Upgrading and Migrating Avaya Aura® applications to Release 7.1.3 from System Manager

Release 7.1.3
Issue 5
May 2018

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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

Contents

Chapter 1: Introduction 9
Purpose 9
Prerequisites 9
Change history 9
Chapter 2: Upgrade overview and considerations 12
Upgrade Management overview 12
Automated upgrades and migrations of Avaya Aura® applications 13
Upgrade automation support by Solution Deployment Manager 14
Upgrade modes using System Manager Solution Deployment Manager 15
Supported upgrades and migrations 16
Supported servers 17
Communication Manager migration considerations 18
Communication Manager Messaging migration considerations 18
Chapter 3: Planning for upgrade 20
Documentation map for Avaya Aura® application upgrade tasks 20
Latest software updates and patch information 21
Software details of System Manager 22
Supported upgrade paths to Avaya Aura® Release 7.1.3 22
Upgrades from System Platform on 6.x to Appliance Virtualization Platform on Avaya Aura® 7.1 25
Utility Services in the Avaya Aura® Virtualized Appliance offer 27
Upgrade order for Avaya Aura® applications 28
Upgrade order for Avaya Aura® applications 28
Upgrade order for Avaya Aura® applications using the Solution Deployment Manager client 30
Required permissions 31
Deployment options for Avaya Aura® Release 7.1.3 applications 31
Software library options 32
Manual addition of elements 32
Profile mapping for Communication Manager 6.x upgrades 33
Licensing upgrades 34
Rehost of license files 34
Chapter 4: Preupgrade tasks 36
Preupgrade tasks overview 36
Key tasks for upgrading Avaya Aura® applications to Release 7.1.3 36
Installing the Solution Deployment Manager client on your computer 39
Upgrade target release selection 41
Selecting the target release for upgrade 41
Preupgrade checklist for Linux® Operating System upgrades 42
Pre-upgrade checklist for System Platform upgrades 43
Virtual machine management 43

Virtual machine management..... 43
Managing the location..... 44
Managing the host..... 52
Downloading the OVA file to System Manager..... 78
Managing the virtual machine..... 79
Certificate validation..... 105
Managing vCenter..... 110
Monitoring a host and virtual machine..... 114
Chapter 5: Common procedures for deployment, upgrades, and migrations..... 116
Creating a backup of the existing configuration..... 116
Configuring servers preinstalled with Appliance Virtualization Platform..... 117
Activating SSH from Utility Services..... 120
Upgrade job status..... 120
Upgrade job status..... 120
Viewing the Upgrade job status..... 121
Editing an upgrade job..... 121
Deleting the Upgrade jobs..... 122
Upgrade Job Status field descriptions..... 122
Utility Services field descriptions..... 123
Recovering a Linux-based application from disaster..... 124
Recovering a System Platform-based application from disaster..... 124
Virtual machine migration from one host to another host..... 125
Chapter 6: Migration from System Platform to Appliance Virtualization Platform..... 126
Migration checklist..... 126
System Platform and template values worksheet..... 128
IP address mapping..... 130
Generating the Appliance Virtualization Platform kickstart file..... 130
Create AVP Kickstart field descriptions..... 130
Configuring the Appliance Virtualization Platform USB drive..... 133
Deploying Appliance Virtualization Platform..... 133
Enabling IP forwarding using Services Port VM for Utility Services..... 135
Appliance Virtualization Platform Out of Band Management..... 136
Teaming NICs from CLI..... 138
Setting the Ethernet port speed..... 140
Validating the migration..... 140
Chapter 7: Upgrade process..... 142
Upgrading Avaya Aura® System Manager..... 142
System Manager upgrade management..... 142
Verifying the installation of System Manager..... 161
Upgrading Avaya Aura® applications..... 161
Checklist for upgrading Avaya Aura® applications to Release 7.1.3..... 161
Upgrading Avaya Aura® applications to Release 7.1.3..... 163
Installing software patches..... 165

Installing custom software patches ... 167
Installed Patches field descriptions ... 169
Upgrade Management field descriptions ... 171
Upgrade Configuration field descriptions ... 173
Edit Upgrade Configuration field descriptions ... 174
Uploading a custom patch ... 183
Uploading custom patch field descriptions ... 183
Upgrading Avaya Aura® Communication Manager ... 184
Upgrading Communication Manager 6.x to Release 7.1.3 ... 184
Preparing duplex Communication Manager for migration ... 187
Migrating duplex Communication Manager on the same server ... 187
Migrating duplex Communication Manager on a different server ... 190
Upgrading Avaya Aura® Session Manager ... 192
Upgrading Session Manager or Branch Session Manager from Release 6.x to 7.1 through SDM ... 192
Upgrading Avaya Aura® applications using Solution Deployment Manager in the Geographic Redundancy setup ... 195
Upgrading Avaya Aura® applications when the primary System Manager is operational and the secondary System Manager is in standby mode ... 195
Upgrading Avaya Aura® applications when the primary System Manager is nonoperational and secondary System Manager is in active standby mode ... 195
Upgrading Avaya Aura® applications when the primary System Manager is operational, and the secondary in standby and pause state ... 196
Chapter 8: Avaya Aura® 7.1 migration scenarios ... 198
Avaya Aura® 7.1.x migration scenarios ... 198
Avaya Aura® application upgrade and migration considerations ... 198
Deploying 6.x applications to Avaya Aura® Release 7.1.3 by using the Solution Deployment Manager client ... 199
Upgrading Avaya Aura® 6.x applications in a customer-provided Virtualized Environment to Avaya Aura® Release 7.1.3 ... 201
Migrating System Platform-based Communication Manager 6.x to Avaya Aura® Release 7.1.3 on Appliance Virtualization Platform ... 203
Migrating Communication Manager 6.x S8300D or CM Simplex on survivable remote template to Avaya Aura® Release 7.1.3 ... 207
Migrating Communication Manager 6.x duplex for main and standby, survivable core, Branch Session Manager 6.x, System Manager 6.3.x, and Gateways ... 210
Migrating Communication Manager 6.x or 5.2.1 on S8800 duplex main or S8800 simplex survivable core with S8300D survivable remote ... 216
Migrating System Manager to Release 7.1.3 ... 218
Migrating Midsize Enterprise to Release 7.1.3 ... 219
Migrating System Platform-based elements or bare metal-based Communication Manager elements to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager ... 221

Migrating Communication Manager 6.x or CM Simplex on survivable remote template or Communication Manager 5.2.1 on S8330D to Avaya Aura® Release 7.1.3 with Appliance Virtualization Platform remote deployment 221
Migrating System Platform-based system and elements in bulk to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager 224
System Platform to Appliance Virtualization Platform migration scenarios 226
Appliance Virtualization Platform installation scenarios 226
Deploying Utility Services and virtual machines when Out of Band Management is enabled 227
Deploying Utility Services and virtual machines on the services port 228
Chapter 9: Post-upgrade tasks 230
Rehosting license files 230
Postmigration tasks for Communication Manager 230
Postmigration tasks for Communication Manager Messaging 231
Enhanced Access Security Gateway (EASG) overview 231
Managing EASG from CLI 231
Viewing the EASG certificate information 232
EASG site certificate 232
Deleting the virtual machine snapshot 233
Deleting the virtual machine snapshot from the Appliance Virtualization Platform host 233
Deleting the virtual machine snapshot from the vCenter managed host or standalone host .. 234
Chapter 10: Rollback process 235
Removing the Appliance Virtualization Platform patch from the ESXi host CLI 235
Upgrade rollback 237
Rolling back an upgrade 237
Chapter 11: Resources 238
Documentation 238
Finding documents on the Avaya Support website 239
Training 239
Viewing Avaya Mentor videos 240
Support 241
Using the Avaya InSite Knowledge Base 241
Glossary 243

Chapter 1: Introduction

Purpose

This document contains checklists and procedures for upgrading the Avaya Aura® applications.

This document is intended for people who upgrade applications in an Avaya Aura® solution by using Solution Deployment Manager that Avaya Aura® System Manager provides.

