Deploying Avaya Aura® Appliance Virtualization Platform

Release 8.0.x
Issue 4
March 2020

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.

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

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.

Contents

Chapter 1: Introduction

Purpose

This document contains checklists and procedures for:

- Deploying Appliance Virtualization Platform
- Configuring Appliance Virtualization Platform
- Administering Appliance Virtualization Platform
- Troubleshooting Appliance Virtualization Platform

The primary audience for this document is anyone who deploys Appliance Virtualization Platform and configures a system with Appliance Virtualization Platform preinstalled at a customer site.

Prerequisites

Before deploying or upgrading Appliance Virtualization Platform, ensure that you have the following knowledge, skills, and tools.

Knowledge

- Linux® Operating System
- Appliance Virtualization Platform

Skills

To administer the System Manager web console and Appliance Virtualization Platform.

Tools

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

Change history

The following changes have been made to this document since the last issue:

Issue	Date	Summary of changes
4	March 2020	Updated the section: Appliance Virtualization Platform overview on page 10
3	January 2019	For Release 8.0.1, updated the following sections: • Deploying AVP Utilities and virtual machines when Out of Band Management is enabled on page 100 • Deploying AVP Utilities and virtual machines on the services port on page 101
2	December 2018	For Release 8.0.1, updated the following sections: • Appliance Virtualization Platform overview on page 10 • Supported servers on page 29 • Appliance Virtualization Platform license on page 65 • Appliance Virtualization Platform licenses for supported servers on page 66
1	July 2018	Release 8.0 document.

Chapter 2: Appliance Virtualization Platform overview

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 provides the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications.

Avaya Aura® Virtualized Appliance offer includes:

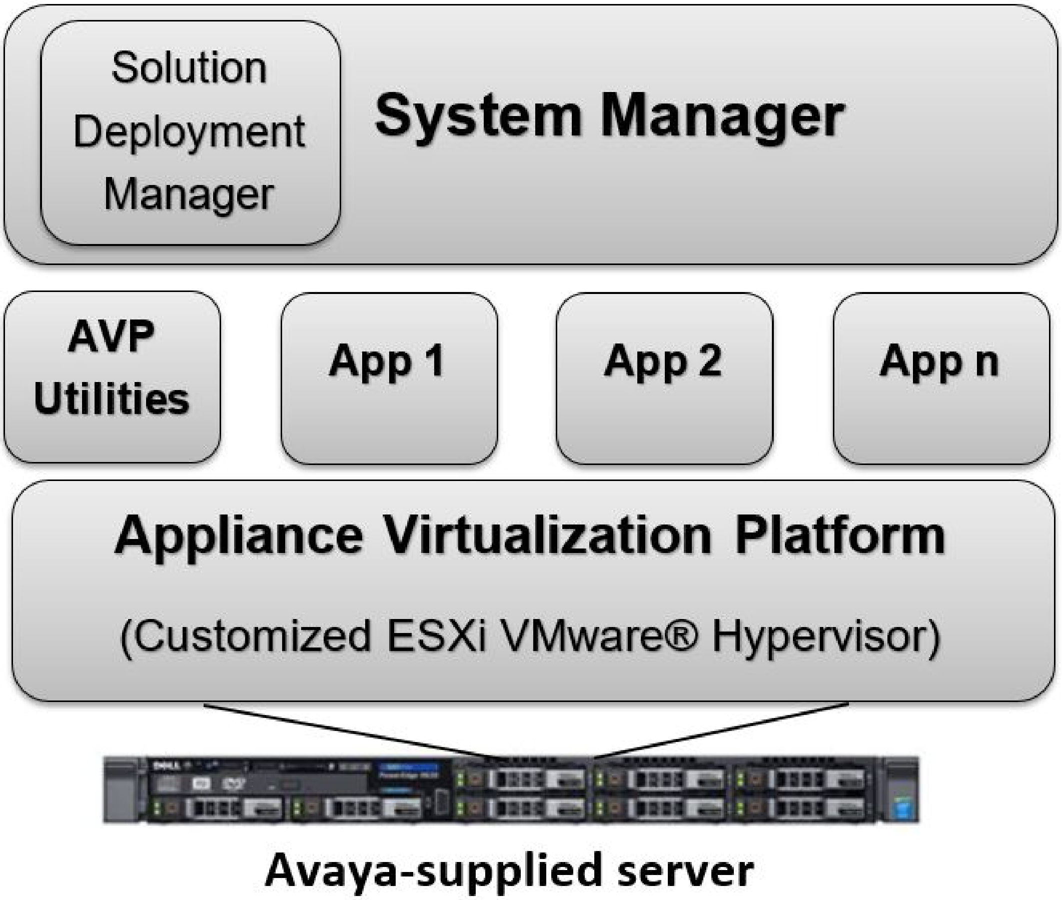
- Common Servers: Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- Avaya S8300E

  Note:

  - With WebLM Release 7.x and later, you cannot deploy WebLM on S8300E Server running on Appliance Virtualization Platform.
  - Common Servers using ESXi 6.0 can require more memory than System Platform or ESXi 5.5. For memory validation process, see PSN027060u or the Release Notes.
- Avaya Converged Platform 120 Server: Dell PowerEdge R640

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.


Solution Deployment Manager
System Manager
AVP Utilities
App 1
App 2
App n
Appliance Virtualization Platform
(Customized ESXi VMware® Hypervisor)
Avaya-supplied server

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

You can deploy the following applications on Appliance Virtualization Platform:

- AVP Utilities 8.0.1
- System Manager 8.0.1
- Session Manager 8.0.1
- Branch Session Manager 8.0.1
- Communication Manager 8.0.1
- Application Enablement Services 8.0.1
- WebLM 8.0.1
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Note:

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

Important:

Due to Avaya enhanced customizations, Appliance Virtualization Platform (aka Avaya Converged Platform120) does not support administration on vCenter. For the Appliance Virtualization Platform administration, System Manager and Solution Deployment Manager are the only management platform supported by Avaya.

Besides not being a supported configuration, if vCenter is connected to any appliance running the Appliance Virtualization Platform, the Avaya hypervisor customization and specific data (such as, logins, Datastore and VM information among others) will be overwritten and corrupted. This can result in making the situation unrecoverable and requires complete fresh re-installation of Appliance Virtualization Platform on the appliance.

Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

From Release 7.1 and later, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x, 7.0.x, and 7.1.x applications to Release 8.0 and later in the customer's Virtualized Environment. For migrating to Release 8.0, you must use Solution Deployment Manager Release 8.0.

Release 7.0 and later support a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Avaya Aura® Virtualized Appliance: Contains a server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 6.0 hypervisor.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.

With Solution Deployment Manager, you can do the following in Virtualized Environment and Avaya Aura® Virtualized Appliance models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

  Note:

  When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

  For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.

- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - AVP Utilities
  - Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices, and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 8.0, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Manage virtual machine lifecycle.	Manage virtual machine lifecycle.

Table continues…

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Deploy Avaya Aura® applications.	Deploy Avaya Aura® applications.
Deploy hypervisor patches only for Appliance Virtualization Platform.	Deploy hypervisor patches only for Appliance Virtualization Platform.
Upgrade Avaya Aura® applications. Release 7.x and later support upgrades from Linux-based or System Platform-based applications to Virtualized Environment or Appliance Virtualization Platform. Release 7.1 and later support Virtualized Environment to Virtualized Environment upgrades.	Upgrade System Platform-based and Virtualized Environment-based System Manager.
Install software patches for Avaya Aura® applications excluding System Manager application.	Install System Manager patches.
Discover Avaya Aura® applications.	Deploy System Manager.
Analyze Avaya Aura® applications.	-
Create and use the software library.	-

Solution Deployment Manager Client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client must be installed on the computer of the technician. The Solution Deployment Manager client provides the functionality to deploy the OVAs or ISOs on an Avaya-provided server, customer-provided Virtualized Environment, or Software-only environment.

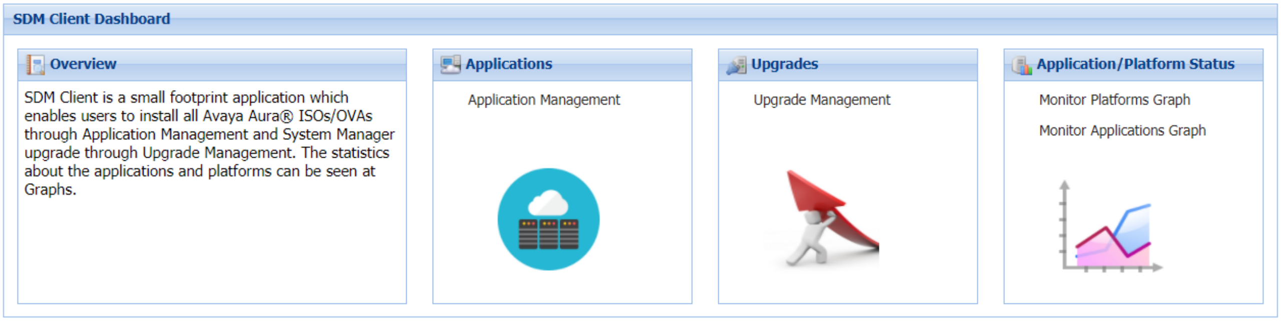
A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade System Platform-based System Manager.
- Upgrade VMware-based System Manager from Release 7.0.x to Release 7.1 and later.
- Upgrade VMware-based System Manager from Release 6.x or 7.x to Release 8.0 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

Note:

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest the Solution Deployment Manager client for deployment.
- You must use Solution Deployment Manager Client 7.1 and later to create the kickstart file for initial Appliance Virtualization Platform installation or recovery.



SDM Client is a small footprint application which enables users to install all Avaya Aura® ISOs/OVAs through Application Management and System Manager upgrade through Upgrade Management. The statistics about the applications and platforms can be seen at Graphs.

Figure 1: Solution Deployment Manager Client dashboard

Related links

Solution Deployment Manager client capabilities on page 15

Solution Deployment Manager client capabilities

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

- Runs 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 the 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 Appliance Virtualization Platform or 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.

  Note:

  - System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 7.1.3.2 before you upgrade Communication Manager to 7.1.3.2.

    All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.
  - Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 7.1.3 OVA, Solution Deployment Manager Client version must be on Release 7.1.3, 7.1.3.1, 7.1.3.2, or 8.0. Solution Deployment Manager Client cannot be on Release 7.1.
- Configures application and networking parameters required for application deployments.
- Supports selecting the application OVA file from a local path or an HTTPS URL. 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 System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 7.1.1, you must use Solution Deployment Manager Client Release 7.1.1 or higher.

  However, to install the patch on System Manager Release 7.0.x, Solution Deployment Manager Client must be on Release 7.0.x.

