# Migrating and Installing Avaya Aura® Appliance Virtualization Platform

Release 7.1.3
Issue 8
April 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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

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

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

### Service Provider

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

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

### Compliance with Laws

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

### Preventing Toll Fraud

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

### Avaya Toll Fraud intervention

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

### Security Vulnerabilities

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

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

### Downloading Documentation

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

### Contact Avaya Support

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

### Trademarks

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

# Contents

# Chapter 1: Introduction

## Purpose

This document contains checklists and procedures related to:

- Installing Appliance Virtualization Platform
- Migrating from Avaya Aura® System Platform to Appliance Virtualization Platform
- Configuring Appliance Virtualization Platform
- Administering Appliance Virtualization Platform
- Troubleshooting Appliance Virtualization Platform

This document is intended for people who need to migrate data from System Platform to Appliance Virtualization Platform or to configure a system with Appliance Virtualization Platform preinstalled.

## Change history

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

| Issue | Date | Summary of changes |
|---|---|---|
| 8 | April 2020 | For Release 7.1.3.6, added the following sections:<br>• Customizing the Appliance Virtualization Platform banner through CLI on page 80<br>• Clearing system event logs from CLI on page 110 |
| 7 | March 2020 | Updated the section: Appliance Virtualization Platform overview on page 21 |
| 6 | October 2019 | For Release 7.1.3, updated the section: Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 98 |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 5 | September 2018 | For Release 7.1.3, updated the following sections:<br>• Deploying Appliance Virtualization Platform on page 43<br>• Configuring servers preinstalled with Appliance Virtualization Platform on page 54 |
| 4 | May 2018 | For Release 7.1.3, updated the following sections:<br>• Appliance Virtualization Platform overview on page 21<br>• Removing the Appliance Virtualization Platform patch from the ESXi host CLI on page 101 |
| 3 | January 2018 | Updated the Configuring servers preinstalled with Appliance Virtualization Platform on page 54 section. |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 2 | December 2017 | For Release 7.1.2, added the following sections:<br>• Appliance Virtualization Platform deployment on page 50<br>• Deploying Appliance Virtualization Platform using a setup script on page 50<br>• Appliance Virtualization Platform license on page 60<br>• Configuring WebLM Server for an Appliance Virtualization Platform host on page 64<br>• WebLM Configuration field descriptions on page 65<br>• Configuring WebLM Server for an Appliance Virtualization Platform host from CLI on page 65<br>• Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager on page 66<br>• Verifying the Appliance Virtualization Platform license status from host CLI on page 67<br>• Extended security hardening on page 82<br>• Appliance Virtualization Platform security hardening policies on page 83<br>• Commercial grade hardening checklist on page 83<br>• Enabling commercial grade hardening for the Appliance Virtualization Platform host on page 84<br>• Adding SSH users and disabling unauthorized network access on page 85<br>• Configuring syslog server for remote logging on page 86<br>• Verifying hardening status and completing remaining hardening settings on page 87<br>• Checking for extraneous device and unauthorized Setuid or Setgid files on page 87<br>For Release 7.1.2, updated the following sections:<br>• Licensing on page 34<br>• Create AVP Kickstart field descriptions on page 41<br>• Upgrading Appliance Virtualization Platform from Solution Deployment Manager  on page 98<br>• Removing the Appliance Virtualization Platform patch from the ESXi host CLI on page 101<br>• Verifying the Appliance Virtualization Platform software release and the ESXi version on page 104 |
| 1 | May 2017 | Release 7.1 document. |

# Chapter 2: 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 Utility Services OVA, the services port IP address for the Utility Services 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 Utility Services 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.

### S8300D

When you install the connection through the media gateway using Appliance Virtualization Platform , Ethernet ports are assigned to the public interface of the virtual machines. When you install the connection through the media gateway backplane using Appliance Virtualization Platform, 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 assigned to a separate VLAN on the public interface. Otherwise all virtual machine interfaces are on the same network.

The Appliance Virtualization Platform management interface is assigned to:

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

**Note:**

To support Out of Band Management on S8300D, you require specific versions of gateway firmware. To ensure that you are running the correct version, see the gateway documentation.

### 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.

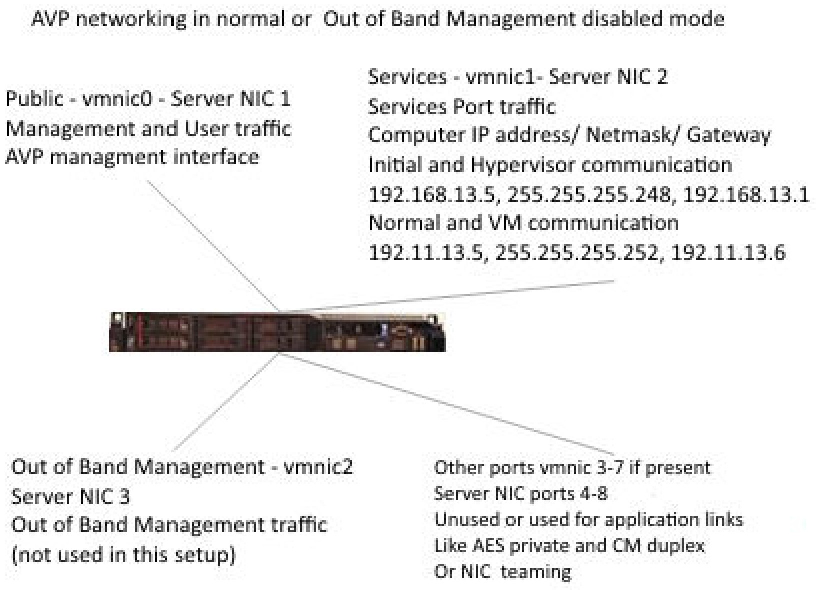
- Appliance Virtualization Platform is installed with a normal or Out of Band Management configuration setup.

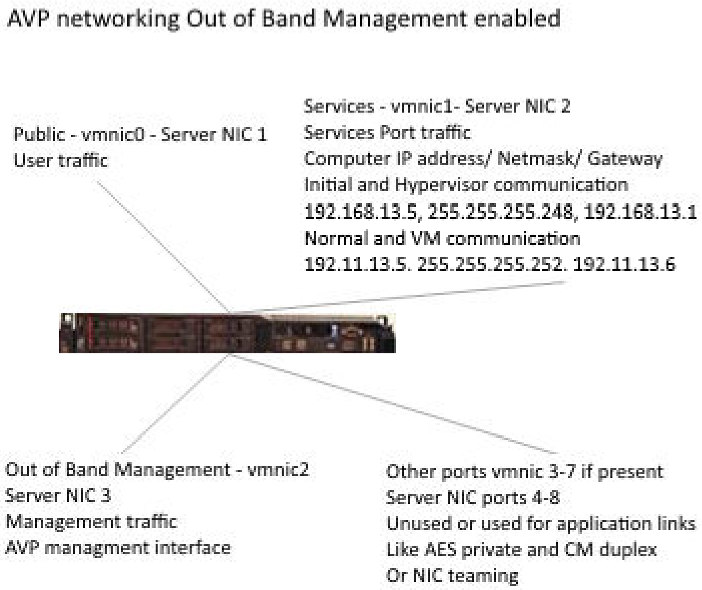
- Appliance Virtualization Platform is installed with Out of Band Management disabled or enabled.
  - If you are installing Appliance Virtualization Platform, you can enable Out of Band Management by using the **Out of Band Management Setup** check box on Create AVP Kickstart for generating the kickstart 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 Utility Services 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 Utility Services 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 Utility Services
    - 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 S8300D and S8300E servers.

## 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 19

# 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 S8300D and S8300E servers.

## 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 supports the TLS version 1.2. By default, TLS versions 1.0 and 1.1 are disabled, but you can enable, if required.

