services 7.0.x offers that used an external WebLM do not require a new license file when upgrading to AE Services 7.1.x. AE Services 7.0.x offers that use the embedded WebLM require a new license file when upgrading to AE Services 7.1.x Software-Only version. All earlier AE Services releases require a new license file when upgrading to AE Services 7.1.x.

Upgrading from AE Services Release 7.0.1 to the Release 7.1.3 does not require new license if you are using the same hardware and the IP address.

Note:

By default, the AE Services server has a 30 days grace period. If a license file has not been installed, the AE Services server will enter 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. From the main menu of the AE Services Management Console, click **Licensing > WebLM Server Access**.
2. From the Web License Manager Logon screen, type your WebLM user name and password, and click the arrow.
3. From 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 136.

6. Verify that the license settings are correct for this customer.
   a. Click **Licensed Products > Application_Enablement**.
   b. Verify that the correct license settings are enabled.
7. From the main menu, click **Logout**.
8. Restart AE Services.

   See Restarting AE Services from the AE Services Management Console on page 135 or Restarting AE Services from the Linux command line on page 135.

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 Console

About this task

You must restart AE Services to use the capabilities of the new license. You can restart AE Services from the command line or through the AE Services Management Console.

Procedure

1. From your browser, log in to the AE Services Management Console. See Logging into the Management Console on page 137 for more information.

2. From the AE Services Management Console main menu, 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 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 137.
`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 7.1.3 license. See Uninstalling the AE Services license on page 137.
`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 137.

2. Log in to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
3. Provision the license file. See Activating license entitlements on page 203 for the procedure.
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. Log in to WebLM using an appropriate user name and password. See Logging in to WebLM and creating a WebLM password on page 133.
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. Log in to WebLM using an appropriate user name and password.

   See Logging in to WebLM and creating a WebLM password on page 133.
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**.

Logging into the AE Services Management Console

About this task

Important:

You cannot log in to the AE Services Management Console with a root account.

Procedure

1. In the address bar of your browser, type the fully qualified domain name or IP address of the AE Services server (for example `https://aserver.example.com`).

   The first time you try to access the AE Services server, your browser presents 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. From the security alert window, click **Yes** to accept the certificate.
3. From the Application Enablement Services welcome page, click **Continue To Login**.
4. In the Username box on the Application Enablement Services Management Console log in page, type your login ID.
5. Click **Continue**.
6. In the Password box, enter your password.

   Note:

   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 box to log in successfully.

   For customer user logins, these options are not presented.

7. Click **Login**.

   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.

   Note:

   If this is the first time you are logging in, the **End User License Agreement** page will be displayed.

Chapter 7: Upgrading AE Services

AE Services upgrade overview

Overview

This section provides upgrade and migration paths from previous versions of AE Services to AE Services 7.1.3.

Upgrade and migration paths

Refer to the following table to see the upgrade and migration paths from previous versions of AE Services to AE Services 7.1.3:

Warning:

Configurations made after applying the SuperPatch (if available during deployment) are not retained when the SuperPatch is removed. The AE Services server data will reflect the configuration of the server immediately before the patch was installed.

Table 4: Upgrade and migration paths to AE Services 7.1.3

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.2	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.2. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1.2 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.2	Virtualized Environment	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.2. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take a backup of AE Services 7.1.2, and using vSphere client, install AE Services 7.1.3 2. Restore data 3. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.2 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.
7.1.2	Software Only	1. Take backup of AE Services 7.1.2 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take backup of AE Services 7.1.2 2. Using vSphere client, install AE Services 7.1.3 3. Restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data
7.1.1	Virtualized Environment	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take a backup of AE Services 7.1.1, and using vSphere client, install AE Services 7.1.3 2. Restore data 3. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.1 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.1	Software Only	1. Take backup of AE Services 7.1.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take backup of AE Services 7.1.1 2. Using vSphere client, install AE Services 7.1.3 3. Restore data
7.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1	Virtualized Environment	1. Take backup of AE Services 7.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take a backup of AE Services 7.1, and using vSphere client, install AE Services 7.1.3 2. Restore data 3. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.
7.1	Software Only	1. Take backup of AE Services 7.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take backup of AE Services 7.1 2. Using vSphere client, install AE Services 7.1.3 3. Restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.0.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.0.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data
7.0.1	Virtualized Environment	1. Take backup of AE Services 7.0.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take a backup of AE Services 7.0.1, and using vSphere client, install AE Services 7.1.3 2. Restore data 3. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.0.1 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0.1	Software Only	1. Take backup of AE Services 7.0.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take backup of AE Services 7.0.1 2. Using vSphere client, install AE Services 7.1.3 3. Restore data
7.0	Virtual Appliance	1. Go to Upgrade Management, and then select AE Services 7.0. 2. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.0 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data
7.0	Virtualized Environment	1. Take backup of AE Services 7.0 2. Using System Manager Solution Deployment Manager, connect to AVP server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take a backup of AE Services 7.0, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.3 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0	Software Only	1. Take backup of AE Services 7.0 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 4. Restore data	1. Take backup of AE Services 7.0 2. Using vSphere client, install AE Services 7.1.3 3. Restore data
6.x	Virtualized Enterprise	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Take backup of AE Services 6.x 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3.	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data
6.x	System Platform	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3.	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
6.x	Software Only	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data
6.x	Bundled Server	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA 4. Restore data

Latest software updates and patch information

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

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

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

Upgrading AE Services applications

Checklist for upgrading Avaya Aura® applications to Release 7.1.3

No.	Task	References	✔
1	Download the OVA files and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at http://support.avaya.com. **Note:** For information about the upgrade sequence and the required patches, see the latest *Avaya Aura® Release Notes* for the specific release on the Avaya Support website.	-	
2	Download the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip` file from the Avaya Support website at http://support.avaya.com.		
3	Install the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe` file.	Installing the Solution Deployment Manager client on your computer on page 36	
4	To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.		
5	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.1 OVA file, and install the Release 7.1.3 bin file by using the Solution Deployment Manager client. • Available: Upgrade System Manager to 7.1 and install the Release 7.1.3 bin file.		
6	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	"Discovering elements" in *Administering Avaya Aura® System Manager*	