  Avaya Aura® applications use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs. The applications that cannot be patched from centralized Solution Deployment Manager, use the application Command Line Interface or web console.

  For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.
- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.

Related links

Solution Deployment Manager Client on page 14

Solution Deployment Manager

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

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

- AVP Utilities 8.0.1
- System Manager 8.0.1
- Session Manager 8.0.1
- Branch Session Manager 8.0.1
- Communication Manager 8.0.1
- Application Enablement Services 8.0.1
- WebLM 8.0.1
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

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

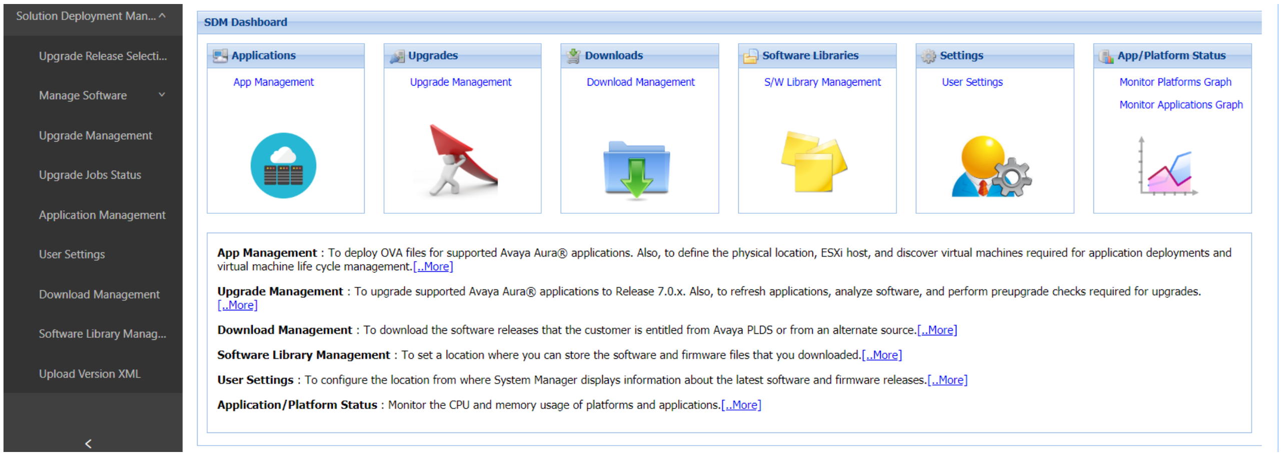
Note:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 8.0.1. 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.



App Management : To deploy OVA files for supported Avaya Aura® applications. Also, to define the physical location, ESXi host, and discover virtual machines required for application deployments and virtual machine life cycle management.[..More]

Upgrade Management : To upgrade supported Avaya Aura® applications to Release 7.0.x. Also, to refresh applications, analyze software, and perform preupgrade checks required for upgrades. [..More]

Download Management : To download the software releases that the customer is entitled from Avaya PLDS or from an alternate source.[..More]

Software Library Management : To set a location where you can store the software and firmware files that you downloaded.[..More]

User Settings : To configure the location from where System Manager displays information about the latest software and firmware releases.[..More]

Application/Platform Status : Monitor the CPU and memory usage of platforms and applications.[..More]

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.x Onwards** or **6.3.8** as the target upgrade. Release 8.0.1 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application 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, and WebLM to Release 8.0.1.
- **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.

Chapter 3: Network

Appliance Virtualization Platform networking

Overview

Appliance Virtualization Platform supports both public and management traffic over the same network interface or separation of public and management traffic over separate interfaces. The default configuration is public and management traffic using the same network interface. When you install Appliance Virtualization Platform, the public network of virtual machines is assigned to vmnic0 or Server Ethernet port 1 of the server.

- If the **Out of Band Management Setup** check box is clear on Create AVP Kickstart, the public and management interfaces of virtual machines are assigned on the public network. Assign public and management interfaces of virtual machines on the same network.

  The management port of Appliance Virtualization Platform is assigned to the public interface.
- If the **Out of Band Management Setup** check box is selected on Create AVP Kickstart, the public interfaces of virtual machines are assigned to vmnic0 or Server Ethernet port 1, and the Out of Band Management interfaces are assigned to vmnic2 or Server Ethernet port 3. Assign separate network ranges to the public and management interfaces of virtual machines. The management port must be given an appropriate IP address of the public and Out of Band Management network.

  The management port of Appliance Virtualization Platform is assigned to the Out of Band Management network.

  Note:

  All virtual machines on an Out of Band Management enabled Appliance Virtualization Platform host must support and implement Out of Band Management.

The vmnic1 or Server Ethernet port 2 of the server is assigned to the services port.

The internal Appliance Virtualization Platform hypervisor IP address from the services port is 192.168.13.6. After deploying the Appliance Virtualization Platform OVA, launch an SSH client while connected to the services port. Configure your computer for direct connection to the server with the following:

- IP Address: 192.168.13.5
- Subnet Mask: 255.255.255.248
- Gateway: 192.168.13.1

After deploying the AVP Utilities OVA, the services port IP address for the AVP Utilities shell is 192.11.13.6. Configure your computer for direct connection to the server with the following:

- IP address: 192.11.13.5
- Subnet Mask: 255.255.255.252
- Gateway: 192.11.13.6

You can access the AVP Utilities shell by using the IP Address 192.11.13.6.

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.

Common servers

When Appliance Virtualization Platform is installed, VMNIC0 is assigned to the public interface of virtual machines.

When deploying or reconfiguring Appliance Virtualization Platform:

- If the **Out of Band Management Setup** check box is clear on Create AVP Kickstart, VMNIC0 is used for both network and management traffic.
- If the **Out of Band Management Setup** check box is selected on Create AVP Kickstart, VMNIC2 is used for management by all the virtual machines on that hypervisor.

S8300E

When Appliance Virtualization Platform installs the connection through the media gateway, Ethernet ports are assigned to the public interface of virtual machines. When Appliance Virtualization Platform installs the connection through the media gateway backplane, the LAN port on the G4x0 Gateway is assigned to the public interface of virtual machines.

If Out of Band Management is enabled, the Out of Band Management network is on the LAN2 interface on the S8300E faceplate.

The Appliance Virtualization Platform management interface is assigned to:

- The public VLAN if Out of Band Management is disabled
- The Out of Band Management network if Out of Band Management is enabled

Appliance Virtualization Platform NIC ports

Terminology

- The OS VMNIC ports numbering starts from 0 and refers to the NIC ports from the operating system.
- The server NIC ports numbering starts from 1 and refers to the external physical NIC ports.

  Note:

  Avaya servers might contain up to 8 NIC ports.

The table provides the first four ports. The numbering continues in the same way for values greater than 4.

NIC port	Server NIC	VMNIC port
First NIC port	Server NIC 1	VMNIC 0 or eth0
Second NIC port	Server NIC 2	VMNIC 1 or eth1
Third NIC port	Server NIC 3	VMNIC 2 or eth2
Fourth NIC port	Server NIC 4	VMNIC 3 or eth3

General

- Appliance Virtualization Platform is installed with a fixed network configuration.

  Important:

  Do not change the vSwitch and port group network configuration on Appliance Virtualization Platform. If you change the Appliance Virtualization Platform network configuration, the deployment or the connection to the deployed virtual machines might fail. Solution Deployment Manager maps and creates port groups while deploying the virtual machines as required.
- Appliance Virtualization Platform is installed with a normal or Out of Band Management configuration setup.
- Appliance Virtualization Platform is installed with Out of Band Management disabled or enabled.
  - If you are installing Appliance Virtualization Platform, you can enable Out of Band Management by using the **Out of Band Management Setup** check box on Create AVP Kickstart for generating the kickstart generator file.
  - If the server has Appliance Virtualization Platform preinstalled, Out of Band Management will be disabled. Enable Out of Band Management only if you require.
- Appliance Virtualization Platform is installed on a common server with the following network configuration if Out of Band Management is disabled:
  - Server NIC 1 (VMNIC0): Public and management port. Appliance Virtualization Platform management port is enabled on this Ethernet, and applications are deployed with both Public and Out of Band Management ports assigned to this interface. All IP addresses must be on the same network.
  - Server NIC 2 (VMNIC1): Services Port for use with the technician laptop. Initial Appliance Virtualization Platform installation must use the IP address 192.168.13.5, subnet mask

  255.255.255.248. Connections after AVP Utilities is deployed, use the IP address 192.11.13.5, subnet mask 255.255.255.252 with the gateway set as 192.11.13.6.

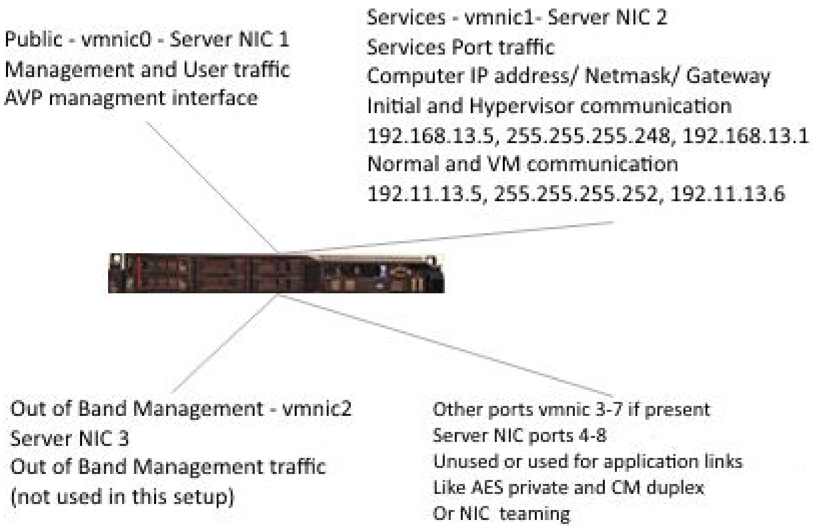
  - Server NIC 3 (VMNIC2): Out of Band Management port. This port is not used in this setup.
  - Server NIC 4–8 (VMNIC3–7): Additional network interfaces for virtual machines, such as duplex Communication Manager and Application Enablement Services private interface. These interfaces can be assigned to a free VMNIC of the installers during the virtual machine deployment.
  - Server NIC 4–8 (VMNIC 8 and later): Any other Ethernet ports that can be used for NIC teaming.

