Using the Solution Deployment Manager client

Release 10.2.x
Issue 1
December 2023

© 2015-2023, Avaya LLC
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 media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

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

Warranty

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

“**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.

Copyright

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

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

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

Service Provider

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Solution Deployment Manager client overview

Solution Deployment Manager Client

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

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

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade VMware-based System Manager from Release 8.1.x or 10.1.x to Release 10.2 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
- Generate the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

Note:

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest Solution Deployment Manager client for deployment.

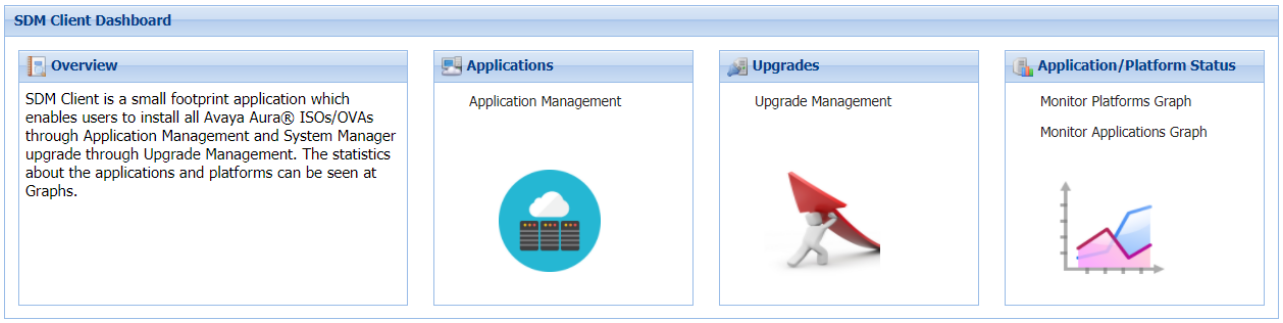


Figure 1: Solution Deployment Manager Client dashboard

Solution Deployment Manager client capabilities

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

- Runs on the following operating systems:
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
  - Windows 11, 64-bit Professional or Enterprise
  - Windows Server 2016, 64-bit Professional or Enterprise
  - Windows Server 2019, 64-bit Professional or Enterprise
  - Windows Server 2022, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deployment of System Manager. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports the Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of Avaya Aura® applications.
- Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

Note:

For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.

  Note:

  - System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.

    All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

  - Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2 or higher. Solution Deployment Manager Client cannot be on Release 10.1.

- Configures application and networking parameters required for application deployments.
- Supports selecting the application OVA file from a local path or an HTTPS URL. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  Note:

  To install the patch on System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 10.2, you must use Solution Deployment Manager Client Release 10.2 or higher.

  However, to install the patch on System Manager Release 10.2, Solution Deployment Manager Client must be on Release 10.2.

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

  For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.

- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.
- Creates the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Supports the Pre-staging feature to prestage the System Manager OVA, service pack or feature pack, or data migration utility files to deploy, upgrade, or update the System Manager application.

Supported Avaya Aura® Release 10.2.x applications

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

- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- Avaya WebLM
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Session Border Controller Release 8.0 and later
- Avaya Breeze® platform Release 3.3 and later
- Avaya Aura® Media Server

Chapter 2: Installing the Solution Deployment Manager client

Installing the Solution Deployment Manager client

Prerequisites for installing the Solution Deployment Manager client

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel** > **Programs** > **Programs and Features**.

   For information about uninstalling the Solution Deployment Manager client, see "Uninstalling the Solution Deployment Manager client".

2. Ensure that Windows 8.1 64-bit, Windows 10 64-bit, Windows 11 64-bit, Windows Server 2016 64-bit, Windows Server 2019 64-bit, or Windows Server 2022 64-bit operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

3. Ensure that at least 5 GB of disk space is available to install the client. To deploy applications, you must have additional 15 GB of disk space on your system.

   Tip:

   Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space.

4. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client and use the Solution Deployment Manager functionality.

Note:

System Manager 10.2.x Port Matrix lists all the ports and protocols that System Manager uses. You can access the System Manager 10.2.x Port Matrix document on the Avaya Support website at https://support.avaya.com/ by using valid credentials.

6. Ensure that ports support Avaya Aura® 10.2.x supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

Tip:

On **Computer**, right-click properties, and perform the following:

a. In the left navigation pane, click **Advanced system settings**.
b. On the System Properties dialog box, click the **Advanced** tab, and click **Environment Variables**.
c. Verify the system variables.

9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

Installing the Solution Deployment Manager client on your computer

About this task

When the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches of only System Manager and hypervisor patches of Appliance Virtualization Platform.

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

Solution Deployment Manager must be used to deploy or upgrade Avaya Aura® applications on Avaya Aura® Appliance Virtualization Platform.

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at https://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Product Support** > **Downloads**, and type the product name as **System Manager**, and Release as **10.2.x**.
3. Click the **Avaya Aura® System Manager Release 10.2.x SDM Client Downloads,10.2.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.

4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

     If the `C:\Program Files\Avaya\AvayaSDMClient` directory is not empty, the installer displays the following message: `To install the SDM client, select an empty directory or manually delete the files from the installation directory.`

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

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

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

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

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

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

      The default application port is 443. If this port is already in use by any of your application on your system, then the system does not enable you to continue the

installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

Note:

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

e. **(Optional)** Click **Reset All to Default** to reset all values to default.

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

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the user must make the required disk space, memory, and the ports available to start the installation process again.

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

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

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

Next steps

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

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

Related links

Uninstalling the Solution Deployment Manager client manually on page 142

Solution Deployment Manager Client logs

The default location of the Solution Deployment Manager client logs is `C:\Program Files\Avaya\AvayaSDMClient\apache-tomcat-8.0.18\logs`. If you change the Solution Deployment Manager client installation directory at the time of deployment, the logs will be at `<Path of the SDM Client Installation directory>\apache-tomcat-8.0.18\logs`.

If you face any issues, zip and copy the `logs` folder to remote server and share the file with Avaya Support Team.

Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform

You can connect the Solution Deployment Manager client to the Appliance Virtualization Platform server through:

- The customer network: When connected through the customer network, the Solution Deployment Manager client can support multiple locations and hosts with unique IP address per host.

  You must have an IP address on the customer network after the installing the Solution Deployment Manager client.

- The services port on the Appliance Virtualization Platform server: To enable the Solution Deployment Manager client to communicate with the services port of Appliance Virtualization Platform, technician computer must be set to:

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

  When connecting through the services port, the Solution Deployment Manager client supports one location and one Appliance Virtualization Platform host. The host IP address is 192.168.13.6 when using the client through the services port.

  When using the Solution Deployment Manager client through the services port, after you complete deploying OVAs on a host, remove the host from the Solution Deployment Manager client.

Accessing the Solution Deployment Manager client dashboard

About this task

Note:

If you perform deploy, upgrade, and update operations from the Solution Deployment Manager client, ignore the steps that instruct you to access System Manager Solution Deployment Manager and the related navigation links.

Procedure

To start the Solution Deployment Manager client, do one of the following:

- On your computer, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client**.
- On your desktop, click  .

Checklist for Appliance Virtualization Platform initial installation using the Solution Deployment Manager client

No.	Task	Link/Notes	✔
1	Download the Solution Deployment Manager client and install the client on your computer. Get the Appliance Virtualization Platform 8.0 on a DVD, generate the kickstart (`avp81ks.cfg`) file from the Solution Deployment Manager client, and save the `avp81ks.cfg` file in a USB stick.	-	
2	Install the Appliance Virtualization Platform 8.0 software on the server. • Determine if Appliance Virtualization Platform is preinstalled. • If not already installed, install the Appliance Virtualization Platform 8.0 software.		
3	Ensure that the computer is connected to the services port of the Appliance Virtualization Platform host.	On your computer, set the following network parameters: • IP address: 192.168.13.5 • Subnetmask: 255.255.255.248 • Default Gateway: 192.168.13.1	
4	Using the SSH client, log in to the Appliance Virtualization Platform server with 192.168.13.6 as admin. • For Appliance Virtualization Platform preinstalled on the common server, change the default password. • Accept the end user license agreement. • Enable EASG. • If preinstalled, using the Solution Deployment Manager client, change Appliance Virtualization Platform IP address through CLI to the customer-provided IP address.	You must add the host only after accepting the EULA.	

Table continues…

No.	Task	Link/Notes	✔
5	Start the Solution Deployment Manager client that is connected to services port, and click Application Management. 1. Add a location. 2. Add the Appliance Virtualization Platform host. If you connect the Solution Deployment Manager client to the host through: • The services port, the IP address of the host is 192.168.13.6 • The customer network, the host will be the IP address assigned through the `avp81ks.cfg` file. 3. Do one of the following: • Install the available Appliance Virtualization Platform patch or service pack. For more information, see “Upgrading the Appliance Virtualization Platform patch from the Solution Deployment Manager client”. • If available in 8.0, using the Solution Deployment Manager client, change IP address for preinstalled Appliance Virtualization Platform server. 4. Add a new virtual machine for AVP Utilities as required per host. 5. Close the Solution Deployment Manager client.	-	

Table continues…

No.	Task	Link/Notes	✔
6	• On your computer, set the following network parameters: - IP address: 192.11.13.5 - Subnetmask: 255.255.255.252 - Default gateway: 192.11.13.6 • Using the SSH client, login to AVP Utilities with 192.11.13.6. • On AVP Utilities, run **`swversion`**, **`ifconfig`**, and **`cat /etc/hosts`** commands. • If you have an AVP Utilities service pack, copy it to the `/tmp` folder, and install the service pack in the AVP Utilities command line interface. • Run the **`IP_Forward enable`** command (By default, IP Forwarding is disabled).		
7	Start Solution Deployment Manager Client with IP address 192.11.13.5/30 to install other virtual machines on the Appliance Virtualization Platform host.	-	

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Supported servers

The following servers are supported for deployments and upgrades to Release 10.2.x and later:

- Avaya Solutions Platform S8300 for Communication Manager and Branch Session Manager

- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640

For fresh installations, use Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

Supported servers for Avaya Aura® applications

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

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.1
Avaya Solutions Platform S8300 Release 5.1 [4]	N	N	N	Y	Y

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 5.1. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 5.1.x.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

[4] Avaya Solutions Platform 130 Appliance uses VMware vSphere ESXi Standard License to support virtualization.

[5] Avaya Solutions Platform S8300 supports virtualization using VMware vSphere ESXi Foundation License for Communication Manager and Branch Session Manager.

Note:

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. Avaya Solutions Platform future release (Release 6.x) will support ESXi 8.0. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. Updating directly from Dell or VMware's website results in an unsupported configuration.
- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.1.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

Supported ESXi version

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

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

Note:

- Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2.

  Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-801-release-notes/index.html.

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

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. Avaya Solutions Platform future release (Release 6.x) will support ESXi 8.0. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. Updating directly from Dell or VMware's website results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- Presence Services is deployed on the Avaya Breeze® platform, which supports VMware 7.0 and 8.0.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

Latest software updates and patch information

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

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

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

Chapter 3: Solution Deployment Manager Client Software library

Software library on your computer

Solution Deployment Manager Client software library is configured at the time of deploying the Solution Deployment Manager client. The default path of the Solution Deployment Manager client software library is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts` on your computer. Use the `Default_Artifacts` directory to save the OVA and patch files. The files that you store in the `Default_Artifacts` directory, can be viewed in the **SW Library** field on Solution Deployment Manager while deploying or upgrading an application.

You can copy the following files to the `Default_Artifacts` directory created during the Solution Deployment Manager client installation:

- Avaya Aura® application OVA files
- System Manager service packs or feature pack

When you deploy an Avaya Aura® application OVA file, you have the options to provide the full path, or browse to your software library, or upload the OVA file. When you install an Appliance Virtualization Platform or System Manager service pack, you must provide the full path to this directory. For example, `C:/Aura/avaya-avap-8.0.x.y.y.y.zip`.

Chapter 4: Virtual machine management

Application management

The Application Management link from Solution Deployment Manager provides the application management capabilities that you can use to do the following.

- Defines the physical location of the **OS**, Appliance Virtualization Platform, Avaya Solutions Platform 130, or the ESXi platforms.
- Supports password change and patch installation of the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform Release 8.x or earlier and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

  Note:

  For the Avaya Aura® Messaging element, trust re-establishment is not required.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

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

Related links

Application Management field descriptions on page 25

Application Management field descriptions

Locations

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

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

Platforms

Name	Description
Platform Name	The name of the platform.
Platform IP	The IP address of the platform.
Platform FQDN	The FQDN of the platform.
IPv6	The IPv6 address of the platform. If the IP address of the ESXi platform only supports IPv4, the column does not display any value.
vCenter FQDN	The FQDN of vCenter.
Current Action	The operation that is currently being performed on the platform.
Last Action	The last operation completed on the platform.
License Status	The status of the license.
Platform Version	The platform version.
Offer Type	The platform type. The options are: • **ASP**: An Avaya Solutions Platform 130 Release 5.1 platform. • **Customer VE**: A customer-provided VMware ESXi platform • **SWONLY**: A customer-provided operating system platform • **AVP**: An Appliance Virtualization Platform platform
SSH Status	The SSH service status. The values are enabled and disabled.

Table continues…

Name	Description
Platform Certificate Status	The certificate status of Appliance Virtualization Platform, Avaya Solutions Platform 130, or standalone ESXi. If the ESXi is managed by vCenter, the system displays the value of this field as NA. The options are: • ✔: The certificate is added in Solution Deployment Manager and is correct. • ⛔: The certificate is not accepted or is invalid. You can click **View** for details of the certificate status.
vCenter Certificate Status	The certificate status of the ESXi host. The options are: • ✔: The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • ⛔: The certificate is not accepted or is invalid. You can click **View** for details of the certificate status.

Note:

Depending on the Appliance Virtualization Platform, Avaya Solutions Platform 130, standalone ESXi, and vCenter certificate status, the system enables the options in **More Actions**.

Button	Description
Auto Refresh	Automatically refreshes the page with the latest changes. For example, the page updates: • The Application state when an application changes. • The license status or certificate status of the platform when the platform changes. The system refreshes the data every minute.
Add	Displays the **Add Platform** section where you can provide the details of the platform that you want to add.
Edit	Displays the Platform Information section where you can change the details of an existing platform.
Remove	Removes the platforms that you select only from the Solution Deployment Manager client. The system moves the platforms associated with the deleted locations to an unknown location.
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.