Prerequisites

Before you deploy or upgrade the product, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Avaya Aura® releases
- Linux® operating system
- VMware® and virtualized environment

Skills

- VMware® and virtualized environment

Tools

- Avaya supported servers or VMware® supported servers
- Solution Deployment Manager client if System Manager is unavailable or unreachable
- System Manager virtual machine resource requirements for each profile.
- Configuration tools and utilities

Change history

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

Issue	Date	Summary of changes
5	May 2018	For Release 7.1.3, added the following sections: • Deleting the virtual machine snapshot by using Solution Deployment Manager on page 74 • Snapshot Manager field descriptions on page 74 • Virtual machine report on page 103 • generate_report.sh command on page 103 • Generating a virtual machine report on page 103 • Viewing the status of the virtual machine report on page 104 • Aborting the virtual machine report generation on page 104 For Release 7.1.3, updated the following sections: • VM Management field descriptions on page 45
4	December 2017	For Release 7.1.2, added the following sections: • Appliance Virtualization Platform license on page 66 • Configuring WebLM Server for an Appliance Virtualization Platform host on page 68 • WebLM Configuration field descriptions on page 68 • Migrating Communication Manager 6.x or CM Simplex on survivable remote template or Communication Manager 5.2.1 on S8330D to Avaya Aura Release 7.1.3 with Appliance Virtualization Platform remote deployment on page 221 • Migrating System Platform-based system and elements in bulk to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager on page 224 For Release 7.1.2, updated the following sections: • Supported upgrades and migrations on page 16 • Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 54 • Create AVP Kickstart field descriptions on page 61 • Update Host field descriptions on page 78 • Edit Upgrade Configuration field descriptions on page 174
3	August 2017	Added the following sections: • Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 233 • Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 234

Table continues…

Issue	Date	Summary of changes
2	August 2017	For Release 7.1.1, updated the following sections: • Adding an Appliance Virtualization Platform or ESXi host on page 52 • Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI on page 64 • Adding a vCenter to Solution Deployment Manager on page 110 • New vCenter and Edit vCenter field descriptions on page 113
1	May 2017	Release 7.1 document.

Chapter 2: Upgrade overview and considerations

Upgrade Management overview

Upgrade Management in Solution Deployment Manager is a centralized upgrade solution of System Manager, provides an automatic upgrade of Avaya Aura® applications. You can upgrade Communication Manager, Session Manager, and Branch Session Manager directly to Release 7.1.3 from a single view. Communication Manager includes associated devices, such as Gateways, TN boards, and media modules. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

Important:

System Manager Release 7.1.3 and later also support the System Manager Release 6.3.8 flow to upgrade Communication Manager, gateways, media modules, and TN boards to Release 6.3.100. However, the Release 6.3.8 user interface is available only when you select **Release 6.3.8** as the target version on the Upgrade Release Selection page.

With Upgrade Management, you can perform the following:

1. Refresh elements: To get the current state or data such as current version of the Avaya Aura® application. For example, for Communication Manager, gateways, media modules, and TN boards.
2. Analyze software: To analyze whether the elements and components are on the latest release and to identify whether a new software is available for the inventory that you collected.
3. Download files: To download files that are required for upgrading applications.

   You can download a new release from Avaya PLDS to the software file library and use the release to upgrade the device software.
4. Preupgrade check: To ensure that conditions for successful upgrade are met. For example, checks whether:
   - The new release supports the hardware
   - The RAID battery is sufficient
   - The bandwidth is sufficient

Note:

You must have the minimum network speed of 2Mbps with up to 100ms delay (WAN).

- The files are downloaded

5. Upgrade applications: To upgrade Avaya Aura® applications to Release 7.1.3.
6. Install patches: To install the software patches, service packs, and feature pack.

Upgrade automation level

- The upgrade of Communication Manager, Session Manager, Branch Session Manager, and Utility Services to Release 7.1.3 is automated. The upgrade process includes creating a backup, deploying OVA, upgrading, installing software patches, feature packs, or service packs, and restoring the backup.
- Upgrade of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVA files.

  However, the upgrade process involves some manual operations for creating backup, installing patches, and restoring the backup data.

Upgrade job capacity

System Manager Solution Deployment Manager supports simultaneous upgrades or updates of Avaya Aura® applications. Solution Deployment Manager supports the following upgrade capacity:

- 5 upgrade or update job groups: Multiple applications combined together in an upgrade or update job is considered a group.
- 20 applications in a job group: Maximum applications that can be combined in an upgrade or update job group is 20. You can combine any application type for upgrade in a group.

The capacity also includes applications that are in the paused state. If five upgrade job groups are running or are in a paused state, you cannot upgrade the sixth group.

Automated upgrades and migrations of Avaya Aura® applications

From System Manager Release 7.1.3, several Avaya Aura® applications support an automated migration path that the central System Manager Solution Deployment Manager facilitates. The migration process includes situations such as:

- Changing the server, operating system, and the hypervisor.
- Creating a backup and restoring a backup in addition to the normal upgrade process for the application.

The following are the objectives of the Avaya Aura® automated upgrade and migration:

- Move from a manual step-by-step procedure that is performed on the application server to an automated migration procedure on a centralized System Manager.

- Eliminate the time spent in waiting for each migration step to an automated sequencing of tasks with the application migration events automatically running in the background.
- Move from multiple manual tasks that require human intervention and assessment that might be error prone to reliable integrated checks that assess and confirm migration readiness.

Release 7.1.3 and later support automated migrations for:

- System Platform-based Communication Manager Release 6.x and Branch Session Manager Release 6.x
- Linux-based Session Manager Release 6.x and Communication Manager Release 5.2.1

The automated migration functionality applies to the appliance offer provided by Avaya and the customer-provided Virtualized Environment solution.

Upgrade automation support by Solution Deployment Manager

You can categorize Avaya Aura® applications upgrades into the following:

Fully automated migration

System Manager Solution Deployment Manager automates the entire migration process that covers creating a backup, deploying 7.1 OVA, installing the patches, feature packs, or service pack, and restoring the backup on the Release 7.1.3 system.

Avaya Aura® applications that supports automated migration flow:

- System Platform-based Communication Manager, Utility Services, and Branch Session Manager Release 6.x.
- Linux-based Session Manager Release 6.x and Communication Manager Release 5.2.1.

Semi automated migration

System Manager Solution Deployment Manager automates the deployment of the 7.1 OVA. You must manually create a backup of the existing system, install the Release 7.1.3 patches, service packs, or feature packs, and restore the data on the Release 7.1.3 system.

Communication Manager Messaging supports the semiautomated migration flow.

Manual migration

In the manual migration process, you must create a backup of the existing system, deploy 7.1 OVA by using the vSphere client, System Manager Solution Deployment Manager, or the Solution Deployment Manager client, install the Release 7.1.3 patches, and restore the data on the Release 7.1.3 system.

All other Avaya Aura® applications use the manual migration process flow. For more information, see the appropriate *Upgrading and migrating to <Avaya Aura application 7.x>* document.

Upgrade modes using System Manager Solution Deployment Manager

Operation	Application Name	Tool or application supported
Fresh deployments	Application Enablement Services Avaya Aura® Device Services. Avaya Aura® Media Server Avaya Aura® Messaging Avaya Breeze™ Avaya Diagnostic Server Branch Session Manager Communication Manager Communication Manager Messaging Session Manager System Manager **Note:** Only from Solution Deployment Manager client. Utility Services WebLM	• System Manager Solution Deployment Manager • Solution Deployment Manager client
Deployment during migration	Upgrade System Manager Install the System Manager patch Install the Appliance Virtualization Platform patch	Solution Deployment Manager client
Automated upgrade	Branch Session Manager Communication Manager Session Manager Utility Services WebLM	System Manager Solution Deployment Manager
Semi-automated upgrade	Communication Manager Messaging	System Manager Solution Deployment Manager

Table continues…

Operation	Application Name	Tool or application supported
Manual upgrade	Application Enablement Services Media Server Presence Services on Avaya Breeze™ SAL or Services VM WebLM	

Supported upgrades and migrations

Supported upgrades

With Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.1.3:

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

  Important:

  Solution Deployment Manager does not support the upgrade of G430 Branch Gateway and G450 Branch Gateway to:

  - Release 7.1.0.2 (Build 38.21.0 and 38.21.30) from any prior release
  - Release 7.1.2.0 (Build 39.5.0 and 39.5.30) from any prior release

  For more information, see *Deploying and Upgrading Avaya G430 Branch Gateway* and *Deploying and Upgrading Avaya G450 Branch Gateway*.

- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- Branch Session Manager associated with Communication Manager
- Linux-based Session Manager
- Customer-provided Virtualized Environment solutions

Supported updates

With Solution Deployment Manager, you can install service packs, feature packs, and software patches for the following Avayaapplications:

- Appliance Virtualization Platform
- Branch Session Manager
- Communication Manager and the associated devices, such as media modules, TN boards, and media gateways
- Communication Manager Messaging

  Note:

  Communication Manager Messaging 7.0.0.1 is currently being tested with Appliance Virtualization Platform 7.1.2. Until testing is completed, do not install Communication Manager Messaging 7.0.0.1 on an Appliance Virtualization Platform 7.1.2 host, and postpone any Avaya Aura® 7.x VM upgrades to 7.1.2 that have a Communication Manager Messaging 7.0.1 VM co-residing on the same Appliance Virtualization Platform host. The Release Notes will be updated when the testing is completed. Once testing is completed and the release notes updated customers can install Communication Manager Messaging 7.0.0.1 on a new Appliance Virtualization Platform 7.1.2 host. The same will apply for upgrades of other Avaya Aura® VMs on a shared Appliance Virtualization Platform host with Communication Manager Messaging 7.0.0.1, they also can upgrade to 7.1.2.
- Session Manager
- Utility Services
- WebLM

Supported upgrades from the Solution Deployment Manager client

You can perform the following only from the Solution Deployment Manager client:

- Upgrading System Manager
- Installing software patches, feature packs, and service packs on System Manager

Supported servers

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

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

- HP ProLiant DL360 G9
- S8300D, for Communication Manager and Branch Session Manager
- S8300E, for Communication Manager and Branch Session Manager
- Intel 1006r server. Only to deploy Utility Services and Avaya Aura® Messaging OVA files.

Communication Manager migration considerations

When you upgrade a duplex Communication Manager, first upgrade the standby Communication Manager. When the standby Communication Manager upgrade is complete, upgrade the active Communication Manager.

Communication Manager Messaging migration considerations

When you upgrade Communication Manager with Communication Manager Messaging, you must:

- Add Communication Manager Messaging from the **Inventory** > **Manage Elements** page.
- Deploy Communication Manager Messaging OVA with a new IP address during Communication Manager migration.
- Create a backup for messaging translations, names, and messages and create a separate backup of announcements if Communication Manager Messaging contains custom recorded announcements

  For more information, see *Upgrading to Avaya Aura® Communication Manager*. The maximum limit for backup is about 50 GB. Communication Manager Messaging backup can be about 250 GB.

Perform the following tasks while creating a Communication Manager Messaging backup:

1. Create a Communication Manager Messaging backup on the Release 5.2.1 and Release 6.3.x systems.
2. For Release 5.2.1, install A9021rf+i.rpm and C1317rf+i.rpm on the Release 5.2.1 system on which Communication Manager Messaging is enabled.

   RPMs are available on the support site in the Communication Manager 5.2.1 version downloads at https://support.avaya.com/downloads.
3. To verify the Communication Manager Messaging release, run the **`swversion`** command.

   The system displays the following:

   ```
   Messaging: +-N5.2.1-13.0---Ci+Ak+----
   ```

4. From the Communication Manager 5.2.1 system, create a backup of Communication Manager Messaging data and save on a different remote server that you can restore after migration.
5. Start the migration process from the System Manager web console.

   The migration process shuts down the earlier Communication Manager and deploys Communication Manager and Communication Manager Messaging. For Communication Manager, System Manager automatically performs the migration process . The process includes installing the migration patch, creating the backup, deploying OVA, installing the feature pack or service pack, and restoring the backup on the Release 7.1.3 system.
6. When creating a backup of the system during the migration from Communication Manager Release 5.2.1 or 6.x with Communication Manager Messaging to Release 7.1.1, check for any additional languages. The languages must be restored on the Release 7.1.1 system before restoring the backup.

Chapter 3: Planning for upgrade

Documentation map for Avaya Aura® application upgrade tasks

The document covers:

- Fully automated upgrade flows or automated migration process by using System Manager Solution Deployment Manager. For example, Communication Manager and Session Manager.
- Semi-automated upgrade flow to migrate the Avaya Aura® applications by manually taking a backup, deploying OVA, and manually restoring the data. For example, Application Enablement Services. For more information, see the *Upgrading and migrating to <Avaya Aura® application>* document for the specific release.

Task	Document
Download the OVA files and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at http://support.avaya.com. **Note:** For information about the upgrade sequence and the required patches, see the latest *Avaya Aura® Release Notes* for the specific release on the Avaya Support website.	-
Obtaining the supported server and installing the server for Avaya-provided appliance deployments.	Installation procedures for servers supported in Release 7.1.3.
Installing Appliance Virtualization Platform.	This document
Installing the Solution Deployment Manager client if System Manager is unavailable.	*Deploying Avaya Aura® applications from System Manager*
Ensuring that System Manager is installed and operational.	*Deploying Avaya Aura® applications from System Manager*
Upgrading System Manager if required using the Solution Deployment Manager client.	*Upgrading Avaya Aura® System Manager*
Configuring SNMP for successful discovery of elements, such as Communication Manager and Session Manager.	"Managing inventory" in *Administering Avaya Aura® System Manager*

Table continues…

Task	Document
Adding elements or automatically discovering applications and associated devices.	“Managing inventory” in *Administering Avaya Aura® System Manager*
Setting up PLDS or alternate source.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Setting up the software library.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Refreshing software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Analyzing the software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Downloading the entitled software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Running the preupgrade check.	This document
Upgrading the application.	This document
Checking preupgrade or upgrade job status	This document
Installing the service pack or feature pack	This document
Post upgrade tasks. For example: • Creating a backup of new system. • Installing the ASG file.	Upgrading <Avaya Aura application>. For example, for postupgrade tasks for Communication Manager, see *Upgrading to Avaya Aura® Communication Manager*.
Verifying the upgrade or migration.	For initial verification, see the Upgrade Management page. For complete verification procedure, see the appropriate upgrade document. For example for upgrading Session Manager, see *Upgrading Avaya Aura® Session Manager*.

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.

Software details of System Manager

You can download the following software from the Avaya PLDS website at http://plds.avaya.com/.

Product name	Release version and Service pack	OVA details
System Manager	Release 7.1.3	• **Profile 1 and Profile 2:** `SMGR-7.1.0.0.1125193-e65-50.ova` • **Profile 3:** `SMGR-PROFILE3-7.1.0.0.1125193-e65-50.ova` • **Patch:** `System_Manager_7.1.3.0_r713007763.bin` • **Data Migration Utility:** `datamigration-146.bin` • **Solution Deployment Manager:** `Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip` contains `Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe`

Supported upgrade paths to Avaya Aura® Release 7.1.3

Table 1: System Manager

Release	Offer and Deployment
7.1	Appliance Virtualization Platform and Virtualized Environment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.3.x, 6.2.x, 6.1.x, or 6.0 Service Pack 1 and 2	System Platform
6.3 or 6.2	Virtualized Environment
5.2	Appliance

Table 2: Application Enablement Services

Release	Offer and Deployment
7.1.x	Appliance Virtualization Platform and Virtualized Environment

Table continues…

Release	Offer and Deployment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.x or 5.2.x	• System Platform • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • The IBM x3550 M2 not supported with Application Enablement Services Release 7.1.3
6.x	Virtualized Environment
6.x	• Non-System Platform • Bundled server • S8510 not supported with Application Enablement Services Release 7.1.3
5.2.x	• Non-System Platform • Bundled server • S8500C or S8510
4.x or 3.x	• Bundled server S8500B, S8500C. • S8510 • IBM x3550 M2 not supported with Application Enablement Services Release 7.1.3

Table 3: Communication Manager

Release	Offer and Deployment
7.1.x	Appliance Virtualization Platform and Virtualized Environment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.3.x, 6.2.x, or 6.0.1	• System Platform • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • S8300D • S8300E from Communication Manager 6.3.6

Table continues…

Release	Offer and Deployment
6.3.x, 6.2.x, or 6.0.1	System Platform on unsupported servers. For example, S8800 and S8510.
6.3.x, 6.2.x, or 6.0.1	Virtualized Environment
5.2.1	Appliance

Table 4: Communication Manager Messaging

Release	Offer and Deployment
6.3	System Platform embedded with Communication Manager 6.3
6.3	Virtualized Environment

Table 5: Session Manager

Release	Offer and Deployment
7.1.x	Appliance Virtualization Platform and Virtualized Environment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.3, 6.2, 6.1, or 6.0	• Appliance • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620, or HP ProLiant DL360p G8
6.3, 6.2, 6.1, or 6.0	Appliance— older servers
6.3 or 6.2	Virtualized Environment
5.2	Appliance on unsupported servers
Release earlier than 5.0	Appliance on unsupported servers

Table 6: Presence Services

Release	Offer and Deployment
6.2.6 with the latest service pack or 6.2.5	• System Platform • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8
6.2.6 or 6.2.5	Software only
6.2.6 or 6.2.5	Virtualized Environment

Table continues…

Release	Offer and Deployment
Release earlier than 6.2.5	System Platform
Release earlier than 6.2.5	Software Only

Table 7: Utility Services

Release	Offer and Deployment
7.1.x	Appliance Virtualization Platform and Virtualized Environment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.2 or 6.3	System Platform
6.2 or 6.3	Virtualized Environment

Table 8: WebLM

Release	Offer and Deployment
7.1.x	Appliance Virtualization Platform and Virtualized Environment
7.0.x	Appliance Virtualization Platform and Virtualized Environment
6.2.x	System Platform
6.2.x or 6.3.0	Virtualized Environment
Release earlier than 6.0	System Platform, standalone WebLM deployed with adopting products.