- Appliance Virtualization Platform is installed on a common server with the following network configuration if Out of Band Management is enabled:
  - Server NIC 1 (VMNIC0): Public port and applications Public VMNICs are deployed to this interface. All public virtual machine IP addresses must be on the same network.
  - Server NIC 2 (VMNIC1): Services Port for use with a technician's laptop. Initial Appliance Virtualization Platform installation must use the IP address 192.168.13.5, subnet mask 255.255.255.248. Connections after AVP Utilities is deployed must use 192.11.13.5, subnet mask 255.255.255.252 with the gateway set as 192.11.13.6.
  - Server NIC 3 (VMNIC2): Out of Band Management port. The Appliance Virtualization Platform management port is assigned to this Ethernet. On virtual machines, application interfaces of Out of Band Management are assigned to this Ethernet. The following IP addresses must be on the same network and different from the Public network:
    - Appliance Virtualization Platform management IP address
    - Out of Band Management network IP address of AVP Utilities
    - Out of Band Management IP address of all virtual machines on this Appliance Virtualization Platform host
  - Server NIC 4–8 (VMNIC3–7): Additional network interfaces for virtual machines to a free VMNIC: During the virtual machine deployment, the installer can assign additional network interfaces for virtual machines to a free VMNIC. Duplex Communication Manager and Application Enablement Services private interfaces require additional network interfaces.
  - Server NIC 4–8 (VMNIC 8 and later): Any other Ethernet ports that can be used for NIC teaming.

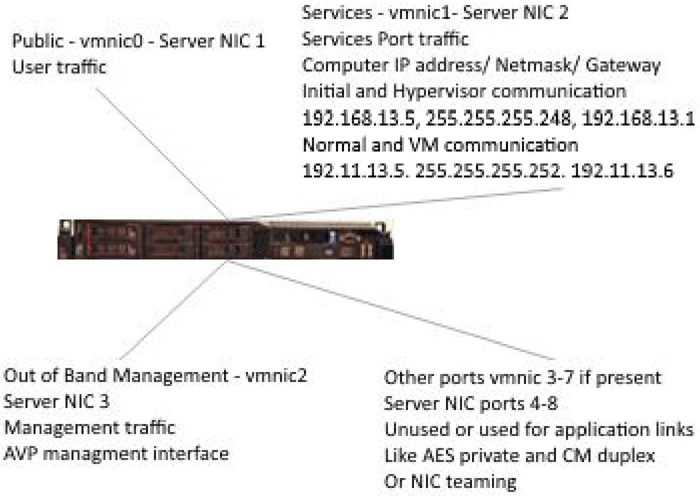
You can change the Out of Band Management state after deployment with the **`set_oobm`** command after you install 7.0.1 on the Appliance Virtualization Platform host. You must perform the configuration through the Services Port on the Appliance Virtualization Platform system and in a very specific order to prevent losing connection to the virtual machines other than is expected during the process.

You must enable Out of Band Management on all virtual machines running on the Appliance Virtualization Platform host. On the same Appliance Virtualization Platform host, you cannot run some virtual machines with Out of Band Management enabled and some with Out of Band Management disabled. Out of Band Management must be enabled from the ks.cfg file on the USB stick or on the Appliance Virtualization Platform by using the **`set_oobm`** command from the Appliance Virtualization Platform shell.

AVP networking in normal or Out of Band Management disabled mode


Public - vmnic0 - Server NIC 1
Management and User traffic
AVP managment interface
Services - vmnic1- Server NIC 2
Services Port traffic
Computer IP address/ Netmask/ Gateway
Initial and Hypervisor communication
192.168.13.5, 255.255.255.248, 192.168.13.1
Normal and VM communication
192.11.13.5, 255.255.255.252, 192.11.13.6
Out of Band Management - vmnic2
Server NIC 3
Out of Band Management traffic
(not used in this setup)
Other ports vmnic 3-7 if present
Server NIC ports 4-8
Unused or used for application links
Like AES private and CM duplex
Or NIC teaming

AVP networking Out of Band Management enabled


Public - vmnic0 - Server NIC 1
User traffic
Services - vmnic1- Server NIC 2
Services Port traffic
Computer IP address/ Netmask/ Gateway
Initial and Hypervisor communication
192.168.13.5, 255.255.255.248, 192.168.13.1
Normal and VM communication
192.11.13.5. 255.255.255.252. 192.11.13.6
Out of Band Management - vmnic2
Server NIC 3
Management traffic
AVP managment interface
Other ports vmnic 3-7 if present
Server NIC ports 4-8
Unused or used for application links
Like AES private and CM duplex
Or NIC teaming

Teaming NICs from CLI

About this task

You can configure the NIC teaming and NIC speeds on Appliance Virtualization Platform from the web interface of the Solution Deployment Manager client and System Manager Solution Deployment Manager. For more information, see *Administering Avaya Aura® System Manager*.

Avaya recommends the use of Solution Deployment Manager web interface for configuring the NIC settings.

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”.

You cannot perform NIC teaming for S8300E server.

Procedure

1. Log in to the Appliance Virtualization Platform host command line, and type `# /opt/avaya/bin/nic_teaming list`.

   The system displays the current setup of the system, and lists all vmnics.

   For example:

   ```
   Current Setup:
   Name: vSwitch0
   Uplinks: vmnic0
   Name: vSwitch1
   Uplinks: vmnic1
   Name: vSwitch2
   Uplinks: vmnic2
   List of all vmnics on host:
   vmnic0
   vmnic1
   vmnic2
   vmnic3
   ```

2. To add a free vmnic to a vSwitch, type `# /opt/avaya/bin/nic_teaming add <vmnic> <vSwitch>`.

   The command changes the links to the active standby mode.

   For example, to add eth3 to the public virtual switch, type `# /opt/avaya/bin/nic_teaming add vmnic3 vSwitch0`. To verify the addition of eth3, type `esxcli network vswitch standard policy failover get -v vSwitch0`.

   The system displays the following message:

   ```
   Load Balancing: srcport
   Network Failure Detection: link
   Notify Switches: true
   Failback: true
   Active Adapters: vmnic0
   Standby Adapters: vmnic3
   Unused Adapters:
   ```

3. To add eth3 to the list of active adapters, type `# esxcli network vswitch standard policy failover set -v vSwitch0 --active-uplinks vmnic0,vmnic3`.

   The command changes the vmnic3 to the active mode.

4. To verify the mode of eth3, type `# esxcli network vswitch standard policy failover get -v vSwitch0`.

The system displays the following message:

```
Load Balancing: srcport
Network Failure Detection: link
Notify Switches: true
Failback: true
Active Adapters: vmnic0, vmnic3
Standby Adapters:
Unused Adapters:
```

5. To remove a vmnic from a vSwtich, type `# /opt/avaya/bin/nic_teaming remove <vmnic> <vSwitch>`.
6. To move an additional vmnic back to standby mode, type `# esxcli network vswitch standard policy failover set -v vSwitch0 --active-uplinks vmnic0 --standby-uplinks vmnic3`

   This puts the additional NIC back to standby mode.
7. To verify if the vmnic is moved to standby, type `# esxcli network vswitch standard policy failover get -v vSwitch0`.

   The system displays the following:

```
Load Balancing: srcport
Network Failure Detection: link
Notify Switches: true
Failback: true
Active Adapters: vmnic0
Standby Adapters: vmnic3
Unused Adapters:
```

⚠ **Warning:**

The management and virtual machine network connections might be interrupted if you do not use correct network commands. Do not remove or change vmnic0, vmnic1, and vmnic2 from vSwitches or active modes.

Related links

NIC teaming modes on page 26

NIC teaming modes

Appliance Virtualization Platform supports two modes of NIC teaming: Active-Standby and Active.

Active-Standby

In normal operation all the traffic goes through the active NIC setup. If this connection fails, the other standby link is activated and all the traffic uses the standby link. The settings for active and standby setup are:

- Network failover detection: Link status only
- Notify Switches: Yes

- Failback: Yes. If the active NIC becomes available again, you can use the active NIC over the standby NIC.

Active-Active

This is an active setup that uses route based load balancing based on the originating virtual port ID. This is a basic form of load balancing that may not provide full capacity of both links.

- Load Balancing: Route based on the originating virtual port ID
- Network failover detection: Link status only
- Notify Switches: Yes
- Failback : Yes

Setting the Ethernet port speed

About this task

Avaya recommends that the Appliance Virtualization Platform server, Ethernet ports, and the switch ports to which the ports are connected must be set to autonegotiate on both the server and the customer network switch.

Important:

Use the procedure only if you must change the Ethernet port speeds. Incorrect setting of Ethernet NIC speeds might result in performance issues or loss of network connection to the system.

You cannot change the Ethernet port speed for the S8300E server.

Procedure

1. Log in to the Appliance Virtualization Platform host command line.
2. To list vmnics, type `#/opt/avaya/bin/nic_port list`.

   You must provide the full path.
3. To set a port to 1000 Mbps full duplex, type `/opt/avaya/bin/nic_port set <100|1000> <vmnic>`.

   Where 100 or 1000 is the speed in Mbps, and vmnic is the vmnic number. For example, vmnic0 for the public interface of the server.

   Note:

   Half duplex and 10 Mbps speeds are not supported for use with Appliance Virtualization Platform. Use 100 Mbps only in specific instances, such as while replacing a server that was previously running at 100Mbps. All NIC ports must be connected to the network at least 1Gbps speeds. Most server NICs support 1Gbps.
4. Type `#/opt/avaya/bin/nic_port set auto vmnic`.

Note:

The default setting for ports is autonegotiate. You do not require to configure the speed in normal setup of the system.

Supported TLS version

Appliance Virtualization Platform Release 7.1 and later supports the TLS version 1.2. By default, TLS versions 1.0 and 1.1 are disabled, but you can enable, if required.

Chapter 4: Planning and preconfiguration

Configuration tools and utilities

You must have the following tools and utilities for deploying, upgrading, and configuring Appliance Virtualization Platform:

- A browser for accessing Appliance Virtualization Platform by using the System Manager web interface
- An Solution Deployment Manager client running on your computer if System Manager is unreachable
- An SFTP client for Windows, for example WinSCP
- An SSH client, for example, PuTTy

Supported servers

In the Avaya appliance model, you can deploy or upgrade to Avaya Aura® Release 8.0.1 applications on the following Avaya-provided servers:

- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9
- S8300E, for Communication Manager and Branch Session Manager
- Avaya Converged Platform 120 Server: Dell PowerEdge R640

  Note:

  - Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.
  - Release 7.0 and later does not support S8510 and S8800 servers.

Software details of Appliance Virtualization Platform

The following table lists the software details of all the supported platform for the application. You can download the softwares from the Avaya PLDS website at http://plds.avaya.com/.

Table 1: Appliance Virtualization Platform build details

Release	Bundle offer type	Installer files
8.0.1	Installer	`avaya-avp-8.0.1.0.0.08.iso`
8.0.1	Upgrade bundle	`upgrade-avaya-avp-8.0.1.0.0.08.zip`
8.0.1	Solution Deployment Manager Client	`Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip` contains the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe` file.

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 of only System Manager and hypervisor patches of Appliance Virtualization Platform.

