Deploying Avaya Aura® AVP Utilities in a virtual appliance

Release 8.1.x
Issue 9
April 2023

© 2018-2023, Avaya Inc.
All Rights Reserved.

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.

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document provides installation, initial configuration, basic maintenance checklists and procedures, and troubleshooting procedures for Avaya Aura® AVP Utilities. This document is intended for people who install and configure at a customer site.

Change history

Issue	Date	Summary of changes
9	April 2023	Added the following sections: • Upgrading AVP Utilities from Release 8.0.x to Release 8.1.x • Pre-upgrade Configuration field descriptions • Edit Upgrade Configuration field descriptions Updated the following sections: • Creating a backup of AVP Utilities • Restoring the AVP Utilities backup
8	October 2020	In Release 8.1.3, updated the following sections: • Creating a backup of AVP Utilities • Restoring the AVP Utilities backup • Checklist to rollback to previous version of Utility Services
7	June 2020	Updated the following sections with Release 8.1.0.0.0.0.6 information: • Installing software patches • Installing patches and service packs using CLI

Table continues…

Issue	Date	Summary of changes
6	May 2020	Updated the following sections: • Creating a backup of Utility Services • Creating a backup of AVP Utilities • Restoring AVP Utilities backup files
5	April 2020	Updated the “Installing patches and service packs using CLI” section.
4	March 2020	In Release 8.1.2, updated the following section: • Network Parameters and Configuration Parameters field descriptions.
3	December 2019	Updated the “Deploying AVP Utilities and virtual machines on the services port” section.
2	October 2019	Updated the “Release details of AVP Utilities” section.
1	June 2019	Release 8.1

Chapter 2: Overview

AVP Utilities overview

In Avaya Aura® Release 8.0, Utility Services is replaced by AVP Utilities. While some of the Utility Services features are migrated to other Avaya Aura® applications, the following features of Utility Services are migrated to AVP Utilities:

- Services Port access for virtual machines
- Appliance Virtualization Platform log collection and alarming
- SSH access for Appliance Virtualization Platform

The following features of Utility Services are migrated to other Avaya Aura® applications:

Features of Utility Services 7.x	Migrated to	Description
Enterprise System Directory (ESD)	Avaya Aura® System Manager 8.0 and later.	Only LDAP integration with Avaya Aura® System Manager is supported. Searching the LDAP directory is supported for SIP phones only.
File Server	Avaya Aura® Device Services 8.0 and later.	Avaya Aura® Device Services provides this feature for IP Phones, but not for Gateway Firmware. .
MyPhone	Avaya Aura® Unified User Portal 8.0 and later.	Existing configurations must be re-applied, if any.

You can use the following features of Utility Services through third-party applications:

Features of Utility Services 7.x	Description
Call Detail Recordings collection	You must use third-party applications. You can also use the Call Detail Recordings data with third-party solutions.
Dynamic Host Configuration Protocol (DHCP)	You must use a separate DHCP server.

Chapter 3: Planning

Planning checklist

Use the following checklist to plan your deployment process:

#	Task	Reference	✔
1	Verify the network interface requirements.	See Network requirements on page 10	
2	Verify the release details of the AVP Utilities OVA file.	See Release details of AVP Utilities on page 11	
3	Download the OVA.	See Downloading software from PLDS on page 11	
4	Ensure that the supported servers are available.	See Supported servers on page 12	
5	Ensure that the supported footprints are available.	See Supported footprints for AVP Utilities on page 12	

Network requirements

The following network interfaces are used for AVP Utilities.

Network Adapter	Ethernet Port	Interface	Function
1	eth0	Public	VM Public Interface
2	eth1	Services	Avaya Services Port, 192.11.13.6/30
	eth1:1		Avaya Services Port, 192.168.13.1/29
3	eth2	Out of Band Management	VM Out of Band Management

Release details of AVP Utilities

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

Downloading software from PLDS

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

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

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    Note:

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

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

Supported servers

AVP Utilities supports deployment on the following servers:

- Avaya Solutions Platform 120 server
- S8300E
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630

Supported footprints for AVP Utilities

To deploy AVP Utilities, the following footprints are required on the ESXi host:

AVP Utilities	Minimum CPU speed based on Xeon E5620 or equivalent processor	vCPUs	RAM (GB)	HDD (GB)
Standard mode	2.2 GHz	1	1	20
Hardened mode	2.2 GHz	1	1	20
Hardened mode (DoD)	2.2 GHz	1	1	20

Chapter 4: Deploying

Deployment modes

You can deploy AVP Utilities in one of the following modes:

- Standard mode
- Hardened mode
- Hardened mode DoD

You can select the deployment mode while deploying AVP Utilities. By default, Out of Band Management (OOBM) is disabled in all the modes.

Supported security hardening grades

The following security hardening grade is supported for each deployment mode:

Deployment mode	Security hardening grade
Standard mode	Standard
Hardened mode	Commercial
Hardened mode (DoD)	Military

Supported security attributes

Depending on the deployment mode selected, the following security attributes are applied on AVP Utilities :

Security attribute	Standard mode	Hardened mode	Hardened mode (DoD)
VMX hardening **Note:** VM ESXi VMX file hardening is applied as part of Solution Deployment Manager deployment.	Y	Y	Y
DoD Banner	N/A	N/A	Y
Password management	Y	Y (more restrictive)	Y (more restrictive)

Table continues…

Security attribute	Standard mode	Hardened mode	Hardened mode (DoD)
Login and session management	Y	Y	Y
System and Application files hardening	Y	Y	Y
Multifactor Authentication (PIV and CAC support) **Note:** You must have root access to configure the use of authorized keys from a “Smart” card for user accounts.	Y (manual)	Y (manual)	Y (manual)
Support for TLS 1.2	Y	Y	Y
FIPS 140-2 compliance	Y (optional)	Y	Y
SELinux enabled	Y (optional)	Y	Y
Audit management	Y (optional)	Y	Y
AIDE (File Tampering Prevention)	Y (optional)	Y	Y

Deployment scenarios

AVP Utilities supports the following deployment scenarios for a fresh deployment:

Deployment scenario	Description
Scenario 1	For a complete fresh deployment, do the following: • Deploy Appliance Virtualization Platform 8.1. • After successful registration of Appliance Virtualization Platform 8.1 on the Solution Deployment Manager client, deploy AVP Utilities 8.1.
Scenario 2	If you already deployed the Appliance Virtualization Platform 8.1, then do the following: • Add Appliance Virtualization Platform 8.1 host on Solution Deployment Manager. • Deploy AVP Utilities 8.1.

Table continues…

Deployment scenario	Description
Scenario 3	If the existing AVP Utilities application is corrupted or inaccessible, then do the following: • Roll back to Utility Services. • Re-deploy AVP Utilities. Rolling back to Utility Services on page 56 Retrying Utility Services to AVP Utilities upgrade on page 56

Note:

While the AVP Utilities deployment is in progress, do not deploy other virtual machines.

Deploying AVP Utilities

About this task

Use this procedure to deploy AVP Utilities on Appliance Virtualization Platform.