Upgrades from System Platform on 6.x to Appliance Virtualization Platform on Avaya Aura® 7.1

In Release 7.1.3 and later, you can select the applications that are installed on a server. Therefore, when planning for upgrade to Release 7.1.3, you must ensure that correct application OVA files are included. In an upgrade, the Avaya Solution Designer (ASD) automatically provisions the OVA files that are required to run the solution on Appliance Virtualization Platform, Appliance Virtualization Platform, and the required license enablement codes.

- Utility Services: You require Utility Services for all deployments with Appliance Virtualization Platform to provide a services port functionality.
- You require a separate instance of WebLM for Application Enablement Services to support Enterprise Licensing with allocation mode which uses a master and local WebLM.
- Presence Services is supported as a snap-in on Avaya Breeze™, so that OVA needs to be installed on the server in Release 7.1.3.

System Platform Template	Applications Included in template on System Platform 6.x	OVAs needed in Release 7.1.3 for upgrade to Appliance Virtualization Platform	Notes
CM Duplex	Communication Manager, with SAL and WebLM as part of System Platform CDOM.	Communication Manager, Utility Services, SAL	Since WebLM is part of System Manager, no separate WebLM OVA is required.
CM Simplex Main	Communication Manager, Communication Manager Messaging, Utility Services, with SAL and WebLM as part of System Platform CDOM.	Communication Manager, Communication Manager Messaging, Utility Services, SAL	Since WebLM is part of System Manager, no separate WebLM OVA is required.
CM Simplex Survivable Core	Communication Manager, Communication Manager Messaging, Utility Services, with SAL and WebLM as part of System Platform CDOM.	Communication Manager, Communication Manager Messaging, Utility Services, SAL	Since WebLM is part of System Manager, no separate WebLM OVA is required.
Survivable Remote	Communication Manager, Branch Session Manager, Utility Services, with SAL and WebLM as part of System Platform CDOM	Communication Manager, Branch Session Manager, Utility Services, SAL	Since WebLM is part of System Manager, no separate WebLM OVA is required
System Manager	System Manager with WebLM, and SAL as part of System Platform CDOM.	System Manager, SAL, Utility Services	Since WebLM is part of System Manager, no separate WebLM OVA is required.
Application Enablement Services	Application Enablement Services with SAL and WebLM as part of System Platform CDOM.	Application Enablement Services, SAL, Utility Services, WebLM	

Table continues…

System Platform Template	Applications Included in template on System Platform 6.x	OVAs needed in Release 7.1.3 for upgrade to Appliance Virtualization Platform	Notes
Midsize Enterprise	Communication Manager or Communication Manager Messaging, Session Manager, System Manager, Presence Services, Application Enablement Services, Utility Services, with SAL and WebLM as part of System Platform CDOM.	Communication Manager, Communication Manager Messaging, Session Manager, System Manager, Presence Services, Avaya Breeze™, Application Enablement Services, Utility Services, SAL	Since WebLM is part of System Manager, no separate WebLM OVA is required.
Presence Services	Presence Services with SAL and WebLM as part of System Platform CDOM.	Presence Services, Avaya Breeze™, Utility Services .	Since WebLM is part of System Manager, no separate WebLM OVA is required.

Related links

Utility Services in the Avaya Aura Virtualized Appliance offer on page 27

Utility Services in the Avaya Aura® Virtualized Appliance offer

From Avaya Aura® Release 7.1.3, Utility Services replaces the console domain (C-dom). Utility Services runs the Services Port connection that was previously run through Dom-0 on System Platform. Therefore, Utility Services with the Services Port is a key component of the Avaya Aura® Virtualized Appliance offer in Release 7.1.3, You must deploy Utility Services on each Appliance Virtualization Platform.

With Services Port, you can connect a laptop directly to Ethernet 1 on an Avaya-supported server, and connect the laptop to any of management interface of applications that run on an Appliance Virtualization Platform host. On the S8300D and S8300E servers, Services Port is on the front plate.

The Services Port virtual machine incorporates the Serviceability Agent for alarming and log collection from System Manager.

From Avaya Aura® Release 7.1.3, Utility Services does not include IP Phone firmware. The administrator must download the latest version of the firmware from PLDS and install on Utility Services.

Utility Services migration

In the Avaya Aura® Virtualized Appliance offer on Appliance Virtualization Platform, you require Utility Services for services static routing. Therefore, you must deploy Utility Services if Utility Services is part of the solution.

In the following two use cases, you might require to deploy Utility Services.

1. Migration of Communication Manager or Session Manager on the Linux® server: Utility Services is mandatory for migration of systems running on the Linux® server. In this case, before you migrate, you must deploy Utility Services from VM Management.
2. Migration of Communication Manager or Session Manager on System Platform: In this case, the template already contains Utility Services. In this case, the process migrates Utility Services, and you do not require to deploy Utility Services separately.

Related links

Upgrades from System Platform on 6.x to Appliance Virtualization Platform on Avaya Aura 7.1 on page 25

Upgrade order for Avaya Aura® applications

Upgrade order for Avaya Aura® applications

Upgrade the applications in the Avaya Aura® solution in the following sequence:

Note:

System Manager is an integral part of the Avaya Aura® solution.

Upgrade using System Manager SDM and the SDM client	Upgrade using the SDM client
Upgrade the Solution Deployment Manager client.	Upgrade the Solution Deployment Manager client.
Using the Solution Deployment Manager client, update the Appliance Virtualization Platform host that hosts System Manager.	Start an SSH session, log in to Utility Services, and enable SSH for Appliance Virtualization Platform.
Using the Solution Deployment Manager client: • In the non-Geography Redundancy setup, update standalone System Manager. • In the Geography Redundancy setup, update the primary System Manager. Avaya recommends that you use System Manager to update Avaya Aura® application.	Shutdown virtual machines on Appliance Virtualization Platform.

Table continues…

Upgrade using System Manager SDM and the SDM client	Upgrade using the SDM client
If updating the host, first update Appliance Virtualization Platform.	Change the IP address to 192.168.13.5 or to the customer network address.
Update Utility Services.	Depends if services port, eth1 or customer network, eth0 is used.
Update all Session Manager servers.	Update Appliance Virtualization Platform.
Update all Branch Session Manager servers.	Start virtual machines running on Appliance Virtualization Platform.
Update Avaya Aura® Device Services.	Update Utility Services.
Update G650 or H.248 gateways if IPSI firmware requires an update.	Using the Solution Deployment Manager client: • In the non-Geography Redundancy setup, update standalone System Manager. • In the Geography Redundancy setup, update the primary System Manager.
Update all survivable remote servers.	In multiple Appliance Virtualization Platform server deployment, upgrade Appliance Virtualization Platform that hosts System Manager.
Update all survivable core servers.	Update all Session Manager servers.
In duplex configuration, update the standby Communication Manager server	Update all Branch Session Manager servers.
In duplex configuration, update the active Communication Manager server.	Update Avaya Aura® Device Services.
Using the application CLI, update Avaya Aura® Media Server.	Update G650 or H.248 gateways if IPSI firmware requires an update.
Using the application CLI, update Avaya Breeze™.	Update all survivable remote servers.
Using Snap-in Manager, update the Avaya Breeze™ snap-in, Presence.	Update all survivable core servers.
Update Application Enablement Services.	Update the active Communication Manager server.
Update SAL.	Using the application CLI, update Avaya Aura® Media Server.
-	Using the application CLI, update Avaya Breeze™.
-	Using Snap-in Manager, update the Avaya Breeze™ snap-in, Presence.
-	Update Application Enablement Services.
-	Update SAL.

Upgrade order for Avaya Aura® applications using the Solution Deployment Manager client

Upgrade the applications in the Avaya Aura® solution using the Solution Deployment Manager client in the following sequence:

Note:

System Manager is an integral part of the Avaya Aura® solution.