Table continues…

No.	Task	References	✔
7	Configure user settings.	“User settings” in *Administering Avaya Aura® System Manager*	
8	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for TN Boards and media gateway upgrades is not supported.	“User settings” in *Administering Avaya Aura® System Manager*	
9	Refresh the elements in the inventory.	“Refreshing elements” in *Administering Avaya Aura® System Manager*	
10	Analyze the software.	“Analyzing software” in *Administering Avaya Aura® System Manager*	
11	Download the required firmware for the Avaya Aura® application upgrade.	“Downloading the software” in *Administering Avaya Aura® System Manager*	
12	Analyze the software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*	
13	Perform the preupgrade check.	“Performing the preupgrade check” in *Administering Avaya Aura® System Manager*	
14	Perform the upgrade.	Upgrading Avaya Aura applications to Release 7.1.3 on page 149	
15	Verify that the upgrade is successful.	-	

Upgrading Avaya Aura® applications to Release 7.1.3

About this task

The procedure covers upgrades on the same server and on a different server. Use the procedure to upgrade the supported Avaya Aura® applications from

- 6.x running on Avaya Aura® to Release 7.1.3
- 7.0.x running on virtualized environment to Release 7.1.3

Note:

6.x upgrades are not supported for AE Services.

Before you begin

- From the Roles page, ensure that you set permissions that are required to perform all upgrade-related operations.
- Configure user settings.

- Complete all required operations up to the preupgrade check.
- To migrate the Avaya Aura® application from old server to ESXi host, add the new host in to VM Management.
- To migrate the Avaya Aura® application to a different server, add the Appliance Virtualization Platform host from the VM Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. To view and select the dependent elements:
   a. Click the element.
   b. On the Displaying Communication Manager Hierarchy page, select an element in the hierarchy.

      When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy. The page displays TN boards and media modules details in a table.
   c. Click **Done**.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

   When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.
6. To provide the upgrade configuration details, click **Edit**.
7. On the Edit Upgrade Configuration page, and perform the following:
   a. In **Service/Feature Pack for auto-install after migration**, provide the Release 7.1.3 patch file.
   b. Complete the details, and click **Save**.
8. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

   If the field displays , review the information on the Edit Upgrade Configuration page.
9. Click **Save**.
10. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.
11. On the Upgrade Configuration page, click **Upgrade**.
12. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.

13. Click **Schedule**.
14. Click **Upgrade**.
15. On the Upgrade Management page, click  .

    Last Action column displays **Upgrade**, and **Last Action Status** column displays  .

    For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, the field displays  . This icon indicates that the upgrade is successful and awaiting commit or rollback.
16. For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, do the following:
    a. On the Upgrade Management page, select the element.
    b. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.

       The system displays the Job Schedule page.
    c. Select the action to be performed under the **Upgrade Action** column.
    d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.
    e. Click **Schedule**.
17. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
18. Verify that the upgrade of the application is successful.

    For upgrades on the same server, the system goes to the pause state.
19. For upgrades on the same server, perform the following:
    a. Install the Appliance Virtualization Platform host.
    b. From the VM Management page, add the Appliance Virtualization Platform host.
    c. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    d. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.
    e. Continue with the upgrade process.

Installing software patches

About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Note:

When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions** > **Installed Patches** on the Upgrade Management page, then perform the following:

1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
2. Refresh the element.

Before you begin

- Perform the preupgrade check.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.

13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. To view the update status, click .

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

    When the update is complete, the **Update status** and **Last Action Status** fields displays .
16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display .

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Installing custom software patches

About this task

With this procedure, you can install a single software file, such as software patch, service pack, or a feature pack to an Avaya Aura® application. With the custom patch deployment, you do not require the System Manager automation and analyze functions, so that the advanced administrators can fully control the deployment of hot fixes, patches, service pack, and feature packs.

You can install custom patches for the following Avaya Aura® applications:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- Communication Manager Messaging
- WebLM
- Application Enablement Services

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
16. To view the update status, click .

The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

17. Click **Upgrade Actions** > **Installed Patches**.
18. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
19. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
20. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
21. Ensure that **Update status** and **Last Action Status** fields display .

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Next steps

To display the latest values in the **Entitled Update Version** column on the Upgrade Management page, click **Pre-upgrade Actions** > **Analyze**. If applied patch is:

- Uploaded as a custom patch in software library, the system does not change the value of the **Entitled Update Version** column.
- Downloaded in software library through the Download Manager page from PLDS or an Alternate source, the system displays the latest entitlement values in the **Entitled Update Version** column.

Installed Patches field descriptions

Name	Description
Commit	The option to select the patches that you can commit.
Uninstall	The option to select the patches that you can uninstall.

Table continues…

Name	Description
Rollback	The option to select the patches that you can rollback.
Show All	The option to display all the available options.

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.
Patch Type	The type of the software patch. The options are: • service pack or software patch • Kernel
Patch State	The state of the software patch. The options are: • Installed • Activated • Deactivated • Removed • Uninstall • Pending

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

Upgrade Management field descriptions

You can apply filters and sort each column in the devices list.

Name	Description
Name	The name of the device that you want to upgrade.
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board.
Sub-Type	The sub type of the device. For example, TN2302AP.
IP Address	The IP address of the device.
Release Status	The release status of the device. The upgrade status can be: For upgrade: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed

Table continues…

Name	Description
Update Status	The update status of the device. The upgrade status can be: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • : Mandatory checks and recommended checks passed • : Mandatory checks are successful, but recommended checks failed. • : Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
Location	The location of the device.

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.

Table continues…

Button	Description
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/Rolback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Management field descriptions

Name	Description
Install on Same Host	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update.
Host FQDN	The Host FQDN to which you want to update. The system displays the CPU and memory details of the host in the Capacity Details section.
VM Name	The virtual machine name displayed on the Add Element page.

Deploy OVA

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is ✔.

Table continues…

Name	Description
SMGR Datamigration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest data migration bin that is available for the System Manager release.
Backup file	The absolute path to the backup of System Manager virtual machine.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see the latest System Manager release notes.

Note:

- For upgrades from System Manager Release 6.3.15 or later, the bin file is mandatory.
- For upgrades from System Manager from 6.3.14 or earlier, the service pack, feature pack or patch file is optional.

  If you provide the service pack or feature pack, the data migration utility automatically deploys the service pack or feature pack on System Manager Release 7.0.0.0 after data migration.