To deploy AVP Utilities, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable.

Before you begin

- Add a location.

  See “Adding a location” in *Administering Avaya Aura® System Manager*.

- Add Appliance Virtualization Platform.

  See “Adding an Appliance Virtualization Platform or ESXi host” in *Administering Avaya Aura® System Manager*.

- Download the AVP Utilities OVA file.

Procedure

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

   The system displays the Applications Deployment section.

4. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

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

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

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the message: `Invalid file content. Avaya Certificate not found or invalid`.
8. Click **Next**.

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

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

    For more information about Configuration Parameters, see “Network Parameters and Configuration Parameters field descriptions”.
11. Click **Deploy**.
12. Click **Accept the license terms**.

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

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

Next steps

1. To activate the serviceability agent registration, reboot the AVP Utilities virtual machine.
2. Deploy all other Avaya Aura® applications at a time.

Related links

Network Parameters and Configuration Parameters field descriptions on page 17

Network Parameters and Configuration Parameters field descriptions

Note:

During the AVP Utilities deployment, if you do not know the **System Manager IP Address** or **Enrollment Password**, then use the dummy values. Dummy values must pass validation. Use the localhost default 127.0.0.1 for the IP address, and `Dummy` as the password.

Name	Description
Networking Properties	
Hostname	Linux hostname or fully qualified domain name for AVP Utilities virtual machine. **Note:** The host name is regardless of the interface that is used to access. The Public interface is the default interface.
Public IP address	The IP address for this interface. Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Public Default Gateway	The IP address of the default gateway. Required field unless you use DHCP. **Note:** The default gateway should be configured for the Public network. You can use the `ovf_set_static` command to allow a static route to be assigned to the OOBM network, enabling OOBM network to reach a second subnet.
Public IPv6 address	The IP address for this interface. Required field unless you use DHCP.
Public IPv6 Prefix	The netmask for this interface. Required field unless you use DHCP.
Default IPv6 Gateway	The IP address of the default gateway. Required field unless you use DHCP.

Table continues…

Name	Description
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.
Out of Band Management IPv6 Address	The IPv6 address for this interface. This field is optional.
Out of Band Management IPv6 Prefix	The IPv6 prefix for this interface. This field is optional.
Network Time Protocol IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
TImezone setting	The selected timezone setting for the AVP Utilities virtual machine.
DNS	The IP address of domain name servers for the AVP Utilities virtual machine. Separate each IP address by a comma. Required field unless you use DHCP. You can specify up to three DNS Servers.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirm Password	The confirmation password.
Application Properties	
AVP Utilities Mode	The mode in which you want to deploy AVP Utilities. You can set the mode during the deployment only. You cannot change the mode after the virtual machine is deployed. The options are: • **standard_mode**: AVP Utilities and services port enabled. The default mode for Appliance Virtualization Platform. • **hardened_mode**: Sets up the system for commercial hardening. • **hardened_mode (dod)**: Sets up the system for military hardening.
Admin User Password	The admin user password.
Confirm Password	The confirmation password.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management. **Note:** **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Data Encryption

Note:

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

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase.
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.

Table continues…

Name	Description
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. If local key store is not enabled, the Passphrase at boot-time must be provided on the application VM console on the Solution Deployment Manager in the following scenarios: • During the first time deployment of the OVA. • During the Service Pack or Feature Pack, upgrade of AVP Utilities util_patch R8.1.2 onwards post reboot. • During the maintenance window which requires reboot. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. If you deploy AVP Utilities Release 8.1E OVA in a hardened mode or hardened_DOD mode with encryption enabled, then *do not* select the **Require Encryption Pass-Phrase at Boot-Time** check box. When the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected, system creates a local key store which helps in uninterrupted deployment through SDM. If you select the **Require Encryption Pass-Phrase at Boot-Time** check box, then you must manually open the VM console of the AVP Utilities machine, and enter the encryption passphrase. Until the passphrase is not entered, the deployment is not marked as complete. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Customer Root Account

Name	Description
Enable Customer Root Account for this Application	Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**. When you accept the root access statement, the system displays the **Customer Root Password** and **Re-enter Customer Root Password** fields.
Customer Root Password	The root password for the application
Re-enter Customer Root Password	The root password for the application

Related links

Deploying AVP Utilities on page 15

Enabling FIPS mode

Before you begin

When AVP Utilities is deployed in a Hardened mode or Hardened mode (DoD), FIPS mode is automatically enabled. However, when AVP Utilities is deployed in standard mode, you must enable the FIPS mode manually.

Warning:

After you enable FIPS mode, AVP Utilities is rebooted and you cannot disable the reboot.

Procedure

1. Log in to AVP Utilities CLI as an administrator.
2. Run the following script: `fips_mode_enable`.

   After the script finishes running, AVP Utilities is rebooted.
3. After the reboot, log in to AVP Utilities again as an administrator.
4. Run the following command to ensure that the FIPS mode is enabled: `sysctl crypto.fips_enabled`.

   AVP Utilities displays **`crypto.fips_enabled = 1`** where 1 indicates that the FIPS mode is enabled.

Security hardening features

About this task

Although AVP Utilities can be deployed in hardened mode, there are options to selectively enable various hardening features when deployed in standard mode. These include:

- FIPS compliance
- AIDE for file integrity check
- Secure Linux (SELinux)
- Auditing at operating system level (Auditd)

Note:

These features may have a performance impact and should only be enabled if required.

Warning:

After you enable FIPS mode, AVP Utilities is rebooted and you cannot disable the reboot.

You can use the following security hardening commands:

- To enable FIPS mode, run the following script: `fips_mode_enable`
- To enable aide, run the following command: `aide_enable`.
- To disable aide, run the following command: `aide_disable`.
- To enable auditd, run the following command: `auditd_enable`.
- To disable aide, run the following command: `auditd_disable`.
- To enable SELinux, run the following command: `selinux_enable`.
- To disable SELinux, run the following command: `selinux_disable`.

Enabling Out of Band Management

About this task

Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems. Out of Band Management (OOBM) is a physically and logically separate network connection. OOBM connects to a customer's private management network and provides secure management and administration of Avaya products.

If OOBM is not enabled as part of the deployment, enable AVP Utilities OOBM as part of a solution-level OOBM implementation. When you enable OOBM on AVP Utilities, the following services connect to the OOBM network with physical connection on the eth2 port. Do not enable OOBM applications individually. Coordinate Enablement of OOBM with all other components that form the solution.

Application	Interfaces for traffic
SSH	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH)	Out of Band Management

Procedure

1. Log in to AVP Utilities as an administrator.
2. Run the following commands as required:
   - To enable Out of Band Management, run `sudo /opt/avaya/common_services/ovf_set_oobm OOBM_Enabled`.
   - To disable Out of Band Management, run `sudo /opt/avaya/common_services/ovf_set_oobm OOBM_Disabled`.

Installing software patches

About this task

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

Note:

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

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

Before you begin

- Perform refresh and analyze operations.
- You must uninstall the previous feature pack or service pack, if available.