# Chapter 3: 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 uses the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

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

  **Note:**

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

**Note:**

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for

Communication Manager LSP and Branch Session Manager with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

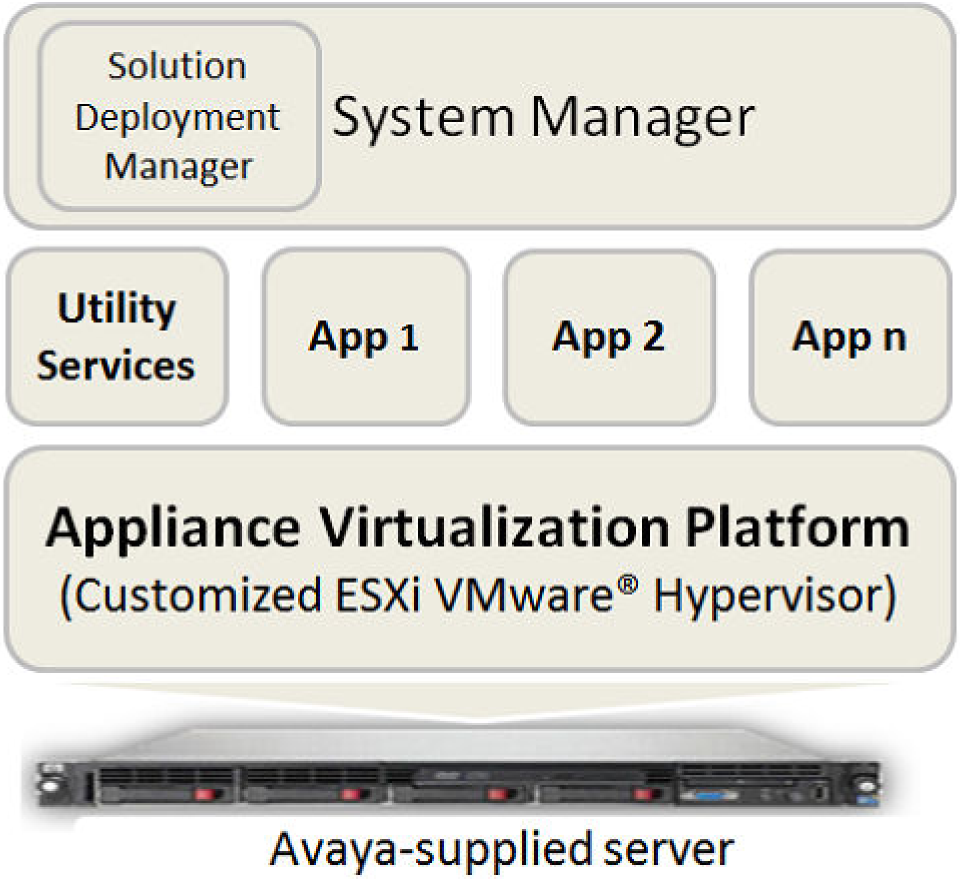
Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to the Release 7.1.3.

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

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

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

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


Solution Deployment Manager
System Manager
Utility Services
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:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

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

**Note:**

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

**Important:**

Due to Avaya enhanced customizations, Appliance Virtualization Platform (aka 120) 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 customer Virtualized Environment and 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 and 7.0.x applications to Release 7.1 and later in customer Virtualized Environment.

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

System Manager is the primary management solution for Avaya Aura® Release 7.0 and later applications.

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.

  From Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.

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

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.
- 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
  - Utility Services
  - 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 7.x, 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 |
| 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<br>Release 7.x supports upgrades from Linux-based or System Platform-based to Virtualized Environment or Appliance Virtualization Platform. Release 7.1 and later supports Virtualized Environment to Virtualized Environment upgrades. | Upgrade System Platform-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 can reside on the computer of the technician. The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized Environment.

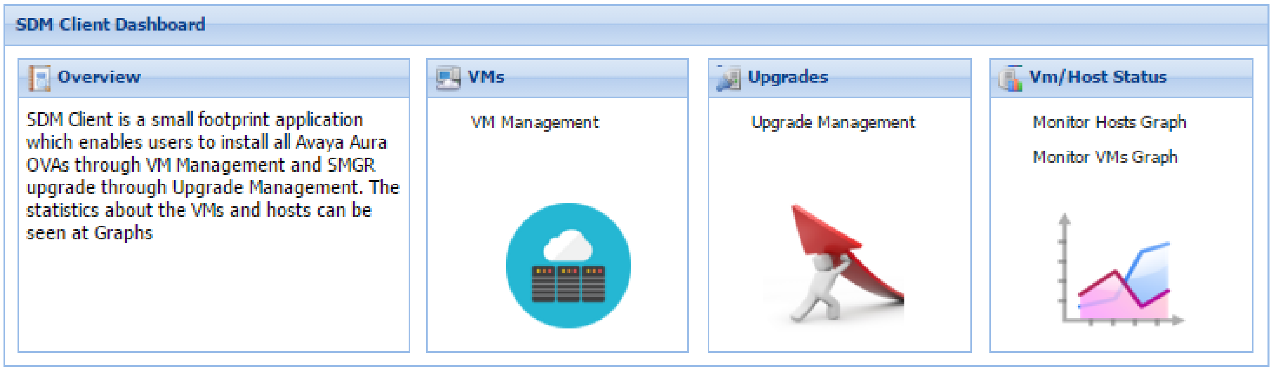
A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances and Virtualized Environment.
- Upgrade System Platform-based System Manager.
- Upgrade Virtualized Environment-based System Manager from Release 7.0.x to Release 7.1 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create 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™.

**Note:**

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.



SDM Client Dashboard

Overview

SDM Client is a small footprint application which enables users to install all Avaya Aura OVAs through VM Management and SMGR upgrade through Upgrade Management. The statistics about the VMs and hosts can be seen at Graphs

**Figure 1: Solution Deployment Manager client dashboard**

**Related links**

Solution Deployment Manager client capabilities on page 26

## Solution Deployment Manager client capabilities

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

- Runs on the technician computer on the following operating systems:
  - Windows 7, 64-bit Professional or Enterprise

  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deploying the System Manager OVA. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of the Avaya Aura® applications.
- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.
- Configures application and networking parameters required for application deployments.
- Supports the local computer or an HTTP URL to select the application OVA file for deployment. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as, IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  **Note:**

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

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

**Related links**

Solution Deployment Manager client on page 25

## Solution Deployment Manager

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

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

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

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

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

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

  **Note:**

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

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

  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

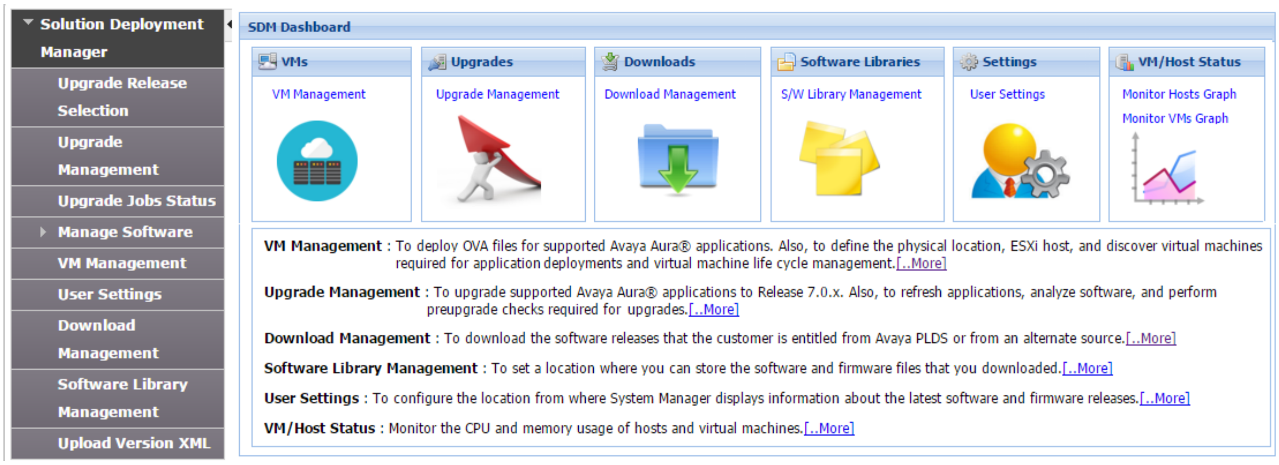
**Note:**

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

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

## Solution Deployment Manager dashboard

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



**VM 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]

**VM/Host Status** : Monitor the CPU and memory usage of hosts and virtual machines.[..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 7.0** or **6.3.8** as the target upgrade. Release 7.1.3 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module (UCM) and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.

    - Generate the Appliance Virtualization Platform Kickstart file.

- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, WebLM to Release 7.1.3.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the `version.xml` file to perform upgrades.

# Chapter 4: Migration planning and considerations

## Required permissions

You must have administrator credentials to perform the data migration from System Platform to Appliance Virtualization Platform.

## Supported migrations

### System Platform to Appliance Virtualization Platform Release 7.1.3

| Template |
|---|
| High Duplex / Communication Manager |
| Duplex Communication Manager Main / Survivable Core |
| Simplex Communication Manager Main / Survivable Core |
| Simplex Survivable Remote |
| System Manager including WebLM |
| Midsize Enterprise |
| SAL or SVM |
| Utility Services |
| Session Manager (Hardware-based) |
| Presence Services |
| Application Enablement Services |

## Planning for migration

### Considerations

- Migration requires physical access to the server.
- The time needed for migration varies by application.

- When scheduling the maintenance window, allocate twice the time that is required for migration if rollback to System Platform is necessary.

  You can purchase the Hard Drive kits to reduce the rollback time.

### Migration times

- Template migration can take between 2 and 8 hours to complete.
- Midsize Enterprise might take up to 15 hours.