Upgrade using the SDM client
Upgrade the Solution Deployment Manager client.
Start an SSH session, log in to Utility Services, and enable SSH for Appliance Virtualization Platform.
Shutdown virtual machines on Appliance Virtualization Platform.
Change the IP address to 192.168.13.5 or to the customer network address.
Depends if services port, eth1 or customer network, eth0 is used.
Update Appliance Virtualization Platform.
Start virtual machines running on Appliance Virtualization Platform.
Update Utility Services.
Using the Solution Deployment Manager client: • In the non-Geography Redundancy setup, update standalone System Manager. • In the Geography Redundancy setup, update the primary System Manager.
In multiple Appliance Virtualization Platform server deployment, upgrade Appliance Virtualization Platform that hosts System Manager.
Update all Session Manager servers.
Update all Branch Session Manager servers.
Update Avaya Aura® Device Services.
Update G650 or H.248 gateways if IPSI firmware requires an update.
Update all survivable remote servers.
Update all survivable core servers.
Update the active Communication Manager server.
Using the application CLI, update Avaya Aura® Media Server.
Using the application CLI, update Avaya Breeze™.
Using Snap-in Manager, update the Avaya Breeze™ snap-in, Presence.
Update Application Enablement Services.
Update SAL.

Required permissions

- The user role to log in to the software library server with privileges to HTTP, FTP, SCP, or SFTP to the element.
- Credentials to gain access to Avaya PLDS and the company ID.
- When you add System Platform to System Manager from **Manage Elements**, provide the username and password of System Platform for admin and root users.
- Require a unique log in to the Communication Manager that has correct privileges. You must create a user profile for this task.
- For successful element discovery, set up SNMPv1 when you configure Communication Manager for the element.

  When you add Communication Manager to System Manager, the administrator account and SNMPv1 access credentials must be the same in Communication Manager System Management Interface and **Manage Elements** on the System Manager web console.

System Manager admin requirements

System Manager provides access permissions to Solution Deployment Manager through Role Based Access Control (RBAC) for elements, such as Communication Manager, Session Manager, Branch Session Manager, and IP Office. System Manager defines flexible access privileges for deployment, migration, upgrade, and update so that the users with administrator credentials can create their own roles.

Set the User Management and VM Management permissions to the user to perform the deployment and upgrade-related operations. For more information, see Managing roles in *Administering Avaya Aura® System Manager*.

Deployment options for Avaya Aura® Release 7.1.3 applications

During upgrades, you can deploy Avaya Aura® Release 7.1.3 applications by using the following:

- System Manager deployment by using the Solution Deployment Manager client only.
- All other Avaya Aura® Release 7.1.3 applications:
  - The centralized Solution Deployment Manager that System Manager provides.
  - The Solution Deployment Manager client when System Manager is unavailable.

In Avaya Aura® Virtualized Appliance model, for fresh deployments, Avaya Aura® is available to end-users through a set of Avaya-supplied common servers. Avaya Aura® Virtualized Appliance is prepackaged with the virtualization software, and delivered to customers in a ready-to-run state.

Software library options

Set one of the System Manager software library options to save the files required for the upgrade process.

- External: Provide an external server and configure with the appropriate configuration to interoperate with Avaya Aura® applications.
- Internal: Use System Manager to store all software and firmware. You configure this option when establishing other configuration parameters as part of solution deployment setup. You can save up to 30 GB on System Manager.

  For more information, see Solution deployment and upgrades in *Administering Avaya Aura® System Manager*.

Related links

Manual addition of elements on page 32

Manual addition of elements

You can manually add an element to the System Manager inventory from the Manage Elements page. For example, System Platform.

You must add the ESXi host from VM Management on Solution Deployment Manager. The system displays the ESXi host on the Manage Elements page.

Related links

Software library options on page 32
Discovery of Avaya Aura applications and associated devices on page 32

Discovery of Avaya Aura® applications and associated devices

To manage and upgrade software from System Manager, you must discover elements in the network. The system performs the discovery by using discovery profiles, where you configure subnetwork, SNMP access profiles, and element types to be discovered.

On the Discovery tab of **Inventory** > **Manage Elements**, you can create discovery profiles and use the profiles to discover elements. The Manage Elements page displays the discovered elements.

You must configure the applicable discovery parameters for System Manager to discover the Avaya Aura® application. System Manager uses SNMPv1 or SNMPv3 to discover Avaya Aura® applications.

For applications such as Communication Manager, you can use SNMP discovery or add the application from Manage Elements.

Note:

To upgrade an Avaya Aura® application by using Solution Deployment Manager, discovery of applications, such as Communication Manager, Session Manager, and Branch Session Manager is a mandatory task.

Related links

Manual addition of elements on page 32

Profile mapping for Communication Manager 6.x upgrades

Before you upgrade Communication Manager from Release 6.x to Release 7.1.3 ensure the correct footprints are available.

The footprint values apply for Communication Manager running on Avaya-provided server or customer-provided Virtualized Environment.

Table 9: Summary of profile mapping

Communication Manager 6.x template	Communication Manager Release 7.1.3 deployment option	Resources
CM_onlyEmbed on S8300D and S8300E	CM Main Max users 1000 Small Main supporting up to 1000 users	2vCPUs, 3900 MHz, 3.5 Gb RAM
CM_SurvRemoteEmbed on S8300D and S8300E	CM Survivable Max users 1000 Small Survivable supporting up to 1000 users	1vCPU, 1950 MHz, 3.5 Gb RAM
CM as part of Midsize_Ent	CM Main Max users 2400 Medium Main only supporting up to 2400 users This profile is targeted as a migration path for Communication Manager on Midsize Enterprise.	2 vCPUs, 4400 MHz, 4.0 Gb RAM
CM_Simplex	CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_SurvRemote	CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_Duplex	CM Duplex Max users 30000 Standard Duplex 30,000 users	3 vCPUs, 6600 MHz, 5.0 Gb RAM

Table continues…

Communication Manager 6.x template	Communication Manager Release 7.1.3 deployment option	Resources
CM_Duplex high capacity	CM High Duplex Max users 36000 High Duplex 36,000 users	3 vCPUs, 7800 MHz, 5.0 Gb RAM

Licensing upgrades

To upgrade or migrate applications to Release 7.1.3 in an Avaya Aura® solution, you require new licenses.

For example, if Communication Manager and Session Manager are part of the solution, generate the new Communication Manager Release 7.1.3 and Session Manager license files from Avaya by using the centralized System Manager WebLM.

- Get the primary host ID from **Services** > **Licenses** > **Server properties** that you require to generate the Release 7.1.3 license file.
- On centralized WebLM, install the Communication Manager Release 7.1.3 and Session Manager Release 7.1.3 license files.

Note:

Appliance Virtualization Platform is automatically licensed when you accept the license terms and conditions. You do not need a separate license file to install or upgrade Appliance Virtualization Platform.

Rehost of license files

When you upgrade an Avaya Aura® application from release earlier than 7.1.3, existing license files become invalid. You must rehost licenses after the upgrade.

You must rehost licenses in the following scenarios:

- Upgrade: During upgrades, you must setup a new virtual machine with new UUID and then restore data on the new virtual machine. When UUID changes, host ID also changes, and any existing license files become invalid.
- Migration from System Platform to Appliance Virtualization Platform or customer Virtualized Environment: The host ID changes during migration.
- Change in IP address: The host ID also changes when the IP address changes.
- VMware cloning of WebLM: UUID changes during VMware cloning. Therefore, host ID also changes.

In customer Virtualized Environment deployments, you do not need to rehost licenses for vMotion moves.

Related links

Rehosting license files on page 230

Chapter 4: Preupgrade tasks

Preupgrade tasks overview

To successfully upgrade the system to Release 7.1.3, you must perform all tasks listed in the Preupgrade tasks section.

Key tasks for upgrading Avaya Aura® applications to Release 7.1.3

The table contains the key tasks that are required to upgrade Avaya Aura® applications to Release 7.1.3.

Performing the preconfiguration steps

Task	Note
For Communication Manager, click **Save Trans** to save the changes that you have made. For Session Manager, using command line interface, create a backup of the system.	
Ensure that sufficient disk space is available for the server that you have attached with the software library.	
Create a user with administrator credentials to gain access for the applications using HTTP, FTP, SCP or SFTP services.	
For the Avaya Aura® application instance that you have created, create a user and the user profile.	
Configure SNMP for the user.	
For the Communication Manager instance, create the EPW file for the following templates: • Embedded CM Main • Embedded Survivable Remote	

Table continues…

Task	Note
Add the Avaya Aura® application 6.x license file.	
Ensure that you have the PLDS access credentials and Company ID.	
Administer Branch Session Manager in System Manager.	

Performing the initial setup

Task	Note
1. Install the physical or virtual servers that support the Avaya Aura® applications that you want to deploy. 2. Deploy System Manager 7.1. 3. For Release 7.1.3 system, install the Release 7.1 OVA file to upgrade to Release 7.1.3.	You require a working knowledge of Communication Manager, System Manager, Session Manager, and Branch Session Manager. You require a working knowledge of the following processes: • Setting up PLDS. • Downloading Avaya Aura® applications from PLDS. • Configuring a standalone FTP, SCP, HTTP, or SFTP server to host Avaya Aura® applications. You must have administrator credentials for the Avaya Aura® applications that you are using.