  For more information on uninstalling the feature pack or service pack by using the Solution Deployment Manager, see Uninstalling the feature pack or service pack by using Solution Deployment Manager on page 60.
- If your current version is 8.1.0.0.0.0.6, run the following command as a root user:

  `rm -rf /tmp/patchins`

  It will delete the existing `patchins` folder, if exists.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.

2. To establish trust, click **More Actions** > **Re-establish Connection**.
3. Click **Refresh VM**.

Procedure

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

   Note:

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

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

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

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

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

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

    The page displays all software patches that you can commit.

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

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

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

Related links

Installed Patches field descriptions on page 25

Installed Patches field descriptions

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

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.
Patch Type	The type of the software patch. The options are: • service pack or feature pack or software patch • Kernel • Security

Table continues…

Name	Description
Patch State	The state of the software patch. The options are: • Active (when patch is activated) • Installed (when patch is unpacked) • Pending (when patch is pending a commit)

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

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

Related links

Installing software patches on page 23

Installing patches and service packs using CLI

About this task

You can install the software patches and service packs using:

- AVP Utilities CLI
- Solution Deployment Manager

Before you begin

- You must uninstall the previous feature pack or service pack, if available.

For more information on uninstalling the feature pack or service pack by using the Solution Deployment Manager, see Uninstalling the feature pack or service pack by using Solution Deployment Manager on page 60.

- As an admin user, do the following on the AVP Utilities CLI:
  - To view the list of patch versions installed, run the following command: **`swversion`**.

    The last line of the command output provides the patch number, if installed.

    You can also run the following command to view the list of patches or service packs installed: **`/opt/avaya/common_services/update -l`**.

    If the patches or service packs are not installed, then the command does not result in an output.
  - To uninstall the previous feature pack or service pack, run the following command: **`update -r <patch tag>`**.

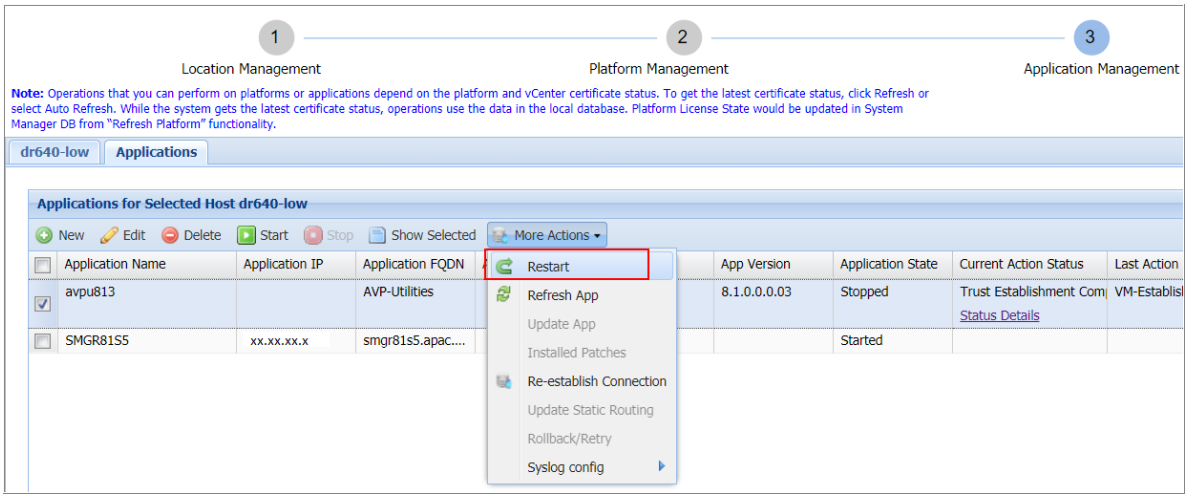
    For example, `update -r 8011006`.
  - If your current version is 8.1.0.0.0.0.6, run the following command as a root user:

    `rm -rf /tmp/patchins`

    It will delete the existing `patchins` folder, if exists.

Procedure

1. Using an SCP client, copy the AVP Utilities update to the `/tmp` directory.
2. Log in to AVP Utilities CLI as an administrator and run the following command: `/opt/avaya/common_services/update -i /tmp/<AVPU update zip filename>`.
3. Respond to the prompt accordingly.
4. After the patch is installed, check the list of installed patch versions using the following command: **`swversion`**.
5. To ensure all updates take effect, reboot AVP Utilities by using Solution Deployment Manager or the Embedded Host Client.



For information about installing software patches by using the Solution Deployment Manager, see Installing software patches on page 23.

Chapter 5: Configuring

Enabling or disabling EASG

About this task

Use this procedure to enable or disable EASG. By enabling EASG, you grant Avaya access to your system. The access maximizes the performance and value of your Avaya support entitlements, and Avaya can resolve product issues in a timely manner. Avaya recommends that you do not disable EASG, because it impacts Avaya's ability to provide support for the product and customers will then have to manage the product themselves.

Procedure

1. Log in to the AVP Utilities as an administrator.
2. Run one of the following scripts as required:
   - To enable EASG: `Enable_EASG.sh`.
   - To disable EASG: `Disable_EASG.sh`.
   - To permanently disable EASG: `PermanentEASGRemoval.sh`.

Viewing the EASG status

About this task

Use this procedure to know whether EASG is enabled or disabled.

Procedure

1. Log in to the AVP Utilities CLI interface as an administrator.
2. Run the following script: `sudo EASGStatus`.

Removing EASG

About this task

Use this procedure to remove Enhanced Access Security Gateway (EASG) and Avaya Services logins. Customers with root access can only remove EASG.

Note:

If you remove EASG, Avaya cannot access your system to provide support. You can use the OVA deployment process to reinstall EASG.

Procedure

1. Log in to the AVP Utilities as an administrator.
2. Type the command: `su root` to gain the root access.
3. Run the following command: `/opt/util/bin/PermanentEASGRemoval.sh`.

Linux kernel configuration

AVP Utilities includes the Red Hat updates to support mitigation of the Meltdown and Spectre vulnerabilities. However, this can affect the performance of AVP Utilities. So a script **`kernel_opts.sh`** is introduced so that the script can control how these vulnerabilities are handled through the setting of kernel options. The effect of running the kernel configuration script is immediate and continues across reboots. You can run the script as an admin user by using the AVP Utilities CLI.

The script has the following arguments:

- status: Displays the current status of the kernel options.
- enable: Enables all flags to provide maximum protection.
- disable: Disables all flags to provide maximum performance.

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 6: Migrating

Supported migration paths

The following migration paths are supported:

From Utility Services	To AVP Utilities
8.0.x	8.1.x
7.x.x	8.1.x
6.x	8.1.x

Supported features of Utility Services after migrating to AVP Utilities

About this task

After you migrate from Avaya Aura® Utility Services to Avaya Aura® AVP Utilities, only the following Utility Services features are supported in AVP Utilities.

- Services Port access for VMs (IP Forwarding enabled).
- AVP alarming and log harvesting.
- Enabling SSH access for Appliance Virtualization Platform.