Table continues…

Button	Description
Refresh Host	Refreshes one or more of the platforms. Solution Deployment Manager displays the following status in the **Current Action** column. • **Refresh Completed**: When the refresh platform action completes. • **Refresh Failed**: When the refresh platform action fails if Solution Deployment Manager is unable to communicate with the platform. • **Refresh Queued**: When the refresh platform action takes time.
More Actions > **AVP Update/ Upgrade Management**	Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **SSH** > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > **SSH** > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the application host. Syslog is only for Appliance Virtualization Platform. You can select multiple platforms and Push syslog configuration on selected platforms.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view syslog profiles of selected Appliance Virtualization Platform platforms.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
More Actions > **Lifecycle Actions** > **Host Restart**	Restarts the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > **Lifecycle Actions** > **Host Shutdown**	Shuts down the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > **Generate/ Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the platform. Depending on the platform type, the options are: • **Generate Certificate**: To generate a certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. • **Accept Certificate**: To accept a valid certificate for the platform or vCenter. • **Decline Certificate**: To decline the certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. You must regenerate the certificate and accept if you decline a platform certificate.

Table continues…

Button	Description
More Actions > **AVP Cert. Management** > **Manage Certificate**	Displays the Load Certificate dialog box from where you can view/ generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected platform.
More Actions > **AVP Cert. Management** > **Generic CSR**	Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.
More Actions > **Snapshot Manager**	Displays the Snapshot Manager dialog box from where you can view and delete the application snapshot.
More Actions > **WebLM Configuration**	Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.
More Actions > **AVP Firewall Rules**	Displays the Firewall Settings dialog box from where you can view the firewall rules details for an Appliance Virtualization Platform host.
More Actions > **Set Login Banner**	Displays the Message of the Day dialog box from where you can push the login banner text to the selected platform. **Note:** This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support **Set Login Banner**.

Applications

Name	Description
Application Name	The name of the application.
Application IP	The IP address of the application.
Application FQDN	The FQDN of the application.
Application IPv6	The IPv6 address of the application, if any.
App Name	The name of the application. For example, Session Manager.
App Version	The version of the application. For example, 8.1.
Application State	The state of the application. The states are: • **Started** • **Stopped**
Current Action Status	The status of the current operation. The options are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the application.

Table continues…

Name	Description
Platform Name	The platform name of the operating system, VMware host, or Appliance Virtualization Platform host on which the application resides.
Platform Type	The platform type of the operating system.
Trust Status	The status of the connection between System Manager and the application. The options are: • **Success** • **Failed** When the connection between System Manager and the application is established, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store name.

Button	Description
New	Displays the Application Deployment section where you can provide the platform and deploy an application.
Edit	Displays the Application Deployment section where you can change the details of an application.
Delete	Turns off the applications and deletes the selected application from platform and Solution Deployment Manager Client.
Start	Starts the selected applications.
Stop	Stops the selected applications.
Show Selected	Displays only the selected applications.
VM Console > **Open VM Console in New Window**	Opens the application VM console in the new browser window.
VM Console > **Open VM Console in New Tab**	Opens the application VM console in the new tab of the browser.
More Actions > **Restart**	Starts the selected applications that were stopped earlier.
More Actions > **Refresh App**	Updates the status of the applications.
More Actions > **Update VM**	Displays the System Manager VM section where you can install the software patches and service packs for System Manager application.
More Actions > **Installed Patches**	Refreshes and displays the latest information of the software patch.
More Actions > **Re-establish connection**	Establishes the connection between System Manager and the application. The **Trust Status** then changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of AVP Utilities for static routing.

Table continues…

Button	Description
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected application.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.

Related links

Application management on page 24

Managing the location

Viewing a location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. Click the Locations tab.

   The Locations section lists all locations.

Adding a location

About this task

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
4. Click **Save**.

   System Manager displays the new location in the **Application Management Tree** section.

Related links

New and Edit location field descriptions on page 31

Editing the location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 31

Deleting a location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. In the Delete confirmation dialog box, click **Yes**.

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

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

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

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

Chapter 5: Managing the platform

Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

About this task

Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or Avaya Solutions Platform 130 Release 5.0 host. You can associate an ESXi host with an existing location.

If you add a standalone ESXi host to the System Manager Solution Deployment Manager or the Solution Deployment Manager client, add the standalone ESXi host using its FQDN.

Note:

You can add a VMware ESXi host in Solution Deployment Manager if the Standard or Enterprise VMware license is applied on the VMware ESXi host.

If the VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or the VMware ESXi host is in the evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

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

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

You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to VMware ESXi host.

Note:

- To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA before you add the host to the SDM inventory.
- To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP Address of the ESXi host. Otherwise, Solution Deployment Manager does not support adding the ESXi host in Solution Deployment Manager.
- To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the IP address to add an Avaya Solutions Platform host.

Before you begin

Add a location.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details such as the platform name, platform FQDN or IP address, username, and password.

      For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root username.
   b. In **Platform Type**, select **AVP/ESXi**.
   c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.
5. Click **Save**.
6. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can accept the certificate. If the certificate is invalid, Solution Deployment Manager displays the error. To generate the certificate, see the VMware documentation.

   In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

Next steps

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Related links

Add and Edit platform field descriptions on page 40

Adding an Avaya Solutions Platform S8300 Release host

About this task

This procedure is required for both preloaded or prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to add an Avaya Solutions Platform S8300 Release 5.1.x host. You can associate an Avaya Solutions Platform S8300 Release 5.1.x and later host with an existing location.

Note:

Select **ASP 130/S8300** in **Platform Type** on the Platforms tab to add an Avaya Solutions Platform 130 Release 5.1 host in the SDM Application Management.

Before you begin

- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1.x is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and add the Avaya Solutions Platform S8300 Release 5.1.x host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface".
- If you are connected to the Avaya Solutions Platform S8300 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- Add Avaya Solutions Platform S8300 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform S8300 host.

Procedure

1. To add an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

     On the desktop, click the SDM icon (), and then click **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform S8300 deployment, you can also provide the root username.

b. In **Platform Type**, select **ASP 130/S8300**.

5. Click **Save**.

   The Avaya Solutions Platform S8300 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform S8300 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

Next steps

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Related links

Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface on page 107

Re-establishing trust for Solution Deployment Manager elements on page 69

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.

- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface".
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

     On the desktop, click the SDM icon (), and then click **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform 130 deployment, you can also provide the root username.

   b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

Next steps

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that the system populates **Application Name** and **Application Version** for each virtual machine.

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 10.2.x, the System Manager system supports the Red Hat Enterprise Linux Release 8.4 (64-bit) operating system.

Before you begin

Add a location.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the username of the base operating system.

   For a software-only deployment, the username must have permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

   If the platform has some applications running, the system automatically discovers those applications and displays the applications in the **Applications** tab.

   - If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
   - If you are adding OS, only **Add** and **Remove** operations are available on the **Platforms** tab. You cannot perform any other operations. On the **Applications** tab, the system enables the **New** option. If the application is System Manager, the system enables **Update App** on Solution Deployment Manager Client.

   The System Manager system displays the added base operating system on the **Platforms** tab.

Editing a platform

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select a platform that you want to update.
4. Change the platform information.

   If you connect the Solution Deployment Manager client to Appliance Virtualization Platform through the services port, the platform IP address must be 192.168.13.6.
5. Click **Save**.

   The system updates the platform information.

Related links

Add and Edit platform field descriptions on page 40

Refreshing a platform

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Platforms** tab, do the following:
   a. In the Platforms for Selected Location <location name> section, select one or more platforms.
   b. Click **Refresh Host**.
      - If you select less than five platforms, Solution Deployment Manager refreshes the selected platforms and displays the status in the **Current Action** column.
      - If you select more than five platforms, Solution Deployment Manager displays the following message:

        ```
        Refresh Host takes a few minutes for each host. Once started,
        this action cannot be cancelled. Do you want to proceed with
        Refresh for the <number of selected hosts> selected hosts?
        ```

        To proceed with the refresh platform action of more than five platforms, click **Yes**.

        Solution Deployment Manager refreshes the platforms and displays the status in the **Current Action** column.

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform. If you connect the Solution Deployment Manager client to Appliance Virtualization Platform through the services port, the platform IP address must be 192.168.13.6.
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

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

Removing a platform

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.

2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

Generating the Avaya Solutions Platform S8300 kickstart file

About this task

This procedure is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Generate the kickstart file for the fresh installation of Avaya Solutions Platform S8300.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Kickstart Generation**.
3. On Create AVP/ASP Kickstart, select **ASP S8300 5.1**.
4. In Generate Kickstart for, select **Fresh Installation**.
5. Enter the appropriate information in the fields.

   For information, see “Create ASP S8300 Kickstart field descriptions”.
6. Click **Generate Kickstart File**.

   Solution Deployment Manager prompts you to save the generated kickstart file on your local computer.

   For Avaya Solutions Platform S8300 Release 5.1 and later, the kickstart file name must be `aspks.cfg` and the contents of the generated aspks.cfg file must never be manually edited or modified.

Related links

Create ASP Kickstart field descriptions on page 41

Create ASP Kickstart field descriptions

This section is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Name	Description
Choose AVP/ASP Version	The field to select the Avaya Solutions Platform S8300 host. For Avaya Solutions Platform S8300, the option is **ASP S8300 5.1**.

Table continues…

Name	Description
Generate Kickstart for	The field to select the option for generating the Avaya Solutions Platform S8300 kickstart file. Use the **Fresh Installation** option to generate the kickstart file for installing Avaya Solutions Platform S8300 Release 5.1 and later. **Note:** Do not use the **Upgrade** option, it is for future use only.
ASP Management IPv4 Address	The IPv4 address is used to access Avaya Solutions Platform S8300 through SSH.
ASP IPv4 Netmask	The IPv4 subnet mask for the Avaya Solutions Platform S8300 host.
ASP Gateway IPv4 Address	The IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
ASP Hostname	The hostname for the Avaya Solutions Platform S8300 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
Main IPv4 DNS Server	The DNS Server IPv4 address for the Avaya Solutions Platform S8300 host.

Button	Description
Generate Kickstart File	Generates the Avaya Solutions Platform S8300 kickstart file and prompts you to save the file on your local computer.

Note:

FQDN is used to add host to SDM.

Related links

Generating the Avaya Solutions Platform S8300 kickstart file on page 41

Enabling and disabling SSH on Avaya Solutions Platform 130 Release 5.1 from Solution Deployment Manager

About this task

Use this procedure to enable SSH on Avaya Solutions Platform 130 from Solution Deployment Manager.

Note:

After installing Avaya Solutions Platform 130, SSH is enabled automatically. The only time this procedure is necessary is if the ASP SSH enable/disable shell script is executed or if SSH is disabled manually from the ESXi embedded host client or via Solution Deployment Manager.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. Select the required host.
4. To enable SSH, do the following:
   a. Click **More Actions** > **SSH** > **Enable SSH**.
   b. In the Confirm dialog box, in **Time (in minutes)**, type the time after which the system times out the SSH connection.

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

      Solution Deployment Manager displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

   Solution Deployment Manager displays `disabled` in the **SSH status** column.

ASP_SSH script

If a customer disables SSH for security reasons, use the **`ASP_SSH`** script to enable SSH for troubleshooting.

The following applications support the **`ASP_SSH`** script:

- Communication Manager
- Session Manager
- System Manager
- Application Enablement Services
- Avaya Session Border Controller
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Aura® Device Services
- Avaya Aura® Web Gateway
- Avaya Experience Portal

Enabling SSH and viewing SSH status on Avaya Solutions Platform 130 Release 5.1 from the application CLI

About this task

Use this procedure to enable SSH and to check the SSH status of the Avaya Solutions Platform 130 Release 5.1 host.

Note:

- By default, the SSH is enabled on ASP without a timeout value.
- If **ASP_SSH** is run by mistake on a setup with SSH enabled while installation or migration, the script overrides the timeout value, and SSH is disabled after 2 hours window.

Before you begin

- The application must be deployed on the Avaya Solutions Platform 130 Release 5.1 host.
- Start an SSH session.
- Log in to the application command-line interface with administrator privilege CLI user credentials.

Procedure

1. To enable SSH, type **ASP_SSH** `enable` and press `Enter`.

   After the script is successfully run, wait for 3 minutes before trying to SSH to ASP.

   The SSH is enabled for 120 minutes.

   By default, the system automatically disables the SSH and blocks any new SSH connections after 120 minutes.

   The system enables the SSH on the Avaya Solutions Platform 130 Release 5.1 host.

2. To view the status of SSH, type **ASP_SSH** `status` and press `Enter`.

   If SSH is enabled, the system displays the following:

   ```
   An ASP SSH status is currently:
   active
   ```

   If SSH is disabled, the system displays the following:

   ```
   An ASP SSH status is currently:
   inactive
   ```

Mapping the ESXi host to an unknown location

About this task

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the left navigation pane, click the **Unknown location Platform mapping** link.
3. In the Host Location Mapping section, select an ESXi host, and click **Edit**.

   The system displays the Host Information page.
4. Select a location and click **Update**.
5. Select the host(s) where location is updated and click **Submit**.

   The system displays the ESXi host in the selected location.

Operations on Appliance Virtualization Platform

Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Kickstart Generation**.
3. On Create AVP/ASP Kickstart, do the following:
   a. Select **AVP 8.1.x**.
   b. Enter the appropriate information in the fields.
   c. Click **Generate Kickstart File**.

      For more information, see “Create AVP Kickstart field descriptions.”

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

      For Appliance Virtualization Platform Release 8.1.x, the kickstart file name must be `avp81ks.cfg`.

Related links

Create AVP Kickstart field descriptions on page 45

Create AVP Kickstart field descriptions

Name	Description
Choose AVP Version	The field to select the release version of Appliance Virtualization Platform.

Table continues…

Name	Description
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. The options are: • **yes**: To enable the IPv6 format. • **no**: To disable the IPv6 format.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
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.

Table continues…

Name	Description
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Out of Band Management Setup	The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • **yes**: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • **no**: To disable Out of Band Management. The default option.
OOBM vLAN ID (Used on S8300E only)	• For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Confirm Password	Admin password for Appliance Virtualization Platform.
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.
Validity in Days (Used on AVP Certificate)	The number of days for the Appliance Virtualization Platform certificate validation. The maximum limit for the certificate validation is 825 days. You can configure from 1 through 825 days.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

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

Related links

Generating the Appliance Virtualization Platform kickstart file on page 45

Changing the network parameters for an Appliance Virtualization Platform host

About this task

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

Note:

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

Before you begin

Install the Solution Deployment Manager client on your computer.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnet mask, and other parameters as appropriate.

   Note:

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

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

   - Public or signaling traffic, Avaya Aura® Appliance Virtualization Platform, and all virtual machines public traffic.
   - Management, Avaya Aura® Appliance Virtualization Platform, and all virtual machine management ports.