Managing elements inventory

Task	Note
Configure Avaya Aura® application for administration and SNMP access.	“Managing inventory” in *Administering Avaya Aura® System Manager*
For Communication Manager, configure the access for the **H.248 Gateway** device.	

Performing the configuration settings required for upgrade

Task	Note
Option 1: Set up PLDS access through the Avaya Support site at https://support.avaya.com.	Log on to the PLDS website at http://plds.avaya.com. Use your PLDS account to get your Company ID. On the System Manager web console, go to **Services** > **Solution Deployment Manager** > **User Settings**. Enter the following details to get entitlements for analyze and artifacts for download: 1. SSO user name 2. SSO password 3. Company ID
Option 2: Set up the PLDS access through an alternate source.	
Set up the software library.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*

Performing the upgrade process

Task	Note
Refresh the elements in inventory.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Perform the analyze software operation for the Avaya Aura® application that you selected.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Download the software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Perform the preupgrade check.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Run the upgrade operation.	Upgrading Avaya Aura applications to Release 7.1.3 on page 163 Checklist for upgrading Avaya Aura applications to Release 7.1.3 on page 161 **Note:** The system takes about 2.5 hours to complete the upgrade process.

Installing feature packs and service packs

Task	Note
Install the Release 7.1.3 feature pack and any required software patches on the Avaya Aura® application.	Installing software patches on page 84
For Communication Manager, updating the H.248 media gateway device.	1. In the alternate source location, download the patch file `g450_sw_36.x.bin`. 2. For the gateway that you have selected, perform the Analyze job. 3. On the Select Gateway (G) panel, select **Library and download protocol**. 4. Click **Download**. 5. Click on active status link to observe the progress of upgrade.

Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

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

Procedure

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

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

4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

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

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

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

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

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

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

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

       Note:

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

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

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

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

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

    The installer creates a shortcut on the desktop.

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

Next steps

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

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

Upgrade target release selection

For backward compatibility, System Manager supports upgrading Communication Manager to Release 6.3.6 or later. By default, the target version is set to System Manager 7.0. Based on the entitlements, to upgrade Communication Manager and the associated applications to Release 6.3.6 or later, you must select 6.3.8 as the upgrade target release.

Related links

Selecting the target release for upgrade on page 41

Selecting the target release for upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select one of the following:
   - **SMGR 7.x**: To upgrade Avaya applications to Release 7.0 or later from the Upgrade Management page.

- **SMGR 6.3.8**: To upgrade Communication Manager and the associated applications to Release 6.3.6 or later from the **Upgrade Management** > **Software Inventory** page.

Important:

By default, the target version is set to Release 7.0.

4. Click **Commit**.
5. Click **OK**.
6. To perform the upgrade, click **Upgrade Management**.

Related links

Upgrade target release selection on page 41

Preupgrade checklist for Linux® Operating System upgrades

Perform the following checks before you start upgrading elements that you have deployed on System Manager on Linux® Operating System to System Manager on Appliance Virtualization Platform, on the same server or a different server:

Note:

No.	Task	✔
1	Ensure that you assign a different IP address for the ESXi host	
2	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all elements.	
3	On the User Settings page, ensure that PLDS or the alternate source are configured correctly.	
4	After you perform the **Analyze** operation, verify on the Upgrade Job status page that the operation you performed is successful.	
5	Download the OVA file for the element that you want to upgrade.	
6	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
7	On the Pre-upgrade Check Job Details page, ensure that the status of the element that you want to upgrade displays **Successful**.	
8	In the **Upgrade Job** status, in the Pre-upgrade Configuration page, verify the configuration values are correct.	

Pre-upgrade checklist for System Platform upgrades

Perform the following checks before you start upgrading elements on System Manager that you have deployed on System Platform to System Manager on System Platform, on the same server or a different server:

Note:

No.	Task	✔
1	Ensure that you assign a different IP address for the ESXi host.	
2	Ensure that you have added all the elements on the System Platform and you have established a structural relationship among all those elements.	
3	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all the elements.	
4	On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.	
5	After you perform the **Analyze** operation, verify on the Upgrade Job Status page that the operation that you performed is successful.	
6	Download the OVA file for the element that you want to upgrade.	
7	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
8	On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as **Successful**.	
9	In the **Upgrade Job Status** section, on the Pre-upgrade Configuration page, verify the configuration values are correct.	

Virtual machine management

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.

Related links

Certification validation on page 105

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.

Related links

New and Edit location field descriptions on page 51

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**.

Related links

New and Edit location field descriptions on page 51

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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Button	Description
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.
DNS Search List	The search list of domain names.

Table continues…

Name	Description
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.

Related links

New and Edit host field descriptions on page 75
Generating and accepting certificates on page 106

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.

Related links

New and Edit host field descriptions on page 75

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.

Related links

Update Host field descriptions on page 78

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.

Related links

Change Network Parameters field descriptions on page 75

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:

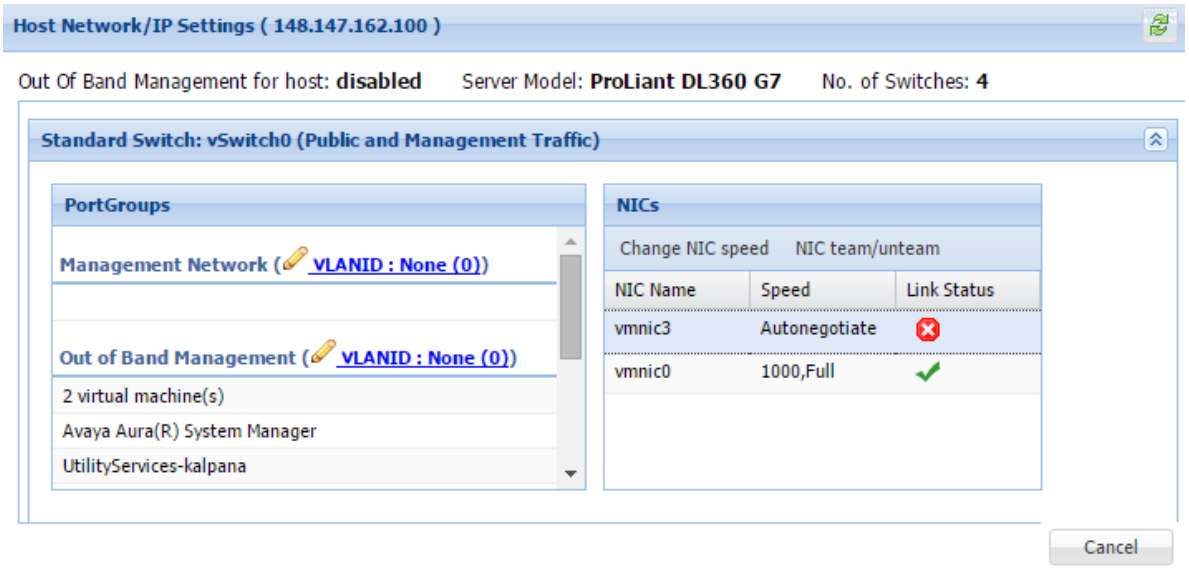
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fails because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

Related links

Host Network / IP Settings field descriptions on page 76

Changing the password for an Appliance Virtualization Platform host

About this task

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

Procedure

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

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

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

Related links

Password policy on page 60
Change Password field descriptions on page 77

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.

Related links

Changing the password for an Appliance Virtualization Platform host on page 60

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.

Related links

Create AVP Kickstart field descriptions on page 61

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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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.

Related links

Generating the Appliance Virtualization Platform kickstart file on page 61

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.

Related links

Snapshot Manager field descriptions on page 74

Snapshot Manager field descriptions

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

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

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 74

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).
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

Table continues…

Name	Description
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.

Table continues…

Name	Description
VLAN ID	Displays the VLAN ID. The options are: • **None (0)** • **1 to 4093** The field displays only unused IDs.
OK	Saves the changes.

NIC speed

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

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

NIC teaming

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

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

Change Password field descriptions

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

Table continues…

Name	Description
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.

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.

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
   - **Duplicate Link**: Only for duplex Communication Manager
   - **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.

Related links

VM Deployment field descriptions on page 91
Network Parameters and Configuration Parameters field descriptions

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
    - **Duplicate Link**: Only for duplex Communication Manager
    - **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

Perform the following for Communication Manager:

1. From the Manage Elements link on System Manager, update the username and password.
2. Before the synchronization and after deployment, add an SMNP profile on Communication Manager.

