Upgrading Avaya Aura® Session Manager

Release 7.1.3
Issue 5
August 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This guide describes the procedures for upgrading the software of an Avaya Aura® Session Manager server from Release 6.x, and Release 7.x to Release 7.1.3.

The primary audience for this guide is anyone who is involved with upgrading and verifying Session Manager.

Change history

Issue	Date	Summary of changes
5	August 2019	Updated the following sections: • Upgrading Session Manager or Branch Session Manager from Release 7.1 to 7.1.3 on VMware through Solution Deployment Manager on page 115 • Upgrading Session Manager from Release 6.x or 7.0.x to 7.1.3 using data migration utility on VMware on page 122
4	May 2018	Updated the ISO filename for the release 7.1.3.
3	December 2017	Updated the ISO filename for the release 7.1.2.
2	August 2017	Updated the ISO filename for the release 7.1.1.
1	May 2017	Release 7.1

Chapter 2: Upgrade overview

The supported direct upgrade paths to Avaya Aura® Session Manager 7.1 are:

- Session Manager 6.0 SP1 and subsequent service packs
- Session Manager 6.1 and subsequent service packs
- Session Manager 6.2 and subsequent service packs.
- Session Manager 6.3 and subsequent service packs.
- Session Manager 7.0 and subsequent service packs.
- Session Manager 7.1 and subsequent service packs.

You must upgrade systems running any earlier version of Session Manager to one of the above releases before you upgrade to Session Manager Release 7.1.x.

To upgrade the Session Manager to Release 7.1.3, upgrade the Session Manager to Release 7.1, and apply Session Manager Release 7.1.3 feature pack to Session Manager Release 7.1.

For information about installing a new Session Manager server, see *Deploying Avaya Aura® Session Manager*.

Schedule the upgrade during hours of little or no system activity. The active call count of Session Manager determines when the upgrade must occur. Ideally, the active call count must be zero.

During an upgrade, the call processing traffic of the Session Manager server that is getting upgraded is handled by the other Session Managers. Calls that are active when the upgrade takes place will remain active. However, the Session Manager server denies any changes to the SIP session, for example, transferring the call.

Note:

- If you upgrade from Release 6.3.x to Release 7.1 using Solution Deployment Manager, the call logs are stored and backed up automatically.
- If you upgrade from Release 6.3.x to Release 7.1 in the VMware virtualized environment, you need to manually back up the call logs.

  For information about backing up the call history using User Data Storage, see *Administering Avaya Aura® Session Manager*.

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

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

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

Third party certificates earlier than Session Manager Release 6.3 are not stored. You must administer these certificates again after upgrade.

Branch Session Manager upgrade overview

See the PCN issued for the Session Manager software release. The Branch Session Manager (BSM) upgrade, in some cases, could involve upgrading Communication Manager Survivable Remote templates as outlined in the document, *Upgrading to Avaya Aura® Communication Manager*. See Product notifications on page 145 for more information about PCNs and PSNs.

Note:

If you are upgrading an active Branch Session Manager, ensure that Branch Session Manager is administered on System Manager and the **Enrollment Password** is active. Before installing or upgrading the Branch Session Manager, ensure that all the Branch Session Managers are configured in DNS or added to the`/etc/hosts` file on System Manager. Also, ensure that the date and time is in sync between System Manager and System Platform. A clock shift can cause certificate and DRS replication problems. You must upgrade Branch Session Manager to be the same level as the core Session Manager.

An example of the contents of the `/etc/hosts` file is:

```
123.45.6.78       bsm.co.avaya.com bsm
123.45.6.88      core-asm1.ca.avaya.com core-asm1
```

The first entry is the IP address, the second entry is the FQDN, and the third entry is the short hostname (FQDN without the domain name).

Feature pack to release mapping

Avaya Aura® Feature Pack	Avaya Aura® Session Manager Release
Avaya Aura® 6.2 Feature Pack 1	Session Manager 6.3
Avaya Aura® 6.2 Feature Pack 2	Session Manager 6.3.2
Avaya Aura® 6.2 Feature Pack 3	Session Manager 6.3.4
Avaya Aura® 6.2 Feature Pack 4	Session Manager 6.3.8

Table continues…

Avaya Aura® Feature Pack	Avaya Aura® Session Manager Release
Avaya Aura® 7.0 Feature Pack 1	Session Manager 7.0.1
Avaya Aura® 7.1 Feature Pack 1	Session Manager 7.1.1
Avaya Aura® 7.1 Feature Pack 2	Session Manager 7.1.2
Avaya Aura® 7.1 Feature Pack 3	Session Manager 7.1.3

Supported servers

Session Manager supports the following servers:

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

Branch Session Manager supports the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- HP ProLiant DL360 G9
- S8300D
- S8300E

These supported servers are only for Appliance Virtualization Platform configurations.

Avaya no longer supports the S8510 and S8800 servers. Any S8510 or S8800 server can be migrated to a supported server using the server replacement procedure.

Note:

Switching cables within a network is must for a Session Manager instance prior to release 7.0.

Supported web browsers

System Manager supports the following web browsers:

- Internet Explorer 11.x
- Firefox 48.0
- Firefox 49.0
- Firefox 50.0

Available media

Avaya provides the following media for Session ManagerRelease 7.1.3:

- Session Manager iso file: `Session_Manager_7.1.3.0.xxxxxx.iso`

Removal of default certificates

Starting with Session Manager Release 6.3.8, Avaya SIP CA issued certificates are no longer supported for new installations. Default certificates, also known as demo certificates, are non-unique identity certificates that were automatically installed on newly shipped Session Manager servers. Default certificates are not secure and do not meet current NIST standards.

New Session Manager servers no longer use the Avaya SIP Product CA issued Default Certificates. New customer networks can request an Identity Certificate from the System Manager Trust Management that is signed by the System Manager Certificate Authority.

For upgrades, Session Manager preserves the previous certificate. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Avaya recommends that customers use the newer certificates as soon as possible.

If you must restore a demo certificate, see Restoring the default SIP Identity Certificate on page 13.

Restoring the default SIP Identity Certificate

Restore the default certificate issued by the SIP CA on the selected Session Manager. You can reinstall demo certificates to quickly restore a previously working environment.

Procedure

1. Log into the Session Manager CLI.

2. Enter the command `initTM --demo`.
3. At the warning message prompt, enter `y`.

   The message `Trust Management initialization completed successfully.` appears when the default certificate has installed.

System component upgrade sequence

Upgrade the system components using the following sequence:

1. Endpoints
2. System Manager. For upgrade information, see:
   - *Upgrading and Migrating Avaya Aura® applications from System Manager*
   - *Deploying Avaya Aura® System Manager*
   - *Deploying Avaya Aura® applications from System Manager*
3. Session Managers in the core
4. Avaya Aura® Device Services
5. Survivable Remote Session Managers or Branch Session Managers in the branches and Communication Manager Survivable Remote Processor (formerly known as Local Survivable Processors)
6. Presence servers
7. Avaya Communication Server 1000
8. Service Providers are optional
9. Decommissioned NRS servers
10. Media gateways
11. Communication Manager Survivable Core Processor
12. Communication Manager feature servers and evolution servers

For Communication Manager upgrades, including the feature servers, evolution servers, Survivable Core Processors, and Survivable Remote Processors, see the Avaya Aura® Communication Manager documentation on the Avaya Support site.

Add a secondary Session Manager or Branch Session Manager after you complete the upgrades to the system components.

If an application is deployed on Appliance Virtualization Platform, use the following sequence to upgrade:

- The Appliance Virtualization Platform host
- Utility Services

- System Managervirtual machine or any other application on Appliance Virtualization Platform

System component upgrade sequence for systems that include Geographic Redundant System Manager configuration

Upgrade system components in a Geographic Redundant System Manager-enabled configuration using the following sequence.

Procedure

1. Upgrade endpoints.
2. Upgrade System Managers:
   a. Disable replication between the primary and the secondary System Managers.
   b. Activate the secondary System Manager.
   c. Upgrade the primary System Manager.

      During this process, the secondary System Manager manages the elements.
   d. Start the primary System Manager.
   e. Deactivate the secondary System Manager.
   f. Upgrade the secondary System Manager.

      During this process, the primary System Manager manages the elements.
   g. For restoring the secondary server, perform recovery on the primary server using the secondary server database.
   h. Enable replication between the primary and secondary servers.

      For more information about upgrading the System Manager servers, see:

      - *Upgrading Avaya Aura® System Manager*
      - *Deploying Avaya Aura® System Manager*
   i. Synchronize System Manager data with the Communication Manager system.
3. Upgrade the Session Managers in the core.
4. Upgrade Avaya Aura® Device Services.
5. Upgrade the Survivable Remote Session Managers or Branch Session Managers in the branches and Survivable Remote Communication Manager
6. Presence servers.
7. Upgrade the Communication Server (CS) 1000 server.

8. Upgrading Service Providers is optional.
9. Upgrade Decommissioned NRS servers.
10. Upgrade Media gateways.
11. Upgrade the Communication Manager Core Survivable Processor.
12. Upgrade the Communication Manager feature servers and evolution servers.

Chapter 3: Preupgrade tasks

Configuring the User settings

Obtaining a company ID

Before you begin

Ensure that you have access and user credentials to log in to the PLDS website at https://plds.avaya.com.

Procedure

1. On the web browser, type the PLDS URL, `https://plds.avaya.com`.
2. In the **Email address** field, enter the user name, and in the **Password** field, enter the password.
3. Click **Submit**.
4. After successful log in, on the Home page, select **Administration** > **My Company**.

The system displays the company ID followed by a company name.

Establishing PLDS connection to Avaya

About this task

Use the procedure to configure the location from where System Manager displays information about the latest software and firmware releases during Analyze operation. The entitlements depend on the credentials that you provide on the **User Settings** page.

Before you begin

- Obtain a company ID to configure PLDS.
- Add the required ports and websites to a firewall of customer.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **User Settings**.
3. On the User Settings page, click **Edit**.
4. Select the **Use Avaya Support Site** check box, and provide the SSO user name and SSO password for PLDS, and the company ID.
5. Configure the PLDS settings and proxy settings for the software download.
6. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.
7. Click **Commit**.

Related links

User Settings field descriptions on page 19

User Settings field descriptions

Source configuration

Field	Description
Use Avaya support site	The option to find the information and download the software releases from the Avaya support site. **Note:** • To download the firmware and analyze the software on System Manager, you must gain access to `plds.avaya.com` `pldsxml.avaya.com`, and `downloads.avaya.com`. • Select the **Use Avaya Support Site** check box, to use **Avaya Support Site**. Enter the SSO user name, SSO password, and the Company ID. The SSO authentication is required to get entitlements for **Analyze** and artifacts for download. • If you select the check box, the **Alternate Source** is unavailable.
Alternate Source	The website location from where you can get the latest software. The alternate source is an HTTP URL and an alternate to the Avaya support site. You must set the alternate source. For more information, see *Setting up an alternate source*. **Note:** • The XML files compare the available software version and the latest available version in PLDS. • Clear the **Use Avaya Support Site** check box, to use alternate source repository. You must enter a http URL, for example `http://148.147.216.220/SUMDATA/`. • The IP address of the alternate source can be the same as the IP address of the software library. However, ensure that the URL location and the server path for software library configuration are different.