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_8.0.1.0.0332099_11.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 **8.0.x**.
3. Click the **Avaya Aura® System Manager Release 8.0.x SDM Client Downloads, 8.0.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_8.0.1.0.0332099_11.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. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:
   1. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   2. To change the default software library directory on windows, 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.
   3. In **Data Port No**, select the appropriate data port.

      The default data port is 1527. The data port range is from 1527 through 1627.
   4. 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.
   5. **(Optional)** Click **Reset All to Default** to reset all values to default.
10. Click **Next**.

11. 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 user must make the required disk space, memory, and the ports available to start the installation process again.

12. Click **Install**.
13. On the Install Complete page, click **Done** to complete the installation of Solution Deployment Manager Client.

    Once the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.

14. To start the client, click the Solution Deployment Manager client icon, SDM CLIENT.

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*.

Chapter 5: Appliance Virtualization Platform deployment and configuration

Appliance Virtualization Platform deployment

You can deploy Appliance Virtualization Platform in two modes: Unattended and Attended.

- **Unattended mode:** In this mode, you need to save a copy of the Appliance Virtualization Platform 8.0 kickstart file (`avp80ks.cfg`) in a USB drive. The USB must be in the FAT32 format. You need to insert the USB drive and the Appliance Virtualization Platform DVD into the server. The system will perform the Appliance Virtualization Platform deployment.

  You can generate the kickstart file (`avp80ks.cfg`) from Solution Deployment Manager.
- **Attended mode:** With Appliance Virtualization Platform Release 7.1.2 and later, this is a new mode of deployment. In this mode, you need to insert the Appliance Virtualization Platform DVD into the server and follow the prompt to deploy Appliance Virtualization Platform.

  The Appliance Virtualization Platform DVD contains the `firstboot.sh` script. After the Appliance Virtualization Platform installation, the default path of the script is `/opt/avaya/bin/firstboot.sh`.

Appliance Virtualization Platform deployment in unattended mode

Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Generate AVP Kickstart**.

3. On Create AVP Kickstart, do the following:
    a. Select **8.0.x**.
    b. Enter the appropriate information in the fields.
    c. Click **Generate Kickstart File**.

       For more information, see "Create AVP Kickstart field descriptions."

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

       For Appliance Virtualization Platform Release 8.0 and later, the kickstart file name must be `avp80ks.cfg`.

Related links

Create AVP Kickstart field descriptions on page 34

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 at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
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

Table continues…

Name	Description
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 S8300E only)	VLAN ID for the S8300E server. 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 the S8300E server.
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 S8300E only)	• For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 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.

Table continues…

Name	Description
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 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 33

Configuring the Appliance Virtualization Platform USB drive

Before you begin

Use the USB drive that Avaya provides in the media kit for this procedure. The provided USB is a FAT 32 format. If you must use a different USB, use a FAT 32 format file.

Procedure

1. Generate the Appliance Virtualization Platform kickstart file by using Solution Deployment Manager.

   See *Migrating and Installing Avaya Aura® Appliance Virtualization Platform*.
2. Save a copy of `avp80ks.cfg` on the USB drive.

Next steps

Install Appliance Virtualization Platform.

Deploying Appliance Virtualization Platform

Before you begin

- Configure the Appliance Virtualization Platform USB drive.
- Ensure that the backup file is saved on a different server because after the Appliance Virtualization Platform installation, server restarts, and all data is lost.
- To use the Solution Deployment Manager client for deploying the virtual machines, install the Solution Deployment Manager client on your computer.

Note:

To deploy Appliance Virtualization Platform server while connected to the customer network, ensure that the IP address used for Appliance Virtualization Platform is not in use by another system. If the configured IP address is already in use on the network during installation, the deployment process stops. You must remove the duplicate IP address, and restart the deployment.

Procedure

1. Insert the USB drive and the Appliance Virtualization Platform DVD into the server.

   Use an external Avaya-approved USB DVD drive for deploying Appliance Virtualization Platform on S8300E. The only supported USB DVD drive is Digistor DIG-72032, Digistor DIG73322, comcode 700406267.

2. Perform one of the following:

   - For new deployment, reboot the server or power-cycle the server.
   - For migrating from System Platform to Appliance Virtualization Platform, log on to the System Platform web console, and click **Server Management** > **Server Reboot/ Shutdown** > **Reboot** to restart the server.

   Warning:

   When the server restarts, Appliance Virtualization Platform is deployed, and all existing data on the server is lost.

   The system deploys Appliance Virtualization Platform and ejects DVD. The deployment process takes about 30 minutes to complete.

   Note:

   If using a monitor, the screen changes to black before the deployment is complete. A message in red text might briefly display, which is an expected behavior. Do not take any action.

3. Remove the USB drive and Appliance Virtualization Platform DVD.

   Note:

   When installing Appliance Virtualization Platform on an HP server, you must remove the USB drive when the server ejects DVD. Otherwise, the server might become nonoperational on reboot. If the server becomes nonoperational, remove the USB drive, and restart the server.

4. Using an SSH client, connect to the server through the eth1 services port by using the following network parameters for your system:

   - IP address: 192.168.13.5
   - Netmask: 255.255.255.248
   - Gateway: 192.168.13.1

   The SSH client must use UTF-8 and TLS 1.2. Alternatively, you can connect to the public network address that was configured during the installation from a computer on the customer network.

   You can access the Appliance Virtualization Platform host with IP address: 192.168.13.6.

5. Log in to Appliance Virtualization Platform as admin and provide the password that is configured in the Kickstart file.

   The system displays the End user license agreement (EULA) screen.

6. Read the EULA, and type `Y` to accept the terms.

   You can press any key to read EULA, and use the space bar to scroll down.

   ⚠ **Warning:**

   Accept EULA before you deploy virtual machines. If deployments are attempted before you accept EULA, deployments fail.

7. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
8. Add a location.
9. Add the Appliance Virtualization Platform host as 192.168.13.6.
10. Install the Appliance Virtualization Platform patch, if applicable.

    For more information, see Installing the Appliance Virtualization Platform patch from Solution Deployment Manager.

11. Perform one of the following:

    - For deploying on new server, deploy the AVP Utilities virtual machine, and then all other virtual machines.
    - For migrating from System Platform Server to Appliance Virtualization Platform, deploy the AVP Utilities virtual machine, and then all other virtual machines with the data that you noted in “System Platform and Template values”.

    For instructions to deploy AVP Utilities and other virtual machines, see *Deploying Avaya Aura® AVP Utilities in a virtual appliance* and product-specific deployment guides.

12. From System Manager Solution Deployment Manager, install the required software patches for the virtual machines.

Appliance Virtualization Platform deployment in attended mode

Deploying Appliance Virtualization Platform using a setup script

About this task

This procedure is applicable only for the Avaya Common Servers and is not applicable for the S8300E server.

Before you begin

- Configure the laptop for direct connection to the server.
- Obtain the Appliance Virtualization Platform DVD.

Procedure

1. Connect the VGA console and USB keyboard from server to computer.
2. Turn on the server.
3. Insert the Appliance Virtualization Platform DVD into the server DVD drive.
4. The server starts from the DVD.
5. On the avaya-avp Boot Menu window, select **NO USB avaya-avp Installer**, and press `Enter`.

   Wait for ESXi to boot. This takes several minutes.
6. To start the deployment, on the Welcome to the VMware ESXi 6.0.0 Installation window, press `Enter`.
7. On the End user License Agreement (EULA) window, select EULA, and press `F11`.
8. On the Select a Disk to Install or Upgrade window, select the correct hard drive is selected, and press `Enter`.

   The system displays a Confirm Disk Selection message.
9. To confirm the disk selection, press `Enter`.
10. **(Optional)** If the system displays the option to upgrade or install, use arrow keys to select Install ESXi, overwrite VMFS datastore, and press `Enter`.

    This will delete all data on the drive.
11. On the Please select a keyboard layout window, select the layout type, and press `Enter`.
12. On the Enter a root password window, type the root password, and press `Enter`.

    The system displays a message for scanning the system. This takes several minutes.
13. To install ESXi 6.0.0, on the Confirm Install window, press `F11`.

    When the system completes the deployment, the system displays the Installation Complete window.
14. Remove the Appliance Virtualization Platform DVD.
15. To reboot the system, press `Enter`.

    The system displays the Rebooting Server window. The system shuts down and reboots the server. The system displays the host IP address as 0.0.0.0.

Next steps

Assign IP address.

Host IP address assignment

The ESXi uses DHCP to assign a local IP address to eth0. If the action fails, you can assign the IP address using the System Customization window.

Assigning host IP address using System Customization

Procedure

1. On the console, press `F2`.

   The system prompts you to provide the credentials that you configured during installation to connect to localhost.
2. On the Authentication Required window, in the **Login Name** and **Password** fields, type the credentials.
3. On the System Customization window, use the arrow key to select **Configure Management Network**.
4. Use the arrow key to select **IP Configuration**, and press `Enter`.

   IP Address must be different from your computer IP address.
5. In the **Netmask** field, type the netmask IP address.
6. Press `Enter`.

Configuring the Appliance Virtualization Platform network and other parameters

Procedure

1. Log in to the ESXi host as root using the link local IP address.
2. To execute the script, run the command **`/opt/avaya/bin/firstboot.sh`**.

   The system prompts you to configure the network parameters.
3. Specify the required parameters in the fields.

   For specifying the required parameters, see “Network parameters field descriptions”.
4. After entering the values, the system displays a message: `Is this what you want?`
5. Type `y`.

   The system displays a message: `Reconfiguration started..`

   Wait for the host to reboot. On the console, the system displays the host IP address that you configured.

6. The system prompts you to enable or disable the stricter password policy. To enable stricter password policy, type `y`.

   The system displays the following message:

   ```
   For security concern, root account will be locked out after AVP
   installation. A new 'admin' account will be created.
   YOU WILL BE ASKED TO ENTER PASSWORD FOR NEW 'admin' ACCOUNT!
   ```

7. Type the new password, which meets the password policy chosen at step 6.
8. At the **Can you log onto this system using 'admin' account** prompt, type one of the following:
   - `y`: If the new password works, the system disables the root account and creates a new admin account.
   - `n`: If the new password does not work, the system prompts you to retype the password for the new admin account.

Related links

Network parameters field descriptions on page 41
Enable Stricter Password Policy field descriptions on page 42

Network parameters field descriptions

Name	Description
IP Address	Specifies the IP address of Appliance Virtualization Platform.
Netmask	Specifies the netmask.
Gateway	Specifies the gateway IP address.
Hostname	Specifies the host name of Appliance Virtualization Platform.
Domain (Optional)	Specifies the domain name.
(Optional) **Primary DNS Server**	Specifies the primary DNS server IP address.
(Optional) **Secondary DNS server**	Specifies the secondary DNS server IP address.
NTP Server	Specifies the NTP server IP address.
Enable OOBM	Enables or disables the Out of Band Management configuration. The values are `y` and `n`. Default value is `n`.