If Utility Services is deployed in ”Services Port Only” mode or “Hardened Mode Services port only” mode, then the hardening settings configured for Utility Services will be retained for AVP Utilities. The mapping of Utility Services modes to AVP Utilities modes is as follows:

Avaya Aura® Utility Services mode	Avaya Aura® AVP Utilities mode
Full functionality	Standard mode
Utility Services only	Standard mode
Services port only	Standard mode
Hardened mode services port only	Hardened mode (Department of Defence)

During migration, you can restore only applicable configuration data from the Utility Services backup file.

Checklist to migrate from Utility Services 7.x to AVP Utilities 8.1

About this task

If you are using Utility Services 7.x, then you can migrate to AVP Utilities 8.1.

Task	Link	✔
Back up the Utility Services configuration files.	See Creating a backup of Utility Services on page 36 **Note:** Before you migrate from Utility Services 7.x to AVP Utilities 8.1, you must perform a full back up of Utility Services and save it on to a remote server. Ensure that you do NOT leave the back up data on the Utility Services virtual machine.	
Upgrade Appliance Virtualization Platform from 7.x to 8.x	See Upgrading Utility Services 7.x to AVP Utilities Release 8.1.3 in bulk during Appliance Virtualization Platform upgrade on page 37	
Deploy AVP Utilities	See Deploying AVP Utilities on page 15	

Checklist to migrate from Utility Services 6.x to AVP Utilities 8.1

Perform the following tasks to migrate from Utility Services 6.x to AVP Utilities 8.1:

Task	Link	✔
Migrate from System Platform 6.x to Appliance Virtualization Platform 8.x	See Migrating System Platform-based system and elements in bulk to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager on page 34	

Table continues…

Task	Link	✔
Backup Utility Services	See Creating a backup of Utility Services on page 36 **Note:** Before you migrate from Utility Services 6.x to AVP Utilities 8.1, you must perform a full back up of Utility Services and save it on to a remote server. Ensure that you do NOT leave the back up data on the Utility Services virtual machine.	
Deploy AVP Utilities	See Deploying AVP Utilities on page 15	

Migrating System Platform-based system and elements in bulk to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager

About this task

Use this procedure to remotely migrate System Platform-based system and elements in bulk to Appliance Virtualization Platform Release 8.1.3. You can remotely migrate:

- Communication Manager, Branch Session Manager, and Utility Services that are running on System Platform.
- Communication Manager Release 5.2.1 bare metal system.

Before you begin

- On the Manage Elements page, add the System Platform system and required elements. For information about adding a new element, see *Administering Avaya Aura® System Manager*.
- Refresh the element.
- Analyze the software.
- Perform the pre-upgrade check.
- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.
- Fill the required system details in the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.

Note:

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.

   The system displays the Upgrade Management page.
3. Select the required element.

   When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Bulk Import Configuration(s)**.
6. On the Upload Xlsx File Configuration dialog box, perform the following:
   a. Click **Browse** and select the file from the local computer.
   b. To upload the spreadsheet, click **Upload**.
   c. Click **Submit**.

      The system displays the file size, timestamp, and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.

      On the Upgrade Management page, the system displays the message: `Please Wait - Saving Import Excel Sheet Configuration ....` You must wait until the system stops showing this message.
7. On the Upgrade Management page, click  .

   The **Configuration Status** column displays .
8. To save the configuration, click **Save Configuration**.

   The update configuration is saved as a job in the Upgrade Jobs Status page.
9. On the Upgrade Configuration page, click **Upgrade**.
10. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
11. On the Upgrade Management page, click  .

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

Creating a backup of Utility Services

About this task

Back up the configuration files of Utility Services to transfer the files or rollback configuration updates. When you back up Utility Services in Hardened mode, the backup includes the following configuration files:

- SSH
- AIDE: /etc/aide.conf
- Audit: /etc/audit/auditd.conf
- Login defs: /etc/login.defs
- Password auth: /etc/pam.d/password-auth
- Password settings: /etc/security/pwquality.conf
- User passwords and group membership:
  - /etc/passwd
  - /etc/shadow
  - /etc/group
  - /etc/gshadow
- rsyslog: /etc/rsyslog.conf
- selinux: /etc/selinux/config
- Access Control List (ACL):
  - /etc/hosts.allow
  - /etc/hosts.deny
- Banner: /etc/issue

Procedure

1. Use an account with administrator-level privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) webpage.
2. Click **Utility Services** > **Utility Admin**.
3. In the navigation pane on the left side of the page, click **Miscellaneous** > **Utility Services Backup and Restore**.
4. Click **Create Backup**.

   The Utility Services creates the backup file.
5. Click **Download the newly created Utility Services Backup File**, and download the backup file.
6. Click **Continue**.

Result

Utility Services backup files are stored in `/tmp` folder.

Upgrading Utility Services 7.x to AVP Utilities Release 8.1.3 in bulk during Appliance Virtualization Platform upgrade

About this task

Use this procedure to upgrade Utility Services 7.x to AVP Utilities Release 8.1.3 in bulk when you are upgrading one or more Appliance Virtualization Platform to Release 8.1.3.

Before you begin

- Take a backup of Utility Services manually.
- Add a location.

  For more information, see “Adding a location” section in *Administering Avaya Aura® System Manager*.
- Select Location and add a host.

  For more information, see “Adding an Appliance Virtualization Platform or ESXi host” section in *Administering Avaya Aura® System Manager*.
- Download a copy of the `hostUSUpgradeInfo.xlsx` spreadsheet from Avaya PLDS website at https://plds.avaya.com/ or from Avaya Support website at https://support.avaya.com. Fill the required system details in the spreadsheet.

  Note:

  If you provide the incorrect data in the spreadsheet, the upgrade might fail.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **AVP Update/Upgrade Management**.

   If Utility Services is not deployed on Appliance Virtualization Platform Release 7.x or trust is not established with the Utility Services application, and you click **Upgrade/Update**, then the system displays the following message.

   ```
   [AVP - <AVP Name in SDM>] Required Utility Services (US) VM is
   absent or not registered with this SDM instance. If absent, deploy
   US. If not registered, refresh host and then select US VM, and
   click More Options > Reestablish Connection.
   ```
3. In **Select patch file**, provide the absolute path to the patch file of the host, and click **AVPU Configuration Import**.

   For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-8.1.0.0.0.xx.zip`.

4. In the Import Configuration Excel File dialog box, do the following:
   a. Click **Browse** and select the file from the local computer.
   b. To upload the spreadsheet, click **Open**.

      The system displays the file size and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.
   c. Click **Submit File**.
5. Click **Update Host** and accept the EULA.
6. 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 Platforms for Selected Location <location name> section, the system displays the update status in the **Current Action** column.

Upgrading Appliance Virtualization Platform from Release 7.x or 8.0.x to Release 8.1.3 using Solution Deployment Manager

About this task

Use the following procedure to upgrade Appliance Virtualization Platform from Release 7.x or 8.0.x to Release 8.1.3 by using the upgrade bundle from Solution Deployment Manager Client or System Manager Solution Deployment Manager.