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

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

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

6. Click **Save**.

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 52

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

About this task

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

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

Note:

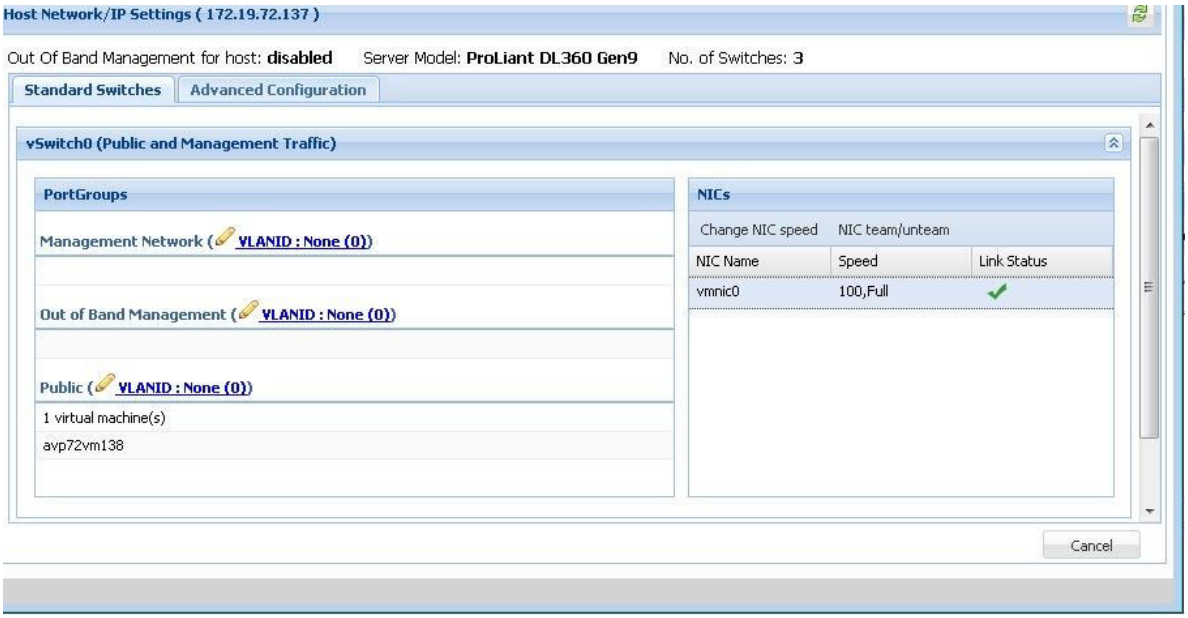
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fail because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

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.

4. Click **Change Network params** > **Change Network Settings**.



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

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.
- **vSwitch3**. No reservations.
- **vSwitch4**. No reservations.
- **vSwitch5**. No reservations.

5. To change VLAN ID, click **Standard Switches**, and perform the following:
   a. Expand the vSwitch<n> section by clicking the downward arrow .

      The section displays the vSwitch details.

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

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

   c. In **VLAN ID**, select an ID.

      For more information about the value, see NIC teaming.

   d. Click **OK**.

The system displays the new VLAN ID.

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

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

      For more information, see VLAN ID assignment.

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

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

   Note:

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

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

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

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

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for the S8300E server.

Related links

Host Network / IP Settings field descriptions on page 53

Change Network Parameters field descriptions

Network Parameters

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

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

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

Host Network / IP Settings field descriptions

Standard Switches

vSwitch <n> displays the PortGroups and NICs sections.

PortGroups

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

Button	Description
OK	Saves the changes.
Cancel	Returns to the **Platforms** tab.

NICs

Name	Description
NIC Name	Displays the name of the NIC. For example, vmnic0.
Speed	Displays the speed of the NIC. For example, 100,Full.
Link Status	Displays the status of the NIC.

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

NIC speed

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

Button	Description
OK	Saves the changes.

NIC teaming

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

Advanced Configuration

Displays the Unused PortGroups section.

Name	Description
Port Group	Displays the port group.
Virtual Switch	Displays the virtual switch.

Button	Description
Delete	Deletes the selected port group.
Cancel	Returns to the **Platforms** tab.

Deleting the unused port

About this task

Use this procedure to delete the unused port of Solution Deployment Manager that is no longer used by applications that are deployed on an Appliance Virtualization Platform host.

For example, you can delete the unused port, if an application is deleted from the Appliance Virtualization Platform host, and the system still has those ports available on the Appliance Virtualization Platform host.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params** > **Change Network Settings**.
5. Click **Advanced Configuration**.
6. In the Unused PortGroups section, select the portgroup.

7. Click **Delete**.

Changing the password for an Appliance Virtualization Platform host

About this task

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, do the following:
   a. Select a host.
   b. Click **More Actions** > **Change Password**.
4. In the Change Password section, type the current password and the new password.

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

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

Related links

Password policy on page 55
Change Password field descriptions on page 56

Password policy

The password must meet the following requirements:

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

Note:

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

Example of a valid password is *myPassword$*.

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

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

Related links

Changing the password for an Appliance Virtualization Platform host on page 55

Change Password field descriptions

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

Button	Description
Change Password	Saves the new password.

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

About this task

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

You can also enable SSH from AVP Utilities.

Procedure

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

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

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

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

Appliance Virtualization Platform license

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

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

To configure the Appliance Virtualization Platform license file:

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

   Note:

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

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

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

Note:

Restricted administrative actions for:

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

Appliance Virtualization Platform licensing alarms

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

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

Before you begin

1. Add an Appliance Virtualization Platform host.

   For information about adding a host, see *Administering Avaya Aura® System Manager*.
2. Obtain the license file from the Avaya PLDS website.
3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions** > **WebLM Configuration**.

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

   For WebLM configuration, if you select:

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

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

6. Click **Submit**.

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

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

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

WebLM Configuration field descriptions

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

Button	Description
Submit	Saves the WebLM Server configuration.
Cancel	Closes the WebLM Configuration dialog box.

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Viewing Appliance Virtualization Platform firewall rules

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host, and click **More Actions** > **AVP Firewall Rules**.

   System Manager displays the Firewall Settings page.
4. To view the additional details, select a row.

   System Manager displays the details in the separate section on the Firewall Settings page.

Applying third-party AVP certificates

Applying third-party certificates to Appliance Virtualization Platform

About this task

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

Before you begin

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

Note:

If you are using a third-party generated CSR, add the private key for the CSR in the file `/etc/vmware/ssl/rui_csr_temp.key` before installing the certificate from Solution Deployment Manager.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

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

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

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

      The system generates CSR for the Appliance Virtualization Platform host.
   f. In the **Current Action** column, click **Status Details** to view the status.

6. To download CSR, do the following:
    a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
    b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
    c. Click **Download CSR**.

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

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

Creating or editing generic CSR

About this task

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

Procedure

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

Next steps

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

Load Certificate field descriptions

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

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

Create or edit CSR field descriptions

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

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

Virtual Machine snapshot on Appliance Virtualization Platform

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

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

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 63
Snapshot Manager field descriptions on page 64

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

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

Procedure

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

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

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

   The system deletes the selected snapshots.

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 63

Snapshot Manager field descriptions

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

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

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 63

Update Host field descriptions

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

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

Shutting down the Appliance Virtualization Platform host

About this task

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

Procedure

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

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

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

Procedure

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

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

Chapter 6: Managing the application

Deploying an OVA file for an Avaya Aura® application

About this task

Use the procedure to deploy an OVA file for an Avaya Aura® application on the virtual machine.

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

Before you begin

- Add a location.
- Add a required host to the location.

  Note:

  Before starting the new virtual machine deployment, you must perform the **Refresh Host** operation on the selected host.
- Ensure that the certificate is valid on the host or vCenter managed hosts.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

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

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

   The Capacity Details section displays the capacity details.
6. Click **Next**.

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

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the following message: `Invalid file content. Avaya Certificate not found or invalid`
8. In **Flexi Footprint**, select the footprint size that the application supports.
9. **(Optional)** To install the patch file for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
   - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
   - **S/W Library**, and select the latest service or feature pack from the drop-down list.
   - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

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

    In Configuration Parameters and Network Parameters sections, Solution Deployment Manager displays the fields that are specific to the application that you deploy.
11. In the Network Parameters section, ensure that the following fields are preconfigured:
    - **Public**
    - **Services**: Only for AVP Utilities.
    - **Duplicate Link**: Only for duplex Communication Manager.
    - **Private**: Only for Application Enablement Services.
    - **Out of Band Management**.

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

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

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

Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.

15. To view details, click **Status Details**.

Related links

Application Deployment field descriptions on page 77

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. 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.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays  and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.

- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions** > **Analyze**.
4. 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.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✔, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application.

Before you begin

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

Procedure

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

5. Click **More Actions** > **Re-establish connection**.
6. Select the release version of the product deployed on the application.

   The options are:

   - **6.3 and below**: When you select this, the system displays the following message:

     `Trust cannot be established for this version VM.`
   - **7.0**
   - **7.1 and above**
   - **others**

   Note:

   When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
7. When you select the version **7.0** or **others**, in **User Name**, type the user name of the application.
8. When you select the version **7.0** or **others**, in **Password**, type the password of the application.
9. Click **Reestablish Connection**.

Editing an application

Before you begin

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

   The system displays the Edit App section.

4. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

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

      Note:

      To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

   c. Click **Update IP/FQDN in Local Inventory**.
   d. Click **Update App IP/FQDN**.
   e. Provide the IP address and FQDN of the application.

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

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. Click **Delete**.

   System Manager displays the following message:

   ```
   Software Only application will be deleted from inventory only.
   Other application(s) will be power off and deleted from Platform.
   Are you sure you want to delete application(s) ?

   Note : If you selected VM for which VM deployment has failed due to
   VM Validation Error then that VM entry will be deleted from local
   inventory only.
   ```
5. Click **Yes** to confirm.

System Manager turns off the applications and deletes the selected applications from the platform.

Updating Services Port Static Routing on an Avaya Aura® application

About this task

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

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

Before you begin

- Update network parameters of AVP Utilities if applicable.
- Ensure that the Avaya Aura® application resides on the same subnet as AVP Utilities.

Procedure

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

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

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

Related links

Update Static Routing field descriptions on page 82

Starting an application from Solution Deployment Manager

Procedure

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

2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

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

Stopping an application from Solution Deployment Manager

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

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

Restarting an application from Solution Deployment Manager

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.

4. Click **Restart**.

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

VM Console overview

From Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab.

To open and manage the application through the console, ensure that the:

- Application must be in running state. The application status must be **Started** for the application on the **Applications** tab in the **Application State** column.
- Application must reside on the Appliance Virtualization Platform host Release 7.1.2 and later.
- Appliance Virtualization Platform host certificate must be added in your browser.

You cannot view the VM Console of the application if the application resides on the customer-provided VMware ESXi host.

Opening a VM console from Solution Deployment Manager

About this task

Use the following procedure to open the VM console in a new browser window or on a new browser tab.

Before you begin

- Add a location.
- Add the Appliance Virtualization Platform host.
- Ensure that the application is hosted on the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host certificate in your browser.

  If you do not add the host certificate in your browser, the system displays the following message when you try to open the VM console in a browser:

  ```
  To open VM Console of an application, add the Platform certificate
  in the browser. Following is the URL of the platform to accept the
  certificate: https://<Host URL where the application resides>:443
  ```

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 **Applications** tab, in the **Applications for Selected Location <location name>** section, select the application.
5. To open the VM console in a new:
   - Browser window, click **VM Console** > **Open VM Console in New Window**.
   - Tab of the browser, click **VM Console** > **Open VM Console in New Tab**.

   When you open the console for the very first time, if the Appliance Virtualization Platform host certificate is not added in your browser, the system opens the browser instance with the following message:

   ```
   To open VM Console of an application, add the Platform certificate
   in the browser. Following is the URL of the platform to accept the
   certificate: https://<Host URL where the application resides>:443
   ```

   If you open the VM console after accepting the Appliance Virtualization Platform host certificate in the browser, the system opens the VM console without any warning message.

   If the browser displays the same error message even after accepting the Appliance Virtualization Platform host certificate, see *Troubleshooting Avaya Aura® System Manager*.

Next steps

On VM Console, log in to the application and perform the required operations.

VM Console field descriptions

Name	Description
Full Screen	Opens the console in full screen mode. You can press the **Esc** key to exit from the full screen mode.
Send Keys	These keys are applied to the VM Linux system and not to your local computer from where you are accessing the VM Console. The options are: • **Send Ctrl+Alt+Del** • **Send Ctrl+c** • **Send Escape**

Table continues…

Name	Description
KeyBoard Layout	Sets the keyboard layout based on the selected language. The options are: • English • Japanese • German • Italian • Spanish • Portuguese • French • Swiss-French • Swiss-German

Common causes for application deployment failure

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

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

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

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

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

Application Deployment field descriptions

Select Location and Platform

Name	Description
Select Location	The location name.
Select Platform	The platform name that you must select.
Platform FQDN	The platform FQDN.
Data Store	The data store for the application. The page populates the capacity details in the Capacity Details section.
Next	Displays the OVA/ISO Details section where you provide the details required for OVA or ISO deployment.

Capacity Details

The system displays the CPU and memory details of the Avaya Solutions Platform 130 or ESXi host. The fields are read-only.

Note:

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

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

Provide admin and root Credentials

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

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

Deploy OVA using System Manager Solution Deployment Manager

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.
Enable enhanced security	The option to enable JITC mode deployment.
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy. **Note:** System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.
Browse Pre-stage Location	The option to provide the prestaged folder. This option is enabled when you deploy System Manager on the Appliance Virtualization Platform Release 8.x or earlier, VMware ESXi, and vCenter platforms by using the Solution Deployment Manager client.
Select Pre-stage Directory	Displays the Datastore Explorer dialog box to select the prestage folder from the data store. The field is available when you select **Browse Pre-stage Location**.
Flexi Footprint	The footprint size supported for the selected application. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA using the Solution Deployment Manager client

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

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

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

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

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

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

With the **URL** option, you can type the URL of the OVA or ISO file. The system displays the following options.

Name	Description
URL	The URL of the OVA or ISO file. The field is available only when you click **URL**.
Submit	Selects the OVA or ISO file to be deployed that is extracted from the URL.

The system displays the following common fields.

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

Configuration Parameters

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

Name	Description
Application Name	The name of the application.
Product	The name of the Avaya Aura® application that is being deployed. The field is read-only.
Version	Release number of the Avaya Aura® application that is being deployed. The field is read-only.

Communication Manager Configuration Parameters

Name	Description
CM IPv4 Address	The IPv4 address of the Communication Manager virtual machine.
CM IPv4 Netmask	The IPv4 network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The IPv4 default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine. The field is optional.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine. The field is optional.
CM IPv6 Gateway	The IPv6 gateway of the Communication Manager virtual machine. The field is optional.
Out of Band Management IPv4 Address	The IPv4 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv4 Netmask	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Server(s)	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). You can type up to three NTP servers. The application supports only the NTP server. It does not support the NTP pool.