Related links

Configuring the Appliance Virtualization Platform network and other parameters on page 40

Enable Stricter Password Policy field descriptions

Name	Description
Enable Stricter Password Policy	Enables or disables the stricter password policy. The default value is n. • n: If you set the value to `n`, the minimum password length is 8. • y: If you set the value to `y`, the minimum password length is 14.

Related links

Configuring the Appliance Virtualization Platform network and other parameters on page 40

Configuring IPv6 using System Customization

Procedure

1. On the console, press `F2`.

   The system prompts you to provide the credentials that you configured during installation to connect to localhost.
2. On the Authentication Required window, in the **Login Name** and **Password** fields, type the credentials.
3. On the System Customization window, use the arrow key to select **IP Configuration**, and press `Enter`.
4. On the IPv6 Configuration dialog box, in the **Static Address #1** field, type the IPv6 address.

   For example: 2a07:2a42:xyz0:20::27::145/46
5. Press `Enter`.

Configuring servers preinstalled with Appliance Virtualization Platform

About this task

For newly purchased common servers, Appliance Virtualization Platform is preinstalled. This does not apply for migration. You must configure the customer network settings through the Solution Deployment Manager client that is installed on a computer that is running Windows. The media comes with the server.

Procedure

1. Turn on the server.
2. Install the Solution Deployment Manager client on the computer.
3. Configure the computer with the following:
    - IP address: 192.168.13.5
    - Netmask: 255.255.255.248
    - Gateway: 192.168.13.1
4. Connect to NIC2 with a network cable.
5. Start an SSH session, log in to 192.168.13.6 with admin credentials.

    The system prompts to change the password immediately.
6. To change the admin password, perform the following:
    a. At the prompt, type the Appliance Virtualization Platform default password: AVaya@01
    b. Type the new password.

        For more information about password rules, see “Password policy”.
    c. Type the password again.

        The system changes the host password.
7. To accept the EULA, in **Do you accept the terms of this EULA? (Y)es/(N)o**, type `Y`.
8. 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.

9. Type `cd /opt/avaya/bin`.

   Not all commands are available in the `/opt/avaya/bin` location, and must be run with ./. For example, `./nic_port`. The system only runs the commands that are specified in the procedure from `/opt/avaya/bin` or as directed by Avaya Services. The system might get incorrectly configured if you run commands that are not specified in the procedure.

   Most systems do not enable Out of Band Management. Use the **`/opt/avaya/bin/set_oobm enable`** command only to enable Out of Band Management for the host and all virtual machines.

10. **(Optional)** To enable Out of Band Management on the Appliance Virtualization Platform host, type `/opt/avaya/bin/set_oobm enable`.

    The system displays `Host Out of Band Management set up is complete`.

11. At the prompt, do the following:

    a. Type `/opt/avaya/bin/./serverInitialNetworkConfig`.

       The host IP address details are mandatory. Though DNS and NTP values are optional, you must provide the values.

    b. At the prompt, provide the following host details:

```
System is not in a default setup, please use SDM to change IP addresses
Do you wish to setup networking? (y/n)  y
Please enter IP address for the AVP host in the format x.x.x.x
For example 172.16.5.1
Please enter value    172.16.107.21
Please enter subnet mask for the AVP host in the format x.x.x.x
For example 255.255.255.0
Please enter value    255.255.255.0
Please enter a default gateway for the AVP host in the format x.x.x.x
For example 172.16.5.254
Please enter value    172.16.107.1
Please enter a hostname for the AVP host.
For example myhost
Please enter value    avphost
Please enter a domain for the AVP host.
For example mydomain.com
Please enter value    mydomain.com
Please enter a main DNS server for the AVP host.
For example 172.16.10.54
Please enter value    172.16.107.1
Please enter a secondary DNS server for the AVP host.
For example 172.16.10.54
Please enter value    172.16.107.2
Please enter a NTP server for the AVP host
For example 172.16.10.55
Please enter value    172.16.107.50
Stopping ntpd
watchdog-ntpd: Terminating watchdog process with PID 33560
Starting ntpd
```

12. To verify the vmk0 settings, type `esxcli network ip interface ipv4 get`.

    Note:

    Do not change the vmk1s address. vmk1s is fixed for the services port.

    The system displays the following details:

```
Name  IPv4 Address   IPv4 Netmask     IPv4 Broadcast  Address Type  DHCP DNS
----  -------------  ---------------  --------------  ------------  --------
vmk1  192.168.13.6   255.255.255.248  192.168.13.7    STATIC           false
vmk0  172.16.107.21  255.255.255.0    172.16.107.255  STATIC           false
```

13. Start the Solution Deployment Manager client when connected to the services port.
14. Add a location.
15. Add the Appliance Virtualization Platform host as 192.168.13.6.
16. Check the version, and install the Release 8.0.1 feature pack on Appliance Virtualization Platform if required.
17. Install an Appliance Virtualization Platform host license and configure the WebLM Server address by using System Manager Solution Deployment Manager or Solution Deployment Manager Client, if it has not been configured in step 11 on page 44.

    For information about installing and configuring Appliance Virtualization Platform license, see “Installing and configuring Appliance Virtualization Platform licensing”.
18. Deploy AVP Utilities.
19. Deploy other Avaya Aura® applications that will reside on this Appliance Virtualization Platform host.
20. Install the Release 8.0.1 patch files for all Avaya Aura® applications, if applicable.

Related links

Password policy on page 46

Enabling IP forwarding using Services Port VM for AVP Utilities

About this task

IP Forwarding is always disabled after an installation, regardless of the mode of deployment. Use the following procedure to enable IP Forwarding.

Note:

For security reasons, you must always disable IP forwarding after finishing your task.

Procedure

1. Start an SSH session.

2. Log in to AVP Utilities as admin.
3. In the command line, perform one of the following:
   - To enable IP forwarding, type `IP_Forward enable`.
   - To disable IP forwarding, type `IP_Forward disable`.
   - To view the status of IP forwarding, type `IP_Forward status`.

Example

```
IP_Forward enable
Enabling IP Forwarding
Looking for net.ipv4.ip_forward in /etc/sysctl.conf
Status of IP Forwarding
..Enabled
```

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 at the end.

  Note:

  An Uppercase letter at the beginning of a password is not counted for the password complexity rule. The Uppercase letter must be within the password.

  Example of a valid password is *myPassword$*.

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.

Activating SSH from AVP Utilities

About this task

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

When you install or preinstall Appliance Virtualization Platform on a server, SSH is enabled. After you accept the license terms during Appliance Virtualization Platform installation, SSH shuts down within 24 hours. After SSH shuts down, you must reactivate SSH by using the **`AVP_SSH enable`** command from AVP Utilities.

Before you begin

Start an SSH session.

Procedure

1. Log in to the AVP Utilities virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type the following:

   ```
   AVP_SSH enable
   ```

   Within 3 minutes, from AVP Utilities, the SSH service starts on Appliance Virtualization Platform and runs for two hours. After two hours, you must reactivate SSH from AVP Utilities.

   When SSH is enabled, you can use an SSH client such as PuTTY to gain access to Appliance Virtualization Platform on customer management IP address or the services port IP address of 192.168.13.6.
3. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
4. To disable SSH, type `AVP_SSH disable`.

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. To continue access, 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** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, do the following:
   a. Click **More Actions** > **SSH** > **Enable SSH**.
   b. In the Confirm dialog box, in the **Time (in minutes)** field, type the time after which the system times out the SSH connection.

      The range is 10 minutes through 120 minutes.
   c. Click **Ok**.

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

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

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

Chapter 6: Administration

Managing the location

Viewing a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application 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** > **Application Management**.
2. On the **Locations** 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 **Application Management Tree** section.

Related links

New and Edit location field descriptions on page 50

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** 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 50

Deleting a location

Procedure

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

   The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

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.

Table continues…

Name	Description
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 operations, and returns to the Locations section.

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 a 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 another host , the system displays the following error message:

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

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
5. In the New Platform section, do the following:
    a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

       For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root user name.
    b. In **Platform Type**, select **AVP/ESXi**.
    c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.
6. Click **Save**.
7. In 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, Solution Deployment Manager displays the error. To generate certificate, see VMware documentation.

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

       For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
    c. Click **More Actions** > **Refresh App**.

> **Important:**
>
> When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure that AVP Utilities is available.

9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** 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. In Application 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.

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 .

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform 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, do 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.

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:

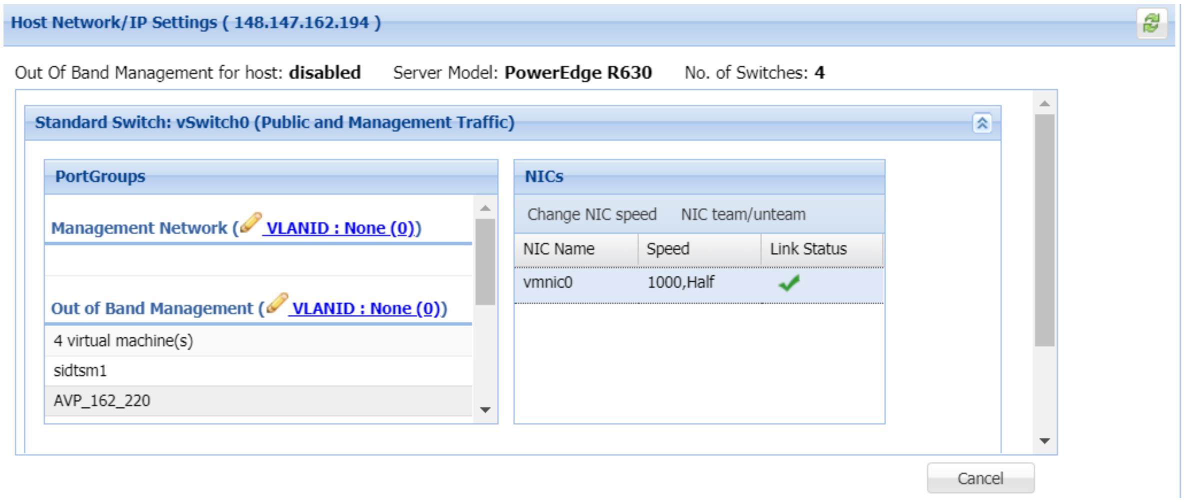
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fail because the 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 so that the FQDN changes reflect in Solution Deployment Manager.

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params** > **Change Network Settings**.