## Supported servers

In the Avaya appliance model, you can deploy or upgrade to Avaya Aura® Release 7.1.3 applications on the following Avaya-provided servers:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9
- S8300D, for Communication Manager and Branch Session Manager
- S8300E, for Communication Manager and Branch Session Manager
- Intel 1006r server. Only to deploy Utility Services and Avaya Aura® Messaging OVA files.

## Installing the Solution Deployment Manager client on your computer

### About this task

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

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

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

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

## Procedure

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

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

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

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

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. Click **Next**.
9. On the Pre-Installation Summary page, review the information, and click **Next**.
10. On the User Input page, perform the following:
    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

    b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

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

       You can save the artifacts in the specified directory.

    c. In **Data Port No**, select the appropriate data port.

       The default data port is 1527. The data port range is from 1527 through 1627.

   d. In **Application Port No**, select the appropriate application port.

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

      **Note:**

      After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

   e. **(Optional)** Click **Reset All to Default**.

11. Click **Next**.
12. On the Summary and Validation page, verify the product information and the system requirements.

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.

13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.

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

### 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*.

# Licensing

You must accept the Appliance Virtualization Platform End User License Agreement (EULA) before deploying applications on Appliance Virtualization Platform. You can accept EULA through an SSH login to the Appliance Virtualization Platform system after installation or first power on.

Appliance Virtualization Platform must be licensed with an appropriate license that is installed on an Avaya WebLM Server. A 30-day grace period will apply in which you must license Appliance Virtualization Platform and during this period, Appliance Virtualization Platform will be in License Error Mode. If after 30-day grace period an Appliance Virtualization Platform license is not acquired, Appliance Virtualization Platform enters in License Restricted Mode and Appliance Virtualization Platform administrative actions will be restricted.

For information about how to install and configure a license for Appliance Virtualization Platform, see “Installing and configuring Appliance Virtualization Platform licensing”.

# Chapter 5: Migration process

## Migration checklist

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Get the backup media. | The backup media contains the following software:<br>• System Platform<br>• Templates<br>• DVD<br>• System Platform service packs and software patches.<br>Download any missing components from the PLDS website. | |
| 2 | Get the migration media. | From the PLDS website, download the following components that are required to migrate to Appliance Virtualization Platform:<br>• The latest Appliance Virtualization Platform DVD<br>• Appliance Virtualization Platform 7.1.3 installation file, `avaya-avp-7.1.0.0.0.x.iso`<br>• Appliance Virtualization Platform 7.1.3 upgrade bundle, `upgrade-avaya-avp-7.1.3.0.0.xx.zip`. It is also available in the Appliance Virtualization Platform ISO image in the `\avp_upgrade_bundle\upgrade-avaya-avp-7.1.3.0.0.xx.zip` folder.<br>• The Solution Deployment Manager client, if required<br>• OVA files for System Manager and other applications<br>• System Manager Release 7.1.3 patch file<br>• Release 7.1.3 patch files for other Avaya Aura® applications<br>Get USB Flash Drive in the FAT32 format. | |

*Table continues…*

| No. | Task | Description | ✔ |
|---|---|---|---|
| 3 | Create a local backup of System Platform and the template data. | Creating a backup of the existing configuration on page 39 | |
| 4 | Create a back up of all virtual machines. | Create a backup of each virtual machine. For more information, see the documentation of the application templates.<br>For System Platform Release 6.0, perform the following:<br>• Log in to the System Platform console.<br>• Navigate to the SAL gateway.<br>• Note the values that you need to enter into the new SAL that you create.<br>Onboard SAL is optional, and might not be operational on System Platform. For remote SAL, update with the new values when the migration is complete. For 6.2 or later systems, you must navigate to the Services virtual machine, and record the settings. | |
| 5 | Record System Platform and template values. | Record the data on the System Platform and template values worksheet on page 38.<br>1. On the Main Console page, note the IP addresses.<br>2. On **Server Management** > **Network Configuration**, note the network configuration settings including DNS.<br>3. On the Date and Time page, note the NTP and timezone.<br>4. On **Server Management** > **SNMP Trap Receiver Configuration**, note the SNMP settings. | |
| 6 | Generate the Appliance Virtualization Platform kickstart file. | Generating the Appliance Virtualization Platform kickstart file on page 40 | |
| 7 | Configure the USB drive. | Configuring the Appliance Virtualization Platform USB drive on page 43 | |
| 8 | Insert the USB drive and Appliance Virtualization Platform DVD into the server and turn on the server. | | |

*Table continues…*

| No. | Task | Description | ✔ |
|---|---|---|---|
| 9 | Install Appliance Virtualization Platform. | Deploying Appliance Virtualization Platform on page 43 | |
| 10 | Install the Appliance Virtualization Platform patch. | Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 98 | |
| 11 | Verify the Appliance Virtualization Platform installation. | | |
| 12 | Deploy System Manager, Utility Services, and other Avaya Aura® applications. | | |
| 13 | Install the patches for all Avaya Aura® applications. | | |

## System Platform and template values worksheet

While migrating the data from System Platform to Appliance Virtualization Platform, make a note of the following values:

| Reference | Name | Value |
|---|---|---|
| A | System Platform Domain 0 IP address | |
| B | System Platform Console Domain IP address | |
| C | Services VM IP address if used | |
| D | Template VM 1 IP | |
| E | Template VM2 IP address | |
| F | Template VM3 IP address | |
| G | Template VM 4 IP address | |
| H | Template VM 5 IP address | |
| I | Template VM6 IP address | |
| J | Template VM 7 IP address | |
| K | Template VM 8 IP address | |
| L | Template VM 9 IP address | |
| M | Subnet mask | |
| N | Gateway | |
| O | Routes | |

*Table continues…*

| Reference | Name | Value |
|---|---|---|
| P | NTP | |
| R | DNS | |
| S | SNMP trap target 1 | |
| T | SNMP trap target 2 | |
| U | SNMP trap target 3 | |
| V | SNMP trap target 4 | |
| W | SNMP trap target 5 | |
| X | Timezone | |

| Parameter | Location on System Platform |
|---|---|
| IP addresses | Main System Platform web console page |
| Network settings that includes DNS | **Server Management** > **Network Configuration** |
| NTP and Timezone | Date and Time page |
| SNMP settings | **Server Management** > **SNMP Trap Receiver Configuration** |

# IP address mapping

| Release | IP address mapping | |
|---|---|---|
| | From | To |
| 6.2 or later | System Platform Domain 0 | Appliance Virtualization Platform host |
| | System Console Domain | Utility Services virtual machine |
| | Services VM | SAL virtual machine |
| 6.0.x | System Platform Domain 0 | Appliance Virtualization Platform host |
| | System Console Domain | SAL virtual machine |
| | Utility Services embedded with Communication Manager | New Utility Services IP address |

# Creating a backup of the existing configuration

## About this task

Use this procedure to create a local backup of the System Platform and the template data prior to migrating to the Appliance Virtualization Platform.

### Procedure

1. Log on to System Platform web console as an administrator.
2. Click **Server Management** > **Backup/Restore**.
3. Click **Backup**.
4. To take a local backup, in **Backup Method**, click **Local**.
5. Click **Backup Now**.

   The system creates a backup file in the `/vspdata/backup/archive` location in the System Platform console domain (C-DOM).
6. Log in to C-DOM.
7. Navigate to `/vspdata/backup/archive`.
8. Save a copy of the backup file in a location from where you can gain access to the file.

   The System Platform backup file contains the backup data from System Platform and the template.

## Generating the Appliance Virtualization Platform kickstart file

### About this task

You can also generate the Kickstart file by using the Solution Deployment Manager client.

### Procedure

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

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

#### Related links

Create AVP Kickstart field descriptions on page 41

## 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.<br>The options are:<br>• **yes**: To enable the IPv6 format.<br>• **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.<br>The hostname:<br>• Can contain alphanumeric characters and hyphen<br>• Can start with an alphabetic or numeric character<br>• Must contain 1 alphabetic character<br>• Must end in an alphanumeric character<br>• 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 |
| **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. |

*Table continues…*

| Name | Description |
|---|---|
| **Secondary IPv6 NTP server** | Secondary IPv6 address or FQDN of customer NTP server. |
| **Main IPv6 DNS server** | Main IPv6 address of customer DNS server. One DNS server entry in each line. |
| **Secondary IPv6 DNS server** | Secondary IPv6 address of customer DNS server. One DNS server entry in each line. |
| **Public vLAN ID (Used on S8300D and E only)** | VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090.<br>Use **Public VLAN ID** only on S8300D and S8300E servers. |
| **Out of Band Management Setup** | The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode.<br>The options are:<br>• **yes**: To enable Out of Band Management<br>The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode.<br>• **no**: To disable Out of Band Management. The default option. |
| **OOBM vLAN ID (Used on S8300D and E only)** | Out of Band Management VLAN ID for S8300D. Use **OOBM VLAN ID** only on the S8300D server.<br>• For S8300E, use the front plate port for Out of Band Management<br>• For common server, use eth2 for Out of Band Management. |
| **AVP Super User Admin Password** | Admin password for Appliance Virtualization Platform.<br>The password must contain 8 characters and can include alphanumeric characters and @!$.<br>You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client. |
| **Confirm Password** | Admin password for Appliance Virtualization Platform. |
| **Enable Stricter Password (14 char pass length)** | The check box to enable or disable the stricter password.<br>The password must contain 14 characters. |
| **WebLM IP/FQDN** | The IP Address or FQDN of WebLM Server. |
| **WebLM Port Number** | The port number of WebLM Server. The default port is 52233. |

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

### Related links

Generating the Appliance Virtualization Platform kickstart file on page 40

# 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 “Generating the Appliance Virtualization Platform kickstart file”.