PLDS configuration

Field	Description
SSO User Name	The user name used as a single sign on for PLDS.

Table continues…

Field	Description
SSO Password	The single sign on password for PLDS.
Confirm SSO Password	The SSO password that you retype in this field.
Company ID	The company ID for PLDS. For more information, see Obtaining a company ID.

Proxy settings

You require proxy settings to use the Avaya PLDS and the Avaya support site. If your network configuration requires a proxy, enter the details in the **Proxy Settings** section.

Field	Description
Use Proxy	The option to use the proxy server for PLDS.
Host	The host name of the proxy.
Port	The port of the proxy.
Password	The password of the proxy server for the Avaya support site.
Confirm Password	The password of the proxy server that you retype for the Avaya support site.

Button	Description
Edit	To display the edit page where you can change the user settings.
Commit	To save the user settings that you enter.
Reset	To reset the page and clear the values that you enter.
Cancel	To cancel your action and return to the previous page.

Related links

Establishing PLDS connection to Avaya on page 18

Creating a software library

Before you begin

Note:

You cannot set System Manager as a software library. You must set an external server as a software library.

For more information about configuring external server as a remote software library, see *Administering Avaya Aura® System Manager*.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **New**.
4. Complete the Add Software Library page.
5. Click **Commit**.
   - To reset the page, click **Clear Configuration**.

Downloading the OVA file to System Manager

About this task

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. Click **Download**.

      The system displays the Upload File page.
5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.
8. Provide a valid file type.

   This system uploads the OVA file from local computer to the designated software library on System Manager.

Note:

If the file type is invalid, System Manager displays an error.

Solution Deployment Manager upgrades and updates

Refreshing elements

Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

  Note:

  Use the same SNMP credentials for the device in System Manager.

- On the User Settings page, configure the user settings.
- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left 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 left 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.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, select an element from the list.

4. In the left navigation pane, click **Download Management**.

   The system displays the File Download Manager page.

5. To change the display settings, click one of the following:

   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.

6. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
7. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

   The time to complete the refresh operation depends on the source configuration in **User Settings**.

8. Click **Show Files**.
9. In **Select Files Download Details**, do the following:

   a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.

   b. Select the files that you want to download.

   c. Click **Download**.

      In File Download Status, the system displays the file that you selected for download.

File Download Manager field descriptions

Select Software/Hardware Types

Name	Description
Family Name	The name of the device family.
Hardware/Software	The name of the associated software or hardware.

Select Files Download Details

Name	Description
Source	The source from where Download Manager gets the software or firmware files. The options are: • **Avaya PLDS/Alternate Source** • **My Computer**

Name	Description
File name	The file name.
Version	The file version.
Entitled	The file entitlements.
File Size (in bytes)	The file size in bytes.
Hardware/Software	The name of the hardware or the software
Family Name	The name of the device family.
Content Type	The type of the content.
Software Library	The status of the file download.
File Description	A description of the file that you download.

Button	Description
Refresh Families	Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page. **Note:** When you add or update details in the `versions.xml` file, you must click **Refresh Families** to get the updated information.
Show Files	Displays the files associated with the element that you selected.

File Download Status

Name	Description
File Name	The file name of the software or firmware file.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.
Status	The status of the download activity.
Scheduled By	The user who scheduled the download job.

Button	Description
Delete	Deletes the files that you have selected.

Performing the preupgrade check

Procedure

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

2. In the left navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   Note:

   To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.
5. 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.
6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

Preupgrade Configuration field descriptions

Pre upgrade Configuration Parameters

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

Table continues…

Name	Description
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

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

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

Chapter 4: Virtual machine management

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

VM Management provides the following capabilities:

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

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

Managing the location

Viewing a location

Procedure

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

   The Locations section lists all locations.

Adding a location

About this task

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

Procedure

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

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

Editing the location

Procedure

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

Deleting a location

Procedure

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

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

VM Management field descriptions

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

Locations

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

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

Hosts

Name	Description
Host Name	The name of the host.
Host IP	The IP address of the host.
Host FQDN	FQDN of the host.
IPv6	The IPv6 address of the host. If the IP address of the ESXi host is an IPv4 address, the column does not display any value.
vCenter FQDN	FQDN of vCentre.
Current Action	The operation that is currently being performed on the host.
Last Action	The last completed operation on the host.
License Status	The status of the license.
Host Version	The host version.

Table continues…

Name	Description
Offer Type	The host type. The options are: • **AVP**: Appliance Virtualization Platform host • **Customer VE**: customer-provided VMware ESXi host
SSH Status	The SSH service status. The values are enabled and disabled.
Host Certificate	The certificate status of the Appliance Virtualization Platform host. The values are: • : The certificate is added in Solution Deployment Manager and correct. • : The certificate is not accepted or invalid. You can click **View** for details of the certificate status.
vCenter Certificate	The certificate status of the ESXi host. The values are: • : The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • : The certificate is not accepted or invalid. You can click **View** for details of the certificate status.

Note:

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

Button	Description
Auto Refresh	The option to automatically refresh the page with the latest changes. For example, the page updates: • The VM state when a virtual machine changes • The license status or certificate status of host when host changes The system refreshes the data every minute.
Add	Displays the New Host section where you can provide the details of the host that you want to add.
Edit	Displays the Host Information section where you can change the details of an existing host.
Remove	Removes the hosts that you select only from the Solution Deployment Manager client. The system moves the hosts associated with the deleted locations to unknown location.

Table continues…

Button	Description
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.
More Actions > **AVP Update/Upgrade Management**	Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **SSH** > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays `SSH enabled successfully`.
More Actions > **SSH** > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the virtual machine host. Also Syslog is only for Appliance Virtualization Platform. You can select multiple Hosts and Push syslog configuration on selected hosts.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view syslog profiles of selected the Appliance Virtualization Platform host.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
More Actions > **Lifecycle Actions** > **Host Restart**	Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Lifecycle Actions** > **Host Shutdown**	Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.

Table continues…

Button	Description
More Actions > **AVP Cert. Management** > **Generate/Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the host. Depending on the host type, the options are: • **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only. • **Accept Certificate**: To accept a valid certificate for the host or vCenter. • **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate.
More Actions > **AVP Cert. Management** > **Manage Certificate**	Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected host.
More Actions > **AVP Cert. Management** > **Generic CSR**	Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.
More Actions > **Snapshot Manager**	Displays the Snapshot Manager dialog box from where you can view and delete the virtual machine snapshot.
More Actions > **WebLM Configuration**	Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.
More Actions > **Set Login Banner**	Displays the Message of the Day dialog box from where you can push the login banner text to the selected host. **Note:** This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support **Set Login Banner**.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM IPv6	The IPv6 address of the virtual machine, if any.

Table continues…

Name	Description
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.1.
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the VMware host or Appliance Virtualization Platform host on which the virtual machine resides.
Trust Status	The status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store name.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machine from host and Solution Deployment Manager Client.
Start	Starts the selected virtual machines.
Stop	Stops the selected virtual machines.
Show Selected	Displays only the selected virtual machines.

Table continues…

Button	Description
More Actions > **Restart**	Starts the selected virtual machines that were stopped earlier.
More Actions > **Refresh VM**	Updates the status of the virtual machines.
More Actions > **Re-establish connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected virtual machine.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.

Table continues…

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

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

Managing the host

Adding an Appliance Virtualization Platform or ESXi host

About this task

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

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

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

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

Before you begin

A location must be available.

Procedure

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

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

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

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

   Important:

   When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.
8. On the **Hosts** tab, select the required host and click **Refresh**.

Next steps

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

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

3. Once you have performed a trust establishment and refresh host operation on all virtual machines, you can perform refresh operation on the host.

Editing an ESXi host

Procedure

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

   The system updates the ESXi host information.

Upgrading Appliance Virtualization Platform from Solution Deployment Manager

About this task

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

Note:

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

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

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

(Gateway 192.168.13.1). If you connect the system using the Utility Services services port (Gateway 192.11.13.1), the Appliance Virtualization Platform update or upgrade fails.

Before you begin

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

Note:

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

Procedure

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

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

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

   Enable: (Recommended)

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

   Disable:

   ```
   By disabling Avaya Logins you are preventing Avaya access to your
   system.
   This is not recommended, as it impacts Avaya’s ability to provide
   ```

```
support for the product. Unless the customer is well versed in
managing the product themselves, Avaya Logins should not be
disabled.
```

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

   Avaya recommends to enable EASG.

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

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

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

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

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

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

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

Next steps

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

Changing the network parameters for an Appliance Virtualization Platform host

About this task

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

Note:

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

Procedure

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

4. In the Host Network/ IP Settings section, change the IP address, subnetmask, and other parameters as appropriate.

   Note:

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

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

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

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

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

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

   The system updates the Appliance Virtualization Platform host information.

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

About this task

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

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

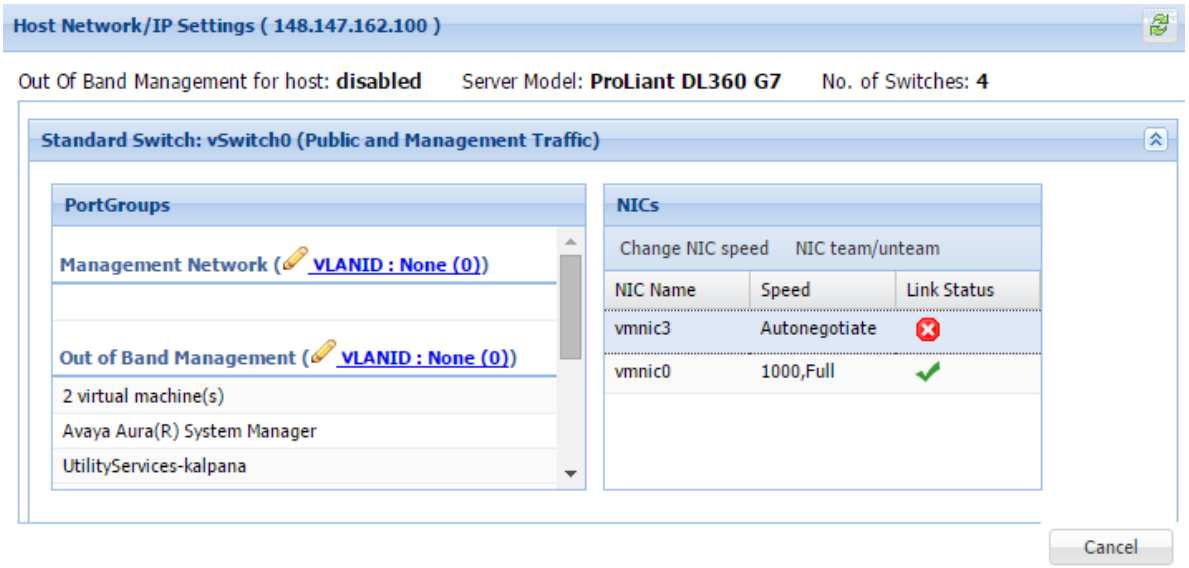
Note:

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

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

Procedure

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



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

You can configure port groups for the following switches:

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

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

      The section displays the vSwitch details.