Note:

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

Before you begin

1. Add a location.

   For information about adding a location, see *Administering Avaya Aura® System Manager*.
2. Select Location and add an Appliance Virtualization Platform host.

   For information about adding the Appliance Virtualization Platform host, see *Administering Avaya Aura® System Manager*.

To upgrade from Appliance Virtualization Platform Release 7.x or 8.0.x to Release 8.1.3, ensure that:

- Appliance Virtualization Platform 7.x is deployed on the server that is supported with Appliance Virtualization Platform 8.x.

- Utility Services 7.x is deployed on Appliance Virtualization Platform Release 7.x and trust is established with the application.
- AVP Utilities 8.x is deployed on Appliance Virtualization Platform Release 8.x and trust is established with the application.

Note:

- If you are upgrading Avaya Aura® Appliance Virtualization Platform from Release 7.x to 8.x, Solution Deployment Manager also upgrades Utility Services to AVP Utilities during the Avaya Aura® Appliance Virtualization Platform upgrade.
- If you are upgrading Avaya Aura® Appliance Virtualization Platform from Release 8.0.x to 8.1.x, you need to manually upgrade AVP Utilities after upgrading Avaya Aura® Appliance Virtualization Platform.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ().
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **AVP Update/Upgrade Management**.

   If Utility Services is not deployed on Appliance Virtualization Platform Release 7.x or trust is not established with the Utility Services application, and you click **Upgrade/Update**, then the system displays the following message.

   ```
   [AVP - <AVP Name in SDM>] Required Utility Services (US) VM is absent or not registered with this SDM instance. If absent, deploy US. If not registered, refresh host and then select US VM, and click More Options > Reestablish Connection.
   ```

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-8.1.x.0.0.xx.zip`.

   - For System Manager Solution Deployment Manager, the patch file must be in the System Manager `swlibrary` directory.

6. Note that, if you attempt to upgrade Appliance Virtualization Platform to Release 8.0 and later on S8300D, Dell™ PowerEdge™ R610, or HP ProLiant DL360 G7 server, the system displays the following message.

   ```
   [AVP - <IP_Address>] You are attempting to Update / Upgrade this
   AVP on host hardware that is not supported for this software
   version: Avaya Common Server R1 (HP DL360G7 or Dell R610) and the
   Avaya S8300D blade are deprecated for this release.
   Please refer to the Release Notes for this release for details of
   the supported host hardware.
   ```

7. **(Optional)** On the AVP Update/Upgrade - Enhanced Access Security Gateway (EASG) User Access window, read the following messages, and do one of the following:

   When you upgrade Appliance Virtualization Platform from Release 7.0.x to Release 7.1 and later, the system displays the AVP Update/Upgrade - Enhanced Access Security Gateway (EASG) User Access window.

   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**.

8. If Utility Services is deployed on Appliance Virtualization Platform Release 7.x, the system upgrades Appliance Virtualization Platform to Release 8.1, and then updates Utility Services to AVP Utilities.

   This step is applicable when you upgrade from Release 7.x to Release 8.1.x.

   The system displays the Utility Services Upgrade window.

9. On the Utility Services Upgrade window, do the following:

   This step is applicable when you upgrade from Release 7.x to Release 8.1.x.

   a. In Platform Details, the data store is auto-selected as server-local-disk, and then click **Next**.
   b. In **OVA**, provide the AVP Utilities OVA file details, and then click **Next**.

      For AVP Utilities OVA, the system automatically performs the resource check and disables the **Flexi Footprint** field.
   c. In Config Parameters, provide the network and configuration parameters details, and click **Update**.

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

    This step is applicable when you upgrade from Release 7.x to Release 8.1.x.

    a. To accept the EULA, click **Accept**.
    b. To decline the EULA, click **Decline**.

    Once Appliance Virtualization Platform is upgraded, the system updates Utility Services to AVP Utilities.

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

Next steps

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

Upgrading AVP Utilities from Release 8.0.x to Release 8.1.x

Before you begin

- Ensure that the Appliance Virtualization Platform and System Manager are running on the release 8.1.x.
- Ensure that the Appliance Virtualization Platform host is added on the System Manager Solution Deployment Manager.
- Ensure the AVP Utilities is re-established on the System Manager Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Upgrade Management**.
2. Select the AVP Utilities 8.0.x for upgrade.
3. Select the element(s) that you want to upgrade and perform the following steps:
   a. Click **Pre-upgrade Actions** > **Refresh Element(s)** and click **Schedule**.
   b. Click **Pre-upgrade Actions** > **Analyze** and click **Schedule**.
   c. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   d. On the Pre-upgrade Configuration page, enter the details as required:

      For same server, provide the mandatory parameters along with the same target host information. Following are the mandatory parameters:

      - **Target platform**: Select the platform on which AVP Utilities is hosted.
      - **Data store**: Select the existing host's data store.
      - **New Target platform**: N/A
      - **Data store**: N/A
      - **Upgrade Source**: Select the upgrade source.
      - **Upgrade/update to**: Select the target AVP Utilities release OVA.
      - **Flexi Footprint**: Select the appropriate footprint.

      For new target server, provide the mandatory parameters along with new target host information. Following are the mandatory parameters:

      - **Target platform**: Select the platform on which AVP Utilities is hosted.
      - **Data store**: Select the existing host's data store.
      - **New Target platform**: Select the target platform on which AVP Utilities should be hosted.
      - **Data store**: Select the target host's data store.
      - **Upgrade Source**: Select the upgrade source.
      - **Upgrade/update to**: Select the target AVP Utilities release OVA.
      - **Flexi Footprint**: Select the appropriate footprint.

      For information about parameters, see Preupgrade Configuration field descriptions on page 44.
   e. Click the **Schedule**.
4. Select the element(s) to upgrade and click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit** to upgrade.

6. On the Edit Upgrade Configuration page, do one of the following:
   - For same server, provide the mandatory parameters along with same target host information, latest patch file, and credentials.
   - For different server, provide the mandatory parameters along with different target host information, latest patch file, and credentials.

   Note:

   In the **Migrate With AVP Install** field, leave the box unchecked because for AVP Utilities, this migration is not applicable.

   For information about parameters, see Edit Upgrade Configuration field descriptions on page 45.

   Complete the details, and click **Save**.
7. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

   If the field displays , review the information on the Edit Upgrade Configuration page.
8. On the Upgrade configuration page, click **Upgrade**.
9. Click **Schedule**.

   You can schedule the job now or for a later time.
10. On the Upgrade Management page, click .

    After successful upgrade, the **Last Action** column displays **Upgrade**, and **Last Action Status** column displays .

    The **Last Action** field displays **COMMIT_ROLLBACK_PENDING** if **Auto Commit** is not selected.
11. To Commit or rollback, do the following:
    a. On the Upgrade Management page, select the element.
    b. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.
    c. Select the action to be performed under the **Upgrade Action** column.
    d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.
    e. Click **Schedule**.

    Note:

    When you commit the changes, the AVP Utilities deletes the old virtual machine.