Table continues…

Name	Description
DNS Server(s)	The DNS IP address of the Communication Manager virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IPv4 address of the reachable WebLM server. The field is mandatory.
EASG User Access	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.
Confirm Password	The password required to be confirmed. The field is mandatory.

Network Parameters

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Private	The field is available only when you deploy Application Enablement Services.
Create Port Group	The field to create new port group for interface.
Out of Band Management	The port number that is mapped to the out of band management port group.

Button	Description
Deploy	Displays the EULA acceptance screen where you must click **Accept** to start the deployment process.

Update Static Routing field descriptions

Name	Description
VM Name	The application name.
VM IP/FQDN	The IP address or FQDN of the application.
Utility Services IP	The IP address of AVP Utilities.

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

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

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

Update App field descriptions

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

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

Reestablish Connection field descriptions

Name	Description
Select Version	Select the required version. The options are: • **6.3 and below** • **7.0** • **7.1 and above** • **others** **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Application Name	The name of the application.
VM IP/FQDN	The IP address or FQDN of the application.

Table continues…

Name	Description
User Name	The user name of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Password	The password of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

Button	Description
Reestablish Connection	Establishes connection between System Manager and the application.
Cancel	Cancels the changes and returns to the previous page.

Chapter 7: System Manager upgrade management

Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client

About this task

Use the procedure to upgrade System Manager to Release 10.2.x from:

- Release 8.1.x running on Appliance Virtualization Platform, VMware, or Avaya Solutions Platform 130.
- Release 10.1.x running on VMware or Avaya Solutions Platform 130.

Note:

- If you are upgrading System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client then the license files are retained. However, you need to install the license file for System Manager Release 10.2.

  For more information, see “License preservation and license regeneration”.
- From Release 10.1 and later, Appliance Virtualization Platform is no longer available. Therefore, if System Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.1 before upgrading System Manager to Release 10.2. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

Before you begin

- Install Solution Deployment Manager Client.

  For information, see Installing the Solution Deployment Manager client on your computer on page 13.
- Add a location.

  For information, see Adding a location on page 30.
- Add the required host.

  For information about adding the host, see “Managing the platform”.

Important:

- If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

  For information about the supported ESXi version, see Supported ESXi version on page 21.

  For information about upgrading ESXi, see the VMware product documentation.
- If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
- If the application is running on the server that is not supported with Release 10.2.x, then deploy Avaya Solutions Platform 130.

  For information about supported servers, see Supported servers for Avaya Aura applications on page 20.

- Select the System Manager 8.1.x or 10.1.x virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For more information, see Re-establishing trust for Solution Deployment Manager elements on page 69.
- Obtain the System Manager software. See “Software details of System Manager”

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Upgrade Management**.
4. Select the System Manager 8.1.x or 10.1.x virtual machine.
5. Click **Upgrade**.
6. In **Platform FQDN**, select the required host.

   If the System Manager system prompts for the certificate, accept the certificate. When you accept the certificate, the system displays the following message: `Certificate added successfully in trust store.`
7. **(Optional)** Select the datastore on the host.

   If more than one datastore is available, select the datastore.

   If the host is part of a VMware cluster, the system displays the following message:

   `Host is in a cluster. Therefore, capacity details of CPU and memory are unavailable! Ensure that the host resource requirements are met before any action.`

   For information about resource details, see Supported footprints of System Manager on VMware on page 103.

8. Click **Next**.
9. On the **OVA** tab, click one of the following:
   - **URL**, in **OVA File**, type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the System Manager OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the System Manager OVA file from the drop-down list.

     To use the **S/W Library** option, the OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation. The system displays the directory name when the **S/W Library** option is selected.
   - **Browse**, select the required OVA file from your local computer, and click **Submit File**.
   - **Browse from Datastore**

     For information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

     This option is applicable only for System Manager Release 10.1 and later.

   When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
10. To upload the data migration utility file, click the Data Migration tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest data migration utility file.
    - **S/W Library**, and select the latest data migration utility file from the drop-down list.

      The data migration utility file must be present in the local software library directory.
    - **Browse**, and select the latest data migration utility file from your local computer, and click **Submit File**.
11. To upload the latest service or feature pack, select the Service or Feature Pack tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
    - **S/W Library**, and select the latest service or feature pack from the drop-down list.
    - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.
12. Click **Next**.
13. In the Config Parameters section, provide the required details.

Note:

Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.

For information, see “Upgrade Management field descriptions”.

14. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
15. Click **Upgrade** and accept the license terms.

    The system takes the backup, shuts down the existing virtual machine (VM), deploys the OVA file, and restores the data on the new virtual machine.
16. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 100–150 minutes depending on the data on System Manager.

    Note:

    The upgrade process might involve multiple reboots during data migration. If you have selected the checkbox **Require Encryption Pass-Phrase at Boot-Time**, you must monitor the VM console for reboots and enter the **Encryption Pass-Phrase** promptly.

    If you fail to enter the **Encryption Pass-Phrase** timely, the upgrade process may timeout and fail. If this happens, restart the upgrade process.
17. Do one of the following:
    - If the upgrade is successfully completed, do the following:
      a. Verify that the new System Manager virtual machine is functional.

         For more information, see “Verifying the functionality of System Manager”.
      b. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

         The system deletes the old virtual machine.
      c. Click **Commit**.

         The system deletes the old virtual machine.

         If you already performed the **Commit** operation or manually deleted the older VM (For example, <vm_name>_old) after successful upgrade on host itself. In these cases, if you re-attempt the **Commit** operation then Solution Deployment Manager displays the warning message `Unable to find <vm_name>_old` on the Commit status page.
    - If the upgrade fails or you want to revert to the old system, then do the following:
      a. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

b. Click **Rollback**.

   The system deletes the newly created virtual machine and starts the old virtual machine.

c. Again refresh both the host to get the latest virtual machine information.

Next steps

Install the valid license file for System Manager Release 10.2.x.

Upgrading System Manager from Release 7.x or 8.0.x to Release 10.2.x through services port by using Solution Deployment Manager Client

About this task

The procedure describes the steps to upgrade Appliance Virtualization Platform-based System Manager Release 7.x or 8.0.x to System Manager Release 10.2.x.

Note:

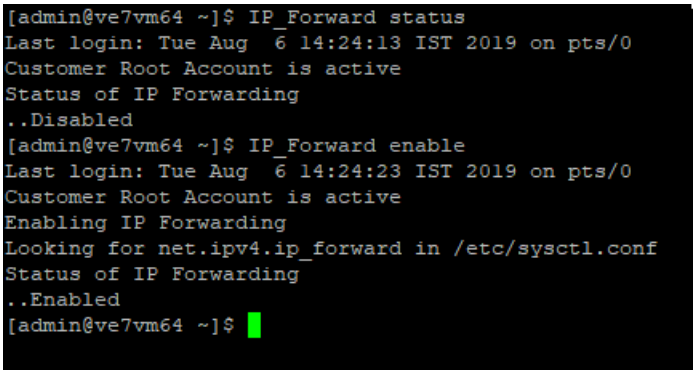
If you are upgrading System Manager Release 7.x or 8.0.x to Release 10.2.x by using the Solution Deployment Manager client then the license files will be retained. However, you need to install the license file for System Manager Release 10.2.x.

Procedure

1. Upgrade Appliance Virtualization Platform and AVP Utilities.
2. Log in to the AVP Utilities CLI with administrative credentials.
3. To check the IP forward status, type the **`IP_Forward status`** command.

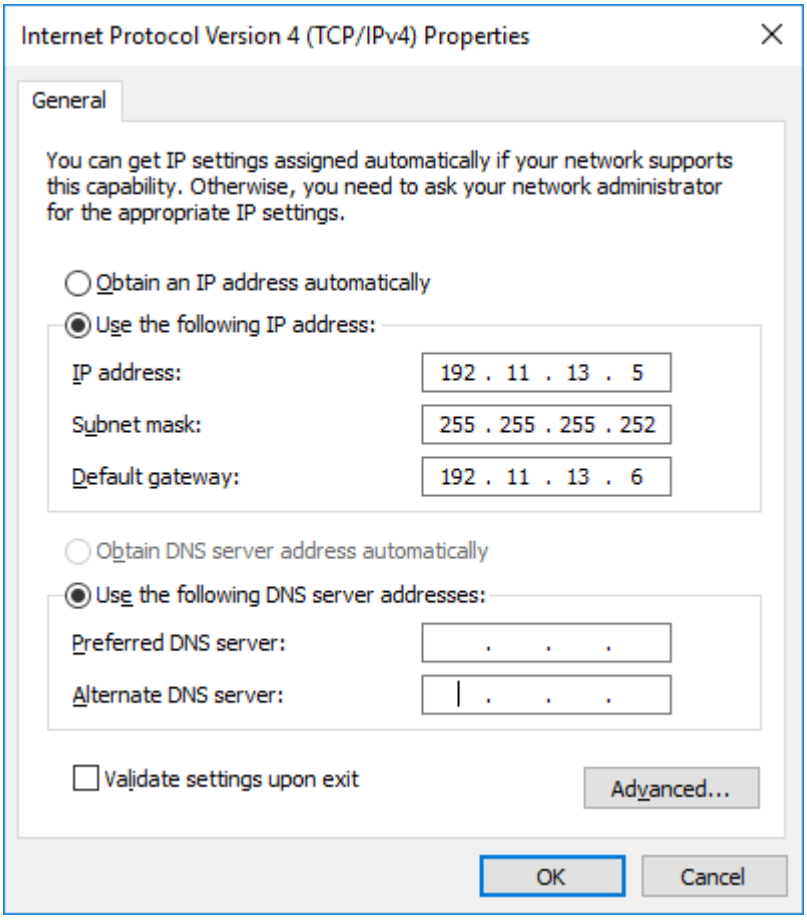
   If the IP forward status is disabled, type the **`IP_Forward enable`** command

   Following is an example of checking the IP forward status and enabling the IP forward status.



4. To configure laptop with below configuration for System Manager, go to **Network or Internet Settings** > **Ethernet** > **Local Area Connection** > **Internet Protocol version 4 (TCP/IPv4) Properties**, do the following:
   a. Select the **Use the following IP address** option.
   b. In the **IP address** field, type `192.11.13.5`.
   c. In the **Subnet mask** field, type `255.255.255.252`.
   d. In the **Default Gateway** field, type `192.11.13.6`

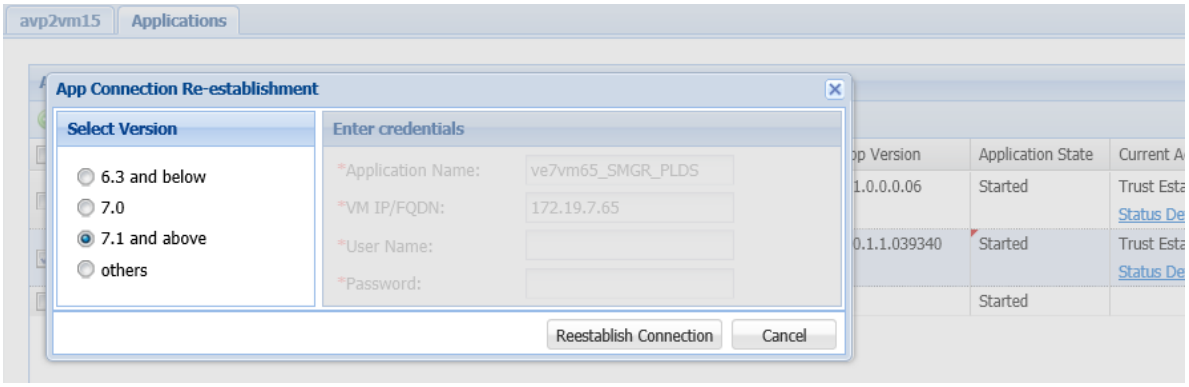
   Following is an example for changing the configuration for the System Manager upgrade.



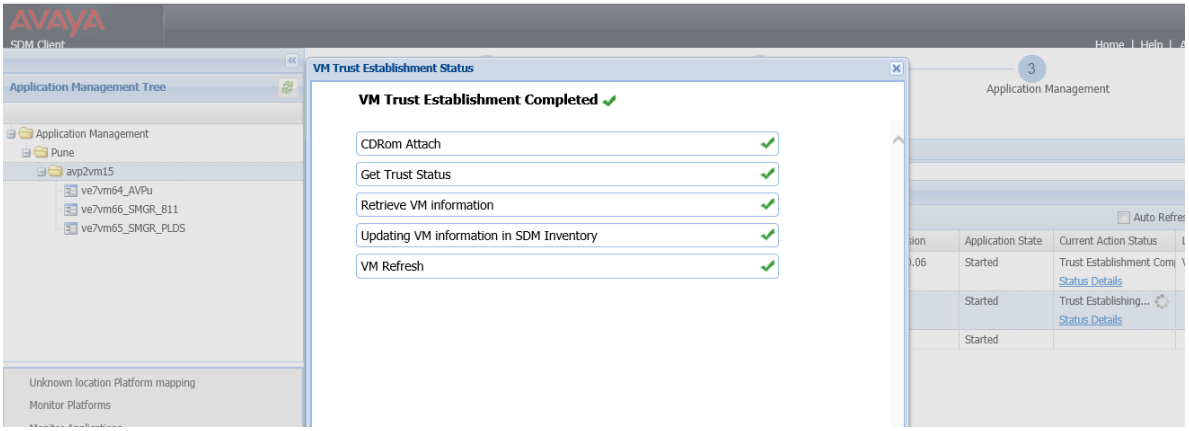
5. To re-establish trust with System Manager that is already deployed on the added Appliance Virtualization Platform host, do the following:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> area, select System Manager.
   b. Click **More Actions** > **Re-establish connection**.

   If you need to re-establish trust with System Manager Release 7.0, select the version as 7.0.

   Following is an example of re-establishing trust with System Manager.



Wait for 3 to 5 minutes for trust establishment to complete without any error as shown in the below screen shot.



6. After re-establishing trust with System Manager, click **Upgrade Management**.

   On the Upgrade Management page, the system displays the System Manager virtual machine.

7. On the Upgrade Management page, select the System Manager virtual machine, and then click **Upgrade**.

   The system displays the SMGR Upgrade window.

8. In **Platform FQDN**, select the required host.

9. **(Optional)** Select the datastore on the host.

   If more than one datastore is available, select the datastore.

10. Click **Next**.

11. On the **OVA** tab, click one of the following:

    - **URL**, in **OVA File**, type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the System Manager OVA file, and click **Submit**.

- **S/W Library**, in **File Name**, select the System Manager OVA file from the drop-down list.

  To use the **S/W Library** option, the OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation. The system displays the directory name when the **S/W Library** option is selected.
- **Browse**, select the required OVA file from your local computer, and click **Submit File**.
- **Browse from Datastore**

  For information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

  This option is applicable only for System Manager Release 10.1 and later.