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

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

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

For more information about the value, see NIC teaming.

d. Click **OK**.

The system displays the new VLAN ID.

Note:

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

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

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

b. Click **Change NIC speed**.

The system displays the selected vmnic dialog box.

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

d. Click **OK**.

For more information, see VLAN ID assignment.

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

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

Note:

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

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

a. Select a vmnic.

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

The system displays the Out of Band Management Properties page.

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

For more information, see NIC teaming modes.

d. Click **OK**.

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

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

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

The system displays the current status of the vmnic.

Note:

You cannot perform NIC teaming for S8300D and S8300E servers.

Changing the password for an Appliance Virtualization Platform host

About this task

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

Procedure

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

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

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

Password policy

The password must meet the following requirements:

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

Examples of invalid passwords:

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

Example of a valid password: myPassword!1ok

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

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

Generating the Appliance Virtualization Platform kickstart file

Procedure

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

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

Create AVP Kickstart field descriptions

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

Table continues…

Name	Description
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300D and E only)	VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on S8300D and S8300E servers.
Out of Band Management Setup	The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • **yes**: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • **no**: To disable Out of Band Management. The default option.
OOBM vLAN ID (Used on S8300D and E only)	Out of Band Management VLAN ID for S8300D. Use **OOBM VLAN ID** only on the S8300D server. • For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Confirm Password	Admin password for Appliance Virtualization Platform.

Table continues…

Name	Description
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain 14 characters.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

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

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

About this task

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

Procedure

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

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

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

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

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

About this task

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

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

Before you begin

Start an SSH session.

Procedure

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

   The system displays the following options:

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

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

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

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

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

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

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

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

Changing the IP address and default gateway of the host

About this task

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

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

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

Before you begin

Connect the computer to the services port.

Procedure

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

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

   For example:

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

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

   For example:

   ```
   esxcfg-route 135.27.162.1
   ```

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

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

Appliance Virtualization Platform license

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

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

To configure the Appliance Virtualization Platform license file:

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

   Note:

   The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance Virtualization Platform license file contains all the necessary licenses for the complete solution.

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

Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

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

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

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

  Note:

  Restricted administrative actions for:

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

Appliance Virtualization Platform licensing alarms

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

Configuring WebLM Server for an Appliance Virtualization Platform host

Before you begin

1. Add an Appliance Virtualization Platform host.

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

Procedure

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

2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions** > **WebLM Configuration**.

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

   For WebLM configuration, if you select:

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

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

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

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

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

WebLM Configuration field descriptions

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

Button	Description
Submit	Saves the WebLM Server configuration.

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

Procedure

1. Perform one of the following:
   - On the System Manager Web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - On the desktop, click the SDM icon (), and then click **VM Management**.

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

Shutting down the Appliance Virtualization Platform host

About this task

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

Procedure

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

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

Removing an ESXi host

Procedure

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

Configuring the login banner for the Appliance Virtualization Platform host

About this task

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

Procedure

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

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

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

Mapping the ESXi host to an unknown location

About this task

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

Procedure

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

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

   The system displays the ESXi host in the selected location.

Applying third-party AVP certificates

Applying third-party Appliance Virtualization Platform certificates

About this task

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

Before you begin

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

Procedure

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

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

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

e. Click **Generate CSR**.

The system generates CSR for the Appliance Virtualization Platform host.

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

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

5. To download CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. Click **Download CSR**.
   c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   d. To view the status, in the **Upgrade Status** column, click **Status Details**.

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

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

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

Creating or editing generic CSR

About this task

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

Procedure

1. In VM Management Tree, select a location.
2. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.

3. Click **More Actions** > **AVP Cert. Management** > **Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

Next steps

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

Load AVP host certificate field descriptions

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

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

Create or edit CSR field descriptions

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

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

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

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

Procedure

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

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

   The system deletes the selected snapshots.

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.

New and Edit host field descriptions

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

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

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IPv4	The IPv4 address of the Appliance Virtualization Platform host.
Subnet Mask	The subnet mask the Appliance Virtualization Platform host.
IPv6	The IPv6 address of the Appliance Virtualization Platform host (if any).

Table continues…

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

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

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

Host Network / IP Settings field descriptions

Port Groups

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

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

NIC speed

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

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

NIC teaming

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

Button	Description
Move Up	Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.
Move Down	Moves the VMNIC from active to standby adapter or from standby to unused adapter.

Table continues…

Button	Description
Refresh	Refreshes the page.
OK	Saves the changes.

Change Password field descriptions

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

Button	Description
Change Password	Saves the new password.

Update Host field descriptions

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

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

Managing vCenter

Adding a vCenter to Solution Deployment Manager

About this task

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

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

Before you begin

Ensure that you have the required permissions.

Procedure

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

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

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

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

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

      PSC must have a valid certificate.

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

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

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

   The system generates the certificate and adds vCenter.

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

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

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

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

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

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

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

The system deletes the vCenter from the inventory.

Map vCenter field descriptions

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

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

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

New vCenter and Edit vCenter field descriptions

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

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

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.

Table continues…

Name	Description
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

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

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

Managing the virtual machine

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

About this task

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

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

Before you begin

- Complete the deployment checklist.

  For information about the deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.
- Add a location.

- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file

Procedure

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

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

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

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

      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Flexi Footprint**, select the footprint size that the application supports.
      - **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
      - **Default**: For all other server platforms.
8. Click **Next**.

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

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

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

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

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

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

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

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

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

14. Reboot the Utility Services virtual machine.

Next steps

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

Deploying an OVA file for an Avaya Aura® application

About this task

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

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

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

Before you begin

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

Procedure

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

The system displays the VM Deployment section.

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

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

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

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the message: `Invalid file content. Avaya Certificate not found or invalid`.
8. In **Flexi Footprint**, select the footprint size that the application supports.
9. **(Optional)** To install the patch file for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
   - Click **URL**, and provide the absolute path to the latest service or feature pack.
   - Click **S/W Library**, and select the latest service or feature pack.
   - Click **Browse**, and select the latest service or feature pack.

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

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

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

    For each application that you deploy, fill the appropriate fields. For more information, see “VM Deployment field descriptions”.

13. Click **Deploy**.
14. Click **Accept the license terms**.

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

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

Next steps

Re-establishing trust for Solution Deployment Manager elements

About this task

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

Before you begin

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

Procedure

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

Installing software patches

About this task

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

Note:

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

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

Before you begin

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

Procedure

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

   Note:

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

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

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

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

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

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

    The page displays all software patches that you can commit.

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

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

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

    Note:

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

Editing a virtual machine

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
  - Utility Services must be available and must be discovered.

- If Utility Services is discovered, the system must display Utility Services in the **VM App Name** column. If the application name in **VM App Name** is empty, perform the following to establish trust between the application and System Manager:
  - Click **More Actions** > **Re-establish connection**.
  - Click **More Actions** > **Refresh VM**.

Procedure

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

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

   Important:

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

      Note:

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

      Note:

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

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

Deleting a virtual machine

Procedure

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

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

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

About this task

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

Before you begin

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

Note:

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

Procedure

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

4. In the Network Parameters section, change the following as appropriate, and click **Save**:
   - IP address, subnetmask, and other parameters
   - Gateway IP address

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

   For more information, see *Administering Avaya Aura® application* available for each application. Also, see “Network Parameters for Avaya Aura® applications”.
6. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services:
   a. In the Edit VMs section, select a virtual machine and click **Edit**.
   b. Click **Update IP/FQDN in Local Inventory**.
   c. Click **Update VM IP/FQDN**.
   d. Provide the IP address and FQDN of the virtual machine.

      Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.
7. Click **Save**.
8. Do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services :
   a. Click **More Actions** > **Re-establish connection**.

      Note:

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

      Note:

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

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

Updating Services Port Static Routing on an Avaya Aura® application

About this task

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

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

Before you begin

- Update network parameters of Utility Services if applicable.
- Ensure that the Avaya Aura® application resides on the same subnetwork as Utility Services.

Procedure

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

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

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

Starting a virtual machine from Solution Deployment Manager

Procedure

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

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

Stopping a virtual machine from Solution Deployment Manager

About this task

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

Procedure

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

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

Restarting a virtual machine from Solution Deployment Manager

Before you begin

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

Procedure

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

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

Common causes for VM deployment failure

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

- Provided an IP which is not on the network.

- Provided wrong network values that causes the network configuration for the VM to not work properly
- Chosen a private virtual network

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

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

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

VM Deployment field descriptions

Select Location and Host

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

Capacity Details

The system displays the CPU and memory details of the host. The fields are read-only.

Note:

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

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

Deploy OVA on System Manager Solution Deployment Manager

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment.
Enable enhanced security	The option to enable JITC mode deployment.
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy. **Note:** System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.
Flexi Footprint	The footprint size supported for the selected host. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA on the Solution Deployment Manager client

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

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

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

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

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

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

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

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

The system displays the following common fields.

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

Configuration Parameters

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

Note:

For configuration parameter fields, for Communication Manager Messaging and Utility Services, see VM Deployment Configuration and Network Parameters field descriptions on page 84.

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

Table continues…

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

Table 1: Configuration Parameters for Communication Manager simplex OVA deployment

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

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 WebLM. 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.
Services	The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Out of Band Management	The port number that is mapped to the out of band management port group.

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

VM Deployment Configuration and Network Parameters field descriptions

Table 2: Configuration Parameters for Communication Manager Messaging deployment

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

Configuration and Network Parameters for Utility Services deployment

Name	Description
Networking Properties	

Table continues…

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

Table continues…

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

Table continues…

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

Table continues…

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

Update Static Routing field descriptions

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

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

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

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

Update VM field descriptions

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

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

Reestablish Connection field descriptions

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

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

Network parameter update for Avaya Aura® applications

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

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

Tip:

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

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

Table continues…

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

Virtual machine report

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

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

Important:

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

generate_report.sh command

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

Syntax

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

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

Generating a virtual machine report

Before you begin

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

Procedure

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

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

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

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

   Note:

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

Viewing the status of the virtual machine report

Procedure

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

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

Aborting the virtual machine report generation

About this task

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

Procedure

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

   The system aborts the virtual machine report generation process.