    When you rollback, the AVP Utilities deletes the newly created virtual machine and starts the old virtual machine.

12. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.

    Check that the AVP Utilities upgrade is successful.

Related links

Pre-upgrade Configuration field descriptions on page 44
Edit Upgrade Configuration field descriptions on page 45

Pre-upgrade Configuration field descriptions

Pre-upgrade Configuration Parameters

Name	Description
Element name	The name of the application that you want to upgrade.
Parent name	The parent of the application that you want to upgrade.
IP Address	The IP address of the application that you want to upgrade.
Current Version	The current version of the application that you want to upgrade.
Target Platform	The Appliance Virtualization Platform or ESXi host of the virtual machine.
Data Store	The data store. When you set the **Target Host** as **Same Box**, the system enables the **Data Store** field.
New Target Platform	The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine. For upgrades on a different server, add Appliance Virtualization Platform or ESXi host from Application Management.
Upgrade Source	The location where OVA or the software patches are available in the local storage or remote server.
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.

Table continues…

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

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

Related links

Upgrading AVP Utilities from Release 8.0.x to Release 8.1.x on page 41

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- **Element Configuration**
- **AVP Configuration**

Element Configuration: General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/ Platform	The new target host on which you want to run the device.

Table continues…

Name	Description
Migrate With AVP Install	The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.
Service/Feature Pack for auto-install after upgrade/ migration	The service pack or feature pack that you want to install.

Element Configuration: Upgrade Configuration Details

The page displays the following fields when you upgrade application and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

Name	Description
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.
Hostname	The hostname of virtual machine.
Public IP Address	The IPv4 address of Virtual Machine for Public Network.
Public Netmask	The IPv4 network mask of Virtual Machine for Public Network.
Public Default Gateway	The IPv4 address of the Virtual Machine gateway.
Public IPv6 Address	he IPv6 address of Virtual Machine for Public Network.
Public IPv6 Prefix	The IPv6 prefix of Virtual Machine for Public Network.
Default IPv6 Gateway	The IPv6 address of the Virtual Machine gateway.
Out of Band Management IP Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnet mask of the virtual machine for out of band management.

Table continues…

Name	Description
Out of Band Management IPv6 Address	The IPv6 address of the Virtual Machine for Out of Band Management.
Out of Band Management IPv6 Prefix	The IPv6 network prefix of the Virtual Machine for Out of Band Management.
Network Time Protocol IP	The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,).
Timezone Setting	The timezone of the virtual machine.
DNS	The DNS IP address of the virtual machine.
Primary System Manager IP address for application registration	The IP address of System Manager.
Enrollment Password	The enrollment password of System Manager.
AVP Utilities Mode	The mode of AVP Utilities deployment. You can select the following options: • standard_mode • hardened_mode • hadened_mode_dod
Admin User Password	The password of admin user for AVP Utilities SSH login.
Out of Band Management Mode	The out of band management mode of AVP Utilities. You can enable or disable Out of Band Management mode by selecting following options: • OOBM_Disabled • OOBM_Enabled
EASG User Access	Enables or disables EASG. The options are: • `1` to enable EASG (Recommended). By enabling Avaya Logins, you are granting Avaya access to your system. This option is necessary to maximize the performance and value of your Avaya support entitlements, enabling 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. See Avaya support site(http://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. • `2` to disable EASG. 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 can manage the product, Avaya Logins should not be disabled.

Table continues…

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: `1` to enable the data encryption. `2` to disable the data encryption.
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.
Enable Customer Root Account for this Application	The option to enable root account of Virtual Machine. To enable, select the check box and click **Accept** when the EULA displays. To disable, clear the check box.
Customer Root Account Password	This field is applicable when customer root account is enabled. The customer root account password.
Re-enter Customer Root Account Password	The customer root account password.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Services	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.

Table continues…

Name	Description
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: End User License Agreement

Name	Description
I Agree to the above end user license agreement	The end user license agreement. You must select the check box to accept the license agreement.

AVP Configuration: Existing Machine Details

Name	Description
Source IP	The source IP address.
Source Administrative User	The source user name with appropriate admin privileges.
Source Administrative Password	The source password of the administrator.
Source Root User	The source user name with appropriate root privileges.
Source Root Password	The source password of the root.

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. **Note:** IPv6 is only supported in a dual stack configuration.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.

Table continues…

Name	Description
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.

Table continues…

Name	Description
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Enhanced Access Security Gateway (EASG)	**Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. **Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled. Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
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
Save	Saves the changes that you made to the Edit Upgrade Configuration page.
Cancel	Cancels the changes that you made to the Edit Upgrade Configuration page.

Related links

Upgrading AVP Utilities from Release 8.0.x to Release 8.1.x on page 41

Chapter 7: Troubleshooting

Checklist to rollback to previous version of Utility Services

After Appliance Virtualization Platform is upgraded and AVP Utilities is successfully deployed, the Utility Services virtual machine is automatically removed and the AVP Utilities virtual machine is available. If you want to rollback to the previous version of Utility Services, then you must first rollback Appliance Virtualization Platform and restore Utility Services.

No.	Task	Link	✔
1	Delete AVP Utilities	See Deleting an application on page 52	
2	Rollback Appliance Virtualization Platform to previous version	See Removing the Appliance Virtualization Platform patch from the ESXi host CLI on page 53	
5	Restore Utility Services	See Restoring the AVP Utilities backup on page 59	

Deleting an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, select one or more application.
4. On the Delete page, click **Delete**, and click **Yes** to confirm the deletion.

   The system turns off the applications, and deletes the selected applications from the platform.

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

- Create a backup of each Avaya Aura® application that is deployed on Appliance Virtualization Platform by using the application's native backup procedures.

  If a problem occurs with the Appliance Virtualization Platform rollback, you can use the application backups to reinstall the applications and to restore its data.
- Start an SSH session.
- Log in to the Appliance Virtualization Platform host command line with admin user credentials.
- Copy the Appliance Virtualization Platform 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 8.1 and later 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.

      For example, to rollback from Appliance Virtualization Platform Release 8.1 to Release 7.0.0.x (`avaya-avp-8.1.0.0.0.x.zip`), type the following command:

      ```
      /opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.0.0.1.0.x.zip
      ```

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

      The system must be rebooted.

3. To rollback from Appliance Virtualization Platform Release 7.1.3 and later 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.

      For example, to rollback from Appliance Virtualization Platform Release 7.1.3 to Release 7.0.0.x (`avaya-avp-7.0.0.1.0.x.zip`), type the following command:

      ```
      /opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.0.0.1.0.x.zip
      ```

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

      The system must be rebooted.

4. 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.x.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`.

      The system must be rebooted.

      When the system is rebooted, start a new Appliance Virtualization Platform SSH session.

   c. To re-enable SSH by using the Solution Deployment Manager client, on Application 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 7.1.2 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-7.0.0.1.0.x.zip>` command.

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

b. Run the following by typing line-by-line or using cut and paste on the Appliance Virtualization Platform CLI.

```
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
```

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

The system must be rebooted.