2. Save a copy of `7.1ks.cfg` on the USB drive.

### Next steps

Install Appliance Virtualization Platform.

# Deploying Appliance Virtualization Platform

### About this task

⚠ **Warning:**

For Appliance Virtualization Platform Release 7.1 and later, you can get the admin password for the Appliance Virtualization Platform system from the kickstart file. Keep the file secure. After deployment, you must change the admin password for the Appliance Virtualization Platform host by using the password change option from Solution Deployment Manager.

### Before you begin

- Configure the 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:**

- If you want to migrate from any load earlier than System Platform 6.3 to Appliance Virtualization Platform, you must manually upgrade from any load earlier than System Platform Release 6.3 to System Platform Release 6.3.
- 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 CD-ROM into the server.

   Use an external Avaya-approved USB CD-ROM drive for deploying Appliance Virtualization Platform on S8300D or S8300E. The only supported USB CD-ROM drive is 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 CD-ROM.

   **Note:**

   When installing Appliance Virtualization Platform on an HP server, you must remove the USB drive when the server ejects CD-ROM. 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**, and then click **VM Management**.
8. Add a location.
9. Add the Appliance Virtualization Platform host as 192.168.13.6.
10. Install the Appliance Virtualization Platform patch.

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

11. Deploy the Utility Services virtual machine, and then all other virtual machines with the data that you noted in “System Platform and Template values”.

    For instructions to deploy Utility Services and other virtual machines, see *Deploying Avaya Aura® applications from System Manager*.

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

**Related links**

Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 98
Removing the Appliance Virtualization Platform patch from the ESXi host CLI on page 101
System Platform and template values worksheet on page 38