Host Network/IP Settings (148.147.162.194)

Out Of Band Management for host: **disabled**   Server Model: **PowerEdge R630**   No. of Switches: **4**

Standard Switch: vSwitch0 (Public and Management Traffic)

PortGroups

Management Network (VLANID : None (0))

Out of Band Management (VLANID : None (0))

4 virtual machine(s)

sidtsm1

AVP_162_220

NICs

NIC Name	Speed	Link Status
vmnic0	1000,Half	✓

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, do the following:
    a. Expand the Standard Switch: vSwitch<n> section by clicking the downward arrow .

    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.

      For more information about the value, see NIC teaming.

   d. Click **OK**.

   The system displays the new VLAN ID.

6. To change the NIC speed, do 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 a check mark ✓ in **Link Status**.

   Note:

   You can change the speed only for common servers. You cannot change the speed for the S8300E server.

7. To change the NIC teaming, do 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 the host network IP settings, click **Refresh** ⟳.

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for the S8300E server.

Related links

Host Network / IP Settings field descriptions on page 61

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. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. At the command prompt of the host, do the following:
    a. To change the IP address, 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
    ```

4. Enable SSH on Appliance Virtualization Platform and run the **`/opt/avaya/bin/./serverInitialNetworkConfig`** command.

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

Related links

Configuring servers preinstalled with Appliance Virtualization Platform on page 42

Enabling or disabling IPv6

About this task

Use the following procedure to convert the IPv4 host system to IPv6.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. To enable IPv6, do the following:
    1. Type the **`/opt/avaya/bin/set_dualstack enable`** command.
    2. Type the IPv6 address with subnet length.
    3. Type the IPv6 gateway address.
    4. To add the IPv6 capable DNS servers, type the IPv6 address of DNS Server.

       The default value is `n`.
    5. To add the IPv6 capable NTP servers, type the IPv6 address of NTP Server.

       The default value is `n`.
3. To disable IPv6, type the **`/opt/avaya/bin/set_dualstack disable`** command.

Changing the password for an Appliance Virtualization Platform host

About this task

Use this procedure to change the password for the Appliance Virtualization Platform host. This is the password for the administrator that you provide when deploying the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, do the following:
    1. Select a host.
    2. 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 46

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** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Lifecycle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Shutting down Appliance Virtualization Platform host from CLI

About this task

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh`.

   The system displays `Are you sure you want to stop all VMs and shutdown?`
3. To confirm the shutdown operation, type `Y`.

   The system shuts down Appliance Virtualization Platform host, and stops all virtual machines running on the Appliance Virtualization Platform host. The host does not restart automatically.

You must manually turn on the Appliance Virtualization Platform server. All virtual machines running on Appliance Virtualization Platform automatically start.

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** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

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

Related links

Restarting Appliance Virtualization Platform or an ESXi host on page 60

Rebooting the Appliance Virtualization Platform host from CLI

Before you begin

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh -r`.

   The system displays `Are you sure you want to stop all VMs and reboot?`.

> **Warning:**
>
> If you fail to provide the -r option, the system displays `Are you sure you want to stop all VMs and shutdown?` and assumes that you want to perform the shutdown operation.
>
> If you use the shutdown option when reset is intended, the host does not restart as part of the process and you must manually start the server.

3. To confirm the reboot operation, type `Y`.

   The system stops all virtual machines that are running on the Appliance Virtualization Platform host. The Appliance Virtualization Platform host reboots and restarts all virtual machines automatically.

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 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 of the Appliance Virtualization Platform host.
IPv6	The IPv6 address of the Appliance Virtualization Platform host (if any).
Host Name	The host name of the Appliance Virtualization Platform host

Table continues…

Name	Description
Domain Name	The domain name of 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 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.
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.

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.

Appliance Virtualization Platform alarming

The Serviceability Agent that runs on AVP Utilities generates Appliance Virtualization Platform SNMP alarm messages. The alarm messages are then sent to the System Manager or Network Management System (NMS) depending on the configuration. Serviceability Agent converts specific rsyslog entries to SNMP traps.

You can configure the destination of alarm messages by using one of the following:

- The System Manager web console.
- AVP Utilities.

Note:

If System Manager does not exist in the solution, then you can configure NMS by using AVP Utilities.

For information about configuring Appliance Virtualization Platform alarming, see *Administering Avaya Aura® AVP Utilities*.

Chapter 7: Installing and configuring Appliance Virtualization Platform licensing

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.

For information about Appliance Virtualization Platform licenses and supported server types, see “Appliance Virtualization Platform licenses for supported servers”.

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 **Platforms** tab of the System Manager Solution Deployment Manager or Solution Deployment Manager Client interfaces. The Appliance Virtualization Platform license statuses on the **Platforms** 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.

  Note:

  Restricted administrative actions for:

  - **AVP Host: AVP Update/Upgrade Management**, **Change Password**, **Host Shutdown**, and **AVP Cert. Management**.
  - **Application: 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 *Administering Avaya Aura® AVP Utilities*.

Appliance Virtualization Platform licenses for supported servers

The following table describes the applicable Appliance Virtualization Platform license type for S8300E and Common Server Release 2 and 3:

Server type	Appliance Virtualization Platform license feature keyword	Appliance Virtualization Platform license feature display name
• Avaya S8300E	VALUE_AVP_1CPU_EMBD_SRVR	Maximum AVP single CPU Embedded Servers
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

Table continues…

Server type	Appliance Virtualization Platform license feature keyword	Appliance Virtualization Platform license feature display name
Common Server Release 3 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9	VALUE_AVP_XL_SRVR	Maximum AVP XL Server

The following table describes the applicable Appliance Virtualization Platform license type for Avaya Converged Platform 120 Server:

Avaya Converged Platform 120 Server: Dell PowerEdge R640	Appliance Virtualization Platform license feature keyword	Appliance Virtualization Platform license feature display name
Profile 2	VALUE_AVP_1CPU_CMN_SRVR	Maximum AVP single CPU Common Servers
Profile 3	• VALUE_AVP_2CPU_CMN_SRVR • VALUE_AVP_XL_SRVR	• Maximum AVP dual CPU Common Servers • Maximum AVP XL Server
Profile 4	VALUE_AVP_1CPU_CMN_SRVR	Maximum AVP single CPU Common Servers
Profile 5	• VALUE_AVP_2CPU_CMN_SRVR • VALUE_AVP_XL_SRVR	• Maximum AVP dual CPU Common Servers • Maximum AVP XL Server

WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

License activations in PLDS require the host ID of the WebLM server for inclusion in the license file. The host ID of the WebLM server is displayed on the Server Properties page of the WebLM server.

Obtaining the license file

About this task

For each licensed Avaya product that you are managing from the WebLM server, you can obtain a license file from PLDS, and install it on the corresponding WebLM server. For additional information on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at https://plds.avaya.com.

⚠ **Caution:**

> Do not modify the license file that you receive from Avaya. WebLM does not accept a modified license file.

You require the host ID of the WebLM server to obtain the license file from PLDS. For client node locking, while generating the license file, you must provide the WebLM server host ID and client host ID.

Procedure

1. Log on to the System Manager web console.
2. On the System Manager Web Console, click **Services** > **Licenses**.
3. In the left navigation pane, click **Server properties**.
4. Note the **Primary Host ID**.
5. Using the host ID, generate the license from PLDS.

Installing a license file

About this task

You can install a license file on the WebLM server. Use the Uninstall functionality to remove the license file from the WebLM server.

Licenses installed for WebLM Release 7.1 and later, must support SHA256 digital signature and 14–character host ID.

Before you begin

- Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
- Log on to the WebLM web console with administrator privilege credentials.
- For standard license file, remove the older license file before you install the new file.

  Note:

  The system displays an error message if an older license file is still available.

  For centralized license file, the system automatically overwrites the older license file during installation.

For information about the license file installation errors while installing the license file, see *Administering standalone Avaya WebLM*.

Procedure

1. In the navigation pane, click **Install license**.
2. On the Install license page, click **Browse**, and select the license file.
3. Read the terms and conditions, and click **Accept the License Terms & Conditions**.
4. Click **Install**.

   WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as:

   - The digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Related links

Install license field descriptions on page 69

Install license field descriptions

Name	Description
Enter license path	The complete path where the license file is saved.
Browse	The option to browse and select the license file.
Avaya Global License Terms & Conditions	Avaya license terms and conditions that the user must agree to continue the license file installation.

Button	Description
Install	Installs the product license file.

Related links

Installing a license file on page 68

Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager

Before you begin

1. Add an Appliance Virtualization Platform host.

   For information about adding a host, see *Administering Avaya Aura® System Manager*.

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** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms 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 **Platforms** tab, click **Refresh**.

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

Related links

WebLM Configuration field descriptions on page 70

Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager on page 72

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.
Cancel	Closes the WebLM Configuration dialog box.

Related links

[Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager](#) on page 69

Configuring WebLM Server for an Appliance Virtualization Platform host from CLI

Before you begin

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

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To configure the Appliance Virtualization Platform WebLM server, type `/opt/avaya/bin/weblmurl <option> <WEBLM_SERVER_IP>`:

   Where, <*WEBLM_SERVER_IP*> is the IP Address and FQDN of WebLM Server on which the license file is installed.

   Options are:

   - **-h or -?:** To display command help.
   - **-c:** To set a complete WebLM URL with IP Address and FQDN.
   - **-x:** To display the current setting of WebLM URL.
   - **-d:** To set the WebLM URL to the default (dummy) URL.
   - **-g:** To display the URL of the WebLM GUI.
   - **-i:** To display the IP Address of the WebLM URL.

   Note:

   a. To set a complete WebLM URL, type `/opt/avaya/bin/weblmurl -c https://<WEBLM_SERVER_IP>:52233/WebLM/LicenseServer`.

      For example: `/opt/avaya/bin/weblmurl -c https://13.16.15.72:52233/WebLM/LicenseServer`

   b. To set a default WebLM URL, type `/opt/avaya/bin/weblmurl -d <WEBLM_SERVER_IP>`.

4. Verify the Appliance Virtualization Platform license status.

Related links

Verifying the Appliance Virtualization Platform license status from host CLI on page 72

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Related links

Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager on page 69

Verifying the Appliance Virtualization Platform license status from host CLI

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. Perform one of the following:
   a. To display license status, type `/opt/avaya/bin/statuslicense --printLicStatus`.
   b. To display feature details associated with the license, type `/opt/avaya/bin/statuslicense --printFeature`.
   c. To display grace period with timestamp, type `/opt/avaya/bin/statuslicense --printGracePeriod`.

Chapter 8: Security

Extended security hardening

Appliance Virtualization Platform supports Standard, Commercial, and Military Grade security hardening. By default, Appliance Virtualization Platform comes with Standard Grade hardening configuration, no additional action is required to set up this configuration.