Monitoring a host and virtual machine

Monitoring a host

Procedure

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

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

Monitoring a virtual machine

Procedure

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

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

4. Click **Generate Graph**.

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

Generating and accepting certificates

About this task

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

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

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

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

Before you begin

Require permissions to add a host to generate certificates.

Procedure

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

      Note:

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

   b. Click **Accept Certificate**.

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

Next steps

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

Certification validation

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

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

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

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

  Note:

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

- Log Certificate Validation Events

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

For the correct certificate:

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

If the certificate is incorrect:

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

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

Note:

Solution Deployment Manager:

- Validates certificate of vCenter

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

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

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

Chapter 5: Upgrading Session Manager to Release 7.1.3

About this task

Important:

- Upgrade the Session Manager servers one at a time to limit service degradation and outages.
- Schedule the upgrade during hours of little or no system activity.
- Most SIP endpoints are assigned to a primary and a secondary SIP Proxy Server (Session Manager). When upgrading the primary Session Manager, the endpoint does not lose service because the secondary Session Manager handles the call. However, Avaya Flare® endpoints only have one Session Manager and lose service during the upgrade.
- Verify firewall settings when performing a system installation or upgrade. For more information, see the Avaya Aura® Port Matrix document for Avaya Aura® Session Manager at https://downloads.avaya.com/css/P8/documents/100182023.

Checklist for upgrading Session Manager or Branch Session Manager from Release 6.x, 7.x to 7.1.3

Use this checklist for upgrading Session Manager or Branch Session Manager on a same server or on a different server.

#	Task	Notes	✔
1	Download the Appliance Virtualization Platform ISO image: `avaya-avp-7.1.0.0.0.xx.iso`. If required, apply the Appliance Virtualization Platform patch.	See Downloading software from PLDS on page 103.	
2	Make a note of the network parameters, IP address, Netmask, default gateway, DNS, NTP, and Timezone details.		

Table continues…

#	Task	Notes	✔
3	Upgrade System Manager to Release 7.1.3.	See *Upgrading Avaya Aura® System Manager* .	
4	Verify the **Enrollment Password** field is still active.	See Verifying Enrollment Password status on page 104.	
5	Archive existing logs to an external server.	Create a log harvester profile and submit a request to archive the logs. See Archiving logs on page 147.	
6	Configure user settings to establish PLDS connection.	Configuring user settings on page 18	
7	Create a remote software library.	Creating a software library on page 20	
8	For Branch Session Manager upgrade: • Administer SNMP Agent, on Communication Manager Survivable Remote (LSP) • Add the Communication Manager Survivable Remote (LSP) details on the System Manager Inventory page. • Add System Platform Console Domain details on the System Manager Inventory page. **Note:** The steps to add Communication Manager Survivable Remote (LSP) are not required for Session Manager upgrade.	• See Administering SNMP Agent on page 104 • See Adding a Communication Manager instance to System Manager on page 106	

Table continues…

#	Task	Notes	✔
9	Download the required software. • Download the Session Manager OVA: `SM-7.1.0.0.xxxxxx-e65-01.ova`. • Download the Branch Session Manager OVA: `BSM-7.1.0.0.xxxxxx-e65-01.ova`. • Download the Communication Manager Simplex OVA: `CM-<Simplex>-07.1.0.0.xx-e65-0.ova`. • Download the Utility Services OVA: `US-7.1.0.0.0.xx-e65-01_OVF10.ova`. • For LSP patch upgrade, download the Communication Manager patch file: `00.0.441.0-xxxxx.tar` • For Session Manager patch upgrade, download the iso file: `Session_manager_7.1.3.0.xxxxxx.iso`	See Downloading the software on page 23	
10	Refresh the elements.	See Refreshing elements in the inventory on page 22	
11	Analyze	See Analyzing inventory using Solution Deployment Manager on page 23	
12	Perform the pre-upgrade check.	See Performing the pre upgrade check using SDM on page 25	
13	Perform the upgrade.	If you are upgrading Session Manager to a different server the upgrade will be successful. See Upgrading Session Manager or Branch Session Manager from Release 6.x to 7.1 through SDM on page 112. **Note:** If you are upgrading Session Manager on the same server proceed with the following steps.	

Table continues…

#	Task	Notes	✔
14	Install Appliance Virtualization Platform on the server.	See Installing Appliance Virtualization Platform on page 111 **Note:** When there are two different subnets, after post installation of Appliance Virtualization Platform, swap the cables. This Note is applicable when you are upgrading Session Managerfrom Release 6.x to 7.x.. For information about NIC teaming, see *Migrating and Installing Avaya Appliance Virtualization Platform*.	
15	Add the ESXi host using the System Manager VM Management page.	See Virtual machine management on page 28.	
17	Perform the upgrade.	See Upgrading Session Manager or Branch Session Manager from Release 6.x to 7.1 through SDM on page 112.	

Checklist for upgrading Session Manager or Branch Session Manager from Release 7.1 to 7.1.3 on VMware through Solution Deployment Manager.

Use this checklist for upgrading Session Manager or Branch Session Manager from Release 7.1 to 7.1.3 on VMware through Solution Deployment Manager.

#	Task	Notes	✔
1	Make a note of the following network parameter details: • IP address • Default gateway • Netmask • DNS • NTP • Timezone		

Table continues…

#	Task	Notes	✔
2	Upgrade System Manager to Release 7.1.3.	See *Upgrading Avaya Aura® System Manager* .	
3	Verify the **Enrollment Password** field is still active.	Verifying Enrollment Password status on page 104.	
4	Archive existing logs to an external server.	Create a log harvester profile and submit a request to archive the logs. See Archiving logs on page 147.	
5	Configure user settings to establish PLDS connection.	Configuring user settings on page 18	
6	Create a remote software library.	Creating a software library on page 20	
7	For Branch Session Manager upgrade: • Administer SNMP Agent, on Communication Manager Survivable Remote (LSP) • Add the Communication Manager Survivable Remote (LSP) details on the System Manager Inventory page. • Add System Platform Console Domain details on the System Manager Inventory page. **Note:** The steps to add Communication Manager Survivable Remote (LSP) are not required for Session Manager upgrade.	• Administering SNMP Agent on page 104 • Adding a Communication Manager instance to System Manager on page 106	
8	Re-establish trust connection.	See Re-establish Connection on page 117	
9	Refresh hosts.	See Refresh host on page 117	
10	Refresh virtual machine.	See Refresh virtual machine on page 118 **Note:** Utility Servicesupgrade is optional. You can proceed to upgrade Session Manageror Branch Session Managerwithout upgrading Utility Services. For more information see *Deploying Avaya Aura® Utility Services*.	

Table continues…

#	Task	Notes	✔
11	Download the required software. • Download the Session Manager OVA: `SM-7.1.0.0.xxxxxx-e55-01.ova`. • Download the Branch Session Manager OVA: `BSM-7.1.0.0.xxxxxx-e55-01.ova`. • Download the Communication Manager Simplex OVA: `CM-<Simplex>-07.1.0.0.xx-e55-0.ova`. • Download the Utility Services OVA: `US-7.1.0.0.0.xx-e55-01_OVF10.ova`. • For LSP patch upgrade, download the Communication Manager patch file: `00.0.441.0-xxxxx.tar` • For Session Manager patch upgrade, download the iso file: `Session_Manager_7.1.3.0.xxxxxx.iso`	See Downloading the software on page 23	
12	Refresh the elements.	See Refreshing elements in the inventory on page 22	
13	Analyze the inventory.	See Analyzing inventory using Solution Deployment Manager on page 23	
14	Perform the preupgrade check.	See Performing the pre upgrade check using SDM on page 25	
15	Perform the upgrade.	See Upgrading Session Manager or Branch Session Manager from Release 7.0.X to 7.1 on page 115	
16	Commit the OVA.	See Commit OVA on page 118.	

Latest software updates and patch information

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

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

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

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Verifying the Enrollment Password status

Session Manager requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Session Manager. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, or if you do not know the password, do one of the following:

- Ask the customer for a password.
- Make up a password.

If **Time Remaining** is not zero, the password is valid. Verify that the time remaining is sufficient for the upgrade.

Procedure

1. On the home page of the System Manager web console, under **Services**, select **Security** > **Certificates** > **Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, you need to reset the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter a password in the **Password** field.
   c. Re-enter the password in the **Confirm Password** field.
   d. Make a note of the password for future reference.
   e. Click **Commit**.

      The system updates the **Time remaining** field.

Administering SNMP Agent

About this task

Caution:

On the duplicated servers, you must administer an SNMP agent exactly the same on both servers.

Procedure

1. Log on to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, in the **Alarms** section, click **SNMP Agents**.

4. Check the status of the Master Agent.
   - If the status of the Master Agent is `up`: Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent reaches to a `Down` state, go to the SNMP Traps screen by clicking **SNMP Traps** on the left navigation pane.
   - If the Master Agent is in a `Down` state, continue with step 3.
5. In the **IP Addresses for SNMP Access** section, select one of the following options:
   - No access: This option restricts all IP address from talking to the agent.
   - Any IP access: This option allows all IP addresses to access the agent.
   - Following IP addresses: You can specify up to five individual IP addresses that has permission to access the agent.
6. In the **SNMP Users/Communities** section: Select one or more versions of SNMP by clicking on the **Enable** box associated with the version.
   - **SNMP Version 1**:
     a. **Enable SNMP Version 1**: Check this box to enable SNMP v1. If the SNMP v1 box is enabled, SNMP v1 can communicate with the SNMP agents on the server.
     b. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).
     c. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).
   - **SNMP Version 2**: Check this box to enable SNMP v2. If the SNMP v2 box is enabled, SNMP v2 can communicate with the SNMP agents on the server.
     a. **Enable SNMP Version 2**: Check this box to enable SNMP v2.
     b. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).
     c. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).
   - **SNMP Version 3**: SNMP v3 provides the same data retrieval facilities as the previous versions with additional security. A User Name, authentication password, and privacy password are used to provide a secure method of authenticating the information so the device knows whether to respond to the query or not.
     a. **Enable SNMP Version 3**: Check this box to enable SNMP v3. If the SNMP v3 box is enabled, SNMP v3 can communicate with the SNMP agents on the server.

        User (read-only) : Entering a user name, authentication password, and security password in this section provides the user with read functionality only.
     b. **User Name**: Type a user name. The user name can be a maximum of any 50 characters with the exception of quotation marks.

c. **Authentication Password**: Type a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

d. **Privacy Password**: Type a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

User (read-write): Entering a user name, authentication password, and security password in this section provides the user with read and write functionality.

e. **User Name**: Enter a user name. The user name can be a maximum of any 50 characters with the exception of quotation marks.

f. **Authentication Password**: Type a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

g. **Privacy Password**: Type a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

7. To save the changes, click **Submit**.
8. Once the SNMP Agent is added, you must start the Master Agent.

   To start the Master Agent, select **Agent Status** and click **Start Agent**.