Configuration Parameters

The system populates most of the fields depending on the OVA file. You must provide information, such as password, FQDN, and timezone.

Management Network Settings

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.
Management Gateway	The gateway IPv4 address to assign to the System Manager virtual machine.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,).

Table continues…

Name	Description
Management FQDN	The FQDN to assign to the System Manager virtual machine. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager virtual machine for out of band management. The field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager virtual machine. The field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.

Public Network Settings

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager virtual machine. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager virtual machine. The field is optional.
Public FQDN	The FQDN to assign to the System Manager virtual machine. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager virtual machine. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • Do not add VFQDN entries in the DNS configuration. • Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to the System Manager virtual machine with administrator privilege credentials. 2. Run the following command, `changeVFQDN`.
Virtual Domain	The virtual domain name of the System Manager virtual machine.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

SMGR CLI USER

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.

Table continues…

Name	Description
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. The system generates an alarm if you do not schedule a System Manager backup every seven days.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.

Table continues…

Name	Description
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description
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 to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

Network Parameters

Name	Description
Out of Band Management IP Address	The port number that you must assign to the Out of Band Management port group. The field is mandatory.
Public	The port number that you must assign to public port group. The field is optional.

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

Upgrade job status

Upgrade job status

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job. You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s)**: To get the latest data like version data for the applications in the system.
2. **Analyze**: To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check**: To evaluate an application that completed the Analyze job.
4. **Upgrade**: To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit**: To view commit jobs.
6. **Rollback**: To view rollback jobs.
7. **Uninstall**: To view uninstall jobs.

Viewing the Upgrade job status

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Status of Upgrade Management Jobs page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **View**.

   The system displays the Upgrade Job Status page.

Editing an upgrade job

Before you begin

You can edit the configuration of an upgrade job that is in pending state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click **Upgrade**.

4. Select a pending upgrade job that you want to edit.
5. Click **Edit Configuration**.

   The system displays the Upgrade Configuration page.
6. To edit the configuration, see Upgrading Avaya Aura applications.

Related links

Upgrading Avaya Aura applications to Release 7.1.3 on page 149

Deleting the Upgrade jobs

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **Delete**.

   The system updates the Upgrade Job Status page.

Upgrade Job Status field descriptions

Name	Description
Job Type	The upgrade job type. The options are: • **Refresh Element(s)**: To view refresh elements jobs. • **Analyze**: To view analyze jobs. • **Pre-Upgrade Check**: To view preupgrade check jobs. • **Upgrade**: To view upgrade jobs. • **Commit**: To view commit jobs. • **Rollback**: To view rollback jobs. • **Uninstall**: To view uninstall jobs.
Job Name	The upgrade job name.
Start Time	The time when the system started the job.
End Time	The time when the system ended the job.
Status	The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.
% Complete	The percentage of completion of the upgrade job.

Table continues…

Name	Description
Element Records	The total number of elements in the upgrade job.
Successful Records	The total number of times that the upgrade job ran successfully.
Failed Records	The total number of times that the upgrade job failed.

Button	Description
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Rollback process

Upgrade rollback

If the upgrade process of an element fails:

- If the admin does not specify rollback all, when the element upgrade fails, the system stops the entire upgrade process and display the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- If the admin specifies rollback all, when the element upgrade fails, the system stops the upgrade and rolls back the overall upgrade process. The system rolls back only the successfully upgraded elements.

Rolling back an upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.

   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message `Selected System Platform or child of System Platform, and System Platform and all child applications.`
4. Click **Upgrade Actions** > **Rollback**.

Post-upgrade tasks

Verifying the Appliance Virtualization Platform software release and the ESXi version

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To verify the Appliance Virtualization Platform software release, run the **`cat /opt/avaya/etc/avaya-avp.version`** command.

   The system displays the following.

   ```
   # Maj.Min.FP.SP.PATCH.BUILD
   Release: 7.1.3.0.0.x
   ```

4. To verify the ESXi version, run the **`esxcli system version get`** command.

   The system displays the following.

   ```
   Product: VMware ESXi
   Version: 6.0.0
   Build: Releasebuild-xxxxxxx
   Update: x
   ```

Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

The system displays the status of EASG.

2. To enable EASG, do the following:
   a. Run the command: **EASGManage --enableEASG**.

      The system displays the following message.

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

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the Avaya
      support site (https://support.avaya.com/ registration) for
      additional information for registering products and
      establishing remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled.`
3. To disable EASG, do the following:
   a. Run the command: **EASGManage --disableEASG**.

      The system displays the following message.

      ```
      By disabling Avaya Services Logins you are denying Avaya access
      to your system. This is not recommended, as it can impact
      Avaya's ability to provide support for the product. Unless the
      customer is well versed in managing the product themselves,
      Avaya Services Logins should not be disabled.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is disabled.`

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **EASGProductCert --certInfo**.

   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on

each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. Log in to the AE Services CLI interface as an administrator associated with the Linux group, easg.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Upgrading the standby and active servers when Geographical Redundancy High Availability feature is enabled

About this task

Use this procedure to upgrade the standby and active servers, when the AE Services server is upgraded and Geographical Redundancy High Availability (GRHA) is enabled.

Note:

This procedure is only used during AE Services deployment using VMware.

Procedure

1. Using the AE Services Management Console, remove High Availability on the active server.
2. Perform a backup of the AE Services server data for the active server.
3. Delete the active and standby AE Services servers from VMware.
4. Install the new active and standby AE Services servers on VMware.
5. Restore the data for the active AE Services server.
6. Using the AE Services Management Console, configure and start High Availability on the active server.

   Note:

   When the Memory/CPU of three AE Services profiles with similar CPU and Memory size are changed, GRHA configuration is not possible. This is because GRHA cannot be configured on profiles with differing CPU and Memory size values.

Upgrading AE Services 7.0.x to AE Services 7.1.x with Out of Band Management systems

For an Out of Band Management system-enabled AE Services 7.0.x installation, a direct upgrade to Out of Band Management system-enabled AE Services 7.1.x using Out of Band Management system-enabled AE Services System Manager Solution Deployment Manager is not allowed. In this scenario, complete a fresh install.

See the following upgrade matrix before deploying Out of Band Management system-enabled AE Services system from one release to higher.