   Note:

   If you fail to update the password, the synchronization operation fails.

Related links

Installing software patches on page 84
VM Deployment field descriptions on page 91

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”.

Related links

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 233
Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 234
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 173
Edit Upgrade Configuration field descriptions on page 174
Installed Patches field descriptions on page 169

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.

Related links

Change Network Parameters field descriptions on page 75
Changing the network parameters for an Appliance Virtualization Platform host on page 56
Network parameter update for Avaya Aura applications on page 102

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.

Related links

Update Static Routing field descriptions on page 100

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.

Table continues…

Name	Description
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 96.

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

Table 10: 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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.

Related links

VM Deployment Configuration and Network Parameters field descriptions on page 96

VM Deployment Configuration and Network Parameters field descriptions

Table 11: 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.

Table continues…

Name	Description
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	
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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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

Table continues…

Name	Description
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
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

Table continues…

Avaya Aura® application	Command	Interface where you perform the task
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.

Certificate validation

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.

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.

Related links

Adding an Appliance Virtualization Platform or ESXi host on page 52
Generating new self-signed certificates for the ESXi host on page 109

Updating the certificate on the ESXi host from VMware

About this task

Use the procedure to update the ESXi host certificate.

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

Before you begin

Start an SSH session on the ESXi host.

Procedure

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

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

   The system generates and installs the certificate.
4. Restart the ESXi host.
5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. From the Direct Console User Interface (DCUI), restart management agents.

   Note:

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

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

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

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

Related links

Generating new self-signed certificates for the ESXi host on page 109

Managing certificates for existing hosts

About this task

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

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

Before you begin

Require permissions to add a host to generate certificates.

Procedure

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

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

Related links

Generating new self-signed certificates for the ESXi host on page 109
Generating and accepting certificates on page 106

Generating new self-signed certificates for the ESXi host

About this task

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

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

Before you begin

Start an SSH session on the ESXi host.

Procedure

1. Log in to the ESXi host as an admin user.
2. To create a backup of any existing certificates, in the `/etc/vmware/ssl` directory, rename the certificates by using the following commands:

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```

   Note:

   Do not perform the step if you are regenerating certificates because you deleted the certificates.
3. To generate new certificates, type `/sbin/generate-certificates`.
4. Restart the ESXi host.

   The generation process places the certificates places in the correct location.
5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. Restart management agents from Direct Console User Interface (DCUI).
6. Do the following to confirm that the host successfully generated new certificates:
   a. Type `ls -la`.
   b. Compare the time stamps of the new certificate files with `orig.rui.crt` and `orig.rui.key`.

Next steps

Replace the self-signed certificate and the key with a trusted certificate and key.

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.

Related links

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

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the 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**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.

Table continues…

Name	Description
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.

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.

Chapter 5: Common procedures for deployment, upgrades, and migrations

Creating a backup of the existing configuration

About this task

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

Procedure

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

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

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

Configuring servers preinstalled with Appliance Virtualization Platform

About this task

For newly purchased common servers, Appliance Virtualization Platform is preinstalled. This does not apply for migration. You must configure the customer network settings through the Solution Deployment Manager client that is installed on a computer that is running Windows. The media comes with the server. The new S8300D and S8300E servers require an installation at the customer site.

If the initial Appliance Virtualization Platform admin password for pre-installed servers is not provided, please contact your Avaya Professional Services or Business Partner Installer. For Common Server migrations, S8300D Server, and S8300E Server the password is assigned through the `7.1ks.cfg` file. The password is encrypted in the file. Please contact the installer who created the `7.1ks.cfg` file for the admin password.

Note:

When possible, perform the deployment from the System Manager Solution Deployment Manager. Only when System Manager is unreachable, use the Solution Deployment Manager client that is installed on the computer.

Procedure

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

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

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

      The system changes the host password.
7. To accept the EULA, in **Do you accept the terms of this EULA? (Y)es/(N)o**, type `Y`.
8. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

Enable: (Recommended)

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

Disable:

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

a. 1: To enable EASG.

   Avaya recommends to enable EASG.

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

b. 2: To disable EASG.

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

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

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

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

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

11. At the prompt, do the following:

    a. Type `./serverInitialNetworkConfig`.

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

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

```
System is not in a default setup, please use SDM to change IP addresses
Do you wish to setup networking? (y/n)  y
Please enter IP address for the AVP host in the format x.x.x.x
```

```
For example 172.16.5.1
Please enter value    172.16.107.21
Please enter subnet mask for the AVP host in the format x.x.x.x
For example 255.255.255.0
Please enter value    255.255.255.0
Please enter a default gateway for the AVP host in the format x.x.x.x
For example 172.16.5.254
Please enter value    172.16.107.1
Please enter a hostname for the AVP host.
For example myhost
Please enter value    avphost
Please enter a domain for the AVP host.
For example mydomain.com
Please enter value    mydomain.com
Please enter a main DNS server for the AVP host.
For example 172.16.10.54
Please enter value    172.16.107.1
Please enter a secondary DNS server for the AVP host.
For example 172.16.10.54
Please enter value    172.16.107.2
Please enter a NTP server for the AVP host
For example 172.16.10.55
Please enter value    172.16.107.50
Stopping ntpd
watchdog-ntpd: Terminating watchdog process with PID 33560
Starting ntpd
```

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

    Note:

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

    The system displays the following details:

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

13. Start the Solution Deployment Manager client when connected to the services port.
14. Add a location.
15. Add the Appliance Virtualization Platform host as 192.168.13.6.
16. Check the version, and install the Release 7.1.3 feature pack on Appliance Virtualization Platform if required.
17. Deploy Utility Services.
18. Deploy other Avaya Aura® applications that will reside on this Appliance Virtualization Platform host.
19. Install the Release 7.1.3 patch files for all Avaya Aura® applications.

Activating SSH from Utility Services

About this task

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

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

Before you begin

Start an SSH session.

Procedure

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

   ```
   ls
   AVP_SSH enable
   ```

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

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

Upgrade job status

Upgrade job status

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job. You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s)**: To get the latest data like version data for the applications in the system.

2. **Analyze**: To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check**: To evaluate an application that completed the Analyze job.
4. **Upgrade**: To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit**: To view commit jobs.
6. **Rollback**: To view rollback jobs.
7. **Uninstall**: To view uninstall jobs.

Viewing the Upgrade job status

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Status of Upgrade Management Jobs page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **View**.

   The system displays the Upgrade Job Status page.

Editing an upgrade job

Before you begin

You can edit the configuration of an upgrade job that is in pending state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click **Upgrade**.
4. Select a pending upgrade job that you want to edit.
5. Click **Edit Configuration**.

   The system displays the Upgrade Configuration page.
6. To edit the configuration, see Upgrading Avaya Aura applications.

Related links

Upgrading Avaya Aura applications to Release 7.1.3 on page 163

Deleting the Upgrade jobs

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **Delete**.

   The system updates the Upgrade Job Status page.

Upgrade Job Status field descriptions

Name	Description
Job Type	The upgrade job type. The options are: • **Refresh Element(s)**: To view refresh elements jobs. • **Analyze**: To view analyze jobs. • **Pre-Upgrade Check**: To view preupgrade check jobs. • **Upgrade**: To view upgrade jobs. • **Commit**: To view commit jobs. • **Rollback**: To view rollback jobs. • **Uninstall**: To view uninstall jobs.
Job Name	The upgrade job name.
Start Time	The time when the system started the job.
End Time	The time when the system ended the job.
Status	The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.
% Complete	The percentage of completion of the upgrade job.
Element Records	The total number of elements in the upgrade job.
Successful Records	The total number of times that the upgrade job ran successfully.
Failed Records	The total number of times that the upgrade job failed.

Button	Description
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.

Table continues…

Button	Description
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Utility Services field descriptions

Utility Services can gain access to the hypervisor and all virtual machines. The Utility Services application provides application routing between the physical port and virtual applications.

Name	Description
Foot print	• Small (S8300D): Reduces the memory allocated for Utility Services virtual machine on the S8300D server that has limited resources. With the default footprint on S8300D, the system might not run all the required virtual machines. • Default : All other server platforms
Mode	The mode in which you can deploy Utility Services. The options are: • Services Port Only: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services. 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. • Utility Servers 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 nonoperational. • Full Functionality: Utility Services and Services port enabled. This is the default mode for AVP. You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed.

Recovering a Linux-based application from disaster

About this task

Use the procedure when a Linux-based application becomes nonoperational after an upgrade or migration. For example,

- Session Manager Release 6.x
- Communication Manager Release 5.2.1

Before you begin

Create a backup of the application during upgrade and migration.