Important:

You can use the Agent Status page to change the state of the Master Agent and to check the state of the subagents. If the subagent is connected to the Master Agent, the status of each subagent is `up`. If the status of the Master Agent is `Down` and the status of the subagent is `up`, the subagent is disconnected from the Master Agent.

Adding a Communication Manager instance to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **Communication Manager**.

   The system displays the Add Communication Manager page.
5. On the General Attributes tab, provide the following information:
   a. Enter the Communication Manager server name.

      For Branch Session Manager upgrades, provide the survivable remote server name.

b. Enter the host name of the Communication Manager server.

   The IP address can be in the IPv4 or IPv6 format.

c. Enter the customer login name that is required to access Communication Manager.

   For Branch Session Manager upgrades, provide the customer login name required to access the survivable remote server.

d. Under **Authentication Type**, select the required option.

e. Enter and reenter the password, or ASG key required to access Communication Manager.

f. Enter the port number of the Communication Manager server.

g. To view this Communication Manager system in the list, select the **Add to Communication Manager** check box.

6. On the SNMP Attributes tab, do the following:

   a. Under **Version**, select **V1**.

   b. Enter the required information.

   c. Under **Device Type** select the type of Communication Manager.

7. Click **Commit**.

   The system displays the Communication Manager instance that you added on the Manage Elements page.

Add Communication Manager field descriptions

General Attributes

Field	Description
Name	The name of Communication Manager instance.
Hostname or IP Address	The IP address can be in the IPv4 or IPv6 format. The host name or the IP address of the Communication Manager instance. For the duplicated Communication Manager, this value references the active server IP address.

Table continues…

Field	Description
Login	The login name that you use to connect to the Communication Manager instance. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system. Do not use the login name to connect to: • The Communication Manager instance from any other application. • The Communication Manager SAT terminal by using command line interface (CLI).
Authentication Type	The type of password that authenticates the SSH or Telnet login name on the element.
Password	The password that authenticates the SSH or Telnet login name on the element.
Confirm Password	The password that you retype for confirmation. **Note:** **Confirm Password** must match **Password**.
ASG Key	The ASG key that authenticates the SSH or Telnet login name on the element. This field is only available if **ASG Key** is selected in **Authentication Type**.
Confirm ASG Key	The ASG key that you retype for confirmation. This field is only available if **ASG Key** is selected in **Authentication Type**. **Note:** **Confirm ASG key** must match **ASG key**.
SSH Connection	An option to use SSH for connecting to the element. By default, the system selects the check box. If you clear the check box, the system uses Telnet to connect to the element.
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the Communication Manager server. For duplex servers, the RSA SSH key is the key of the active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH key of the standby Communication Manager server. Use the DSA SSH key only for duplex servers.
Description	A description of the Communication Manager server.
Alternate IP Address	The alternate IP address of the element. For duplex servers, the alternate IP address is the IP address of the standby server.

Table continues…

Field	Description
Enable Notifications	A real-time notification whenever an administrative change occurs in Communication Manager. For example, when you add or delete an extension from Communication Manager outside System Manager. The options are: • Selected: Enables the CM Notify sync feature for this Communication Manager instance. • Cleared: Disables the CM Notify sync feature for this Communication Manager instance. After you enable this feature, and register the System Manager IP address on Communication Manager, the system sends changes that are administered on Communication Manager to System Manager asynchronously. **Note:** Communication Manager 6.2 or later supports this feature.
Port	The port on which the service provided by the element is running. The default SSH port is 5022. **Note:** From Communication Manager Release 7.1 and later, the telnet port 5023 is disabled. If the telnet port is configured for the Communication Manager element, select the **SSH Connection** checkbox. When you select this checkbox, the system auto populates the default port value to 5022.
Location	The location of the element.
Add to Communication Manager	An option to select the Communication Manager that you want to view in the communication manager list.

SNMPv1 Attributes

The below fields are available only if **V1** is selected in the **Version** field.

Field	Description
Version	The SNMP protocol type.
Read Community	The read community of the device.
Write Community	The write community of the device.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds an application polls a device without receiving a response before timing out.

Table continues…

Field	Description
Device Type	The Communication Manager application type. The options are: • **Avaya Aura(R) Communication Manager SP** for Communication Manager 6.3.100 on System Platform. • **Avaya Aura(R) Communication Manager VE** for Virtualized Environment-based Communication Manager 6.3.100 and Release 7.1.3.

SNMPv3 Attributes

The below fields are available only if **V3** is selected in the **Version** field.

Field	Description
Version	The SNMP protocol type.
User Name	The user name as defined in the application.
Authentication Protocol	The authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. The possible values are: • **MD5 (default)** • **SHA** • **None**
Authentication Password	The SNMP authentication password.
Confirm Authentication Password	The SNMP authentication password that you retype for confirmation. **Authentication Password** and **Confirm Authentication Password** must match.
Privacy Protocol	The encryption policy for SNMP V3 users. The possible values are: • **AES**: Use the AES encryption for the SNMP-based communication. AES is the default protocol. • **DES**: Use the DES encryption for the SNMP-based communication. • **None**: Do not encrypt traffic for this user.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Retries	The number of times the application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds the application waits for the response from the device being polled.
Device Type	The type of device.

Button	Description
Commit	Adds a Communication Manager instance in the inventory.

Table continues…

Button	Description
Clear	Clears all the entries.
Cancel	Cancels your action and return to the previous page.

Configuring the Appliance Virtualization Platform USB drive

Before you begin

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

Procedure

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

   See “Generating the Appliance Virtualization Platform kickstart file”.

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

Next steps

Install Appliance Virtualization Platform.

Installing Appliance Virtualization Platform

Before you begin

- Download the Appliance Virtualization Platform ISO image and burn the ISO image in a DVD: `avaya-avp-7.1.0.0.0.xx.iso`. If required, apply the Appliance Virtualization Platform patch.
- Create a `ks.cfg` file.

Procedure

1. Insert the USB drive and the Appliance Virtualization Platform DVD into the server.
2. Click **Server Management** > **Server Reboot/Shutdown** > **Reboot** to restart the server.
3. The system installs Appliance Virtualization Platform and ejects the DVD.

   This may take up to 30 minutes to complete.

4. Remove the USB drive and DVD.
5. Connect to the server through eth1 services port using the IP address such as 192.168.13.5 for your system. Alternatively, you can use the public network address that was configured during installation.

6. Using the vSphere client 5.5, connect to the Appliance Virtualization Platform ESXi host by using the credentials provided in the `ks.cfg` file.
7. Go to **System Manager** > **Solution Deployment Manager**.
8. Add the ESXi host using the System Manager VM Management page.
9. First, deploy the Utility Services OVA.

   For information about deploying Utility Services, OLH see *Deploying Avaya Aura® Utility Services*.

Upgrading Session Manager or Branch Session Manager from Release 6.x to 7.1 through SDM

About this task

Use the procedure to upgrade Session Manager or Branch Session Manager to 7.1.

To upgrade Session Manager by using Solution Deployment Manager, you must have System Manager 7.0 or later.

For information about upgrading Session Manager by using the SDM client when System Manager is unavailable, see *Upgrading and Migrating Avaya Aura® applications from System Manager*.

Before you begin

- To upgrade on a different server, install Appliance Virtualization Platform on a different server and add the location and ESXi host on the VM Management page.
- If required, apply the Appliance Virtualization Platform and Utility Services patches.

  For information about installing patches, see *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* and *Deploying Avaya Aura® Utility Services*.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select the Session Manager application to upgrade.
4. Click **Upgrade Actions** > **Upgrade/Update**.

   The system displays the Upgrade Configuration page.
5. To view the devices associated with the application that you want to upgrade, perform the following:
   a. Click **Details** and review the dependent devices.
   b. Click **Done**.

6. To continue with upgrade when the recommended checks fail during the preupgrade check, select the **Override preupgrade check** check box.

   Note:

   For Branch Session Manager, the system displays the three check boxes: **Utility Server**, **Branch Session Manager**, and **LSP**. You need to select one check box at a time and select the **Override preupgrade check** check box.

7. To provide the upgrade configuration details, click **Edit**.

   Note:

   For Branch Session Manager, perform this step for Utility Services, Branch Session Manager, and remote survivable server, separately.

8. On the Edit Upgrade Configuration page, you can add the following:

   - In **Service/Feature Pack for auto-install after migration**, provide the patch file.

     The system automatically installs the patch file after the upgrade.

   - To upgrade on the same server:
     - Select **ESXI host** as Same Box.
     - In **Existing Administrative User**, type the customer login name.
     - In **Existing Administrative Password**, type the customer login password.
     - Click **Pre-populate Data**.

       The system populates the data of the **IP Address**, **Short Hostname**, **Network Domain**, **Netmask**, **Default gateway**, **DNS server(s)**, **Timezone**, **NTP server(s)**, **Login Name**, **Enter Customer Account Password**, **Primary System Manager IP**, and **Enrollment Password** fields.
     - In the **Flexi Footprint** field, select the footprint based on the user requirement.
     - Do one of the following in the **EASG User Access** field:
       - Type 1 to enable EASG.

         Note:

         Avaya recommends to enable EASG.
       - Type 2 to disable EASG.
   - To upgrade on a different server:
     - Select the ESXi host IP address of the different server and the data store.
     - Click **Schedule**.

   Note:

   For Branch Session Manager, perform this step for Utility Services, Branch Session Manager, and LSP, separately.

9. Ensure that the **Configuration Status** field displays .

   If the field displays , review the information on the Edit Upgrade Configuration page.
10. Click **Save**.
11. On the Upgrade Configuration page, click **Upgrade**.
12. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
13. Click **Schedule**.
14. Perform these steps, only when you are upgrading Session Manager or Branch Session Manager on the same server. On the Upgrade Management page, the status of the **Release Status** and **Last Action Status** fields changes to pause state.
    a. Install Appliance Virtualization Platform.
    b. Add the ESXi host using the System Manager VM Management page.
    c. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    d. On the Resume Configuration page, select the ESXi host IP address and the data store.
    e. Click **Edit** under the Network Configuration column. On the Network Configuration page, select the network parameters, and click **Done**.
    f. Click **Schedule**.
15. On the Upgrade Management page, click .

    The **Last Action** column displays **Upgrade**, and the **Last Action Status** column displays .
16. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In **Job Type**, click **Upgrade**.
    c. Click the upgrade job that you want to view.
17. For upgrades on the same server, do the following:
    a. Install the Appliance Virtualization Platform host.
    b. From the VM Management page, add the Appliance Virtualization Platform host.
    c. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    d. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.
    e. Continue with the upgrade process.

Next steps

Verify that the upgrade of Session Manager or Branch Session Manager is successful.