Table 5: Upgrading AE Services with Out of Band Management

Release 7.0.x AE Services	Release 7.1.x System Manager Solution Deployment Manager	Upgrade to Release 7.1.x
OOBM Enabled	OOBM Enabled	Not Allowed
OOBM Disabled	OOBM Enabled	Not Allowed
OOBM Enabled	OOBM Disabled	Not Allowed
OOBM Disabled	OOBM Disabled	Allowed

Chapter 8: Migrating AE Services

AE Services migration overview

Overview

Migrate to AE Services for Virtualized Environment from one of the following AE Services offers:

- AE Services Software Only offer.
- AE Services on VMware offer.

Upgrade and migration paths

Refer to the following table to see the upgrade and migration paths from previous versions of AE Services to AE Services 7.1.3:

Table 6: Upgrade and migration paths to AE Services 7.1.3

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.2	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.2. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1.2 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.2	Virtualized Environment	1. Take backup of AE Services 7.1.2 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1 and restore data.	1. Take a backup of AE Services 7.1.2, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.2 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.
7.1.2	Software Only	1. Take backup of AE Services 7.1.2 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take backup of AE Services 7.1.2 2. Using vSphere client, install AE Services 7.1.3 and restore data.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data
7.1.1	Virtualized Environment	1. Take backup of AE Services 7.1.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take a backup of AE Services 7.1.1, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.3 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1.1	Software Only	1. Take backup of AE Services 7.1.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take backup of AE Services 7.1.1 2. Using vSphere client, install AE Services 7.1.3 and restore data.
7.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.1	Virtualized Environment	1. Take backup of AE Services 7.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take a backup of AE Services 7.1, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.3 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.
7.1	Software Only	1. Take backup of AE Services 7.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take backup of AE Services 7.1 2. Using vSphere client, install AE Services 7.1.3 and restore data.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0.1	Virtual Appliance	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Go to Upgrade Management, and then select AE Services 7.0.1. 3. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.0.1 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data
7.0.1	Virtualized Environment	1. Take backup of AE Services 7.0.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take a backup of AE Services 7.0.1, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.3 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0.1	Software Only	1. Take backup of AE Services 7.0.1 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data.	1. Take backup of AE Services 7.0.1 2. Using vSphere client, install AE Services 7.1.3 and restore data.
7.0	Virtual Appliance	1. Go to Upgrade Management, and then select AE Services 7.0. 2. Use the upgrade option to upgrade to AE Services 7.1.3.	1. Take backup of AE Services 7.0 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data
7.0	Virtualized Environment	1. Take backup of AE Services 7.0 2. Using System Manager Solution Deployment Manager, connect to AVP server, update if required 3. Install AE Services 7.1.3 and restore data	1. Take a backup of AE Services 7.0, and using vSphere client, install AE Services 7.1.3 and restore data. 2. Using System Manager Solution Deployment Manager: a. Connect the host or Vcenter to System Manager Solution Deployment Manager. b. Select the AE Services 7.1.3 VM. Establish a trusted connection. c. Go to upgrade management and upgrade AE Services to Release 7.1.3 using the upgrade option.

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
7.0	Software Only	1. Take backup of AE Services 7.0 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform server, update if required 3. Install AE Services 7.1.3 and restore data	1. Take backup of AE Services 7.0 2. Using vSphere client, install AE Services 7.1.3 and restore data
6.x	Virtualized Enterprise	1. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 2. Take backup of AE Services 6.x 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data
6.x	System Platform	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3.	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data

Table continues…

AE Services From Release	From Offer and Deployment	To: 7.1.3 Virtual Appliance	To: 7.1.3 Virtualized Environment
6.x	Software Only	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data
6.x	Bundled Server	1. Take backup from AE Services 6.x 2. Using System Manager Solution Deployment Manager, connect to Avaya Virtualization Platform, update if required 3. Install AE Services 7.1.3 on Avaya Virtualization Platform using Solution Deployment Manager 4. Restore data on AE Services 7.1.3	1. Take backup of AE Services 6.x 2. Using vSphere client, connect to ESXi host 3. Deploy AE Services 7.1.3 OVA and restore data

Migration checklist for using the backup restore method

Use the following procedure for migrating the AE Services virtual appliance:

Note:

If you have AE Services Release 5.2.4, 6.x, or 7.0.x installed and you want to upgrade to AE Services 7.1.3, deploy AE Services 7.1.3 using the direct OVA method. Apply the pre-upgrade patch on the 6.3.x machine where the backup needs to be taken. It is the server that will be migrated to AE Services for Virtualized Environment.

#	Action	✔
1	Back up the current AE Services database.	
2	Shut down the AE Services virtual machine.	
3	When migrating from older releases AE Services, install the AE Services 7.1.3 OVA as VA or VE offer . Use the same configuration as the AE Services virtual machine that you want to upgrade.	
4	Restore the AE Services database that you backed up in Step 1 to the AE Services virtual machine you created in Step 3.	
5	After the restore is complete, verify that the AE Services application is operational.	

Backing up the AE Services server data

About this task

This procedure is required for upgrading all releases.

Procedure

1. From your browser, log in to the AE Services Management Console with the appropriate user account and password.
2. From the AE Services Console main menu, select **Maintenance > Server Data > Backup**.
3. If you do not want to encrypt the backup file, click **Continue**.
4. If you want to encrypt the backup file, perform the following steps:
   a. Click the **Encrypt Backup File** check box, and then click **Continue**.
   b. In the Password box, enter the password you want to use for the encrypted backup file. The password must consist of 15 to 256 characters. This password cannot contain the following characters: ` (single quotation), " (double quotation), ' (apostrophe) , \ (back slash), and % (percent).
   c. Click **Continue**.
5. Click the **Here** link to download the file.

   The File Download dialog box appears. You can specify the location where you want to save the backup file. Be sure to save the backup file to a safe location that the upgrade will not affect. For example, save the file to your local computer or another computer used for storing backups.

   The backup file is named *ServerName_AESReleaseVersion*_aesvcsdb*DDMMYYYY*.tar.gz.enc where *DDMMYYYY* is a date stamp, and *enc* indicates that the file is encrypted. If the file is not encrypted, *enc* will not appear in the file name.