When you select the OVA, the system:

- Displays the CPU, memory, and other parameters in the Capacity Details section.
- Disables the **Flexi Footprint** field.

12. To upload the data migration utility file, click the Data Migration tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest data migration utility file.
    - **S/W Library**, and select the latest data migration utility file from the drop-down list.

      The data migration utility file must be present in the local software library directory.
    - **Browse**, and select the latest data migration utility file from your local computer, and click **Submit File**.
13. To upload the latest service or feature pack, select the Service or Feature Pack tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
    - **S/W Library**, and select the latest service or feature pack from the drop-down list.
    - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.
14. Click **Next**.
15. In the Config Parameters section, provide the required details.

    Note:

    Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.

    For information, see “Upgrade Management field descriptions”.
16. In the Network Parameters section, select the required Public and Out of Band Management network interface details.

17. Click **Upgrade** and accept the license terms.

    The system takes the backup, shuts down the existing virtual machine (VM), deploys the OVA file, and restores the data on the new virtual machine.

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

    The complete process takes about 100–150 minutes depending on the data on System Manager.

    Note:

    The upgrade process might involve multiple reboots during data migration. If you have selected the checkbox **Require Encryption Pass-Phrase at Boot-Time**, you must monitor the VM console for reboots and enter the **Encryption Pass-Phrase** promptly.

    If you fail to enter the **Encryption Pass-Phrase** timely, the upgrade process may timeout and fail. If this happens, restart the upgrade process.

19. Do one of the following:

    - If the upgrade is successfully completed, do the following:

      a. Verify that the new System Manager virtual machine is functional.

         For more information, see “Verifying the functionality of System Manager”.

      b. Click **Commit**.

         The system deletes the old virtual machine.

         If you already performed the **Commit** operation or manually deleted the older VM (For example, <vm_name>_old) after successful upgrade on host itself. In these cases, if you re-attempt the **Commit** operation then Solution Deployment Manager displays the warning message `Unable to find <vm_name>_old` on the Commit status page.

    - If the upgrade fails or you want to revert to the old system, click **Rollback**.

      The system deletes the newly created virtual machine and starts the old virtual machine.

Installing service packs and software patches on System Manager by using Solution Deployment Manager Client

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using Solution Deployment Manager Client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the Applications for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. Click **More Actions** > **Refresh App**.

   If **Refresh App** is disabled or fails, proceed to next step.
6. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **More Actions** > **Refresh App**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
7. Click **More Actions** > **Update App**.

   If Solution Deployment Manager detects a previous uncommitted patch, the system displays a dialog box with **Commit** and **Rollback**. You need to either commit previous uncommitted patch or rollback. Only after this, the system displays the System Manager Update dialog box to provide the patch file.
8. Click **Select bin file from Local SDM Client** and provide the absolute path to the software patch or service pack.

   Note:

   The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.
9. **(Optional)** Click the **Auto commit the patch** check box.
10. Click **Install**.

    In the Applications for Selected Location <location name> section, the system displays the status.
11. To view the details, in the **Current Action** column, click **Status Details**.

    SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.
12. On the Installed Patches page, perform the following:
    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.

b. Click **Get Info**.

c. Select the patch, service pack or feature pack, and click **Commit**.

Note:

To **Commit** or **Rollback** the System Manager patch, use this step.

Related links

Update App field descriptions on page 83

Upgrade Management field descriptions

Upgrade Elements

Name	Description
SMGR Name	System Manager name.
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
C-DOM IP/FQDN	The IP address or the FQDN of console domain.
Element Type	The type of the element.
Current Version	The current version of the element.
Upgrade To Version	The upgrade to version for the element.
Upgrade Status	The status of the upgrade process. The status can be **Upgrading**, **Completed**, or **Failed**. The **Status Details** link provides more information about the System Manager upgrade.
Last Action	The last upgrade action.
Related VM	The associated virtual machine.

Button	Description
Add Elements	Displays the Add Element page where you add System Manager.
Upgrade	Displays the Upgrade Management page where you upgrade the System Manager virtual machine.
Edit	Displays the Edit Element page where you can change the details of System Manager that you added.
Delete	Deletes the System Manager virtual machine.
Commit	Saves the changes and upgrades the System Manager virtual machine.
Rollback	Reverts the upgrade of the System Manager virtual machine.

Add Element field descriptions

System Platform: Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN.
C-DOM SSH User Name	The C-DOM SSH user name.
C-DOM SSH Password	The C-DOM SSH password.
C-DOM Root User Name	The C-DOM root user name.
C-DOM Root password	The C-DOM root password.

Virtual Machine Platform (6.x): Required Host/VM Details Information

Name	Description
Hosts	The host of the virtual machine.
Virtual machines	The virtual machine.

System Platform/Virtual Machine Platform (6.x): Required Element Information

Name	Description
SMGR IP	The IP address of System Manager.
SMGR VM NAME	The name of the System Manager virtual machine.
SMGR SSH User Name	The SSH user name of System Manager.
SMGR SSH Password	The SSH password of System Manager.

Button	Description
Save	Saves the element that you added.

Edit Elements field descriptions

Required Element information

Name	Description
SMGR IP	The IP address of System Manager.
SMGR NAME	The name of System Manager virtual machine.
SMGR SSH User Name	The SSH user name of System Manager.
SMGR SSH Password	The SSH password of System Manager.

Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN
C-DOM SSH User Name	The C-DOM SSH user name
C-DOM SSH Password	The C-DOM SSH password
C-DOM Root User Name	The C-DOM root user name
C-DOM Root password	The C-DOM root password

Button	Description
Update	Updates the changes to the element.

Upgrade Management field descriptions

Name	Description
Install on Same Host	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update. **Note:** When upgrading from System Platform-based System Manager to AVP or ESXi, the system displays this field.
Platform FQDN	The platform FQDN to which you want to upgrade. The system displays the CPU and memory details of the platform in the Capacity Details section.
Application Name	The application name displayed on the Add Element page.

OVA/ISO Details

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.

Table continues…

Name	Description
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Browse from Datastore	The option to provide the prestaged folder. This option is enabled when you upgrade the application on the Appliance Virtualization Platform, VMware ESXi, and vCenter platforms. For upgrade, this option is applicable only for System Manager.
Select Pre-stage Directory	Displays the Datastore Explorer dialog box to select the prestage folder from the data store. The field is available when you select **Browse Pre-stage Location**
View Prestage Details	Displays the details of the prestage folder.
Validate checksum of OVA files	Validates the checksum of the OVA file.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is .
SMGR Data migration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest data migration bin that is available for the System Manager release.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.

Configuration Parameters

The system populates the values for most of the fields from the 7.x or 8.0.x system. You must provide information, such as password, FQDN, time zone, and EASG.

Management Network Settings

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application for Out of Band Management. This field is an optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager application.

Table continues…

Name	Description
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. This field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. This field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. This field is optional.
Default Search List	The search list of domain names. This field is optional.

Public Network Settings

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

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.

Table continues…

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

SMGR CLI USER

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

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.

Table continues…

Name	Description
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Network Parameters

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

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

Supported footprints of System Manager on VMware

The following table describes the resource requirements to support different profiles for System Manager on Customer-provided VMware and Avaya-supplied Avaya Solutions Platform 130.

Note:

- Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.
- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware*.

  Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

Resource	Profile 2	Profile 3	Profile 4
vCPU Reserved	6	8	18
Minimum vCPU Speed	2185 MHz	2185 MHz	2185 MHz
CPU reservation	13110 MHz	17480 MHz	39330 MHz
Virtual RAM	12 GB	18 GB	36 GB
Memory reservation	12288 MB	18432 MB	36864 MB
Virtual Hard Disk	170 GB	270 GB	850 GB
Shared NICs	1	1	1
IOPS	44	44	44

Note:

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Chapter 8: Additional Solution Deployment Manager client functionality

Managing certificates

Certification validation

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

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

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

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

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

For the correct certificate:

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

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.

- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

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

Note:

Solution Deployment Manager:

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

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

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

Generating and accepting the Appliance Virtualization Platform host certificates

About this task

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

If the certificate is invalid:

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

Before you begin

Get permissions to add a host to generate certificates.

Procedure

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

5. To accept the certificate, in the Certificate dialog box, click **Generate Certificate**, and do the following:
   a. In the Generate Certificate dialog box, in the **Validity in Days** field, type the validity of the certificate in days.
   b. Click **Generate Certificate**.

      The system displays the message: `Certificate is generated`.
   c. Click **Ok**.
6. To accept the certificate, click **Accept Certificate**.
7. To view the certificate validity status, click the **View link** in the **Platform Certificate Status** column.

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

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

   Note:

   An alarm is generated everyday if the certificate expiry is below 60 days. This alarm can be cleared by installing a new identity certificate, which has the validity more than 60 days.

Generating and updating the certificate on the ESXi host from VMware

About this task

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

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

Procedure

To generate and update ESXi host and vCenter certificates, see the VMware documentation.

Next steps

Note:

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

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

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

Managing certificates for existing hosts

About this task

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

Before you begin

Gain permissions to add a host to generate certificates.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions** > **Generate/ Accept Certificate**, and click **Accept Certificate**.
   - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

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

Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface

About this task

Before adding an Avaya Solutions Platform 130 host, to regenerate the Avaya Solutions Platform 130 self-signed certificate with FQDN, perform the following steps:

For information about adding an Avaya Solutions Platform 130 host, see Adding an Avaya Solutions Platform 130 Release 5.1 host on page 36.

Procedure

1. Log in to the Avaya Solutions Platform 130 command line interface.
2. To change the FQDN, type the following command:

   ```
   esxcli system hostname set --fqdn=server.abc.com
   ```

   Here, *server.abc.com* is the FQDN of the ESXi host.

For more information, see Changing the host name on the VMware documentation website.

3. To regenerate the self-signed certificate, do the following:
   a. Enable SSH on the ESXi host, then put the ESXi host into the maintenance mode.
   b. SSH to the ESXi host and use the following commands to take backups of the current certificate file and private key file.

      ```
      cd /etc/vmware/ssl
      mv rui.crt rui.crt.bkp
      mv rui.key rui.key.bkp
      ```

   c. To regenerate a new certificate, type the following command:

      ```
      /sbin/generate-certificates
      ```

      Verify that the new certificate file and private key file are generated.
   d. To restart the ESXi Server management agent, reboot the host.

      The ESXi host generates a new self-signed certificate.

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

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. Click **Monitor Platforms**.
3. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

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

Monitoring an application

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.

2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

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

Managing vCenter

Creating a role for a user

About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**
      - **Datastore cluster**
      - **Distributed switch**
      - **Folder**
      - **Host profile**
      - **Network**
      - **Resource**
      - **Tasks**
      - **Virtual machine**

- **vApp**

Note:

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

b. In All Privileges, expand **Host**, and select the **Configuration** check box.

Note:

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

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

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.

- The FQDN value must match with the value of the **SAN** field of the vCenter certificate. The FQDN value is case sensitive.

b. In **User Name**, type the user name to log in to vCenter.

c. In **Password**, type the password to log in to vCenter.

d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

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

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

PSC must have a valid certificate.

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

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

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

The system generates the certificate and adds vCenter.

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

Related links

Editing vCenter on page 111
Map vCenter field descriptions on page 112
New vCenter and Edit vCenter field descriptions on page 113

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:

- Select an ESXi host and click the edit icon ().

- Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.

7. Click **Commit** to get an updated list of managed and unmanaged hosts.

   If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

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

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

Table continues…

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

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

New vCenter and Edit vCenter field descriptions

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

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

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.

Table continues…

Name	Description
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the desktop, click the SDM icon (), and then click **Application Management**.
3. In the lower pane, click **Job History**.

4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

   The page displays the details of jobs that you selected.

Related links

Job History field descriptions on page 115

Job History field descriptions

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

History

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

Related links

Viewing the job history of virtual machine operations on page 114

Managing syslog profiles

Adding a remote Syslog server profile

About this task

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

Before you begin

To view the Syslog data from AVP Utilities or application, ensure that:

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

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. Click **Application Management**.
3. In the lower pane, click **Configure Remote Syslog Profile**.
4. On the Syslog Receiver Configuration page, click **Add**.

   System Manager displays the Add Syslog Receiver dialog box
5. In **Profile Name**, type the profile name of the Syslog server.
6. In **IP/FQDN**, type the IP address or FQDN of the Syslog server.
7. In **Port**, type the port of the Syslog server.
8. In **Protocol**, click **TCP** or **UDP**.
9. If the remote host is TLS based, select **TLS Authentication**.
10. In **Authentication options**, click **Server certificate authentication** or **Mutual TLS authentication**.
11. Click **Save**.

Syslog Receiver Configuration field descriptions

Name	Description
Profile Name	The name of the Syslog server configuration.
IP/FQDN	The IP address or host name of the Syslog server configuration.
Port	The port number of the Syslog server configuration. The default port is 514.
Protocol	The type of port used for the Syslog server configuration. The options are: • **TCP** • **UDP** When the **tcp** protocol is selected, the system enables the **TLS Authentication** option.

Table continues…

Name	Description
TLS Authentication	The option to select if the remote host is TLS based. When **TLS Authentication** is selected, the system displays the following options: • **Server certificate authentication** • **Mutual TLS authentication** When you select **TLS Authentication**, the port value is 6514.
Server certificate authentication	The server certificate authentication. This option is available, if **TLS Authentication** is selected.
Mutual TLS authentication	The mutual certificate authentication. This option is available, if **TLS Authentication** is selected.

Button	Description
Add	Displays the Add Syslog Receiver dialog box where you can add the Syslog server configuration.
Edit	Displays the Add Syslog Receiver dialog box where you can edit the configuration of the selected Syslog server.
Delete	Deletes the selected Syslog server configuration.

Pushing system logs to Syslog servers

About this task

Use this procedure to a send log files to Syslog servers.

From Release 8.1, you can push more than one Syslog profiles to Syslog servers

Note:

The feature to push, view, and delete syslog server profile on virtual machine is supported only for AVP Utilities, System Manager (through Solution Deployment Manager Client), and Session Manager applications.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **Push**.
5. In the Push Syslog Configuration dialog box, select one or more Syslog profile, and click **Push**.

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

Viewing configured Syslog servers

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **View**.
5. In the View Syslog Configuration dialog box, select the required Syslog profile to view it.

Deleting configured Syslog servers

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **Delete**.
5. In the Delete Syslog Configuration dialog box, select the required Syslog profile, and click **Delete**.
6. On the confirmation dialog box, click **Yes**.

Chapter 9: Pre-staging

Pre-staging overview

With Release 10.1, the Solution Deployment Manager client supports the Pre-staging feature to prestage the System Manager OVA, service pack or feature pack, or data migration utility files to deploy, upgrade, or update only the System Manager application. If you are on a low bandwidth zone, this is a recommended option to prestage the data.