Upgrading Session Manager or Branch Session Manager from Release 7.1 to 7.1.3 on VMware through Solution Deployment Manager

About this task

Use the procedure to upgrade Session Manager or Branch Session Manager 7.1 to 7.1.3.

To upgrade Session Manager by using Solution Deployment Manager, you must have System Manager 7.0 or later.

For information about upgrading Session Manager by using the SDM client when System Manager is unavailable, see *Upgrading and Migrating Avaya Aura® applications from System Manager*.

Before you begin

- To upgrade on a different server, install Appliance Virtualization Platform on a different server and add the location and ESXi host on the VM Management page.
- If required, apply the Appliance Virtualization Platform and Utility Services patches.

  For information about installing patches, see *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* and *Deploying Avaya Aura® Utility Services*.
- Ensure that the CDR files are manually backed up before upgrading. For more information about retrieving CDR files, see *Maintaining Avaya Aura® Session Manager*.

Procedure

1. On the Session Manager Dashboard change **Service State** of the Session manager server to **Deny New Service**.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
3. In the navigation pane, click **Upgrade Management**.
4. Select the Session Manager to upgrade and **Pre-Upgrade > Refresh Element(s).**
5. On the next page, click **Schedule.**
6. After refresh is done, select **Pre-Upgrade>Analyze.**
7. On the next page, click **Schedule.**
8. Select the Session Manager application to upgrade.
9. Click **Upgrade Actions** > **Upgrade/Update**.

   The system displays the Upgrade Configuration page.

10. To view the devices associated with the application that you want to upgrade, perform the following:
    a. Click **Details** and review the dependent devices.
    b. Click **Done**.
11. To continue with upgrade when the recommended checks fail during the preupgrade check, select the **Override preupgrade check** check box.

    Note:

    For Branch Session Manager, the system displays the three check boxes: **Utility Server**, **Branch Session Manager**, and **LSP**. You need to select one check box at a time and select the **Override preupgrade check** check box.
12. To provide the upgrade configuration details, click **Edit**.

    Note:

    For Branch Session Manager, perform this step for Utility Services, Branch Session Manager, and remote survivable server, separately.
13. On the Edit Upgrade Configuration page, do the following:
    a. Select **Update** for **Operation.**
    b. Select the **Software Library** to which the Feature/Service Pack was downloaded.
    c. Select the feature Feature/Service Pack.
    d. Accept the EULA.
14. Ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
15. Click **Save**.
16. On the Upgrade Configuration page, click **Upgrade**.
17. 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.
18. Click **Schedule**.
19. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In **Job Type**, click **Upgrade**.
    c. Click the upgrade job that you want to view.
20. Verify that the upgrade of Session Manager or Branch Session Manager is successful.
21. On the Session Manager Dashboard change **Service State** of the Session Manager server to **Accept New Service**.

After the upgrade is complete and it is determined that the patch is working correctly, commit the patch.

Note:

Running with uncommitted patches can result in performance problems.

22. On the System Manager web console, click **Services > Solution Deployment Manager > Upgrade Management.**
23. Select the Session Manager to upgrade and click **Upgrade Actions > Installed Patches.**
24. In the Patch Operation box, select **Commit.**
25. Select the patch and then **Schedule.**

Re-establishing trust connection

About this task

Use this procedure to upgrade an application that was *not* deployed from Solution Deployment Manager.

Procedure

1. On the home page of System Manager Web Console, in **Services**, click **Solution Deployment Manager** > **VM Management**.
2. On the VM Management page, select the virtual machine.
3. To establish trust, click **More Actions** > **Re-establish Connection**.
4. Type the credentials and click **Reestablish Connection**.

   The **Current Action Status** column displays the status of the virtual machine reestablishment.
5. Select the same virtual machine, and click **More Actions** > **Refresh VM**.

   The **Current Action Status** column displays the status of the virtual machine.

Refreshing host

Procedure

1. On the home page of System Manager Web Console, in **Services**, click **Solution Deployment Manager** > **VM Management** .
2. On **VM Management Tree**, click the required location.
3. Click the **Hosts** tab.

The system displays the list of hosts for the selected location.

4. Select the required host.
5. Click **Refresh**.

   The **Current Action Status** column displays the status of the host.

Refreshing the virtual machine

Procedure

1. On the home page of System Manager Web Console, in **Services**, click **Solution Deployment Manager** > **VM Management**.
2. On **VM Management Tree**, click the required location.
3. Click the **Virtual Machines** tab.

   The system displays the list of virtual machines for the selected location.
4. Select the required virtual machine.
5. Click **More actions** > **Refresh VM**.

   The **Current Action Status** column displays the status of the virtual machine.

Committing OVA

Procedure

1. On System Manager Web Console, click **Services** > **Solution Deployment Manager**.
2. In the navigation panel, click **Upgrade Management**.
3. Select the Session Manager application to upgrade.
4. Click **Upgrade Actions** > **Commit/Rollback upgrade**.
5. In the **Upgrade Actions** column, click **Commit**.
6. 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.
7. Click **Schedule**.

   The Upgrade Management page displays the last action as **Commit**.
8. Ensure that the **Upgrade status** and **Last Action Status** columns display a green check mark.

Installing software patches

About this task

Use the procedure to install the software patches for Session Manager, and commit the software patches that you installed.

To install patches for Session Manager by using Solution Deployment Manager, you must have System Manager 7.0 or later.

Before you begin

- Download the Session Manager patch file, `Session_Manager_7.1.x.x.xxxxxx.iso`.
- Re-establish connection.

Note:

To install software patches without using the Solution Deployment Manager, see *Upgrading Avaya Aura® Session Manager*.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select the Session Manager virtual machine to install the patch.
4. Select the virtual machine, click **Pre-upgrade Actions** > **Refresh Element(s)**.
   a. On the Job Schedule page, in the **Job Name** field, type the job name.
   b. Click **Schedule**.
5. Select the virtual machine, click **Pre-upgrade Actions** > **Analyze**.
   a. On the Job Schedule page, in the **Job Name** field, type the job name.
   b. Click **Schedule**.

   After analyzing the software, the system enables the **Pre-upgrade Actions** > **Pre-upgrade Check**.
6. Select the virtual machine, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   a. On the Pre-upgrade Configuration page, specify the **Target Host**, **Data Store**, **Upgrade Source**, and **Upgrade/Update To** details.
   b. On the Job Schedule page, in the **Job Name** field, type the job name.
   c. Click **Schedule**.

   After performing the Pre-upgrade check, the system enables the **Upgrade Actions** > **Upgrade/Update**.
7. Click **Upgrade Actions** > **Upgrade/Update**.
8. On the Upgrade Configuration page, click **Edit**.
9. In the **General Configuration Details** section, in the **Operation** field, click **Update**.

10. In the **Upgrade Source** field, select the software library where you have downloaded the patch.
11. In the **Select patches for update** section, the page displays the available patches.
12. Select the patch that you want to install.
13. **(Optional)** Select the **Auto Commit** check box, if you want the system to automatically commit the patch.

    Note:

    If you do not select **Auto Commit**, then follow Steps 22 through 26.
14. In the **Upgrade Configuration Details** section, select the patch file that you want to install.
15. Accept the license agreement.
16. Click **Save**.
17. Ensure that the **Configuration Status** field displays .
18. Click **Upgrade**.
19. 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.
20. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** columns display .
21. To view the upgrade status, click .

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

    When the update is complete, the **Upgrade Status** and **Last Action Status** columns display .
22. Click **Upgrade Actions** > **Installed Patches**.
23. On the Installed Patches page, in the **Patch Operation** section, click **Commit**.

    The page displays all software patches that you can commit.

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

    You can use the **Schedule later** option to commit the patch at a later time.
25. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
26. Ensure that the **Upgrade Status** and **Last Action Status** columns display .

Supporting mixed Session Manager and Branch Session Manager upgrades

About this task

Session Manager 6.x, Session Manager 7.0.x and Session Manager 7.1 systems can be managed by a single System Manager for periods during a network upgrade. This is a transient state during the upgrade period, compared to a permanent steady state. To accomplish this, the System Manager needs to be upgraded to 7.1 and the Session Manager licenses must be 7.1.3 licenses for the 7.1, 7.0.x and 6.x systems. There are no license charges for the license upgrade for Session Manager from Release 6 to 7.0, so there are no additional costs during the transition period.

Procedure

1. Within Avaya Solution Designer, upgrade all the Session Manager or Branch Session Managers in the network, even those that will not be upgraded immediately.

   This process upgrades the Release 7.1.3 license for each Session Manager.

2. Activate the Release 7.1.3 licenses in PLDS for all the Session Manager instances in the network.

3. Install the resulting Release 7.1.3 license file on System Manager WebLM. System Manager checks a valid Release 7.1.3 license for each Session Manager instance in the network. If Release 7.1.3 license file is not installed on System Manager WebLM, Session Manager servers are placed in license error mode with a 30-day grace period. If the grace period expires before a valid Release 7.1.3 license file is installed, then the Session Manager servers are out of service until a valid license file is installed.

Chapter 6: Data Migration of Session Manager in VMware Environment

Upgrading Session Manager from Release 6.x or 7.0.x to 7.1.3 using data migration utility on VMware

About this task

You must perform this procedure to get data migration tool certificates to avoid the loss of alarming and configuration data.

The Data Migration Utility is not required for a Session Manager or a Branch Session Manager upgrade that is being done on Avaya provided servers running Application Virtual Appliance software when Solution Deployment Manager is used to facilitate the upgrade.

Procedure

1. Log in to the Session Manager with the customer account.
2. Go to the customer's home directory. For example, `cd /home/cust`.
3. Download the latest version of the data migration utility to the local directory.
4. Run the `dmutility-7.1.x.0.xxxxx.bin` utility.

```
$ bash dmutility-7.1.x.0.xxxx.bin

Verifying signature...                                  [  OK  ]
Checking integrity of install.sh                        [  OK  ]
Checking integrity of sm_backup.sh                      [  OK  ]
Checking integrity of cs_functions.sh                   [  OK  ]
Mounted ISO image /tmp/tmp.GUqkp31591 to /iso
Removing any previous backup files
Backing up data
Moving backup file to the current directory
Data backup is complete.
Copy /home/cust/Session_Manager_backup.tgz to a remote server before shutting
down Session Manager.
```

5. Copy the backup file to a remote server.

   In most cases, the backup file is `/home/cust/Session_Manager_backup.tgz`. The `dmutility` displays the exact location of the backup file as an output.