   An example of an encrypted backup file is *acme_r6 -2-0-11-0_aesvcsdb18062012.tar.gz.enc*.

An example of an unencrypted backup file is *acme_r6 -2-0-11-0_aesvcsdb18062012.tar.gz*.

6. Click **Save**.

Note:

The tar file MD5 checksum is displayed on the web page. Use this checksum to verify the file was downloaded correctly.

Stopping a virtual machine from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.
4. Click **Stop**.

   In **VM State**, the system displays `Stopped`.

Deploying AE Services OVA using System Manager Solution Deployment Manager or Solution Deployment Manager client

Procedure

1. To deploy AE Services:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager** and then click,**VM Management**.
   - For Solution Deployment Manager Client, on the desktop, click the Solution Deployment Manager icon and then click **VM Management**.
2. Click on **Location > Host > Virtual Machines**
3. Click on **New** to create Virtual Machine
4. On the **VM** Name Field, enter the Host Name of AE Services.

Note:

Make sure you are installing AE Services on the correct Location and Host.

5. Select the Data Store.
6. On the Deploy OVA section, deploy AE Services OVA.

   Important:

   Before deploying AE Services OVA, see *Upgrading Avaya Aura® applications to Release 7.1* for the following:

   - Downloading the AE Services OVA.
   - Deploying the AE Services OVA.
7. Select the software library.
8. Select the OVA File.
9. Select the **Footprint**.
10. In the Configuration Parameters Section, enter the AE Services Network Configuration information.
11. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

    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 Avaya Logins you are preventing Avaya access to your
    system.
    This is not recommended, as it impacts Avaya's ability to provide
    support for the product. Unless the customer is well versed in
    managing the product themselves, Avaya Logins should not be
    disabled.
    ```

    a. 1: To enable EASG.

       Avaya recommends to enable EASG.

       You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

    b. 2: To disable EASG.
12. In the Network Parameters field, assign the NICs to the private port.
13. Accept the EULA Acceptance.

14. Verify the AE Services Deployment Status steps by clicking the **Status Details Link** in the AE Services Entry of the Virtual Machine list.
15. AE Services OVA deployment is successful. Verify the AE Services deployment status clicking the status link.

    For more information, see *Deploying Avaya Aura® applications from System Manager*.

    Install the latest Avaya Aura® Application Enablement Services 7.1.3 Super Patch (if available), and other release patches as applicable.

    For more information, see Avaya Aura® 7.1.3 Release Notes.

Restoring the AE Services server data

About this task

Note:

The database backup file includes the license file in the preserved server data. If a restore is made on a newer AE Services major release than the release in the database backup file (older releases to 7.0), you must remove the license file that was restored from the previous release. See Deploying AE Services chapter for more information.

Procedure

1. From your browser, log in to AE Services Management Console.
2. From the main menu, select **Maintenance > Server Data > Restore**.
3. From the Restore Database Configuration page, click **Browse** .
4. Select the appropriate AE Servicesbackup file, and click **Restore**.

   If the backup file is encrypted, the Password box appears on the Restore Database Configuration page. In the Password box, enter the password for the backup file, and then click **Continue**.

   On the Restore Database Configuration page, the following message appears:

   ```
   A database restore is pending. You must restart the Database
   Service and the AE Server for the restore to take effect. To
   restart these services now, click the Restart Services button
   below.
   ```

5. Click **Restart Services**.

   Caution:

   If you make any changes during the time between clicking **Restore** and **Restart Services**, these changes will be lost.

Logging into the AE Services Management Console

About this task

Important:

You cannot log in to the AE Services Management Console with a root account.

Procedure

1. In the address bar of your browser, type the fully qualified domain name or IP address of the AE Services server (for example `https://aserver.example.com`).

   The first time you try to access the AE Services server, your browser presents 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. From the security alert window, click **Yes** to accept the certificate.
3. From the Application Enablement Services welcome page, click **Continue To Login**.
4. In the Username box on the Application Enablement Services Management Console log in page, type your login ID.
5. Click **Continue**.
6. In the Password box, enter your password.

   Note:

   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 box to log in successfully.

   For customer user logins, these options are not presented.

7. Click **Login**.

   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.

   Note:

   If this is the first time you are logging in, the **End User License Agreement** page will be displayed.

Chapter 9: Virtualized Environment footprint flexibility

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

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

The applications that currently support Virtualized Environment footprint flexibility are:

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

Related links

Hardware resources reconfiguration to support AE Services footprint flexibility on page 188

Hardware resources reconfiguration to support AE Services footprint flexibility

AE Services 7.1.x supports the following footprint matrix:

		DMCC — Third party call control: Microsoft OCS/ Lync, IBM Sametime, 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 GB RAM**	1K 10K	20K BHCC 6K BHCC	1K	9K BHCC	1K MPS
Profile 2	**2 CPU and 4 GB RAM**	2.5K 12K	50K BHCC 12K BHCC	2.4K	18K BHCC	1K MPS
Profile 3	**4 CPU and 6 GB RAM**	5K 20K	100K BHCC 24K BHCC	8K	36K BHCC	2K MPS

Procedure

Modify the AE Services footprint flexibility using vSphere as follows:

Note:

Install the AE Services 7.1.x OVA, or later before continuing with this procedure.

1. Connect to the host or cluster using the VMware vSphere 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 2400. For example, if the number of CPUs is 3, the **Reservation** should be set to 7200. One CPU should be equal to 2190.
    g. (Optional) Uncheck the **Unlimited** checkbox.
    h. (Optional) Verify the **Limit** slide is set to the same value as the **Reservation**.
7. Click **OK**.
8. Wait until the virtual machine finishes the reconfiguration procedure.
9. Power on the virtual machine.

Related links

Virtualized Environment footprint flexibility on page 188

Chapter 10: Related resources

Documentation

The following documents supplement the information in this guide.

Title	Description	Audience
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.	Sales Engineers
Avaya Aura® Application Enablement Services Overview and Specification	Provides an overview of Application Enablement Services including new features, architecture, product summary, capacities, and compatibility.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering and Maintaining Avaya Aura® Application Enablement Services	Provides a common reference for basic Application Enablement Services (AE Services) administrative tasks.	Administrators, Implementation Engineers, Support Personnel

Related links

Accessing the port matrix document on page 191

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.