Note:

The Pre-staging feature is supported to deploy, upgrade, and update System Manager on the Appliance Virtualization Platform Release 8.1.x and earlier system, VMware ESXi, and vCenter platforms.

Prestage process

If you plan to deploy, upgrade, or update System Manager by using the Pre-staging feature, the process has to be completed in two phases:

1. Create a prestaging job. You can create:
   - Prestaging job to upload and store the files on the datastore of the host.

     Note:

     For upgrade, some files are also stored on the old System Manager system.
   - Local prestaging job to store the files on the local system in the `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts` folder.

   You can create, view status, cancel, retry, and delete the prestaging job by using the Solution Deployment Manager client.
2. Select the prestaged files by using the **Browse Pre-stage Location** option while deploying, upgrading, or updating System Manager.

Related links

[Deploying the System Manager OVA file by using the Pre-staging feature of Solution Deployment Manager Client](#) on page 132

[Upgrading System Manager from Release 8.1.x or 10.1.x to Release 10.2.x by using the Pre-staging feature of Solution Deployment Manager Client](#) on page 135

[Installing service packs and software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client](#) on page 138

Creating a prestaging job

Creating a prestaging job for deployment

About this task

Use this procedure to create the prestaging job to upload and store the OVA and service or feature pack files on the datastore of the host that you can use while deploying System Manager.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Click **New**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click **Deployment**.
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.
8. In the Location and Platform Details section, do the following:
   a. In **Select Location**, click the location of the host.
   b. In **Select Platform**, click the platform name.

      When you select the platform name, Solution Deployment Manager fetches the host details and populates the data store configured on the host in **Datastore**.
   c. In **Select Prestage Folder**, click **Browse**.

      Solution Deployment Manager displays the DataStore Explorer window.
9. In the DataStore Explorer window, do one of the following:
   - To select the prestage folder location, navigate to the required folder, and click **Submit**.

     While selecting a folder on the VMware datastore ensure that the folder is empty.
   - To create a new prestaging folder location, click **New**.

     While creating a new folder, do not select any folder that has virtual machine files in it.
     a. In Folder Select, in **Enter Folder Name**, type the folder name, click **OK**.

b. Click **Submit**.

Solution Deployment Manager displays the Status pop-up message with the path of the prestage folder.

c. Click **OK**.

10. Click **Next**.
11. On the **OVA** tab, click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager OVA file.
    - **SW Library**, in the **File Name** field, select the System Manager OVA file.

    To use the **SW Library** option, the System Manager OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
12. To upload and store the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack file.
    - **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

    To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
13. Click **Submit**.

    Solution Deployment Manager creates the prestaging job on the Pre-Staging page.

Creating a prestaging job for upgrade

About this task

Use this procedure to create the prestaging job to upload and store the service or feature pack and datamigration bin file on the datastore of the host that you can use while upgrading System Manager.

Note:

For upgrade, the files are also stored on the old System Manager system.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.

4. Click **New**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click **Upgrade**.
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.
8. In the Location and Platform Details section, do the following:
   a. In **Select Location**, click the location of the host.
   b. In **Select Platform**, click the platform name.

      When you select the platform name, Solution Deployment Manager fetches the host details and populates the data store configured on the host in **Datastore**.
   c. In **Virtual Machine**, click the System Manager virtual machine.

      The **Virtual Machine** field is applicable only when you select the **Upgrade** prestage operation type.

      Ensure that you selected the platform on which the System Manager virtual machine is residing.
   d. In **Select Prestage Folder**, click **Browse**.

      Solution Deployment Manager displays the DataStore Explorer window.
9. In the DataStore Explorer window, do one of the following:
   - To select the prestage folder location, navigate to the required folder, and click **Submit**.

     While selecting a folder on the VMware datastore ensure that the folder is empty.
   - To create a new prestaging folder location, click **New**.

     While creating a new folder, do not select any folder that has virtual machine files in it.
     a. In Folder Select, in **Enter Folder Name**, type the folder name, click **OK**.
     b. Click **Submit**.

        Solution Deployment Manager displays the Status pop-up message with the path of the prestage folder.
     c. Click **OK**.
10. Click **Next**.
11. To upload and store the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack file.

- **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

  To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.

12. To upload and store the data migration bin file, click the **Datamigration bin** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager data migration bin file.
    - **SW Library**, in the **File Name** field, select the System Manager data migration bin file.

      To use the **SW Library** option, the System Manager data migration bin file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
13. Click **Submit**.

    Solution Deployment Manager creates the prestaging job on the Pre-Staging page.

Creating a prestaging job for update

About this task

Use this procedure to create the prestaging job to upload and store the OVA, service or feature pack and datamigration bin files on the datastore of the host that you can use while updating System Manager.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Click **New**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click **Update**.
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.

8. In the Location and Platform Details section, do the following:
   a. In **Select Location**, click the location of the host.
   b. In **Select Platform**, click the platform name.

      When you select the platform name, Solution Deployment Manager fetches the host details and populates the data store configured on the host in **Datastore**.
   c. In **Select Prestage Folder**, click **Browse**.

      Solution Deployment Manager displays the DataStore Explorer window.
9. In the DataStore Explorer window, do one of the following:
   - To select the prestage folder location, navigate to the required folder, and click **Submit**.

     While selecting a folder on the VMware datastore ensure that the folder is empty.
   - To create a new prestaging folder location, click **New**.

     While creating a new folder, do not select any folder that has virtual machine files in it.
     a. In Folder Select, in **Enter Folder Name**, type the folder name, click **OK**.
     b. Click **Submit**.

        Solution Deployment Manager displays the Status pop-up message with the path of the prestage folder.
     c. Click **OK**.
10. Click **Next**.
11. On the **OVA** tab, click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager OVA file.
    - **SW Library**, in the **File Name** field, select the System Manager OVA file.

      To use the **SW Library** option, the System Manager OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
12. To upload and store the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack file.
    - **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

      To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.

13. To upload and store the data migration bin file, click the **Datamigration bin** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager data migration bin file.
    - **SW Library**, in the **File Name** field, select the System Manager data migration bin file.

      To use the **SW Library** option, the System Manager data migration bin file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
14. Click **Submit**.

    Solution Deployment Manager creates the prestaging job on the Pre-Staging page.

Creating a local prestaging job

About this task

Use this procedure to create the local prestaging job so that you can store the OVA, service or feature pack, metadata, or data migration utility files on your local system.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Click **Advanced** > **Local Pre-staging**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click one of the following:
   - **Deployment**
   - **Upgrade**
   - **Update**
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.
8. In the Parent Folder Details section, Solution Deployment Manager displays the path of the local prestage parent folder.

The default path for the local pre-stage folder is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

9. Click **Next**.
10. On the **OVA** tab, click one of the following:

    Solution Deployment Manager enables the **OVA** tab when you select the **Deployment** or **Upgrade** prestage operation type.

    - **Local Path**, in the **URL** field, type the absolute path of the System Manager OVA file.
    - **SW Library**, in the **File Name** field, select the System Manager OVA file.

      To use the **SW Library** option, the System Manager OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.

11. To upload the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:

    Solution Deployment Manager enables the **Service or Feature Pack** tab when you select the **Deployment**, **Upgrade**, or **Update** prestage operation type.

    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack.
    - **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

      To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.

12. To upload the data migration utility file, click the **Datamigration bin** tab, and click one of the following:

    Solution Deployment Manager enables the **Datamigration bin** tab when you select the **Upgrade** prestage operation type.

    - **Local Path**, in the **URL** field, type the absolute path of the System Manager data migration bin file.
    - **SW Library**, in the **File Name** field, select the System Manager data migration bin file.

      To use the **SW Library** option, the System Manager data migration bin file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.

13. Click **Submit**.

    Solution Deployment Manager saves the files on the local system at `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

    - For the local prestage deployment, the files are stored in the `<SMGROVAfile><JobID>_PRE-STAGING` folder.

This folder contains the `Vmware_datastore_files` folder and the `Instructions` file.

- For the local prestage upgrade, the files are stored in the `<SMGROVAfile><JobID>_PRE-STAGING` folder.

  This folder contains the `Vmware_datastore_files` folder, the `Old_SMGR_files` folder and the `Instructions` file.

- For the local prestage update, the files are stored in the `PATCH_<JobID>_PRE-STAGING` folder.

  This folder contains the `Vmware_datastore_files` folder that has the `Instructions` file and the patch file in `sdmpatch.iso`.

Next steps

1. Upload the locally stored prestaged files to the data store of the host.
2. Use the **Browse Pre-stage Location** option to select these files at the time of deploying, upgrading, or updating System Manager.

Viewing the status of the prestaging job

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Select a prestaging job and click **View Status**.

   System Manager displays the status of the prestage job in the Prestage Job Status window.

Canceling a prestaging job

About this task

When the status of a prestaging job is **IN-PROGRESS** or **PARTIALLY-COMPLETED**, Solution Deployment Manager enables the **Cancel** button.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Select a prestaging job and click **Cancel**.

   System Manager displays the following message:

   ```
   This will cancel the prestage and delete corresponding files from
   the datastore. Do you really want to continue?
   ```
5. To proceed, click **Yes**.

   Solution Deployment Manager cancels the selected prestaging job and deletes the corresponding files.

Retrying the configuration of a prestaging job

About this task

When the status of the prestaging job is **Failed**, Solution Deployment Manager enables the **Retry** button.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Select a prestaging job and click **Retry**.

   By default, you can retry the creation of prestaging job up to 3 times.

   System Manager retries the prestaging job creation.

Deleting a prestaging job

About this task

When the status of a prestaging job is either **Completed** or **Failed**, Solution Deployment Manager enables the **Delete** button.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Select a prestaging job and click **Delete**.

   System Manager displays the following message:

   ```
   This will delete the prestage and corresponding files from the
   datastore. Do you really want to continue?
   ```
5. Click **Yes**.

   Solution Deployment Manager deletes the selected prestaging job and the corresponding files.

Pre-staging Job field descriptions

Name	Description
Name	Specifies the prestaging job name.
Operation Type	Specifies the operation type for the prestaging job. The options are: • **PRESTAGE-DEPLOY** • **PRESTAGE-UPGRADE** • **PRESTAGE-UPDATE** • **LOCAL-PRESTAGE-DEPLOY** • **LOCAL-PRESTAGE-UPGRADE** • **LOCAL-PRESTAGE-UPDATE**
Location	Specifies the prestaging job location.
Platform Name	Specifies the platform name.
Prestage Location	Specifies the prestaged file location.

Table continues…

Name	Description
Current Action Status	Specifies the progress of the prestaging job. The options are: • **COMPLETED**: When the prestaging job is successfully completed. • **FAILED**: When the prestaging job is failed. • **IN-PROGRESS**: When the prestaging job is inprogress. • **PARTIALLY-COMPLETED**: When the prestaging job is partially completed. • **NOT-STARTED**: When the prestaging job is not yet started. • **CANCEL-IN-PROGRESS**: When the cancellation of the prestaging job is in-progress. • **CANCELLED**: When the prestaging job is canceled. • **DELETE-IN-PROGRESS**: When the deletion of the prestaging job is in-progress.

Button	Description
New	Displays the Application Pre-Stage window for creating the prestage job for deploying, upgrading, or updating System Manager.
View Status	Displays the status of the prestage job.
Cancel	Cancels the prestage job.
Retry	Retries the prestage job. By default, you can retry the creation of prestaging job up to 3 times.
Delete	Deletes the selected prestage job.
Advanced > **Local Pre-staging**	Displays the Application Pre-Stage window for creating the local prestage job for deploying, upgrading, or updating System Manager.

Application Pre-Stage field descriptions

Select Pre-Stage Operation Type

Name	Description
Select Pre-Stage Operation	You can create the pre-staging job for deploying, upgrading, or updating System Manager. The options are: • **Deployment** • **Upgrade** • **Update**

Prestage Details: Job Details

Name	Description
Name	The pre-staging job name.
Description	The pre-staging job description.

Prestage Details: Parent Folder Details

When you select the **Advanced** > **Local Pre-staging** option, Solution Deployment Manager displays this section.

Name	Description
Local Pre-stage Parent Folder	The path of the local prestage parent folder. The default path for the local pre-stage folder is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

Prestage Details: Location and Platform Details

When you select the **Advanced** > **Local Pre-staging** option, Solution Deployment Manager does not display this section.

Name	Description
Select Location	The location name.
Select Platform	The platform name that you must select.
Virtual Machine	The virtual machine name. **Note:** The **Virtual Machine** field is available only when you select the **Upgrade** prestage operation type.
Datastore	The data store of the platform. The page populates the capacity details in the Capacity Details section.
Select Prestage Folder	You can click the **Browse** button to display the DataStore Explorer window and to select the pre-staging folder. When you click **New**, you can create a new prestaging folder.
New	Displays the Folder Select dialog box.
Enter Folder Name	Specifies the prestaging folder name.
Submit	Saves the prestaging folder path and displays next to the **Select Prestage Folder** field.

Select Artifacts

Based on the selected Select Pre-Stage Operation Type option, Solution Deployment Manager displays one or more of the following tabs. You can specify either the local path or the Software library path for the System Manager OVA, service pack, or data migration file.

- **OVA**

Solution Deployment Manager enables the **OVA** tab when you select the **Deployment** or **Upgrade** prestage operation type.

- **Service or Feature Pack**

  Solution Deployment Manager enables the **Service or Feature Pack** tab when you select the **Deployment**, **Upgrade**, or **Update** prestage operation type.

- **Datamigration bin**

  Solution Deployment Manager enables the **Datamigration bin** tab when you select the **Upgrade** prestage operation type.

Name	Description
Local Path	The option to specify the absolute path from where you can get the System Manager OVA, service pack, or data migration bin file.
URL	Specify the absolute path from where you can get the System Manager OVA, service pack, or data migration bin file.
SW Library	The option to specify the absolute path of the software library from where you can get the System Manager OVA, service pack, or data migration bin file. You can save the files in the `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts` folder.
File Name	The option to select the System Manager OVA, service pack, or data migration bin file.

Button	Description
Submit	Saves the prestaging job.

Deploying the System Manager OVA file by using the Pre-staging feature of Solution Deployment Manager Client

About this task

Use the procedure to deploy System Manager by using the Pre-staging feature of Solution Deployment Manager Client.

For more information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

Before you begin

- Install the Solution Deployment Manager client on your computer.
- Add a location.

  For information, see Adding a location on page 30.

- Add the required host.

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

For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 110.

- Create a prestaging job for deployment.

  For more information, see “Creating a prestaging job for deployment”.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Host <host name> section, click **New**.

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

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

   The Capacity Details section displays the capacity details.
6. Click **Next**.
7. On the **OVA** tab, click **Browse Pre-stage Location**, and do the following:
   a. In **Select Pre-stage Directory**, click **Browse**.
   b. In the DataStore Explorer dialog box, select the data store folder where the System Manager OVF file are stored, and click **Select**.