6. Run the **smconfig** command and note the values of IP addresses, hostnames, and other parameters.

   These values are required to deploy the Session Manager Release 7.1 OVA file.
7. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Deny New Service**.
8. Deploy the Release 7.1 Session Manager or Branch Session Manager OVA.
9. Download the 7.1.3 ISO service pack on the newly deployed Session Manager.
10. Run **upgradeSM** <session_manager_7.1.3.0.xxxxxx.iso> to install and apply 7.1.3 patch.
11. To restore the backup, copy the backup file to the newly deployed Session Manager home directory.
12. Log in to the Session Manager with customer account. Use the **upgradeSM** command to run the restore utility.

```
$ upgradeSM Session_Manager_backup.tgz
Performing data migration
VSP_PROGRESS[[Starting restore]]VSP_PROGRESS
VSP_PROGRESS[[Stopping Session Manager]]VSP_PROGRESS
...
Trust Management Initialization started.
Trust Management Initialization with System Manager started.
Trust Management Initialization completed.
Upgrading saved certificates
Saving upgrade files to /opt/Avaya/prev-upgrade
Downloading System Manager root CA
Waiting for WebSphere components to startup...
Waiting for WebSphere components to startup...
...
Waiting for Management components to startup...
Waiting for Management components to startup...
Thu Apr  9 16:06:37 MDT 2015: DRS Replication registration succeeded
Please go to the System Manager Replication Page to check the synchronization
state
```

13. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Accept New Service**.
14. For VMware Virtualized Environment, delete the old Session Manager virtual machine.

Chapter 7: Post-upgrade verification

Post-upgrade checklist for Session Manager or Branch Session Manager

Use this checklist after upgrading Session Manager or Branch Session Manager from Release 6.x to 7.1.3.

#	Task	Notes	✔
1	After the server reboots, log in to the server.	After the upgrade, log in with customer login name and password.	
2	If applicable, configure the Session Manager server in a System Manager Geographically Redundant environment.	See Configuring Session Manager in a geographically redundant environment on page 125.	
3	Enter the **swversion** command and verify that the upgrade is completed successfully.	The Release must start with 7.1.3. If the upgrade is not successful, contact Avaya Technical Support.	
4	On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.	On the Session Manager Dashboard page:	
5	Run the Session Manager server tests.	See Testing the Session Manager instance on page 125	
6	Verify data replication between System Manager and Session Manager. The system synchronizes the data in about 15 minutes. Refresh the page as necessary.	See Verifying Data Replication on page 126	
7	Verify the Security Module is active for the Session Manager server.	See Viewing Security Module status on page 127	
8	If SIP monitoring is provisioned for Session Manager, verify the links are active for the Session Manager instance. The system updates the status in about 10 minutes. Refresh the page as necessary.	See Viewing Session Manager Entity Link Connection Status on page 128	

Table continues…

#	Task	Notes	✔
9	Change **Service State** of the Session Manager or Branch Session Manager server to **Accept New Service**.	See Accepting new service on page 129	
10	Make test calls to ensure the Session Manager server is processing calls properly.		

Configuring Session Manager in a System Manager in a geographically redundant environment

In a System Manager geographic redundant environment where the Primary System Manager is down, perform this procedure *after* upgrading the Session Manager server.

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for remote login.

   Note:

   You can connect your laptop directly to the service port of the server.

2. Enter **`changeMgmtIP`** and ensure that all fields are set correctly.
3. Enter **`dnat_failover.sh <SECONDARY_SMGR_IP>`**.
4. Enter **`initTM`**.

Testing the Session Manager instance

Procedure

1. On the System Manager web console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **Select System Manager or a Session Manager to test** field, select the Session Manager instance from the drop-down menu.
3. Select **Execute all Tests**.
4. Verify the **Test Result** field displays **Success**.

   If any of the tests fail, see *Troubleshooting Avaya Aura® Session Manager* and *Maintaining Avaya Aura® Session Manager*.

Installing the license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Install license**.
3. Click **Browse** to specify the location of the Session Manager license file on your computer.
4. Click **Accept the License Terms & Conditions**.
5. Click **Install**.

   The system displays Session Manager in the **Licensed products** section.

Verifying Data Replication

Procedure

1. On the System Manager web console, under **Services**, click **Replication**.
2. Verify the status for the appropriate replica group is **Synchronized**.
3. If the status for the replica group is not **Synchronized**, see Troubleshooting Data Replication on page 126.

Troubleshooting Data Replication

Procedure

1. On the home page of the System Manager Web console, under **Services**, click **Replication**.
2. If the status for the replica group is not **Synchronized**:
   a. Select the affected replica group.
   b. Click **View Replica Nodes**.
   c. Verify that an instance exists in the replica group under **Replica Group Host Name**.
   d. Select the appropriate instance under **Replica Group Host Name**.
   e. Click **View Details**.
   f. Under the Synchronization Statistics section, wait until the **Pending Batches** value is zero. Refresh the page as necessary by clicking **Refresh**.
3. If the **Pending Batches** value does not change to zero:
   a. Click **Done**.
   b. On the **Replica Group** page, click **Repair**.

c. Click **OK** in the dialog box.

4. Wait until the status of the replica group changes to **Synchronized**. Refresh the page as necessary.

Viewing the Security Module page

Possible causes for the Security Module status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.
- The security module may not have received security module configuration information from System Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. If the Security Module state of Session Manager does not display as **Up**:
   a. Click on the status text of the Security Module for Session Manager to display the Security Module Status page.
   b. Verify the IP address for Session Manager is correct.
   c. Select Session Manager.
   d. Click **Synchronize**.
   e. If the status remains **Down**, click **Reset**.

      Warning:

      Session Manager cannot process calls while the security module is being reset.

Related links

Troubleshooting Security Module Sanity failure on page 127

Troubleshooting Security Module Sanity failure

Procedure

1. On the System Manager Web Console, select **Elements** > **Session Manager** > **System Status** > **Security Module Status**.
2. Select **Refresh** to display the current status.
3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.

5. If the status is selected as **Down**, reset the security module:
   a. Select the appropriate Session Manager instance from the table.
   b. Click **Reset**.

      Warning:

      Session Manager cannot process calls while the system resets the security module.
6. Select **Refresh** to display the current status.

Related links

Viewing the Security Module page on page 127

Viewing the Session Manager entity link connection status

About this task

Use this procedure to view Session Manager entity link connection status.

Note:

Entity Monitoring does not apply to a Branch Session Manager. The monitoring status of a Branch Session Manager is always unknown (---).

An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all the connections are up, then the Entity Link status is **up**. If one or more connections are down but at least one connection is up, the link status is **partially down**. If all the connections are down, the Entity Link status is **down**.

On the Session Manager dashboard page, the number of down links and total links are shown in the **Entity Monitoring** column. The values have the format **# of Down links / # of Total links**.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. Under the **Entity Monitoring** column, red values indicate that at least one entity link is down. Click the red values link to display the Session Manager Entity Link Connection Status page.

   The Session Manager Entity Link Connection Status page displays the details for each link. If a link is down, the page displays a reason code.
3. To view the SIP Entity Link Monitoring Status Summary page, click **Summary View**.

Accepting new service

About this task

Use this procedure to change the state of a new service to accept..

Note:

Even though the Security Module displays the status as **Up**, the security module might take 5 to 10 minutes before the security module can begin routing calls.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
3. Click **Service State**.
4. Select **Accept New Service** from the drop-down menu.
5. Click **Confirm**.

Enhanced Access Security Gateway

Session Manager supports Enhanced Access Security Gateway (EASG), an authentication interface that secures the system administration and logins on the system. EASG provides a secure method for Avaya services personnel to access the Avaya Aura® applications remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

EASG uses a challenge and response protocol to confirm the validity of a user. This process reduces the opportunity for unauthorized access.

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

Related links

Checking EASG status on page 130
Enabling and disabling EASG on page 130
Enabling and disabling EASG through System Manager on page 130
EASGManage on page 131
Loading and managing site certificate on page 132

Checking EASG status

Before you begin

Log in with the customer account.

Procedure

1. On the command line interface, type `EASGStatus`.
2. Press `Enter`.

   The system displays one of the following:

   - **`EASG is enabled`** — if EASG is enabled.
   - **`EASG is disabled`** — if EASG is disabled.

Related links

Enhanced Access Security Gateway on page 129

Enabling and disabling EASG

Before you begin

Log in with the customer account.

Procedure

1. On the command line interface, do one of the following:
   - To enable EASG, type `EASGManage --enableEASG`.
   - To disable EASG, type `EASGManage --disableEASG`.

   The system displays the message **`Do you want to continue [yes/no] ?`**
2. Type `yes` or `no`.
3. Press `Enter`.

Related links

Enhanced Access Security Gateway on page 129

Enabling and disabling EASG through System Manager

About this task

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. In the navigation pane, click **Dashboard**.
3. Click the **EASG** field.
4. Click one of the following:
   - **Enable EASG**.
   - **Disable EASG**.
5. Click **Confirm**.

Related links

Enhanced Access Security Gateway on page 129

EASGManage

Use **`EASGManage`** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--
userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

--enableEASG	Enables Enhanced Access Security Gateway (EASG) authentication.
--disableEASG	Disables EASG authentication.
--enable	Enables EASG authentication only for the Avaya Services logins specified in the *user* variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft.
--disable	Disables EASG authentication only for the Avaya Services logins specified in the *user* variable.
--userStatus	Displays the EASG status of the user specified in the *user* variable.
--listUsers	Lists the available EASG users.
--f	Forces the enable or disable action to run without prompts.
--printDisableWarning	Displays the warning message for disabling EASG on the system.
--printEnableWarning	Displays the warning message for enabling EASG on the system.

Related links

Enhanced Access Security Gateway on page 129

Loading and managing site certificate

About this task

Site certificates are used by the onsite technicians not having access to the Avaya network to generate a response to the Enhanced Access Security Gateway (EASG) challenge. The technician will generate and provide the site certificate to the customer. The customer must load this site certificate on each server (AVP Host) and virtual machine that the technician needs to access. Once this is done the technician can use EASG Site Manager to login with the EASG challenge. After the technician is done the customer can remove the site certificate from the server or they will be removed by the EASG software after the site certificate expires (~15 days later).

A customer can load a site certificate using `EASGSiteCertManage --add <pkcs7_file_path>` and will need to specify a Site Authentication Factor (SAF). The SAF will need to be provided to the technician and is also used by EASG Site Manager to generate a response to the EASG challenge.

Before you begin

Customers must complete the following before loading and managing site certificates:

- Have a valid login and password.
- Use a tool such as WinSCP. Log in using a customer login, for example `cust`. Copy the certificate to `/home/cust directory` (where `cust` is the customer directory).
- Use a 10 to 20 character Site Authentication Factor (SAF) for instance 12345abcwxyz.
- Be familiar with CLI type shell commands.

Procedure

1. Log in to a Linux® shell by using the customer account.

   The customer account is created during the deployment procedure.

2. At the command line type:

```
[cust@host ~]$  EASGSiteCertManage --add johndoe.p7b
You are about to install this site certificate into your trusted repository:
Technician Name: johndoe
Expiration Date: Nov 10 17:02:15 2016 GMT
Do you want to continue [yes/no]? yes
Please enter a site authentication factor (SAF) for the technician to use when
getting access to your machine. The SAF is alphanumeric with at least 10
characters and no more than 20 characters.
  Please enter your SAF:  Site Authentication Factor
  Please confirm your SAF: Site Authentication Factor
Site Certificate installed successfully.
[cust@host  ~]$
```

   Save the Site Authentication Factor to share with the technician once on site.