Commercial and military grade hardening apply specific security attributes as summarized in the following table:

Security attribute	Commercial grade	Military grade
Restricting system Access (SSH, DCUI, ESXi Shell) to appropriate users	Y	Y
Limiting session connections and ensuring that these time out and disconnect if not in use. See Appliance Virtualization Platform security hardening policies on page 74.	Y	Y
Reducing running services to a minimum	Y	Y
Limiting open ports and applying appropriate firewall rules	Y	Y
Requiring the use of strong passwords and ensuring password complexity. See Appliance Virtualization Platform security hardening policies on page 74.	Y	Y
Disabling the use of weak ciphers and ensuring client-server connections are secured with strong SSL protocols. See Appliance Virtualization Platform security hardening policies on page 74.	Y	Y
Configuring of remote logging to a central log host to provide a secure, centralized store of ESXi logs	Y	Y
Limiting of network access by disabling unauthorized networks	Y	Y
Periodic checking for extraneous device files and unauthorized setuid or setgid files, and unauthorized modification to authorized setuid or setgid files	Y	Y
VMware Managed Object Browser (MOB) disabled by default	Y	Y

Table continues…

Security attribute	Commercial grade	Military grade
VMware Embedded Host Client (EHC) is disabled by default. To enable, run the **`/opt/avaya/bin/harden/set_ehc enable`** command.	Y	Y
EASG access disabled	—	Y
Military grade specific banner	—	Y

Related links

[Appliance Virtualization Platform security hardening policies](#) on page 74

Appliance Virtualization Platform security hardening policies

This section describes the policies of the Appliance Virtualization Platform hardened system.

Appliance Virtualization Platform system session restrictions

- SSH access must be enabled and will time out after a pre-defined period.
- DCUI session will timeout after 600 seconds of non-use.
- ESXi Shell session will timeout after 600 seconds of non-use.

Appliance Virtualization Platform password policies

- A user is allowed three attempts to type the password. After three attempts the account will be locked for 15 minutes.
- Passwords must meet the following length and complexity requirements:
  - At least one character each of the four different character classes: number, special character, UPPER_CASE, and lower_case.
  - Minimum length of 15 characters.
  - A new password must not be similar to the old one.

Ciphers supported

- Only FIPS-approved ciphers are supported: aes256-ctr, aes192-ctr, and aes128-ctr.
- Appliance Virtualization Platform only supports TLS 1.2.

Commercial grade hardening checklist

Use the checklist to configure the commercial grade hardening for the Appliance Virtualization Platform host.

No.	Task	Link/Notes	✔
1.	Enable the commercial grade hardening.	Enabling commercial grade hardening for the Appliance Virtualization Platform host on page 75	
2.	Add users, groups, and network IPs to establish connection with Appliance Virtualization Platform host services.	Adding SSH users and disabling unauthorized network access on page 76	
3.	Configure syslog server for remote logging.	Configuring syslog server for remote logging on page 77	
4.	Verify the commercial grade hardening status.	Verifying hardening status and completing remaining hardening settings on page 78	
5.	Run weekly check for extraneous device, unauthorized setuid or setgid files	Checking for extraneous device and unauthorized Setuid or Setgid files on page 78	

Enabling commercial grade hardening for the Appliance Virtualization Platform host

Before you begin

Enable SSH for the Appliance Virtualization Platform host.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To enable commercial grade hardening, type the `/etc/init.d/avaya-harden start` command.

   The system displays the following message:

   ```
   After running this script, the AVP Landing Page, Embedded Host Client and
   access will be disabled. Ensure that AVP is registered with an SDM to allow
   for management functions and the enablement of SSH access.

   The Embedded Host Client can be enabled by using the AVP CLI set_ehc script.
   This should only be enabled for troubleshooting purposes and disabled when
   finished. By enabling Avaya Logins you are granting Avaya access to your
   system.
   ```
4. To continue the hardening process, type `y`.

   The system starts the hardening process.

   When the process completes, the system displays the message: `ok`.

For applying the changes, the system displays the following message to reboot the system: `To let the changes take effect, the system needs to be rebooted`.

5. To reboot the system, type `y`.

   You can also reboot the system later.

Related links

Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager on page 47
Rebooting the Appliance Virtualization Platform host from CLI on page 60
Activating SSH from AVP Utilities on page 46

Adding SSH users and disabling unauthorized network access

About this task

Access for Avaya Services requires the following network to be allowed: 192.168.13.0/29.

Before you begin

Enable SSH for the Appliance Virtualization Platform host.

Note:

For Active Directory users, this procedure considers that the network administrator has already configured the Active Directory server and is accessible. Configuration of the Active Directory server is beyond the scope of this document, please refer relevant Microsoft documentation.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. At the prompt, type the `/etc/init.d/avaya-harden manual_fixes` command.
4. To add additional users to the list of allowed users to enable SSH access, follow the prompt, and perform the following.
    a. To add local users, type the local user names separated by a space.

       For example: `user1 user2`

    b. To add Active Directory (AD) users, type the AD user names including the AD domain separated by a space.

       For example: `<AD domain>\user1 <AD domain>\user2`

5. To add additional groups to the list of allowed groups to enable SSH access, follow the prompt, and perform the following.
    1. Type the AD domain.
    2. To add local groups, type the local group names separated by a space.

       For example: `group1 group2`
    3. To add AD groups, type the AD group names including the AD domain separated by a space.

       For example: `<AD domain>\group1 <AD domain>\group2`

       You must add the defined AD group *AVP Admins* as: <AD domain>\avp^admins.
6. To modify the currently allowed network IPs that can establish connection with AVP host services, follow the prompt, and type the IP addresses.

   AVP host services are: CIM Server, CIM Secure Server, cmmds, DNS Client, ipfam, NFC, rdt, SSH Server, vsanvp, vSphere Client, watchd, and vSphere Web Access.

   The system applies the configuration changes to the selected services and sets up the configured values.

Configuring syslog server for remote logging

Before you begin

Enable SSH for the Appliance Virtualization Platform host.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To configure Syslog.global.logHost to the site-specific syslog server, type the `esxcli system syslog config set --loghost udp://192.168.13.1,<transport protocol://site specific syslog server address:port>` command.

   You can configure multiple hosts separated by a comma (,).

   Note:

   You must include the rsyslog destination (udp://192.168.13.1) as this is used for Appliance Virtualization Platform alarming functionality.
4. To verify the syslog server setting, type the `esxcli system syslog config get` command.

Verifying hardening status and completing remaining hardening settings

About this task

After enabling the commercial grade hardening, adding SSH user and groups, disabling unauthorized network access, and establishing network connection with Appliance Virtualization Platform host services, use this procedure to verify the hardening status and identify any settings that might require manual updates. If required, perform the manual updates that are identified during the execution of the script.

Before you begin

Enable SSH for the Appliance Virtualization Platform host.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. At the prompt, type the `/etc/init.d/avaya-harden status` command.

   The system starts the process and displays the system hardening settings that you need to manually update.
4. Perform the manual updates that are identified during the execution of the script.

Checking for extraneous device and unauthorized Setuid or Setgid files

About this task

After setting up the Appliance Virtualization Platform security hardening, you must run the weekly check for extraneous device files, unauthorized Setuid or Setgid files, and unauthorized modification to authorized Setuid or Setgid files.

Before you begin

Enable SSH for the Appliance Virtualization Platform host.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To check for extraneous device files, type `cat /vmfs/volumes/server-local-disk/jitc/log/devicefiles/result.txt`.

The system displays the message: `OK: device files unchanged`.

Note:

If SSH sessions are open at the time the cron job runs or if the Appliance Virtualization Platform host ESXi Shell is accessed by different users, the extraneous device files check can report false error result. These scenarios can cause differences in the `/dev/char/pty` and `/dev/char/tty` directories that lead to display of false error result in the `result.txt` file.

4. To reset the extraneous device files checking, remove the log files. To remove the log files, type `rm -rf /vmfs/volumes/server-local-disk/jitc/log/devicefiles`.
5. To check for unauthorized setuid, type `cat /vmfs/volumes/server-local-disk/jitc/log/setuid/result.txt`.

   The system displays the message: `OK: setuid unchanged`.
6. To check for unauthorized setgid, type `cat /vmfs/volumes/server-local-disk/jitc/log/setgid/result.txt`.

   The system displays the message: `OK: setgid unchanged`.

Result

All result files must indicate `OK`.

Appliance Virtualization Platform certificate management

The following certificates are applicable for Appliance Virtualization Platform:

- **X.509 certificates:** Appliance Virtualization Platform uses standard X.509 certificates to encrypt session information sent over SSL connections between server and client systems. When a client application initiates an SSL session with the server, the server sends its certificate to the client application, which checks the X.509 certificate against a list of known Certificate Authorities (CAs) to verify the authenticity of the certificate.
- **AVP server certificates:** Appliance Virtualization Platform server certificates are created during the installation process where the certificate name matches the DNS name of the server. These certificates are not signed by an official root CA but are used by System Manager Solution Deployment Manager or the Solution Deployment Manager client to validate a secure connection.

Related links

Certification validation on page 80
Generating and accepting the Appliance Virtualization Platform host certificates on page 81
Creating or editing generic CSR on page 82
Create or edit CSR field descriptions on page 82
Applying third-party certificates to Appliance Virtualization Platform on page 83

Load Certificate field descriptions on page 84

Certification validation

With System Manager Solution Deployment Manager and the 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 and later applications. This connection provides secure communication between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using self-signed certificates or third-party certificates.

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

- Certificate validity dates
- Origin of Certificate Authority
- Chain of Trust
- CRL
- 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. The certificate must be in date.
- Appliance Virtualization Platform does not automatically regenerate their certificates when host details such as IP address or hostname and domain change. 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.

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

Related links

Appliance Virtualization Platform certificate management on page 79

Generating and accepting the Appliance Virtualization Platform host certificates

About this task

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

Before you begin

Get permissions to add a host to generate certificates.

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 (SDM CLIENT).
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Generate/Accept Certificate**.
5. In the Certificate dialog box, click the following:
    a. **Generate Certificate**

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

    b. **Accept Certificate**

    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.

    In the Platforms for Selected Location <location name> section, the **Platform Certificate Status** column must display a check mark ✓.

Related links

Appliance Virtualization Platform certificate management on page 79

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 **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms 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.

Related links

Appliance Virtualization Platform certificate management on page 79

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.

Related links

Appliance Virtualization Platform certificate management on page 79

Applying third-party certificates to Appliance Virtualization Platform

About this task

Use this procedure to create, download, upload, and push third-party 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 on the Appliance Virtualization Platform host is valid.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

   If you add the generic CSR details, the system pre-populates the values in the View/ Generate CSR dialog box.

   For more information about creating the generic CSR, see “Creating or editing generic CSR”.
5. To generate CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **View/Generate CSR**.