6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

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

Related links

Documentation on page 191

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 click **Go** to search for the course.

Course code	Course title
4100	Avaya Aura® Application Enablement Services Implementation Test.
ATI02595IEN	Avaya Aura® Application Enablement Services Implementation and Administration.
ATI02595VEN	Avaya Aura® Application Enablement Services Implementation and Administration.
4301W	Avaya Unified Communications - Core Components.
7120V	Integration Basics for Avaya Enterprise Team Engagement Solutions (Virtual Instructor Led).

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 http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 193
Using the Avaya InSite Knowledge Base on page 193

Using the Avaya InSite Knowledge Base

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

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

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

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

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

   The system displays the Avaya Support page.

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

Related links

Support on page 12
Support on page 12

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. The root user, however 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 8 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: $ (dollar sign), ’ (apostrophe), " (quotation mark), \ (backslash), the space character, 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 Tripwire 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 installed the Avaya Services package (cs-service) • AE Services using VMware® in the Virtualized Environment	suserssecurityadminusrsvc_admin	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)
cust (customer account) Available on: • AE Services Software-Only Server only if you installed the Avaya Services package (cs-service) • AE Services using VMware® in the Virtualized Environment	suserssecurityadminusrsvc_admin easg	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 • User Management (AE Services sets up the craft account with access to Security) • Utilities
avaya (customer account) Available on: • AE Services Software-Only Server only if you installed the Avaya Services package (cs-service) • AE Services using VMware® in the Virtualized Environment	Not applicable	Read and write access to the User Management menu only

Default AE Services accounts

Account name (log-in identifier)	Linux Group	Access privileges
craft Available on AE Services Software-Only Server only if you installed the Avaya Services package (cs-service).	suserssecurityadminusr svc_admin	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 only if you installed the Avaya Services package (cs-service).	suserssecurityadminusr svc_admin	Intended for customers. 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 - root`**) • Remote - Log in from a remote console with a secure shell client (ssh), as craft, and then access the root account (**`su - root`**)
avaya Available on AE Services Software-Only Server only if you installed the Avaya Services package (cs-service).	Not applicable	User Management administration only. You do not have access to any other administrative menus.

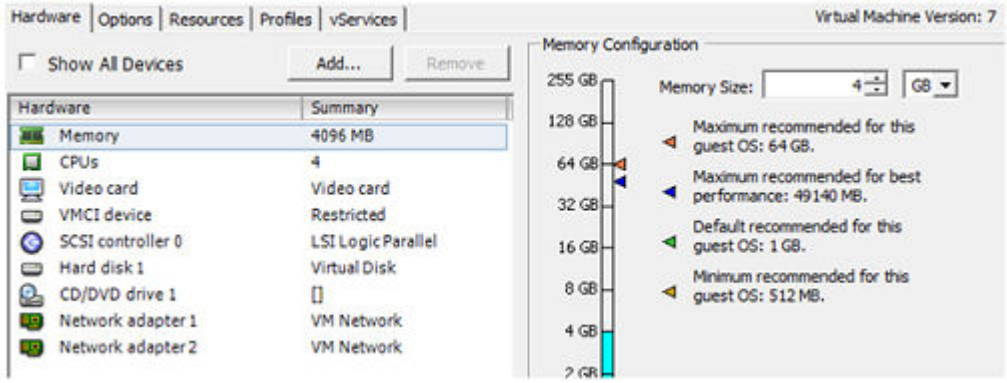
Modifying reservations on Application Enablement Services

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.

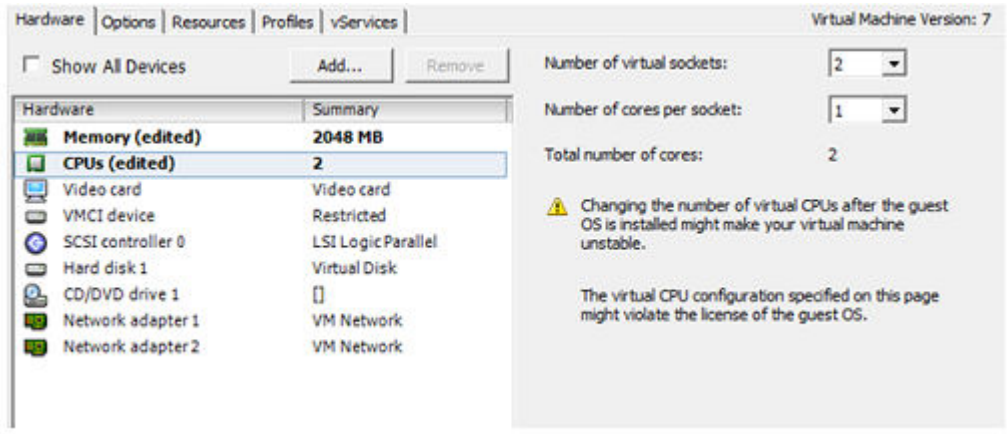
c. In the left pane, under **Hardware**, select **Memory**.



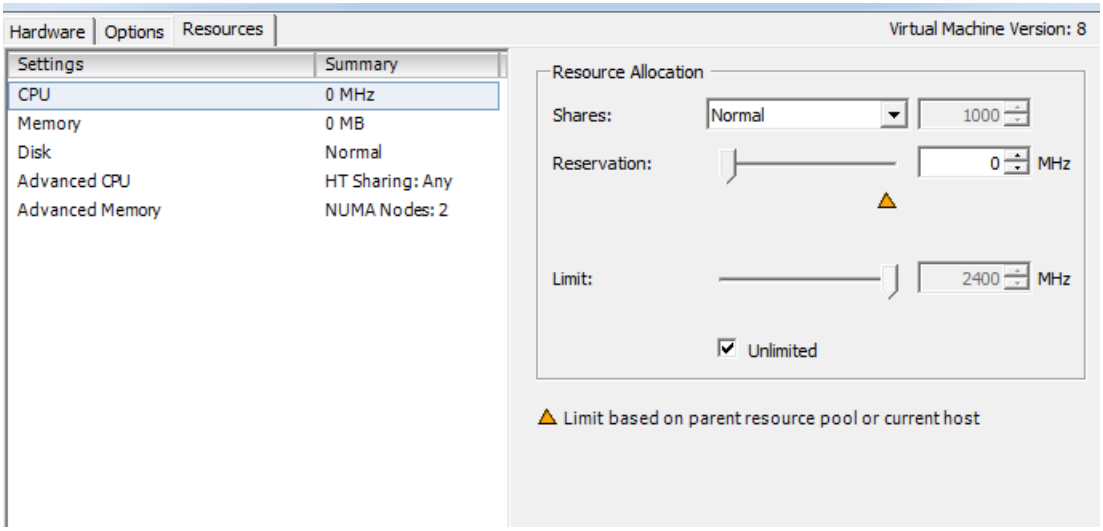
d. In the right pane, change the **Memory Size** value from the existing value to the desired value.

e. In the left pane, select **CPUs**.

f. In the right pane, adjust the **Number of virtual sockets** from the existing value to the desired value.