3. You can view information about a particular certificate by using `EASGSiteCertManage --show <pkcs7_file_path>` and the certificate name is obtained from certificate list output.

```
[cust@host ~]$ EASGSiteCertManage --show johndoe.p7b
Subject:        CN=Avaya Technician johndoe, OU=EASG, O=Avaya Inc.
User Name:      johndoe
Expiration:     Nov 10 17:02:15 2016 GMT
Trust Chain:
    1. O=Avaya, OU=IT, CN=AvayaITrootCA2
    2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
    3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
    4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya Inc.
    5. CN=Avaya Technician johndoe, OU=EASG, O=Avaya Inc.
```

4. The customer can delete the site certificate using `EASGSiteCertManage --delete <pkcs7_file_path>` and the certificate name is obtained from the certificate list output.

```
[cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
Successfully removed Site Cert: johndoe.p7b
[cust@host ~]$
```

Related links

Enhanced Access Security Gateway on page 129

Alarming Configuration

Note:

Not all upgrade paths require alarming configuration. The upgrade checklists contain the alarm configuration step if the upgrade path requires alarming configuration.

Related links

Network Management Systems Destinations on page 133
Activating and managing the Session Manager serviceability agent on page 134
Alarming configuration checklist on page 135
Adding Session Manager to the SAL Gateway on page 135
Generating a test alarm on page 136

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

- SAL Gateway, mandatory trap destination
- System Manager trap listener
- Third-party NMS

- Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with SAL Gateway as a trap destination. You can configure the serviceability agent by using the System Manager web console. You must also configure Session Manager as a managed device on SAL Gateway.

Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure the Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager*.

Related links

Alarming Configuration on page 133

Activating and managing the Session Manager serviceability agent

Use the System Manager web console to activate and manage the Session Manager serviceability agent. To add a Network Management System (NMS) destination, you first create a target profile for the NMS destination and then attach the target profile to a serviceability agent.

For more information on activating agents and attaching target profiles, see the SNMP Support chapter in *Administering Avaya Aura® Session Manager*.

For the Geographic Redundant system setup, administer both System Manager instances as targets for alarming.

Related links

Alarming Configuration on page 133

Alarming configuration checklist

#	Action	Link/Notes	✔
1	Configure the Serviceability Agent for Session Manager.	See SNMP support for Session Manager in *Administering Avaya Aura® Session Manager*.	
2	Add Session Manager to the SAL Gateway.	Adding a Session Manager to the SAL Gateway on page 135.	
3	Generate a test alarm.	Generating a test alarm on page 136.	

Related links

Alarming Configuration on page 133

Adding Session Manager to the SAL Gateway

Configure alarming and remote access for a Session Manager instance.

Do not perform this procedure if you are upgrading the Session Manager server that is already configured on a SAL Gateway.

Before you begin

The Secure Access Link (SAL) Gateway must already be set up for System Manager Release 6.3.

Procedure

1. Log in to the System Platform Web console.
2. Click **Server Management** > **SAL Gateway Management**.
3. On the **SAL Gateway Management** page, click **Launch SAL Gateway Management Portal**.
4. When the SAL Gateway login page appears, enter the same user ID and password that you used when you logged in to the System Platform Web Console.
5. In the navigation pane of the SAL Gateway user interface, select **Secure Access Link Gateway** > **Managed Element**.
6. On the **Managed Element** page, click **Add new**.
7. Enter information in the following fields:
   - **Host Name**: Host Name of the Session Manager server.
   - **IP Address**: IP Address of the Session Manager server.
   - In the **Model** field, select **SessionMgr_x.x.x.x** from the drop-down menu.

     The **Product** field is filled in automatically after you select Session Manager.

- **Solution element ID**: The Solution Element ID (SE ID) of Session Manager. The format of the ID is (NNN)NNN-NNNN where N is any digit from 0 to 9.
- **Product ID**: The Product ID of Session Manager.
- Select the **Provide remote access to this device** check box.
- Select the **Transport alarms from this device** check box.

Important:

The SAL Gateway forwards alarms for this Session Manager only after you select the **Provide remote access to this device** and **Transport alarms from this device** check boxes.

8. Click **Add**.
9. Click **Apply** to apply the changes.
10. Restart the SAL Gateway for the configuration changes to take effect:
    a. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Apply Configuration Changes**.
    b. Click **Apply** next to **Configuration Changes**.

    The system restarts the SAL Gateway and updates the SAL Gateway with the new configuration values.

Related links

Alarming Configuration on page 133

Generating a test alarm

Generate a test alarm to the targets assigned to the serviceability agent. These targets can include:

- A SAL Gateway

  The alarm is forwarded to ADC
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

Procedure

1. If using the Session Manager CLI:
    a. Login to the Session Manager server.
    b. Run the Session Manager CLI command **generateTestAlarmSM.sh**.

2. If using the **Generate Test Alarm** button on the **Serviceability Agents** screen:
   a. On the System Manager web console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
   b. Select a hostname from the list, and click **Generate Test Alarm**.
3. To verify that the System Manager received the test alarm message, do one of the following:
   a. On the System Manager web console, in **Services**, click **Events** > **Alarms**.
   b. Check that the system displays the message **Test alarm for testing only, no recovery action necessary** in the **Description** column.
4. If the serviceability agent is configured with other targets, verify that the other targets also received the test alarm and also verify the clearing of the alarm.

Note:

The test alarms are not generated when Session Manager is in Maintenance Mode.

Related links

Alarming Configuration on page 133

Chapter 8: Resources

Documentation

The following documents are available at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 7.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel

Table continues…

Title	Description	Audience
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
Upgrading and Migrating Avaya Aura® applications from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Aura® Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel

Table continues…

Title	Description	Audience
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Finding documents on the Avaya Support website

Procedure

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

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

Training

The following table contains courses that are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration

Table continues…

Course code	Course title
5U00082R	Session Manager and System Manager Administration
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 142

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

Related links

Support on page 142

Appendix A: OS-level logins for Session Manager

The following is a list of logins that are created during the Session Manager software installation:

- **asset:** A login created during the installation of the Security Module software. By default, access to the system using this login is disabled.
- **csadmin:** Login used by the Solution Deployment Manager to manage Session Manager remotely.
- **CDR_User:** A restricted shell login for the Call Detail Recording (CDR) feature. CDR collects call data from the Session Manager server. This login is restricted to sftp access only.
- **craft:** An Avaya services login to gain access to the system remotely for troubleshooting purposes.
- **customer:** A login that the **`SMnetSetup`** script creates. The default name of the *customer* login is **`cust`**. The customer must ensure the security of this login account. The *customer* login can run software tools which do not require root access on the Session Manager servers.
- **init:** An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **jboss:** A login created for running the management jboss and is not a login account.
- **postgres:** A login created by the installation of the Session Manager software PostgresSQL database system. Access to the system using this login is disabled.
- **spirit:** A login created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **sroot:** An Avaya services root permission login to gain access to the system remotely for troubleshooting purposes. You cannot gain access to the sroot login directly from a login prompt except on the server console.
- **wsuser:** A login created for running WebSphere. This login is not a login account.

Warning:

In Session Manager 7.1, Enhanced Access Security Gateway secures the following logins and prevents unauthorized access to the Session Manager servers by non-Avaya services personnel:

- **`sroot`**
- **`init`**
- **`craft`**

Using the customer login account, you can run most of the maintenance and troubleshooting commands. You do not need root access for standard maintenance and support purposes. For more information, see PSN (PSN003925U).

Appendix B: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing Product Correction Notices and Product Support Notices

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Appendix C: Archiving logs

The logs are located in various subdirectories on the Session Manager server. Running a log harvester on the Session Manager server, copies all the current logs, and archives them on the System Manager server for viewing at a later time, if necessary.

For more information about the log harvester and field descriptions, see *Administering Avaya Aura® System Manager*.

Log harvester

The log harvesting service manages the retrieval, archival, and analysis of harvested log files stored in Serviceability Agent enabled hosts or elements. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. With a successful harvest request related to a harvest profile, the logging service accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same computer or on different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface and the status of each archive is available in the user interface table.

You can perform the following operations using the log harvesting service:

- Create a log harvesting profile to specify the products for which you want to harvest the logs.
- Submit the log harvesting request defined in a profile to the product.
- View the status of the log harvesting request.
- Store the harvested log files of a product in an archive file.
- View the harvested log files stored in the archive file.
- Download the harvested log files to a local computer.
- Search for a matching text in the harvested log files.

Accessing the Log Harvester service

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

To create a new log harvesting profile, you must specify:

- The host name of the server on which the product is running.
- The product name.
- The directories or log files.
- The filter text if you select one or more directories.

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Procedure

1. On the home page of the System Manager web console, under **Services**, click **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvest page, click **New**.
3. Enter the appropriate information in the **Profile Name** and **Profile Descriptions** fields.
4. Select the host name of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective drop-down menus, press `CTRL` and click the directories or files.
   - To clear a selection, press `CTRL` and click the item.
   - To add another log harvesting request for a different product or for another instance of the same product, click the plus sign (**+**).
5. If you select one or more directories, in the **File Name Filter** field, enter a text pattern for the filter criteria.

   During the harvesting operation, the system harvests only those files that match the filter criteria.
6. Click **Save** to save the profile and the log harvesting requests in the profile.

Create New Profile field descriptions

Use this page to create a new log harvesting profile for harvesting log messages from the log files for one or more products. The files can reside on one or more servers.

Name	Description
Profile Name	The name of the log harvesting profile.
Profile Description	A brief description of the profile. This is an optional field.
Host Name	The host name of the server on which products are installed.
Product	The products for which you can harvest logs.
Directories	A list of directories that contains the log files for the selected product.
Files	The log files that you can harvest for the selected product.
File Name Filter	The text on which to filter the log file names that display under the selected directory. For example: If you select the directory **/a/b/c** and enter **com** in the **File Name Filter** field, the harvest operation for this profile harvests the log files that are in the directory **/a/b/c**. The log files contain **com** in the file name. The field does not support wild cards.

Button	Description
+	Add another log harvesting request for a product.
–	Delete a log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for harvesting requests in the database.
Cancel Profile	Cancel the profile request.

Submitting a request for harvesting log files

About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. After the request is successfully processed, the system on which the products are installed returns the harvested log files that are specified in the request. When you select a profile and click **Request**, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, enter the relevant information in the **Archive Name** and **Archive Description** fields.

   The system saves the harvested log files in the specified archive file.
5. Click **Run Profile** to send a request.

   The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then the system creates a zip file containing the harvested log files and saves the file in the specified location.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W