When the system is rebooted, start a new Appliance Virtualization Platform SSH session.

d. To re-enable SSH by using the Solution Deployment Manager client, on Application 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
```

6. 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 by using the **`cat /opt/avaya/etc/avaya-avp.version`** command.

Restoring a backup of Utility Services

Procedure

1. Use an account with administrator-level privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) webpage.
2. Click **Utility Services** > **Utility Admin**.
3. In the navigation pane on the left side of the page, click **Miscellaneous** > **Utility Services Backup and Restore**.
4. Click **Browse** and select the backup file that you want to restore from the local machine.
5. Click **Upload Backup**.

The system restores the backup file.

6. Click **Continue**.

Rolling back to Utility Services

About this task

Use this procedure to rollback Utility Services to 7.x if the upgrade from Utility Services to AVP Utilities fails from Release 7.x to Release 8.1 and later.

Before you begin

- Add a location.
- Select Location and add a host.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions** > **Rollback/Retry**.

   If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions** > **Rollback/Retry** after selecting the Utility Services application.
3. In the Import Configuration Excel File dialog box, click **Rollback**.

   To upgrade Utility Services to AVP Utilities, use the Upgrade Management page of System Manager Solution Deployment Manager.

   The system displays the confirmation message to accept the rollback.

Retrying Utility Services to AVP Utilities upgrade

About this task

If the upgrade from Utility Services to AVP Utilities fails, use this procedure to retry the upgrade of Utility Services to AVP Utilities.

Before you begin

- Add a location.
- Select Location and add a host.
- Download a copy of the `hostUSUpgradeInfo.xlsx` spreadsheet from Avaya PLDS website at https://plds.avaya.com/or from Avaya Support website at https://support.avaya.com. Fill the required system details in the spreadsheet.

Note:

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions** > **Rollback/Retry**.

   If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions** > **Rollback/Retry** after selecting the Utility Services application.
3. On the Import Configuration Excel File dialog box, do the following:
   a. Click **Browse** and select the file from the local computer.
   b. To upload the spreadsheet, click **Open**.

      The system displays the file size and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.
   c. Click **Submit File**.

      Once the file is successfully uploaded, the system enables the **Retry** button.
   d. Click **Retry**.

      The system starts the upgrade of Utility Services to AVP Utilities.

Creating a backup of AVP Utilities

Before you begin

Ensure that the system runs release 8.1.3 of AVP Utilities. As part of the upgrade to this release, the `initTM` script sets up the required trust management infrastructure to restore previously installed certificates including third party certificates, before the backup.

About this task

Create a backup for the current release of AVP Utilities. The system creates the backup file in the `/tmp` folder, which includes the following configuration files:

- SSH
- AIDE: `/etc/aide.conf`
- Audit: `/etc/audit/auditd.conf`
- Login defs: `/etc/login.defs`
- Password auth: `/etc/pam.d/password-auth`
- Password settings: `/etc/security/pwquality.conf`

- User passwords and group membership:
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/group`
  - `/etc/gshadow`
- rsyslog: `/etc/rsyslog.conf`
  - `/etc/pki/certrev`
  - `/etc/pki/tls/ca_ldap.pem`
  - `/etc/pki/tls/certs`
- selinux: `/etc/selinux/config`
- Access Control List (ACL):
  - `/etc/hosts.allow`
  - `/etc/hosts.deny`
- Banner: `/etc/issue`
- Spirit agent: `/etc/spirits/security`

Note:

Backup or restore is only applicable for same machine. Backup or restore does not work on different machines.

Procedure

1. Log on to the AVP Utilities CLI as an administrator.
2. Create a backup. Run the following script:

   `/opt/avaya/common_services/backup -b <file name>`

   Note:

   When creating the backup, the system sometimes displays the following errors:

   `/bin/tar:<file name>: Cannot start: No such file or directory.`

   `/bin/tar: Exiting with failure status due to previous errors.`

   Check if the backup file already exists in the `/tmp` folder. If not, run the script again.
3. **(Optional)** Create a secured backup.

   The secured backup file has a `.gpg` extension. For example, if the original backup file has the `backup.tar.gz` file name, the encrypted file has the `backup.tar.gz.gpg` file name.

   a. Run the following script:

      `/opt/avaya/common_services/backup -s -b`

The argument: `-s` creates the secured backup.

b. Enter a password of your choice when prompted.

Important:

Ensure that you remember this password because you need it when you restore the backup.

Restoring the AVP Utilities backup

Before you begin

Ensure that the system runs release 8.1.3 of AVP Utilities. As part of the upgrade to this release, the `initTM` script sets up the required trust management infrastructure to restore all previously installed certificates, including third party certificates.

About this task

Restore the backup for the current release of AVP Utilities.

Note:

Backup or restore is only applicable for same machine. Backup or restore does not work on different machines.

Procedure

1. Log on to the AVP Utilities CLI as an administrator.
2. Restore the backup:
   a. Ensure that the backup files are in the `/tmp` directory.
   b. Run the following script:

      `/opt/avaya/common_services/backup -r <backup file name>`

      Note:

      When you restore the backup, the system sometimes displays the following error:

      ```
      /bin/tar: <backup file name>: Not found in archive.
      /bin/tar: Exiting with failure status due to previous errors.
      ```

      Check if the backup file already exists in the `/tmp` folder. If not, run the script again.
3. **(Optional)** Restore a secured backup:
   a. Ensure that the backup file is in the `/tmp` directory.
   b. Run the following script:

```
/opt/avaya/common_services -s -r <backup file name>
```

c. When prompted, enter the password used to create the backup file.

Uninstalling the feature pack or service pack by using Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select AVP Utilities, and click **Upgrade Actions** > **Installed Patches**.
4. In the **Patch Operation**, select **Uninstall**.
5. Select the patch that you want to uninstall.
6. Set the **Schedule Job** options as required, and click **Schedule**.

Chapter 8: Resources

AVP Utilities documentation

The following table lists the documents related to Avaya Aura® AVP Utilities. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Avaya Aura® AVP Utilities Overview and Specifications	Provides an overview of the Avaya Aura® AVP Utilities features.	Sales Engineers
Deploying Avaya Aura® AVP Utilities	Describes the instructions for deploying and migrating to Avaya Aura® AVP Utilities.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administering Avaya Aura® AVP Utilities	Describes the instructions for administering Avaya Aura® AVP Utilities.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Appliance Virtualization Platform and AVP Utilities Data Privacy Guidelines	Describes how to administer Avaya Aura® AVP Utilities to fulfill Data Privacy requirements.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.

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 only displays the documents for the selected category.

7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.

- Add content to your collection by using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

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

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

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

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

Note:

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

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
20980W	What's New with Avaya Aura® Release 8.1

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

Appendix A: Deploying AVP Utilities and other virtual machines

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

Before you begin

Install the Solution Deployment Manager client on your computer.

Procedure

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

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

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

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

   If Out of Band Management is enabled, provide information in the Out of Band Management-related fields. If Out of Band Management is disabled, leave the fields blank.
8. Deploy AVP Utilities, and wait for the virtual machine to deploy successfully.
9. Install the AVP Utilities 8.1.3 feature pack.

Note:

The following applies *only* when you install a service or feature pack using the AVP Utilities CLI.

Before you install a service or feature pack, ensure that you install the pre-upgrade patch. Verify the pre-upgrade patch installation using the CLI command **`swversion`**. Service and feature packs are cumulative and include all the security remediation and bug fixes from previous service or feature packs.

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

Related links

Enabling IP forwarding using Services Port VM for AVP Utilities

Deploying AVP Utilities and virtual machines using services port

Before you begin

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

Procedure

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

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

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

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

7. Enter the IP address details for AVP Utilities, deploy AVP Utilities, and wait for the virtual machine to deploy successfully.
8. Install the AVP Utilities 8.1.3 feature pack.

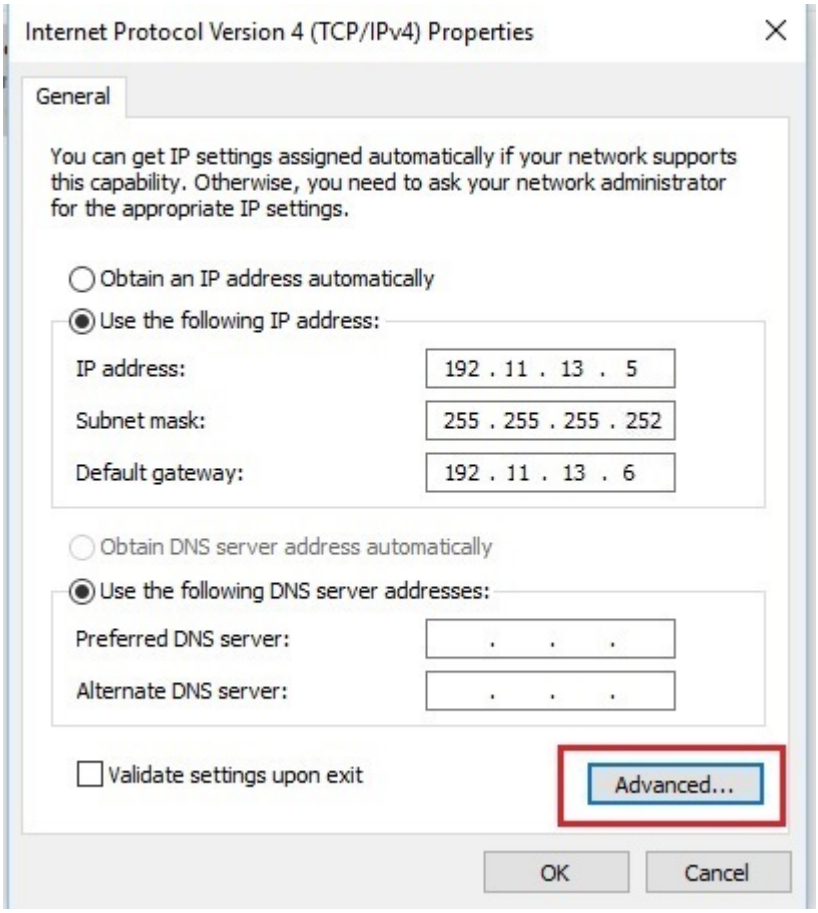
   Note:

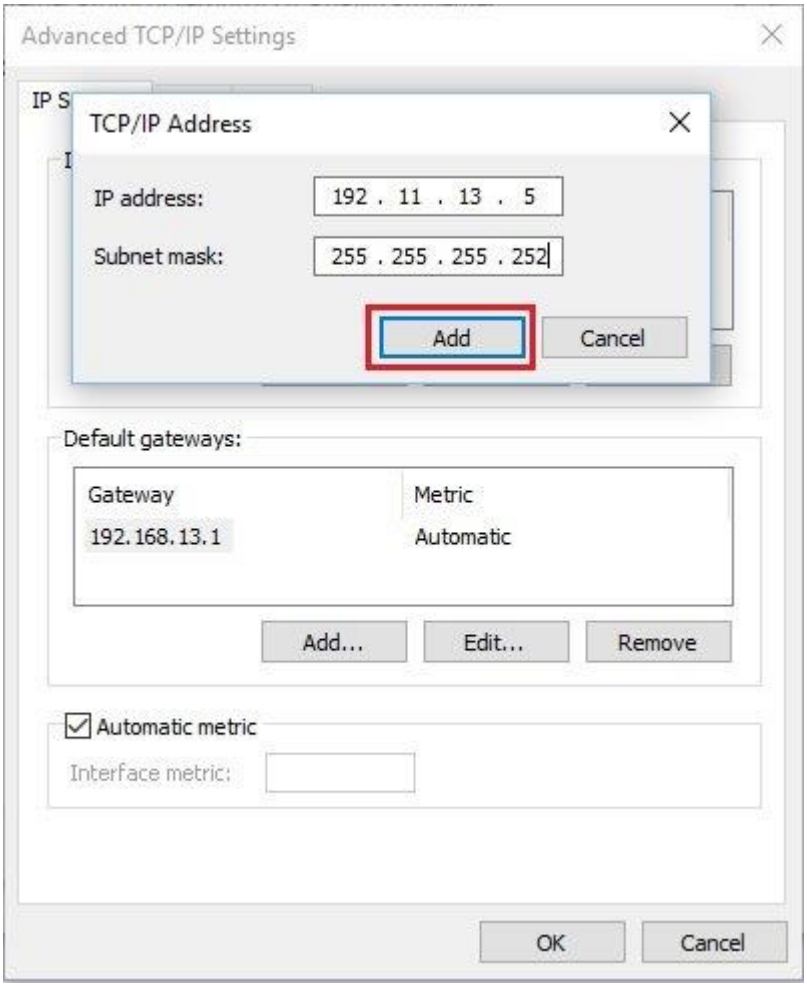
   The following applies *only* when you install a service or feature pack using the AVP Utilities CLI.

   Before you install a service or feature pack, ensure that you install the pre-upgrade patch. Verify the pre-upgrade patch installation using the CLI command **`swversion`**. Service and feature packs are cumulative and include all the security remediation and bug fixes from previous service or feature packs.
9. Change the AVP Utilities configuration parameters to the following:
   - **IP address**: 192.11.13.5
   - **Netmask**: 255.255.255.252
   - **Gateway**: 192.11.13.6

   On the Solution Deployment Manager client, in the Appliance Virtualization Platform host, leave the IP address as 192.168.13.6.

10. **(Optional)** If you want to deploy or access virtual machine using services port while Wi-Fi or other network connection is enabled, then go to **Network & Internet settings** of your computer and enter the values as shown below.





11. Ensure that the IP forwarding feature is enabled on AVP Utilities.
12. Deploy all other virtual machines in the solution one after the other.
13. **(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.
14. Install the feature pack for Avaya Aura® applications.
15. Validate the system.

Related links

[Enabling IP forwarding using Services Port VM for AVP Utilities]

Index

M

N

O

P

R

S

T

U

V

W