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

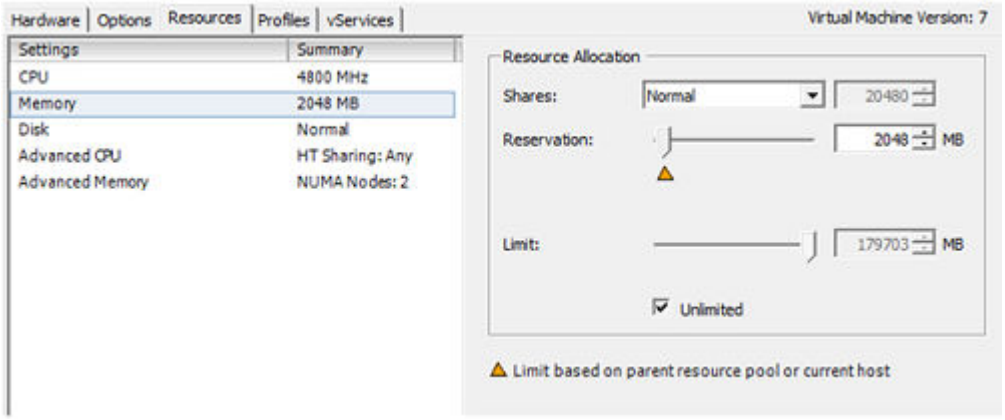


h. In the left pane, select **CPU**.

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

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 **magnifying glass** 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 209
VMware Tools on page 211
Timekeeping on page 211
VMware networking best practices on page 212
Storage on page 216
Thin vs. thick deployments on page 217

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 at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-tuning-latency-sensitive-workloads-white-paper.pdf.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers
- HP ProLiant Servers

Related links

Best Practices for VMware performance and features on page 209
Intel Virtualization Technology on page 210
Dell PowerEdge Server on page 210
HP ProLiant Servers on page 211

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 and HP 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 209

Dell PowerEdge Server

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 209

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

Related links

BIOS on page 209

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 209

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 `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

- 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 **ntpd**. 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 209

VMware networking best practices

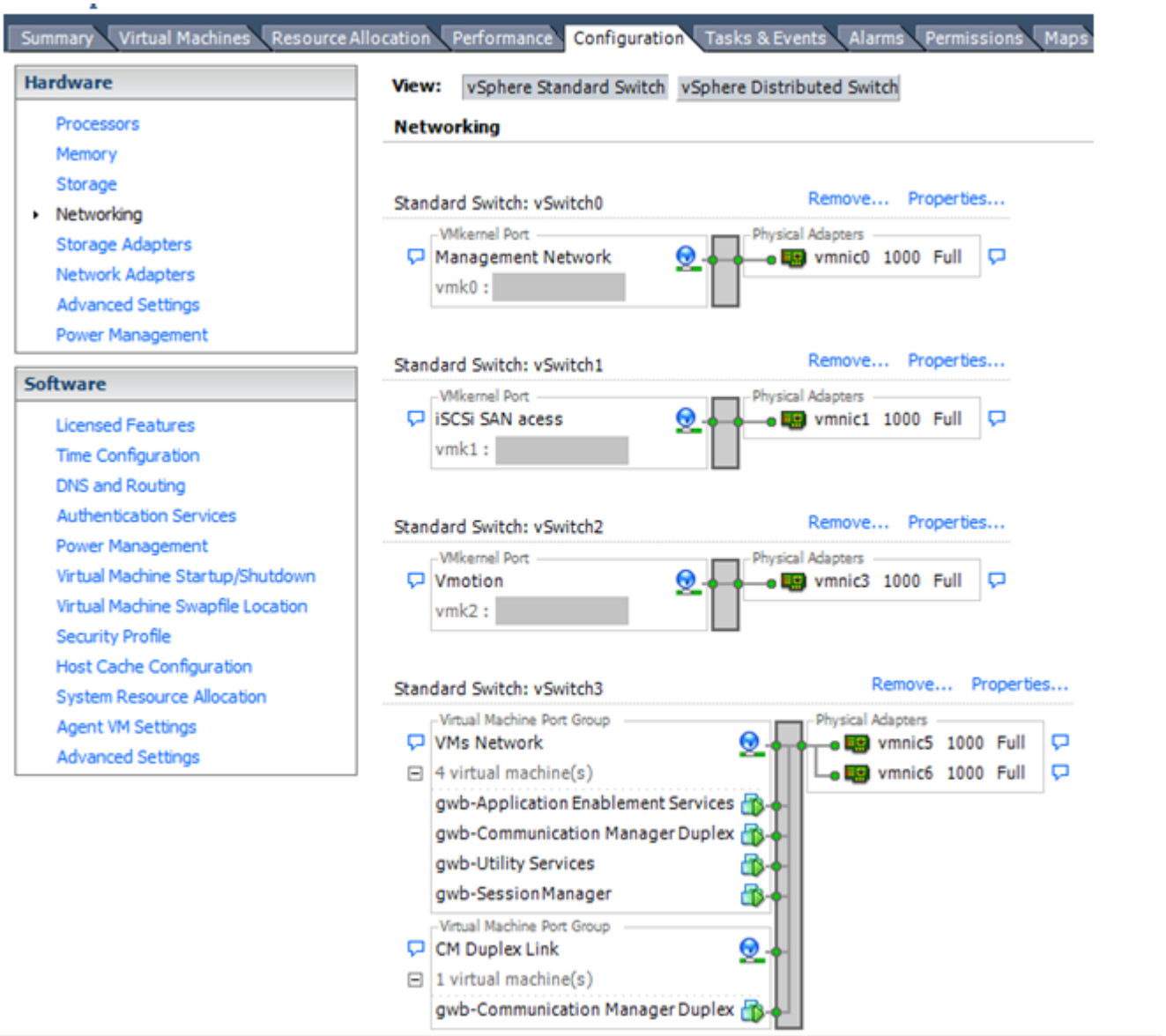
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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).