      For information about prestaging the System Manager files, see “Creating a prestaging job for deployment”.
   c. To validate the checksum of the OVA file, click **Validate checksum of OVA files**.

   This option is enabled when you deploy System Manager in the VMware virtualized environment. This option is applicable only for System Manager.

   When you select the OVA, the system:

   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
8. To install the System Manager bin file, click **Service or Feature Pack**, and do the following:
   a. Click **Browse Pre-stage Location**.
   b. In **Select Pre-stage Directory**, click **Browse**.

c. In the DataStore Explorer dialog box, select the data store folder where the System Manager bin file is stored, and click **Select**.

For information about prestaging the System Manager files, see “Creating a prestaging job for deployment”.

You can install the System Manager Release 10.2.x bin file now or after completing the System Manager OVA deployment.

If you do not provide the System Manager Release 10.2.x patch file at the time of deploying the System Manager OVA, the system displays the following message:

```
Installation of the latest System Manager patch is mandatory. Are
you sure you want to skip the patch installation?
If Yes, ensure to manually install the System Manager patch later.
```

9. Click **Next**.

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

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

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

11. In the Network Parameters section:

- For Appliance Virtualization Platform, the system auto populates the following fields and these fields are read only:
  - **Public**
  - **Out of Band Management**
- For the ESXi host, select the required port groups.

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

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

Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.

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

Next steps

To configure System Manager, log on to the System Manager web console. At your first log in, change the System Manager web console credentials.

Update the user password for the system to synchronize the data from applications.

When System Manager is operational, you can use Solution Deployment Manager from System Manager to deploy all other Avaya Aura® applications or continue to use the Solution Deployment Manager client.

Upgrading System Manager from Release 8.1.x or 10.1.x to Release 10.2.x by using the Pre-staging feature of Solution Deployment Manager Client

About this task

The procedure describes the steps to upgrade System Manager by using the Pre-staging feature of Solution Deployment Manager Client.

For more information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

- Appliance Virtualization Platform-based System Manager Release 8.1.x to System Manager Release 10.2.x

  Note:

  From Release 10.1 and later, Appliance Virtualization Platform is no longer available. Therefore, if System Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.1 before upgrading System Manager to Release 10.2. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

- VMware-based System Manager Release 8.1.x or 10.1.x to System Manager Release 10.2.x

Before you begin

- Install Solution Deployment Manager Client.

  For information, see Installing the Solution Deployment Manager client on your computer on page 13.

- Add a location.

  For information, see Adding a location on page 30.

- Add the ESXi, vCenter, Appliance Virtualization Platform, or Avaya Solutions Platform 130 host.

  For information about adding the host, see “Managing the platform”.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 110.

  Important:

  - If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

    For information about the supported ESXi version, see Supported ESXi version on page 21.

    For information about upgrading ESXi, see the VMware product documentation.

  - If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.

- If the application is running on the server that is not supported with Release 10.2.x, then deploy Avaya Solutions Platform 130.

  For information about supported servers, see Supported servers for Avaya Aura applications on page 20.

- Create a prestaging job for upgrade.

  For more information, see “Creating a prestaging job for upgrade”.

- Select the System Manager 8.1.x or 10.1.x virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For more information, see Re-establishing trust for Solution Deployment Manager elements on page 69.

- Obtain the System Manager software. See “Software details of System Manager”

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Upgrade Management**.
4. On the Upgrade Management page, select the System Manager virtual machine.
5. Click **Upgrade**.
6. In **Platform FQDN**, select the required host.

   If the system prompts for the certificate, accept the certificate. When you accept the certificate, the system displays the following message: `Certificate added successfully in trust store.`
7. **(Optional)** Select the datastore on the host.

   If more than one datastore is available, select the datastore.

   If the host is part of a VMware cluster, the system displays the following message:

   `Host is in a cluster. Therefore, capacity details of CPU and memory are unavailable! Ensure that the host resource requirements are met before any action.`

   For information about resource details, see Supported footprints of System Manager on VMware on page 103.
8. Click **Next**.
9. On the **OVA** tab, click **Browse from Datastore**, and do the following:
   a. In **Select Pre-stage Directory**, click **Browse**.
   b. In the DataStore Explorer dialog box, select the data store folder where the System Manager OVF file are stored, and click **Select**.

For information about prestaging the System Manager files, see “Creating a prestaging job”.

This option is enabled when you upgrade System Manager in the VMware virtualized environment. This option is applicable only for System Manager.

When you select the OVA, the system:

- Displays the CPU, memory, and other parameters in the Capacity Details section.
- Disables the **Flexi Footprint** field.

10. To upload the latest service or feature pack, click Data Migration, and do the following:
    a. Click **Browse from Datastore**.
    b. In **Select Pre-stage Directory**, click **Browse**.
    c. In the DataStore Explorer dialog box, select the data store folder where the System Manager bin file is stored, and click **Select**.

       For information about prestaging the System Manager files, see “Creating a prestaging job for upgrade”.
11. To upload the latest service or feature pack, click **Service or Feature Pack**, and do the following:
    a. Click **Browse from Datastore**.
    b. In **Select Pre-stage Directory**, click **Browse**.
    c. In the DataStore Explorer dialog box, select the data store folder where the latest System Manager data migration utility file is stored, and click **Select**.

       For information about prestaging the System Manager files, see “Creating a prestaging job for upgrade”.
12. Click **Next**.
13. In the Config Parameters section, provide the required details.

    Note:

    Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.

    For information, see “Upgrade Management field descriptions”.
14. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
15. Click **Upgrade** and accept the license terms.

    The system takes the backup, shuts down the existing virtual machine (VM), deploys the OVA file, and restores the data on the new virtual machine.
16. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 100–150 minutes depending on the data on System Manager.

Note:

The upgrade process might involve multiple reboots during data migration. If you have selected the checkbox **Require Encryption Pass-Phrase at Boot-Time**, you must monitor the VM console for reboots and enter the **Encryption Pass-Phrase** promptly.

If you fail to enter the **Encryption Pass-Phrase** timely, the upgrade process may timeout and fail. If this happens, restart the upgrade process.

17. Do one of the following:
    - If the upgrade is successfully completed, do the following:
        a. Verify that the new System Manager virtual machine is functional.

           For more information, see “Verifying the functionality of System Manager”.

        b. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

           The system deletes the old virtual machine.

        c. Click **Commit**.

           The system deletes the old virtual machine.
    - If the upgrade fails or you want to revert to the old system, then do the following:
        a. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

        b. Click **Rollback**.

           The system deletes the newly created virtual machine and starts the old virtual machine.

        c. Again refresh both the host to get the latest virtual machine information.

Next steps

Install the valid license file for System Manager Release 10.2.x.

Installing service packs and software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client.

For more information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

Before you begin

- Install the Solution Deployment Manager client.
- Create a prestaging job for update.

  For more information, see “Creating a prestaging job for update”.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the Applications for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. Click **More Actions** > **Refresh App**.

   If **Refresh App** is disabled or fails, proceed to next step.
6. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **More Actions** > **Refresh App**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
7. Click **More Actions** > **Update App**.

   If Solution Deployment Manager detects a previous uncommitted patch, the system displays a dialog box with **Commit** and **Rollback**. You need to either commit previous uncommitted patch or rollback. Only after this, the system displays the System Manager Update dialog box to provide the patch file.
8. Click **Browse Pre-stage Location** and do the following:
   a. In **Select Pre-stage Directory**, click **Browse**.
   b. In the DataStore Explorer dialog box, select the data store folder where the System Manager patch file is stored, and click **Select**.

      For information about prestaging the System Manager files, see “Creating a prestaging job for update”.
9. **(Optional)** Click the **Auto commit the patch** check box.
10. Click **Install**.

    In the Applications for Selected Location <location name> section, the system displays the status.
11. To view the details, in the **Current Action** column, click **Status Details**.

SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.

12. On the Installed Patches page, do the following:
    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.

    b. Click **Get Info**.
    c. Select the patch, service pack or feature pack, and click **Commit**.

Chapter 10: Uninstalling the Solution Deployment Manager client

Uninstalling the Solution Deployment Manager client using Windows Control Panel

About this task

Use the procedure to uninstall the client by using Add/Remove Programs or Uninstall or change a program from `Control Panel\Programs\Programs and Features`.

Uninstall the Solution Deployment Manager client before you install a new version of the client on your computer.

Procedure

1. In the Run window, type `control`, and click **Programs and Features**.
2. In the Programs and Features window, select **AvayaSDMClient** and click **Uninstall/ Change**.
3. In the Change AvayaSDMClient Installation window, click **Uninstall**.
   - If the windows displays an uninstallation error, manually uninstall the Solution Deployment Manager client.

     For more information, see “Uninstalling the Solution Deployment Manager client manually”.
   - If the installer detects that some of the files and folders are still in use, and is unable to delete the files, you must manually delete the files. If required, reboot the machine.

Related links

Uninstalling the Solution Deployment Manager client manually on page 142

Uninstalling the Solution Deployment Manager client manually

About this task

Use the procedure to uninstall the client manually, if you are unable to remove the client by using Add/Remove Programs, Uninstall. or change a program from `Control Panel\Programs\Programs and Features`.

Uninstall the Solution Deployment Manager client before you install a new version of the client on your computer.

Procedure

1. In the Run window, type `services.msc`, and stop the Solution Deployment Manager service.

   If the Solution Deployment Manager service does not stop properly, reboot the machine.

2. At the windows command prompt, log in as administrator, and type `sc delete sdm` to delete the Solution Deployment Manager service.