# Enabling IP forwarding using Services Port VM for Utility Services

### 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 Utility Services 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
```

# Validating the migration

1. Verify that the ping to virtual machine is successful.
2. Verify if you can log on to each virtual machine successfully.
3. Verify that the customer configuration is restored correctly.
4. Verify that applications are licensed.
5. Verify that endpoints are registered.
6. Perform the postmigration validation steps that are specific to each application.

    For more information on postmigration validation checks, see the appropriate application documentation.

# Migrating from System Platform to Appliance Virtualization Platform by using hard disk drives

## Installing Appliance Virtualization Platform by using hard disk drive

### Before you begin

- Connect a monitor and USB keyboard to the server.
- Obtain the Appliance Virtualization Platform drive kit. The kit contains the following:
    - Hard disk drives
    - RAID configuration disk for your system

- RAID documentation
- Dell server import document, required if you must perform a rollback on the Dell server

  For more information about the drive kits, see “Appliance Virtualization Platform Drive Kits”.

- A marker to label the removed disk drives.

## Procedure

1. Shut down System Platform, and turn off the power to the server.

   For more information, see System Platform and the server documentation.

2. Remove each hard disk drive from the server, and mark the drive with the designated slot number.
3. Keep the removed drives in a safe place.

   These drives are required to rollback to System Platform.

4. Insert new hard disk drives into the server hard disk drive slots starting with the lowest order server slot number.

   For example, Dell slot 0 and HP slot 1.

5. Turn on the power to the server.
6. Open the DVD drive tray, and insert the appropriate server RAID configuration disk.

   The server boots from the RAID configuration disk. For more information, see the RAID documentation for your system.

7. **(Optional)** If the server does not start from the RAID configuration disk, perform the following:

   a. Press `Control+Alt+Delete` a couple of times.

   b. If server does not still start from the disk, press F9 for HP or F2 for Dell to check the boot order in the server setup menu.

8. When the RAID configuration tool starts, follow the instructions to view RAID Array configuration progress.

   The tool automatically configures the Array Controller to: 2xHDD = RAID 1. 3x, 4x and 5xHDD = RAID 5. When the RAID configuration is complete, the system shuts down the server, and ejects the disk.

9. Install Appliance Virtualization Platform.

   For instructions, see “Deploying Appliance Virtualization Platform”.

### Related links

Deploying Appliance Virtualization Platform on page 43

Appliance Virtualization Platform drive kits on page 48

## Appliance Virtualization Platform drive kits

700511583 R610, R620 300GB 10K HDD 5 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700506756 | 5 | R620 300GB 10K SAS 2.5" HDD |
| 700501523 | 1 | SOFTWARE, Dell R610 RAID1 to RAID5 UPGR + Doc |
| 700506915 | 1 | SOFTWARE, R620 RAID1 to RAID5 UPGR +Doc |
| - | 1 | Document for Setup of HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511584 R610, R620 300GB 10K HDD 3 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700506756 | 3 | R620 300GB 10K SAS 2.5" HDD |
| 700501523 | 1 | SOFTWARE, Dell R610 RAID1 to RAID5 UPGR + Doc |
| 700506915 | 1 | SOFTWARE, R620 RAID1 to RAID5 UPGR +Doc |
| - | 1 | Document for Setup of HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511585 R610, R620 300GB 10K HDD 2 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700506756 | 2 | R620 300GB 10K SAS 2.5" HDD |
| 700501523 | 1 | SOFTWARE, Dell R610 RAID1 to RAID5 UPGR + Doc |
| 700506915 | 1 | SOFTWARE, R620 RAID1 to RAID5 UPGR +Doc |
| - | 1 | Document for Setup of HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511586 DL360G7 300GB 10K HDD 3 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700501314 | 3 | DL360G7 300GB 10K SAS 2.5" HDD |
| 700501446 | 1 | SOFTWARE, HP DL360G7 RAID1 to RAID5 UPGR + Doc |
| - | 1 | Document to Setup of HDDs in Upgrade Kits |

*Table continues…*

| Code | Qty | Component |
|---|---|---|
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511587 DL360G7 300GB 10K HDD 2 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700501314 | 2 | DL360G7 300GB 10K SAS 2.5" HDD |
| 700501446 | 1 | SOFTWARE, HP DL360G7 RAID1 to RAID5 UPGR + Doc |
| - | 1 | Document to Setup of HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511588 DL360PG8 300GB 10K HDD 3 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700506773 | 3 | DL360PG8 300GB 10K SAS 2.5" HDD |
| 700501523 | 1 | SOFTWARE, DL360/380PG8 RAID1 to RAID5 UPGR+ Doc |
| - | 1 | Document to Setup HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

700511589 DL360PG8 300GB 10K HDD 2 DRIVE KIT

| Code | Qty | Component |
|---|---|---|
| 700506773 | 2 | DL360PG8 300GB 10K SAS 2.5" HDD |
| 700501523 | 1 | SOFTWARE, DL360/380PG8 RAID1 to RAID5 UPGR+ Doc |
| - | 1 | Document to Setup HDDs in Upgrade Kits |
| - | 1 | Instructions to get the latest *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* document in “Finding documents on the Avaya Support website at http://support.avaya.com”. |

**Related links**

Finding documents on the Avaya Support website on page 112

# Chapter 6: Appliance Virtualization Platform deployment and configuration

## Appliance Virtualization Platform deployment

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

- **Attended mode:** With Appliance Virtualization Platform Release 7.1.2, this is a new mode of deployment. In this mode, you need to insert the Appliance Virtualization Platform CD-ROM 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`.

- **Unattended mode:** In this mode, you need to save a copy of the Appliance Virtualization Platform 7.1 kickstart file (7.1ks.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 CD-ROM into the server. The system will perform the Appliance Virtualization Platform deployment.

  You can generate the kickstart file (7.1ks.cfg) from Solution Deployment Manager.

## Appliance Virtualization Platform deployment in attended mode

### Deploying Appliance Virtualization Platform using a setup script

#### Before you begin

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

## Procedure

1. Connect the VGA console and USB keyboard from server to computer.
2. Turn on the server.
3. Insert the Appliance Virtualization Platform CD-ROM into the server CD-ROM drive.
4. The server starts from the CD-ROM.
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 CD-ROM.
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 53
Enable Stricter Password Policy field descriptions on page 54

## 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 52

## Enable Stricter Password Policy field descriptions

| Name | Description |
|---|---|
| **Enable Stricter Password Policy** | Enables or disables the stricter password policy. The default value is n.<br>• n: If you set the value to `n`, the minimum password length is 8.<br>• 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 52

# 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. The new S8300D and S8300E servers require an installation at the customer site.

## 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 **`set_oobm`** 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 `# ./set_oobm on`.

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

11. At the prompt, do the following:

    a. Type `./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 7.1.3 feature pack on Appliance Virtualization Platform if required.
17. Install an Appliance Virtualization Platform host license and configure the WebLM Server address, if it has not been configured during initial network configuration in Step 11.

    For information about installing and configuring Appliance Virtualization Platform license by using System Manager Solution Deployment Manager, or Solution Deployment Manager Client, or Appliance Virtualization Platform CLI, see “Installing and configuring Appliance Virtualization Platform licensing”.
18. Deploy Utility Services.
19. Deploy other Avaya Aura® applications that will reside on this Appliance Virtualization Platform host.
20. Install the Release 7.1.3 patch files for all Avaya Aura® applications.

**Related links**

Password policy on page 57

# Password policy

The password must meet the following requirements:

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

Examples of invalid passwords:

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

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

Example of a valid password: myPassword!1ok

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

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

# Activating SSH from Utility Services

### 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 Utility Services.

### Before you begin

Start an SSH session.

### Procedure

1. Log in to the Utility Services virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type `cd /opt/avaya/common_services`.
3. Type the following:

   ```
   ls
   AVP_SSH enable
   ```

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

   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.
4. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
5. 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. You must enable the SSH service on Appliance Virtualization Platform from Solution Deployment Manager.

### Procedure

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

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

   The system displays `enabled` in the **SSH status** column.
7. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

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

# 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. The following table describes the applicable Appliance Virtualization Platform license type according to the supported server types.

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

To configure the Appliance Virtualization Platform license file:

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

   **Note:**

   The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance Virtualization Platform license file contains all the necessary licenses for the complete solution.
3. Configure the applicable **WebLM IP Address/FQDN** field for each Appliance Virtualization Platform host by using either System Manager Solution Deployment Manager, Solution Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

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

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

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

  **Note:**

  Restricted administrative actions for:

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

## Appliance Virtualization Platform licensing alarms

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

# WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM is a Web-based license manager that 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) Web site 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

### Before you begin

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

### 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.

### 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 server.
- 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.

If you experience problems while installing the license file, see “License file installation errors” in *Administering standalone Avaya WebLM*.

### Procedure

1. In the left 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 64

## 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 63

## Configuring WebLM Server for an Appliance Virtualization Platform host

### Before you begin

1. Add an Appliance Virtualization Platform host.

   For information about adding a host, see “Adding an Appliance Virtualization Platform or ESXi host”.
2. Obtain the license file from the Avaya PLDS website.
3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

### Procedure

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

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

   For WebLM configuration, if you select:

   - Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.

- Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.

5. In **Port Number**, type the port number of WebLM Server.

   Embedded System Manager WebLM Server supports both 443 and 52233 ports.

6. Click **Submit**.

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

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

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

**Related links**

WebLM Configuration field descriptions on page 65

Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager on page 66

## 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. |

**Related links**

Configuring WebLM Server for an Appliance Virtualization Platform host on page 64

## 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 67

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

### Procedure

1. Perform one of the following:

   - On the System Manager Web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.

- On the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.

2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

**Related links**

Configuring WebLM Server for an Appliance Virtualization Platform host on page 64

## 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: Administration

## Adding an Appliance Virtualization Platform or ESXi host

### About this task

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

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

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

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

### Before you begin

A location must be available.

### Procedure

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

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

   In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.

7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:

    a. On the **Virtual Machines** tab, in the VMs for Selected Location <location name> section, select the required virtual machine.

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

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

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

    **Important:**

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

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

### Next steps

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

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

## Changing the network parameters for an Appliance Virtualization Platform host

### About this task

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

**Note:**

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

### Procedure

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

   ✱ **Note:**

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

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

   - Public or signaling traffic, Appliance Virtualization Platform, and all virtual machines public traffic.
   - Management, Appliance Virtualization Platform, and all virtual machine management ports.
5. To change the gateway IP address, perform the following:
   a. Click **Change Gateway**.

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

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

   The system updates the Appliance Virtualization Platform host information.

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

### About this task

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

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

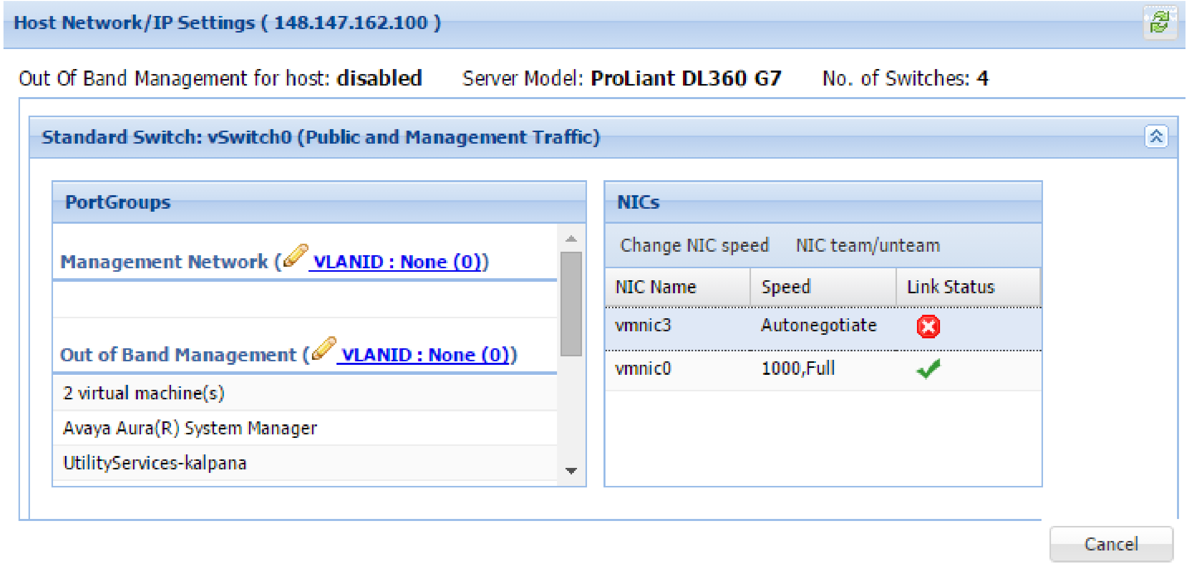
**Note:**

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

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

## Procedure

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



Host Network/IP Settings ( 148.147.162.100 )

Out Of Band Management for host: **disabled**    Server Model: **ProLiant DL360 G7**    No. of Switches: **4**

Standard Switch: vSwitch0 (Public and Management Traffic)

PortGroups

Management Network ( VLANID : None (0))

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

2 virtual machine(s)

Avaya Aura(R) System Manager

UtilityServices-kalpana

NICs

Change NIC speed    NIC team/unteam

| NIC Name | Speed | Link Status |
|---|---|---|
| vmnic3 | Autonegotiate | ✗ |
| vmnic0 | 1000,Full | ✓ |

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

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.

- **vSwitch3**. No reservations.

5. To change VLAN ID, perform the following:

    a. To expand the Standard Switch: vSwitch<n> section, click ︾.

    The section displays the vSwitch details.

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

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

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

    For more information about the value, see NIC teaming.

    d. Click **OK**.

    The system displays the new VLAN ID.

    **Note:**

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

6. To change the NIC speed, perform the following:

    a. Ensure that the system displays a vmnic in the **NIC Name** column.

    b. Click **Change NIC speed**.

    The system displays the selected vmnic dialog box.

    c. In **Configured speed, Duplex**, click a value.

    d. Click **OK**.

    For more information, see VLAN ID assignment.

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

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

    **Note:**

    You can change the speed only for common servers. You cannot change the speed for S8300D and S8300E servers.

7. To change the NIC teaming, perform the following:

    a. Select a vmnic.

    b. Click **NIC team/unteam**.

    The system displays the Out of Band Management Properties page.

    c. To perform NIC teaming or unteaming, select the vmnic and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.

For more information, see NIC teaming modes.

d. Click **OK**.

The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.

e. To check the status of the vmnic, click **NIC team/ unteam**.

8. To get the latest data on host network IP settings, click **Refresh** 🔄.

The system displays the current status of the vmnic.

**Note:**

You cannot perform NIC teaming for S8300D and S8300E servers.

**Related links**

Host Network / IP Settings field descriptions on page 77

# Changing the IP address and default gateway of the host

## About this task

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

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

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

## Before you begin

Connect the computer to the services port.

## Procedure

1. Using an SSH client, log in to the Appliance Virtualization Platform host.
2. Connect the Solution Deployment Manager client to services port on the Appliance Virtualization Platform host, and do the following:

   a. To change the IP address, at the command prompt of the host, type the following:

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

   For example:

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

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

For example:

```
esxcfg-route 135.27.162.1
```

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

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

**Related links**

[Configuring servers preinstalled with Appliance Virtualization Platform](#) on page 54

# 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:
   a. Type the **`/opt/avaya/bin/set_dualstack enable`** command.
   b. Type the IPv6 address with subnet length.
   c. Type the IPv6 gateway address.
   d. To add the IPv6 capable DNS servers, type the IPv6 address of DNS Server.

      The default value is `n`.
   e. 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

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

### Procedure

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

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

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

**Related links**

Password policy on page 57

## Shutting down the Appliance Virtualization Platform host

### About this task

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

### Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **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**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.
4. Click **More Actions** > **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 76

# 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:<br>• **None (0)**<br>• **1 to 4093**<br>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:<br>• **Autonegotiate**<br>• **10,Half**<br>• **10,Full**<br>• **100,Half**<br>• **100,Full**<br>• **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 the Appliance Virtualization Platform host. |

*Table continues…*

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

| Button | Description |
|---|---|
| **Change IPv4 Gateway** | Makes the **IPv4 Gateway** field available, and displays **Save IPv4 Gateway** and **Cancel IPv4 Gateway Change** buttons. |
| **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 Utility Services 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.
- Utility Services CLI.

**Note:**

If System Manager does not exist in the solution, then you can configure NMS by using the Utility Services CLI.

For information about configuring Appliance Virtualization Platform alarming, see *Accessing and Managing Avaya Aura Utility Services*.

# Customizing the Appliance Virtualization Platform banner through CLI

## About this task

You can use the following procedure to customize the login banner of the Appliance Virtualization Platform host and Direct Console User Interface (DCUI) of an ESXi host.

## Procedure

1. Enable SSH on Appliance Virtualization Platform by using either AVP Utilities or Solution Deployment Manager Client.

2. Create the `<banner>.txt` file with your custom message.
3. Copy the `<banner>.txt` file to the `/tmp/` directory of Appliance Virtualization Platform by using SCP.
4. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
5. Type the following command:

   ```
   /opt/avaya/bin/set_banner /tmp/<banner>.txt
   ```

   On successful execution of the command, Appliance Virtualization Platform displays the following message:

   ```
   Banner is replaced successfully.
   ```

6. To verify that Appliance Virtualization Platform displays the newly customized Appliance Virtualization Platform banner, do the following:
   a. Log out of the Appliance Virtualization Platform CLI.
   b. Log in to the Appliance Virtualization Platform CLI.

      On the login screen, Appliance Virtualization Platform displays the message that you added in the `<banner>.txt` file.

   c. Type the following command:

      ```
      dcui
      ```

      Appliance Virtualization Platform displays the message that you added in the `<banner>.txt` file.

# Chapter 9: 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 83. | 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 83. | 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 83. | 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 83

## 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 84 | |
| 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 85 | |
| 3. | Configure syslog server for remote logging. | Configuring syslog server for remote logging on page 86 | |
| 4. | Verify the commercial grade hardening status. | Verifying hardening status and completing remaining hardening settings on page 87 | |
| 5. | Run weekly check for extraneous device, unauthorized setuid or setgid files | Checking for extraneous device and unauthorized Setuid or Setgid files on page 87 | |

# 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 59

[Rebooting the Appliance Virtualization Platform host from CLI](#) on page 77

[Activating SSH from Utility Services](#) on page 58

## 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.
   1. To add local users, type the local user names separated by a space.

      For example: `user1 user2`
   2. 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`.

## Certification validation

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

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

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

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

**Note:**

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

- Log Certificate Validation Events

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

For the correct certificate:

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

If the certificate is incorrect:

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

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

**Note:**

Solution Deployment Manager:

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

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

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

**Related links**

Updating the certificate on the ESXi host from VMware on page 89

# Updating the certificate on the ESXi host from VMware

### About this task

Use the procedure to update the ESXi host certificate.

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

### Before you begin

Start an SSH session on the ESXi host.

### Procedure

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

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

   The system generates and installs the certificate.
4. Restart the ESXi host.
5. **(Optional)** Do the following:

   a. Move the ESXi host to the maintenance mode.

   b. Install the new certificate.

   c. From the Direct Console User Interface (DCUI), restart management agents.

      **Note:**

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

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

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

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

# Generating and accepting certificates

### About this task

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

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

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

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

### Before you begin

Require permissions to add a host to generate certificates.

### Procedure

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

    **Note:**

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

    b. Click **Accept Certificate**.

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

### Next steps

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

## Applying third-party Appliance Virtualization Platform certificates

### About this task

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

### Before you begin

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

### Procedure

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

2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. To generate CSR, do the following:
    a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
    b. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.
    c. Click **View/Generate CSR**.

       The system displays the View/Generate CSR dialog box.
    d. Add or edit the details of the generic CSR.

       For more information, see “Creating or editing generic CSR”.
    e. Click **Generate CSR**.

       The system generates CSR for the Appliance Virtualization Platform host.
    f. To view the status, in the **Upgrade Status** column, click **Status Details**.

       The time required for the complete process varies depending on the data on System Manager.
5. To download CSR, do the following:
    a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
    b. Click **Download CSR**.
    c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.
    d. To view the status, in the **Upgrade Status** column, click **Status Details**.

       The time required for the complete process varies depending on the data on System Manager.
    e. When the system displays a prompt, save the file.
6. Extract the downloaded certificates, and ensure that the third-party signs them.
7. To upload and push the signed certificate from third-party CA, do the following:
    a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
    b. Click **Browse** and select the required certificates for one or more Appliance Virtualization Platform hosts.
    c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.
    d. Agree to add the same certificate on Solution Deployment Manager.
    e. Click **Push Certificate**.

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

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

# Creating or editing generic CSR

## About this task

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

## Procedure

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

## Next steps

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

# Load AVP host certificate field descriptions

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

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

# Create or edit CSR field descriptions

| Name | Description |
|---|---|
| **Organization** | The organization name of the CSR. |
| **Organization Unit** | The organization unit of the CSR. |
| **Locality** | The locality of the organization associated with the CSR. |
| **State** | The state of the organization associate with the CSR. |
| **Country** | The country of the organization associate with the CSR.<br>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. |

# Managing certificates for existing hosts

## About this task

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

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

## Before you begin

Require permissions to add a host to generate certificates.

## Procedure

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

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

   b. In the Certificate dialog box, accept certificate, and click **Save**.

# Chapter 10: Rollback process

## Rolling back to System Platform

### About this task

**Note:**

The S8300D does not need to use this rollback procedure. Due to the on-board flash drive, you can reinstall System Platform without the recovery DVD. You require the recovery disk for S8300E and common servers.

### Before you begin

Keep the System Platform backup handy.

### Procedure

1. Insert the recovery CD-ROM into the server.

   The **Avaya Aura ® Appliance Virtualization Platform 7.0 CentOS Recovery ISO** disk is available on PLDS and the Avaya Support site. Also, the 700510424 media kit contains the disk.

2. Log on to System Platform web console.
3. Restart the system.
4. Connect the laptop to the following:
   - For HP server, eth0 port, the first port on the back of an HP server
   - For common server R1 or R2, eth1 port on the rear side of the server
   - For S8300D or S8300E server, service port network on the front panel
5. Reconfigure the laptop to the following:
   - IP address: 192.11.13.5
   - Netmask: 255.255.255.252
6. Start an SSH session, and connect to 192.11.13.6.
7. Log in as admin and provide the password admin01.
8. To change to the super user, type `su - root`.
9. Do the following:
   - For S8300E, type `parted /dev/sdb`.

- For other servers, type `parted /dev/sda`.

10. Type `mklabel msdos`.
11. To confirm, type `yes`.
12. To install System Platform, do the following:
    a. Insert the System Platform CD-ROM into the server.
    b. Restart the system.
    c. Reposition cables to the correct ports.
    d. Connect a computer to the network.
    e. On the System Platform web console, install software patches for System Platform.
    f. Restore the System Platform backup.

**Related links**

Rolling back to System Platform by using hard disk drive on page 97

# Rolling back to System Platform by using hard disk drive

### Procedure

1. Retrieve the hard disk drives that you removed during the installation of Appliance Virtualization Platform.
2. Turn off the server, and perform the following:
    a. Connect the monitor, keyboard, and mouse to the server.
    b. Insert the hard disk drives that you want to import into the original slots of the server.
3. Turn on the power to the server.
4. Perform one of the following:
    - If the server is Dell™ PowerEdge™ R610 or Dell™ PowerEdge™ R620, press `f` on the server console when system prompts to import the foreign array.

      For more information, see the Dell server import document.
    - If the server is HP ProLiant DL360 G7 or HP ProLiant DL360p G8, the server automatically imports and no user interaction is required.

      When you confirm the server boot from hard disk drives, the system displays the login prompt on server console.

**Related links**

Installing Appliance Virtualization Platform by using hard disk drive on page 46
Rolling back to System Platform on page 96

# Chapter 11: Upgrading Appliance Virtualization Platform

## Upgrading Appliance Virtualization Platform from Solution Deployment Manager

### About this task

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

**Note:**

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

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

  If you are installing a patch on a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.
- If you are using services port to update or upgrade Appliance Virtualization Platform, connect the system directly with the Appliance Virtualization Platform services port (Gateway 192.168.13.1). If you connect the system using the Utility Services services port (Gateway 192.11.13.6), the Appliance Virtualization Platform update or upgrade fails.

### Before you begin

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

**Note:**

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

## Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **AVP Update/Upgrade Management**.
4. On the Update Host page, click **Select Patch from Local SMGR**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.

   The patch file location is different for Solution Deployment Manager Client and System Manager Solution Deployment Manager.

   - For Solution Deployment Manager Client, the patch file must be available on windows machine where the Solution Deployment Manager client is hosted.

     For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-7.1.x.0.0.xx.zip`.

   - For System Manager Solution Deployment Manager, the patch file must be in the System Manager `swlibrary` directory.
6. On the AVP Update/Upgrade - Enhanced Access Security Gateway (EASG) User Access page, read the following messages, and do one of the following:

   **Enable: (Recommended)**

   ```
   By enabling Avaya Logins you are granting Avaya access to your
   system.
   This is necessary to maximize the performance and value of your
   Avaya support entitlements, allowing Avaya to resolve product
   issues in a timely manner.
   In addition to enabling the Avaya Logins, this product should be
   registered with Avaya and technically onboarded for remote
   connectivity and alarming. Please see the Avaya support site
   (support.avaya.com/registration) for additional information for
   registering products and establishing remote access and alarming.
   ```

   **Disable**:

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