Networking Avaya applications on VMware ESXi – Example 1

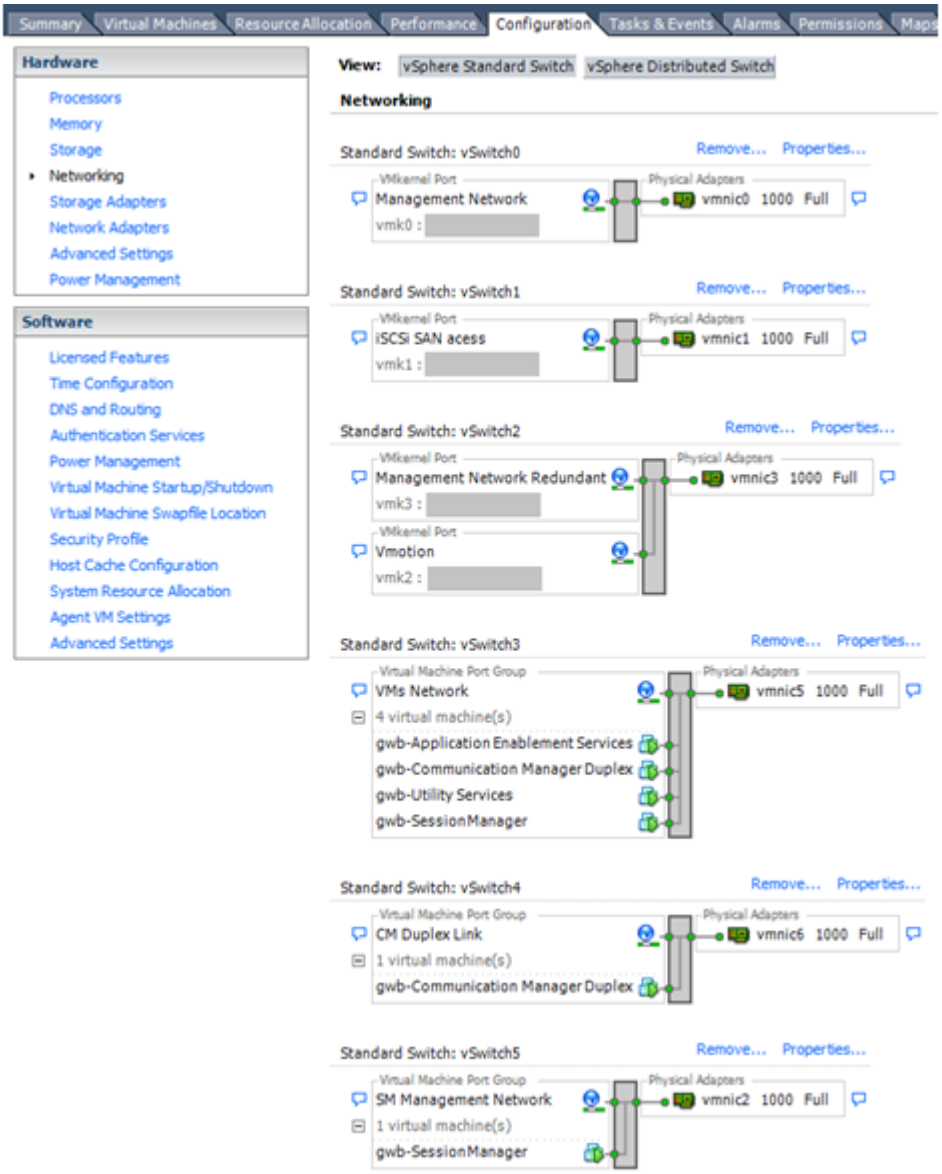


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- 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.

- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.
- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere® 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
Performance Best Practices for VMware vSphere® 6.0	http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware vSphere 6.5 Documentation	http://pubs.vmware.com/vsphere-65/index.jsp
VMware vSphere 6.0 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Related links

Best Practices for VMware performance and features on page 209

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 209

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate 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 format 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 Microsoft Windows format tool 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 209

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.

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.
- 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 Virtual Machine Snapshot** window, clear the **Snapshot the 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

Table continues…

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
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

Related links

Best Practices for VMware performance and features on page 209

Deployment of cloned and copied OVAs

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 on the virtual machine. At this time, Avaya only supports the deployment of new OVAs.

Related links

Best Practices for VMware performance and features on page 209

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 209

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 209

Related resources

Documentation

The following documents supplement the information in this guide.

Title	Description	Audience
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.	Sales Engineers
Avaya Aura® Application Enablement Services Overview and Specification	Provides an overview of Application Enablement Services including new features, architecture, product summary, capacities, and compatibility.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering and Maintaining Avaya Aura® Application Enablement Services	Provides a common reference for basic Application Enablement Services (AE Services) administrative tasks.	Administrators, Implementation Engineers, Support Personnel

Related links

Accessing the port matrix document on page 191

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 click **Go** to search for the course.

Course code	Course title
4100	Avaya Aura® Application Enablement Services Implementation Test.

Table continues…

Course code	Course title
ATI02595IEN	Avaya Aura® Application Enablement Services Implementation and Administration.
ATI02595VEN	Avaya Aura® Application Enablement Services Implementation and Administration.
4301W	Avaya Unified Communications - Core Components.
7120V	Integration Basics for Avaya Enterprise Team Engagement Solutions (Virtual Instructor Led).

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 193
Using the Avaya InSite Knowledge Base on page 193

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

Related links

Support on page 12
Support on page 12

Glossary

Application	A software solution development by Avaya that includes a guest operating system.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
EASG	Enhanced Access Security Gateway. The Avaya Services Logins to access your system remotely. The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make

	storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Client	The vSphere Client is an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based client version is VMware 6.5 and later.

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W