3. Delete the following registry entry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\SDMClient
   ```

4. Delete the Solution Deployment Manager client installation directory and the content in the directory.

   If the client is installed at the default location, then delete `C:\Program Files\Avaya\AvayaSDMClient`.

5. Delete the Solution Deployment Manager client shortcut from the `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avaya\AvayaSDMClient` location and the desktop.

Chapter 11: Resources

System Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

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

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list

8. In **Choose Release**, select the required release number.
9. 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.
10. Press **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation 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 keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  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 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 the 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 in to the website. The available functionality depends on your role.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you login to the website, enter the course code or the title in the **Search** field and click **Go** 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®
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager Release 10.1
61451V	Administering Avaya Aura® Communication Manager Release 10.1

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 keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 147

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.

4. Enter your **PASSWORD** and click **Sign On**.

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

Related links

Support on page 147

Appendix A: Adding Avaya Solutions Platform 130 using the services port

Adding an Avaya Solutions Platform 130 Dell R640 Server in Solution Deployment Manager Client through the Services port

About this task

This section includes the steps for adding the Avaya Solutions Platform 130 (ASP 130) server into the Solution Deployment Manager client for the application OVA deployment.

Procedure

1. Download and install the SDM client on your computer or laptop.

   For more information about installing SDM Client, see Installing the Solution Deployment Manager client on your computer on page 13.

2. Ensure that the computer is connected to the services port of the ASP 130 server.

   For more information, see the “ASP 130 Installation Configuration Script” section in the *Installing the Avaya Solutions Platform 130 Series* Release 5.0 document.

   Note:

   The ASP 130 Installation Configuration Script is formerly known as the Services Port Script.

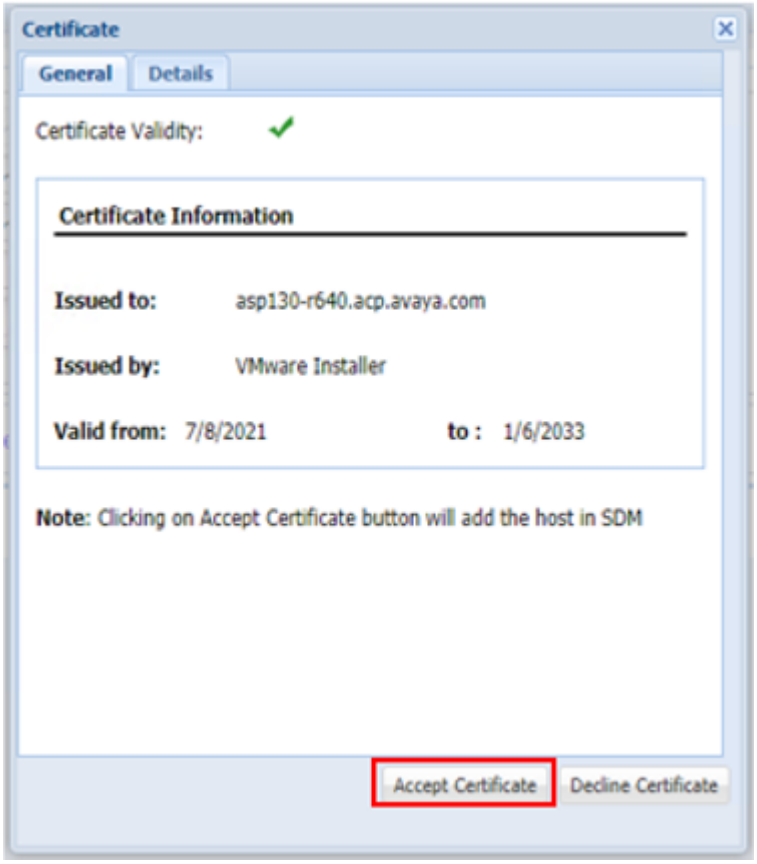
3. Start the Solution Deployment Manager client.
   a. Click **Application Management**.
   b. Add a location.
   c. To add the ASP130 (ESXi) host, on the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.

      Important:

      When adding the ASP 130 host in SDM Client, use the FQDN as ASP 130 is an ESXi deployment. If the FQDN cannot be resolved with the DNS Server, you

have to edit the `/etc/hosts` file on the computer or laptop to include the host information. For more information, see Adding the ASP 130 host information into the /etc/hosts file on page 151

d. Click **Save** and then click **Accept Certificate**.



Important:

- If you receive a certificate error when trying to add the ASP 130 server, see Regenerating the self-signed certificate on an ASP 130 host on page 152 to overcome the issue if an SSL certificate is used.
- Third-party CA signed certificates are supported on the ASP 130 server and can be successfully added into SDM Client by using a CA signed certificate. The certificate must use or include the FQDN, as the host can only be added

into SDM using the FQDN. IP address is not supported. If a CA signed certificate is required to be regenerated, see the “Certificate Administration” section in the *Installing the Avaya Solutions Platform 130 Series* Release 5.0 document.

- A license must be installed on the ASP 130 ESXi host to successfully add the host in SDM Client.

4. After the ASP 130 server is added into SDM Client, deploy the supported applications.

Related links

Adding the ASP 130 host information into the /etc/hosts file on page 151
Regenerating the self-signed certificate on an ASP 130 host on page 152

Adding the ASP 130 host information into the /etc/hosts file

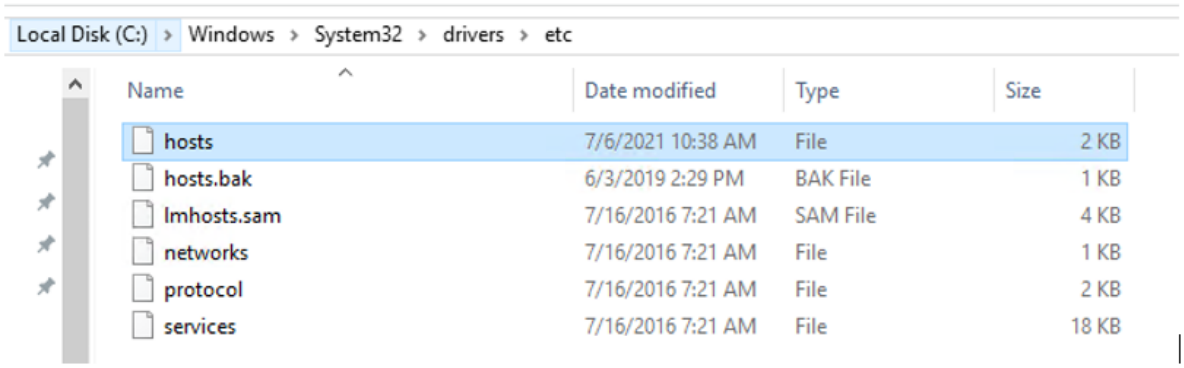
About this task

This section covers the procedure for adding the ASP 130 ESXi host information into the installer’s computer, laptop, or `/etc/hosts` file to resolve the FQDN of the host. When adding a host in SDM Client, use the FQDN as ASP 130 is an ESXi deployment. Do not use the IP Address and 192.11.13.6.

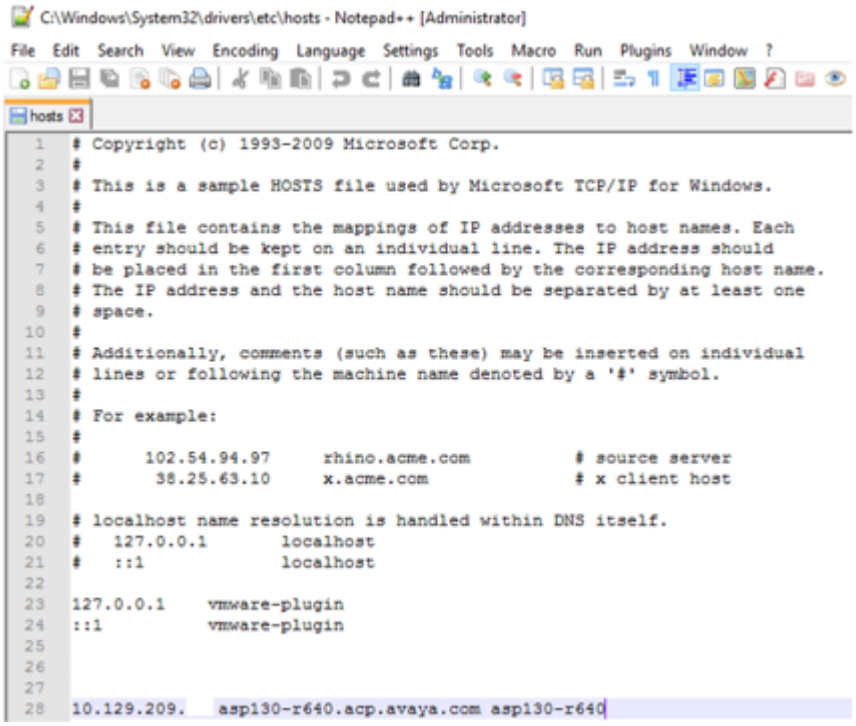
Procedure

1. From the computer or laptop, open a Windows Explorer window.
2. Go to **Local Disk (C:)** > **Windows** > **System32** > **drivers** > **etc**.
3. Right-click the **hosts** file and select **edit**.

   A text editor of choice can be used. For example, Notepad++, notepad.



4. In the hosts file, add the ESXi host IP address, FQDN, and a short host name.



5. To save the changes, go to **File** and click **Save,**.

Related links

[Adding an Avaya Solutions Platform 130 Dell R640 Server in Solution Deployment Manager Client through the Services port](#) on page 149

Regenerating the self-signed certificate on an ASP 130 host

About this task

This section covers the procedure to regenerate the self-signed certificate on an ASP 130 ESXi host, if it fails with a certificate error while adding the server into SDM Client.

Note:

- This activity can be conducted remotely and does not affect the service for the virtual machines running on the ESXi host. It is still strongly recommended to conduct this activity in a customer approved maintenance window, during off-peak business hours.
- The ESXi host is not required to be entered into maintenance mode to conduct this activity.

Warning:

Avoid administrative tasks such as, creating backups, taking VM snapshots, or making any configuration changes to the ESXi host when conducting this activity.

Before you begin

Ensure you have the following:

- Access to the ASP 130 server management network through the direct services port connection onsite
- SSH tool (that is, PuTTY)
- Root password for server access

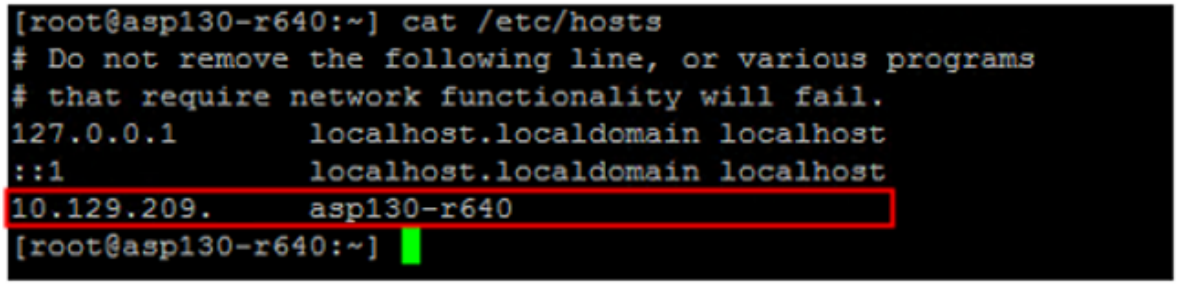
Procedure

1. SSH in to the ASP 130 host using PuTTY. Log in with the root credentials.
2. Run the following command to confirm if the host FQDN and host name are present:

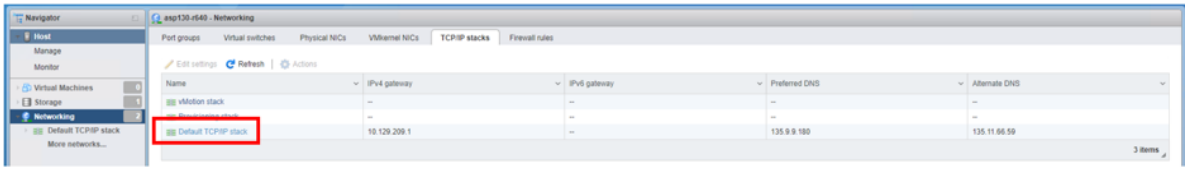
   ```
   cat /etc/hosts
   ```

   If the FQDN and host name are defined, proceed to step 9.

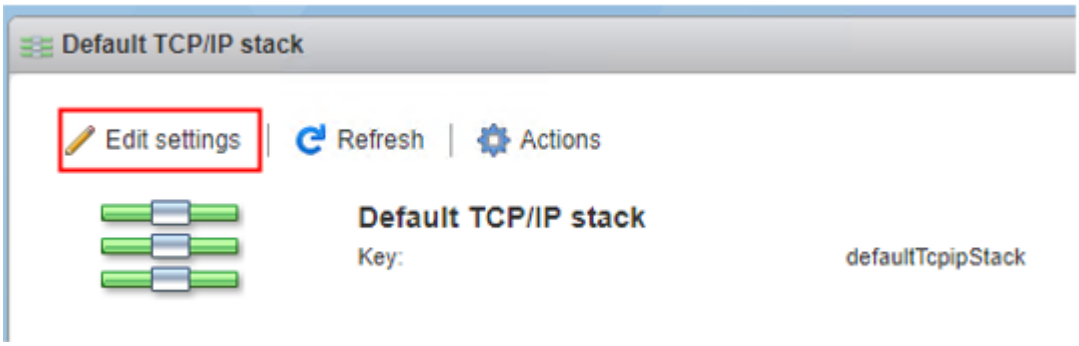
   If the FQDN and host name are not defined, proceed to the next step.

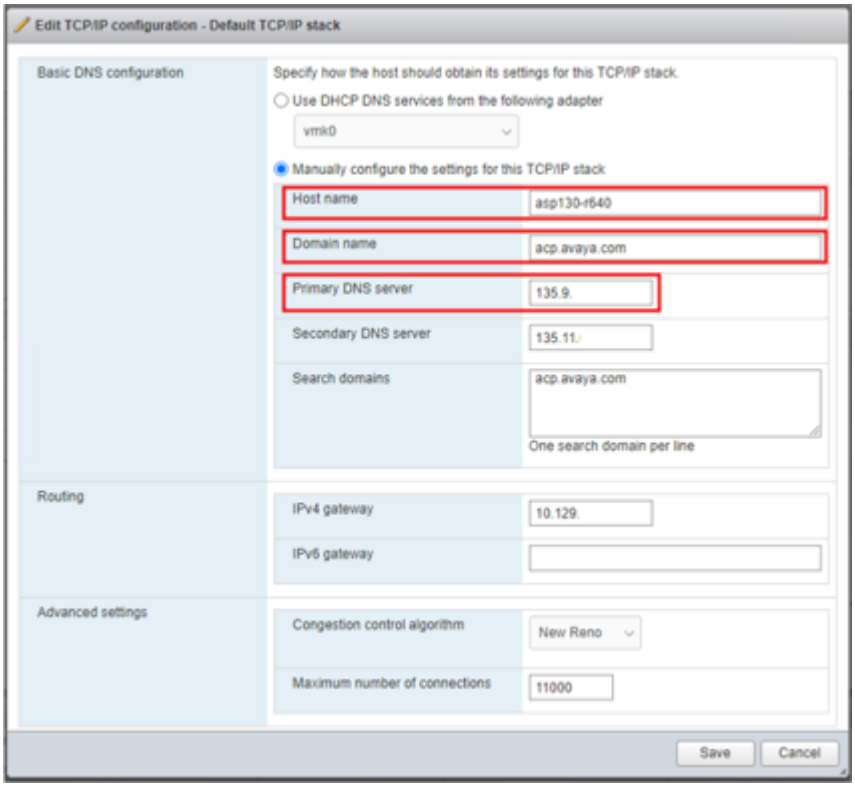
3. Log in to the ASP 130 host through the vSphere Web Client with the root credentials.
4. Go to **Networking** > **TCP/IP stacks** > **Default TCP/IP stack**.

5. Click **Edit settings**.

6. If the **Host name**, **Domain name**, and **Primary DNS server** fields are blank, type the required information.



7. Click **Save** to apply the changes.
8. Return to the SSH session and run the following command to confirm that the IP, FQDN, and host name are now present in the `/etc/hosts` file of the ESXi host:

   `cat /etc/hosts`

```
[root@asp130-r640:~] cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain localhost
::1             localhost.localdomain localhost
10.129.209.     asp130-r640.acp.avaya.com asp130-r640
[root@asp130-r640:~]
```

9. Type `cd /etc/vmware/ssl` to change the directory, and back up the existing certificates by renaming them using the following commands:

   `mv rui.crt orig.rui.crt`

   `mv rui.key orig.rui.key`

Note:

If this is a fresh install with a factory staged ASP 130 server, it is not required to copy these certificate files.

```
[root@asp130-r640:~] cd /etc/vmware/ssl
[root@asp130-r640:/etc/vmware/ssl] ls
castore.pem               rui.key                   vsan_kms_client_old.crt
iofiltervp.pem            vsan_kms_castore.pem      vsan_kms_client_old.key
iofiltervp_castore.pem    vsan_kms_castore_old.pem  vsanvp_castore.pem
openssl.cnf               vsan_kms_client.crt
rui.crt                   vsan_kms_client.key
[root@asp130-r640:/etc/vmware/ssl] mv rui.crt orig.rui.crt
[root@asp130-r640:/etc/vmware/ssl] mv rui.key orig.rui.key
[root@asp130-r640:/etc/vmware/ssl] ls
castore.pem               orig.rui.key              vsan_kms_client_old.crt
iofiltervp.pem            vsan_kms_castore.pem      vsan_kms_client_old.key
iofiltervp_castore.pem    vsan_kms_castore_old.pem  vsanvp_castore.pem
openssl.cnf               vsan_kms_client.crt
orig.rui.crt              vsan_kms_client.key
[root@asp130-r640:/etc/vmware/ssl]
```

10. To generate new certificates, type the following command:

    /sbin/generate-certificates

```
[root@asp130-r640:/etc/vmware/ssl] /sbin/generate-certificates
[root@asp130-r640:/etc/vmware/ssl] ls
castore.pem               orig.rui.key              vsan_kms_client.crt
iofiltervp.pem            rui.crt                   vsan_kms_client.key
iofiltervp_castore.pem    rui.key                   vsan_kms_client_old.crt
openssl.cnf               vsan_kms_castore.pem      vsan_kms_client_old.key
orig.rui.crt              vsan_kms_castore_old.pem  vsanvp_castore.pem
[root@asp130-r640:/etc/vmware/ssl]
```

11. To restart the hostd Management Agent service on the ESXi host, type the following command:

    /etc/init.d/hostd restart

12. After the host restarts, to power on the VMs, click **VM** > **Go to Actions** > **Power** > **Power on**.

13. Return to the SSH session and confirm that the host successfully generated new certificates by running the following commands:

    cd /etc/vmware/ssl

    openssl x509 -in rui.crt -noout -text

```
[root@asp130-r640:/etc/vmware/ssl] openssl x509 -in rui.crt -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 129272060197376 (0x75927f3a3a00)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=VMware Installer
        Validity
            Not Before: Jul  8 15:16:36 2021 GMT
            Not After : Jan  6 15:16:36 2033 GMT
        Subject: C=US, ST=California, L=Palo Alto, O=VMware, Inc, OU=VMware ESX Server De
fault Certificate/emailAddress=ssl-certificates@vmware.com, CN=asp130-r640.acp.avaya.com/
unstructuredName=1625757396,564d77617265520496e632e
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Confirm in the subject the CN= entry displays the FQDN of the ASP 130 host.

14. Launch the SDM client to add the ASP 130 as an ESXi host and accept the certificate.
15. Deploy the supported application OVAs on the ASP 130 host.

Related links

Adding an Avaya Solutions Platform 130 Dell R640 Server in Solution Deployment Manager Client through the Services port on page 149

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W