```
managing the product themselves, Avaya Logins should not be
disabled.
```

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

      Avaya recommends to enable EASG.

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

   b. To disable EASG, click **Disable EASG**.

7. On the EULA Acceptance page, read the EULA, and do one of the following:

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

   b. To decline the EULA, click **Decline**.

8. To view the details, in the **Current Action** column, click **Status Details**.

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

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

### Next steps

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

#### Related links

Update Host field descriptions on page 100

## Update Host field descriptions

| Name | Description |
|---|---|
| **Patch location** | The location where the Appliance Virtualization Platform patch is available. The options are:<br>• **Select Patch from Local SMGR**: To use the Appliance Virtualization Platform patch that is available on the local System Manager.<br>• **Select Patch from software library**: To use the Appliance Virtualization Platform patch that is available in the software library. |

*Table continues…*

| Name | Description |
|---|---|
| **Ignore Signature Validation** | Ignores the signature validation for the patch.<br>**Note:**<br>If the Appliance Virtualization Platform patch is unsigned, you must select the **Ignore signature validation** check box. |
| **Select patch file** | The absolute path to the Appliance Virtualization Platform patch file. |

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

# Removing the Appliance Virtualization Platform patch from the ESXi host CLI

## About this task

Use the procedure to restore the Appliance Virtualization Platform software to the earlier version.

In this procedure, the command installs the older release on the new release that you want to replace.

**Note:**

You can remove the Appliance Virtualization Platform patch only from the host CLI. You cannot use System Manager Solution Deployment Manager or the Solution Deployment Manager client.

## Before you begin

- Start an SSH session.
- Log in to the Appliance Virtualization Platform host command line with admin user credentials.
- Using the backup and restore capability of the application, create a backup of the Avaya Aura® application.

  You need the backup to reinstall and restore the applications.
- Copy the patch of the earlier version to the `/vmfs/volumes/server-local-disk` folder on the system.

## Procedure

1. To stop all virtual machines that are running on the Appliance Virtualization Platform host, at the prompt, type `/opt/avaya/bin/stopallvms.py`.

2. To rollback from Appliance Virtualization Platform Release 7.1.3 to any of the previous releases, perform the following:

   a. Type the `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<complete path name of the rollback patch>` command.

      Ensure to type the complete path name of the rollback patch. Do not use a relative path.

      To rollback from Appliance Virtualization Platform Release 7.1.3 to Release 7.0.0.x (`avaya-avp-7.0.0.1.0.2.zip`), type the following command:

      `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.1.0.0.0.9.zip`

   b. To reboot the system, type `/opt/avaya/bin/avpshutdown.sh -r`.

3. To rollback from Appliance Virtualization Platform Release 7.1.2 to Release 7.1.0.x, perform the following:

   a. Type the `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<avaya-avp-7.1.0.0.0.9.zip>` command.

      Ensure to type the complete path name of the rollback patch. Do not use a relative path.

   b. To reboot the system, type `/opt/avaya/bin/avpshutdown.sh -r`.

   c. To enable SSH by using the Solution Deployment Manager client, on VM Management, click **More Actions** > **Enable SSH**.

      You can also enable SSH by using the VMware vSphere client.

   Issue the following commands after reboot:

   ```
   /opt/avaya/bin/reduceReservation.sh
   /opt/avaya/bin/installvibs.sh
   reboot
   ```

4. To rollback from Appliance Virtualization Platform Release 7.1.2 to Release 7.0.0.x, perform the following:

   a. Type the `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<avaya-avp-7.1.0.0.0.9.zip>` command.

      ```
      ramgb=$(($(esxcli --formatter=keyvalue hardware memory get \
       | grep -e "Memory\.PhysicalMemory\.integer" \
       | cut -d "=" -f 2) / (1024 * 1024 * 1024)))
      if [ "$ramgb" -le 48 ]; then
      memMinFreePct=1
      if [ "$ramgb" -le 16 ]; then
      memMinFreePct=2
      fi
      esxcli system settings advanced set -o /Mem/MemMinFreePct -i $memMinFreePct
      fi
      ```

      Ensure to type the complete path name of the rollback patch. Do not use a relative path.

   b. To reboot the system, type `/opt/avaya/bin/avpshutdown.sh -r`.

   c. To enable SSH by using the Solution Deployment Manager client, on VM Management, click **More Actions** > **Enable SSH**.

      You can also enable SSH by using the VMware vSphere client.

   Issue the following commands after reboot:

```
/opt/avaya/bin/reduceReservation.sh
/opt/avaya/bin/installvibs.sh
reboot
```

5. To rollback from Appliance Virtualization Platform Release 7.0.1.0.5 or 7.1.0.x to Release 7.0.0.0.0.21, type `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<avaya-avp-7.0.0.0.0.21.zip>`.

### Next steps

Verify the Appliance Virtualization Platform software release and the ESXi version.

# Chapter 12: Post-upgrade tasks

## Verifying the Appliance Virtualization Platform software release and the ESXi version

### Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. To verify the Appliance Virtualization Platform software release, run the `cat /opt/avaya/etc/avaya-avp.version` command.

   The system displays the following.

   ```
   # Maj.Min.FP.SP.PATCH.BUILD
   Release: 7.1.3.0.0.x
   ```

4. To verify the ESXi version, run the `esxcli system version get` command.

   The system displays the following.

   ```
   Product: VMware ESXi
   Version: 6.0.0
   Build: Releasebuild-xxxxxxx
   Update: x
   ```

## Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

# Managing EASG from CLI

## About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, or view the status of EASG.

## Before you begin

Log in to the application CLI interface.

## Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message.

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

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the Avaya
      support site (https://support.avaya.com/ registration) for
      additional information for registering products and
      establishing remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled`.

3. To disable EASG, do the following:

   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message.

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

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is disabled`.

## Viewing the EASG certificate information

### Procedure

1. Log in to the application CLI interface.
2. Run the command: **`/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 13: 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 `7.1ks.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 7.1.3 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 Utility Services 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 Utility Services or from Solution Deployment Manager. For more information, see Activating SSH from Utility Services.

### 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 Utility Services on page 58

## 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 76

## Viewing installation log traces

### Solution

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

# Clearing system event logs from CLI

## About this task

When Appliance Virtualization Platform continues to generate alarms even after replacing the faulty hardware component, you must clear the system event logs to suppress false alarms.

For example, if the memory module is replaced and Appliance Virtualization Platform continuously generates the MEM_FAULT alarm.

## Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. Type the following command:

   ```
   esxcli hardware ipmi sel clear
   ```

   System event logs get cleared from Appliance Virtualization Platform.

# Chapter 14: Resources

## Documentation

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

| Title | Use this document to: | Audience |
|---|---|---|
| Overview | | |
| Avaya Aura® Virtualized Environment Solution Description | Understand the high-level solution features and functionality | Customers and sales, services, and support personnel |
| *Avaya Aura® System Manager Overview and Specification* | Understand the high-level solution features and functionality | Customers and sales, services, and support personnel |
| Administering | | |
| *Accessing and Managing Avaya Aura® Utility Services* | Perform administration tasks | System administrators |
| *Administering Avaya Aura® System Manager* | Perform administration tasks | System administrators |
| *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504 | Administer the network components of Communication Manager | System administrators |
| *Administering Avaya Aura® Communication Manager*, 03-300509 | Administer Communication Managercomponents, such as trunks, signalling groups, and dial plans, setting up telephony features, such as conferencing, transfer, and messaging. | System administrators |
| Using | | |
| *Using the Solution Deployment Manager client* | Deploy Avaya Aura® applications and install patches on Avaya Aura® applications. | System administrators |
| Implementing | | |
| *Deploying Avaya Aura® Utility Services*<br>s | Install and configure Utility Services. | Implementation personnel |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| *Deploying Avaya Aura® applications from System Manager* | Install and configure Avaya applications | Implementation personnel |
| *Upgrading and Migrating Avaya Aura® applications from System Manager* | Upgrade Avaya Aura® applications to Release 7.x and later on Appliance Virtualization Platform running on Avaya-provided servers, and on customer Virtualized Environment | System administrators and IT personnel |
| Troubleshooting | | |
| *Troubleshooting Avaya Aura® System Manager* | Perform troubleshooting tasks | |

**Related links**

Finding documents on the Avaya Support website on page 112

## Finding documents on the Avaya Support website

### Procedure

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

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

**Related links**

Documentation on page 111

# Training

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

| Course code | Course title |
|---|---|
| Avaya Aura® core implementation | |
| 1A00234E | Avaya Aura® Fundamental Technology |
| 4U00040E | Avaya Aura® Session Manager and System Manager Implementation |
| 4U00030E | Avaya Aura® Communication Manager and Communication Manager Messaging Implementation |
| 10U00030E | Avaya Aura® Application Enablement Services Implementation |
| 8U00170E | Avaya Aura® Presence Services Implement and Support |
| AVA00838H00 | Avaya Aura® Media Server and Media Gateways Implementation Workshop |
| ATC00838VEN | Avaya Aura® Media Server and Gateways Implementation Workshop Labs |
| Avaya Aura® core support | |
| 5U00050E | Session Manager and System Manager Support |
| 5U00060E | ACSS - Avaya Aura® Communication Manager and CM Messaging Support |
| 4U00115I<br>4U00115V | Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x) |
| 1A00236E | Avaya Aura® Session Manager and System Manager Fundamentals |
| 2008W | What is New in Avaya Aura® Application Enablement Services 7.0 |
| 2008T | What is New in Avaya Aura® Application Enablement Services 7.0 Online Test |
| 2009W | What is New in Avaya Aura® Communication Manager 7 |
| 2009T | What is New in Avaya Aura® Communication Manager 7.0 Online Test |
| 2010W | What is New in Avaya Aura® Presence Services 7.0 |
| 2010T | What is New in Avaya Aura® Presence Services 7.0 Online Test |
| 2011W | What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0 |
| 2011T | What is New in Avaya Aura® Session Manager and Avaya Aura® System Manager 7.0 Online Test |
| 2013V | Avaya Aura® 7 Administration |
| Avaya Aura® core administration and maintenance | |
| 9U00160E | Avaya Aura® Session Manager for System Administrators |
| 1A00236E | Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals |
| 5U00051E | Avaya Aura® Communication Manager Administration |
| 5M00050A | Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance & Troubleshooting |
| 2012V | Migrating and Upgrading to Avaya Aura® 7.0 |
| 2012I | Migrating and Upgrading to Avaya Aura® 7 |
| 2017 | Avaya Aura® 7 Administration Delta |
| 2017V | Avaya Aura® 7 Administration Delta |

## Viewing Avaya Mentor videos

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

### About this task

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

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

## Support

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

**Related links**

Using the Avaya InSite Knowledge Base on page 114

## Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

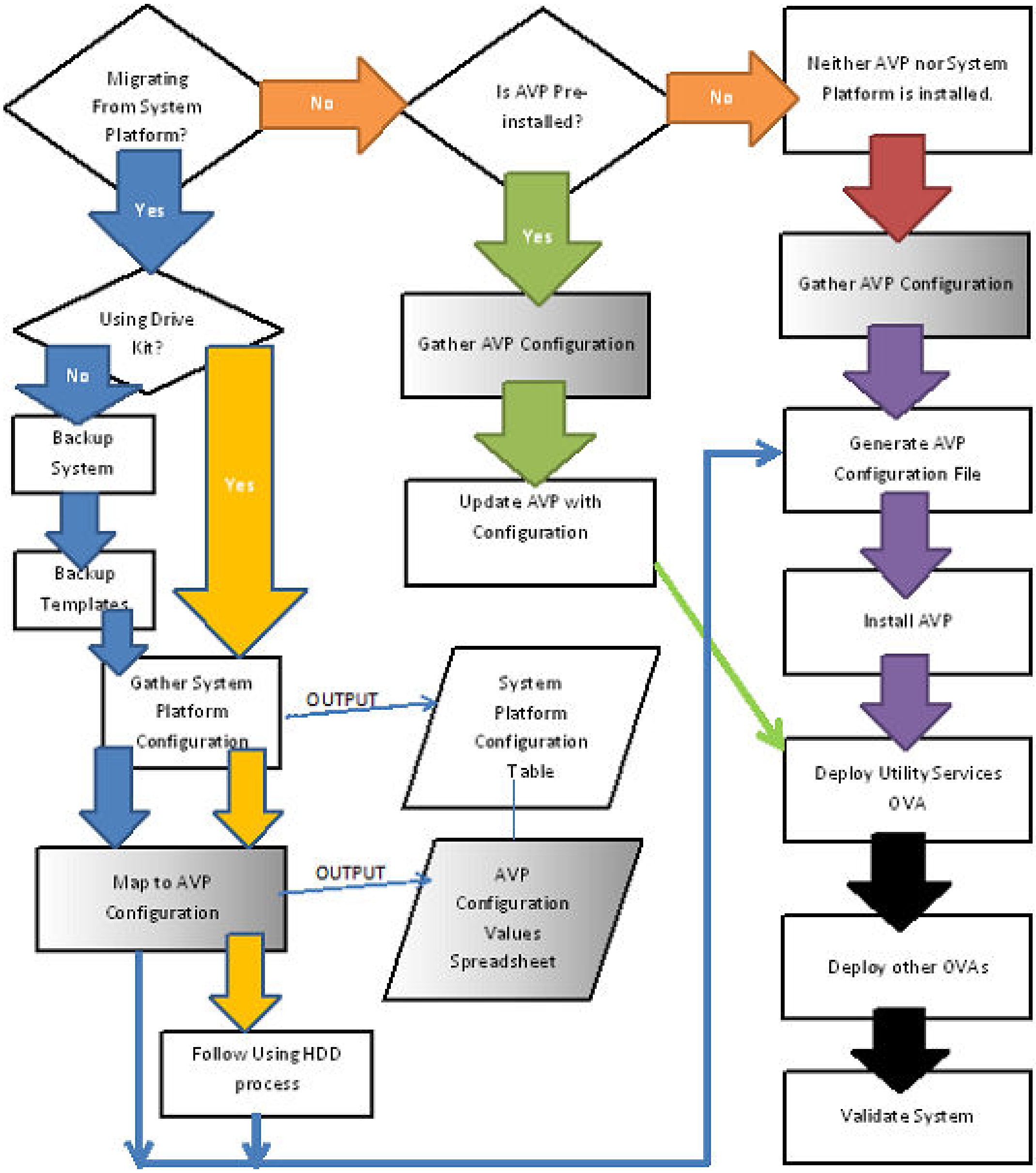
   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select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

**Related links**

Support on page 114

# Appendix A: System Platform to Appliance Virtualization Platform migration scenarios

## Appliance Virtualization Platform installation scenarios


Migrating From System Platform?
No
Is AVP Pre-installed?
No
Neither AVP nor System Platform is installed.
Yes
Yes
Gather AVP Configuration
Using Drive Kit?
No
Gather AVP Configuration
Backup System
Yes
Generate AVP Configuration File
Update AVP with Configuration
Backup Templates
Install AVP
Gather System Platform Configuration
OUTPUT
System Platform Configuration Table
Deploy Utility Services OVA
Map to AVP Configuration
OUTPUT
AVP Configuration Values Spreadsheet
Deploy other OVAs
Follow Using HDD process
Validate System

# Deploying Utility Services 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 Utility Services 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 Utility Services.
7. Fill in the Utility Services 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 Utility Services, and wait for the virtual machine to deploy successfully.
9. Install the Utility Services 7.1.3 feature pack.
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 Utility Services on page 45

# Deploying Utility Services 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**: 192.168.13.6

   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 Utility Services 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 Utility Services.
7. Enter the IP address details for Utility Services, deploy Utility Services, and wait for the virtual machine to deploy successfully.
8. Install the Utility Services 7.1.3 feature pack.
9. Change the Utility Services 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 Utility Services.

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 Utility Services on page 45

# Index