      System Manager displays the View/Generate CSR dialog box.
   d. If the generic CSR details are not added for the Appliance Virtualization Platform host, add the details of the generic CSR.
   e. Click **Generate CSR**.

      The system generates CSR for the Appliance Virtualization Platform host.
   f. In the **Current Action** column, click **Status Details** to view the status.
6. To download CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.

   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Download CSR**.

      In case of Firefox browser, the system prompts you to save the `CSR.zip` file.
   d. In the **Current Action** column, click **Status Details** to view the status.

      In the Download CSR Status dialog box, the system displays the path of the downloaded `CSR.zip` file.
7. Extract the downloaded certificates, and ensure that the third-party signs them.
8. To upload and push the signed certificate from a third-party CA, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Browse** and select the required certificates from the local computer.
   d. Click **I Agree to accept to add the same certificate in SDM**.
   e. Click **Push Certificate**.
   f. In the **Current Action** column, click **Status Details** to view the status.

Related links

Appliance Virtualization Platform certificate management on page 79

Load Certificate field descriptions

Name	Description
Platform IP	The IP address of the Appliance Virtualization Platform host.
Platform 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
View/Generate CSR	Displays the View/Generate CSR dialog box to generate CSR.
Download CSR	Downloads CSR for the selected host.

Table continues…

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.

Related links

Appliance Virtualization Platform certificate management on page 79

Chapter 9: Post-deployment and 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: 8.0.x.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
   ```

Virtual Machine snapshot on Appliance Virtualization Platform

When you apply an update by using Solution Deployment Manager, snapshots are left on Appliance Virtualization Platform. If a snapshot is left on Appliance Virtualization Platform, it is detrimental to system performance and over time can utilize all the available disk space. Therefore, ensure that snapshots are not left on Appliance Virtualization Platform for an extended period of time and are removed on a timely manner.

You can review and delete Virtual Machine snapshots from Appliance Virtualization Platform by using Solution Deployment Manager Snapshot Manager.

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 87
Snapshot Manager field descriptions on page 87

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 (SDM CLIENT).
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms 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**.

   You must review all listed snapshots and remove snapshots that are more than 24 hours old.

   The system deletes the selected snapshots.

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 86

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.

Table continues…

Name	Description
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

Virtual Machine snapshot on Appliance Virtualization Platform on page 86

Enhanced Access Security Gateway overview

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: **`/opt/avaya/easg/.bin/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. 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.
2. 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.
3. 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.

Chapter 10: Troubleshooting

Troubleshooting Appliance Virtualization Platform

Appliance Virtualization Platform does not install

Perform the following as appropriate:

- Ensure that you are connected to the services port on the server with the following network configuration on the laptop:
  - IP address: 192.168.13.5
  - Netmask: 255.255.255.248
  - Gateway: 192.168.13.1
- Defective USB drive. Place the `avp80ks.cfg` kickstart file on another USB and connect the USB to the server
- Unsupported server: Release 7.1 and later does not support S8500 and S8800 servers. Change to a Release 8.0.1 supported server.
- Duplicate IP address for Appliance Virtualization Platform management interface already on the network. Remove the duplicate IP address and reinstall Appliance Virtualization Platform.
- USB stick left plugged in on HP servers. Remove the USB stick, and reboot the server.
- Deployments take longer duration or fail. Ensure that the network settings and network configuration is correct for the virtual machine that is being deployed.

Virtual machine deployment fails during the sanity check

- Ensure that IP forwarding is enabled on AVP Utilities if you deploy virtual machines from the services port with the Solution Deployment Manager client.
- Ensure that System Manager Solution Deployment Manager or Solution Deployment Manager client can connect to the management IP address of the application being deployed.
- Ensure that the server is physically connected. If Out of Band Management is enabled, ensure that the Appliance Virtualization Platform host and the virtual machines are deployed with Out of Band Management configurations.

Virtual machine deployment fails

Ensure that you accept EULA by gaining access to Appliance Virtualization Platform using SSH, and accepting the EULA.

Cannot SSH to Appliance Virtualization Platform

SSH has shutdown. Activate SSH from AVP Utilities or from Solution Deployment Manager. For more information, see Activating SSH from AVP Utilities.

On the monitor, the screen displays a warning message in red and then goes blank

During the Appliance Virtualization Platform installation, the monitor displays blank screen, which is a normal behavior. No action is required.

Related links

Activating SSH from AVP Utilities on page 46

Unable to connect to Appliance Virtualization Platform host from vSphere Web Client

Condition

The vSphere Web Client throws an SSL verification failure error when you gain access to the Appliance Virtualization Platform host for which you regenerated the certificate.

Cause

The vSphere Web Client might use the old certificate of the Appliance Virtualization Platform host from the cache instead of the regenerated certificate.

Use the following procedure if the system displays an SSL verification error when you gain access to the Appliance Virtualization Platform host from vSphere Web Client.

Solution

1. Restart the Appliance Virtualization Platform host.
2. Using vSphere Web Client, gain access to the Appliance Virtualization Platform host.

Related links

Restarting Appliance Virtualization Platform or an ESXi host on page 60

Viewing installation log traces

Solution

To view the installation log traces, press `ALT-F12`.

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** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

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

Related links

Restarting Appliance Virtualization Platform or an ESXi host on page 60

Rebooting the Appliance Virtualization Platform host from CLI

Before you begin

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh -r`.

   The system displays `Are you sure you want to stop all VMs and reboot?`.

   ⚠ **Warning:**

   If you fail to provide the -r option, the system displays `Are you sure you want to stop all VMs and shutdown?` and assumes that you want to perform the shutdown operation.

   If you use the shutdown option when reset is intended, the host does not restart as part of the process and you must manually start the server.

3. To confirm the reboot operation, type `Y`.

   The system stops all virtual machines that are running on the Appliance Virtualization Platform host. The Appliance Virtualization Platform host reboots and restarts all virtual machines automatically.

Chapter 11: Resources

Appliance Virtualization Platform documentation

The following table lists the documents related to Appliance Virtualization Platform. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Implementing		
Deploying Avaya Aura® Appliance Virtualization Platform	Deploy, configure, and administer Avaya Aura® Appliance Virtualization Platform.	Implementation personnel
Upgrading Avaya Aura® Appliance Virtualization Platform	Upgrade Avaya Aura® Appliance Virtualization Platform.	Implementation personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

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**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.

- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
20980W	What's New with Avaya Aura® Release 8.0

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos` 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 do one of the following:
    - 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 https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

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.

Appendix A: Deploying AVP Utilities and other virtual machines

Deploying AVP Utilities and virtual machines when Out of Band Management is enabled

Before you begin

Install the Solution Deployment Manager client on your computer.

Procedure

1. Connect the computer to the Out of Band Management network with access to the Appliance Virtualization Platform Management Network IP address that you configured in the kick start generator file.
2. Using the Solution Deployment Manager client, create a location.
3. In the location that you created, create a host of Appliance Virtualization Platform by using the Management Network IP address of Appliance Virtualization Platform.
4. Ensure that AVP Utilities OVA is saved in the sub-folder in the `Default_Artifacts` directory during the Solution Deployment Manager client installation.

   You can save OVA files of all virtual machines that you want to deploy.
5. Create a new virtual machine in the host that you created in Step 3.
6. To set the OVA software library, select the complete path to the `Default_Artifacts` directory.

   In the Configuration Parameters section, the page displays parameters that are specific to AVP Utilities.
7. Fill in the AVP Utilities parameters.

   Provide the IP address that you want to allocate to Communication Manager.

   If Out of Band Management is enabled, provide information in the Out of Band Management-related fields. If Out of Band Management is disabled, leave the fields blank.
8. Deploy AVP Utilities, and wait for the virtual machine to deploy successfully.
9. Install the AVP Utilities 8.0.1 feature pack.

Note:

Before installing any service pack or feature pack, you must remove any pre-installed Service packs or Feature packs from the system. To verify the pre-installed service pack or feature pack installation status, run the **`swversion`** command from the command line interface. To remove the pre-installed service packs/feature packs run the **`update -e <service tag>`** command. Service and Feature packs are cumulative and include all of the security remediation and bug fixes of previous service or feature packs.

10. Deploy all other virtual machines in the solution one after the other.
11. Install the feature pack for Avaya Aura® applications.
12. Validate the system.

Related links

Enabling IP forwarding using Services Port VM for AVP Utilities on page 45

Deploying AVP Utilities and virtual machines on the services port

Before you begin

- Download the Solution Deployment Manager client from the PLDS website.
- Install the Solution Deployment Manager client on your computer.

Procedure

1. Using the Solution Deployment Manager client, create a location.
2. To connect the computer to the services port on the server, configure the following:
    - **IP address**: 192.168.13.5
    - **Netmask**: 255.255.255.248
    - **Gateway**: 192.168.13.1

    On the Solution Deployment Manager client, in the Appliance Virtualization Platform host, provide the IP address 192.168.13.6.
3. In the location that you created, create a host of Appliance Virtualization Platform by using the Management Network IP address of Appliance Virtualization Platform.
4. Ensure that AVP Utilities OVA is saved in the sub-folder in the `Default_Artifacts` directory during the Solution Deployment Manager client installation.

    You can save OVA files of all virtual machines that you want to deploy.
5. Create a new virtual machine in the host that you created in Step 3.

6. To set the OVA software library, select the complete path to the `Default_Artifacts` directory.

   In the Configuration Parameters section, the page displays parameters that are specific to AVP Utilities.
7. Enter the IP address details for AVP Utilities, deploy AVP Utilities, and wait for the virtual machine to deploy successfully.
8. Install the AVP Utilities 8.0.1 feature pack.

   Note:

   Before installing any service pack or feature pack, you must remove any pre-installed Service packs or Feature packs from the system. To verify the pre-installed service pack or feature pack installation status, run the **`swversion`** command from the command line interface. To remove the pre-installed service packs/feature packs run the **`update -e <service tag>`** command. Service and Feature packs are cumulative and include all of the security remediation and bug fixes of previous service or feature packs.
9. Change the AVP Utilities configuration parameters to the following:
   - **IP address**: 192.11.13.5
   - **Netmask**: 255.255.255.252
   - **Gateway**: 192.11.13.6

   On the Solution Deployment Manager client, in the Appliance Virtualization Platform host, leave the IP address as 192.168.13.6.
10. Ensure that the IP forwarding feature is enabled on AVP Utilities.
11. Deploy all other virtual machines in the solution one after the other.
12. **(Optional)** During the deployment, if the sanity check fails, verify the host network configuration.

    The deployment might be successful, however, sanity check can fail due to a bad network connection.
13. Install the feature pack for Avaya Aura® applications.
14. Validate the system.

Related links

Enabling IP forwarding using Services Port VM for AVP Utilities on page 45

Index