Procedure

1. Using a Linux® Operating System Recovery CD-ROM, partition reset.
2. Install Linux® Operating System and use the application network settings that you recorded at the beginning of the upgrade or migration.

   The application network settings include all IP addresses, subnet mask, gateway, DNS address, and NTP Server.
3. Restore the backup of the application that you created before the upgrade or migration.

Recovering a System Platform-based application from disaster

About this task

Use the procedure when a System Platform-based application becomes nonoperational after an upgrade or migration. For example:

- Communication Manager Release 6.x
- Utility Services
- SAL
- WebLM
- Application Enablement Services

Before you begin

Create a System Platform backup.

The backup contains the application template and System Platform backup details.

Procedure

1. Using a Linux® Operating System Recovery CD-ROM, partition reset.
2. Install System Platform and use the application network settings that you recorded at the beginning of the upgrade or migration.

The application network settings include all IP addresses, subnet mask, gateway, DNS address, and NTP Server.

3. Restore the System Platform backup that you created before the upgrade or migration.

Virtual machine migration from one host to another host

When a user moves a virtual machine from one host to another host, the system displays the entry of the virtual machine on both the hosts until the user explicitly refreshes the old host. Also, if the user refreshes the new host before refreshing the old host, the system displays the entry of the virtual machine on both the hosts. This results in displaying duplicate entries of virtual machines. If trust is already established, you can also view the duplicate entries of virtual machines under the System Manager inventory.

To remove the duplicate entry of virtual machine, refresh the old host.

Chapter 6: Migration from System Platform to Appliance Virtualization Platform

Migration checklist

No.	Task	Description	✔
1	Get the backup media.	The backup media contains the following software: • System Platform • Templates • DVD • System Platform service packs and software patches. Download any missing components from the PLDS website.	

Table continues…

No.	Task	Description	✔
2	Get the migration media.	From the PLDS website, download the following components that are required to migrate to Appliance Virtualization Platform: • The latest Appliance Virtualization Platform DVD • Appliance Virtualization Platform 7.1.3 installation file, `avaya-avp-7.1.0.0.0.x.iso` • Appliance Virtualization Platform 7.1.3 upgrade bundle, `upgrade-avaya-avp-7.1.3.0.0.xx.zip`. It is also available in the Appliance Virtualization Platform ISO image in the `\avp_upgrade_bundle\upgrade-avaya-avp-7.1.3.0.0.xx.zip` folder. • The Solution Deployment Manager client, if required • OVA files for System Manager and other applications • System Manager Release 7.1.3 patch file • Release 7.1.3 patch files for other Avaya Aura® applications Get USB Flash Drive in the FAT32 format.	
3	Create a local backup of System Platform and the template data.	Creating a backup of the existing configuration on page 116	
4	Create a back up of all virtual machines.	Create a backup of each virtual machine. For more information, see the documentation of the application templates. For System Platform Release 6.0, perform the following: • Log in to the System Platform console. • Navigate to the SAL gateway. • Note the values that you need to enter into the new SAL that you create. Onboard SAL is optional, and might not be operational on System Platform. For remote SAL, update with the new values when the migration is complete. For 6.2 or later systems, you must navigate to the Services virtual machine, and record the settings.	

Table continues…

No.	Task	Description	✔
5	Record System Platform and template values.	Record the data on the System Platform and template values worksheet on page 128. 1. On the Main Console page, note the IP addresses. 2. On **Server Management** > **Network Configuration**, note the network configuration settings including DNS. 3. On the Date and Time page, note the NTP and timezone. 4. On **Server Management** > **SNMP Trap Receiver Configuration**, note the SNMP settings.	
6	Generate the Appliance Virtualization Platform kickstart file.	Generating the Appliance Virtualization Platform kickstart file on page 61	
7	Configure the USB drive.	Configuring the Appliance Virtualization Platform USB drive on page 133	
8	Insert the USB drive and Appliance Virtualization Platform DVD into the server and turn on the server.		
9	Install Appliance Virtualization Platform.	Deploying Appliance Virtualization Platform on page 133	
10	Install the Appliance Virtualization Platform patch.	Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 54	
11	Verify the Appliance Virtualization Platform installation.		
12	Deploy System Manager, Utility Services, and other Avaya Aura® applications.		
13	Install the patches for all Avaya Aura® applications.		

System Platform and template values worksheet

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

Reference	Name	Value
A	System Platform Domain 0 IP address	
B	System Platform Console Domain IP address	
C	Services VM IP address if used	
D	Template VM 1 IP	
E	Template VM2 IP address	
F	Template VM3 IP address	
G	Template VM 4 IP address	
H	Template VM 5 IP address	
I	Template VM6 IP address	
J	Template VM 7 IP address	
K	Template VM 8 IP address	
L	Template VM 9 IP address	
M	Subnet mask	
N	Gateway	
O	Routes	
P	NTP	
R	DNS	
S	SNMP trap target 1	
T	SNMP trap target 2	
U	SNMP trap target 3	
V	SNMP trap target 4	
W	SNMP trap target 5	
X	Timezone	

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

IP address mapping

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

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.

Related links

[Create AVP Kickstart field descriptions](#) on page 61

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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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.

Related links

Generating the Appliance Virtualization Platform kickstart file on page 61

Configuring the Appliance Virtualization Platform USB drive

Before you begin

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

Procedure

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

   See “Generating the Appliance Virtualization Platform kickstart file”.

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

Next steps

Install Appliance Virtualization Platform.

Deploying Appliance Virtualization Platform

About this task

Warning:

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

Before you begin

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

Note:

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

Procedure

1. Insert the USB drive and the Appliance Virtualization Platform CD-ROM into the server.

Use an external Avaya-approved USB CD-ROM drive for deploying Appliance Virtualization Platform on S8300D or S8300E. The only supported USB CD-ROM drive is Digistor DIG73322, comcode 700406267.

2. Log on to the System Platform web console, and click **Server Management** > **Server Reboot/Shutdown** > **Reboot** to restart the server.

   Warning:

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

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

   Note:

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

3. Remove the USB drive and CD-ROM.

   Note:

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

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

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

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

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

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

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

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

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

Warning:

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

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

    For more information, see Installing the Appliance Virtualization Platform patch from Solution Deployment Manager.
11. Deploy the Utility Services virtual machine, and then all other virtual machines with the data that you noted in “System Platform and Template values”.

    For instructions to deploy Utility Services and other virtual machines, see *Deploying Avaya Aura® applications from System Manager*.
12. From System Manager Solution Deployment Manager, install the required software patches for the virtual machines.

Enabling IP forwarding using Services Port VM for Utility Services

About this task

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

Note:

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

Procedure

1. Start an SSH session.
2. Log in to Utility Services as admin.
3. In the command line, perform one of the following:
   - To enable IP forwarding, type `IP_Forward enable`.
   - To disable IP forwarding, type `IP_Forward disable`.
   - To view the status of IP forwarding, type `IP_Forward status`.

Example

```
IP_Forward enable
Enabling IP Forwarding
```

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

Appliance Virtualization Platform Out of Band Management

Overview

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

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

  The management port of Appliance Virtualization Platform is assigned to the public interface.

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

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

  Note:

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

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

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

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

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

- IP address: 192.11.13.5
- Subnet Mask: 255.255.255.252

- Gateway: 192.11.13.6

You can access the Utility Services shell by using the IP Address 192.11.13.6.

Note:

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

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

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

Common servers

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

When deploying or reconfiguring Appliance Virtualization Platform:

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

S8300D

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

If Out of Band Management is enabled, the Out of Band Management network is assigned to a separate VLAN on the public interface. Otherwise all virtual machine interfaces are on the same network.

The Appliance Virtualization Platform management interface is assigned to:

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

Note:

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

S8300E

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

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

The Appliance Virtualization Platform management interface is assigned to:

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

Teaming NICs from CLI

About this task

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

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

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

You cannot perform NIC teaming for S8300D and S8300E servers.

Procedure

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

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

   For example:

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

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

   The command changes the links to the active standby mode.

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

The system displays the following message:

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

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

   The command changes the vmnic3 to the active mode.

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

   The system displays the following message:

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

5. To remove a vmnic from a vSwtich, type `# /opt/avaya/bin/nic_teaming remove <vmnic> <vSwitch>`.

6. To move an additional vmnic back to standby mode, type `# esxcli network vswitch standard policy failover set -v vSwitch0 --active-uplinks vmnic0 --standby-uplinks vmnic3`

   This puts the additional NIC back to standby mode.

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

   The system displays the following:

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

Warning:

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

Setting the Ethernet port speed

About this task

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

Important:

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

You cannot change the Ethernet port speed for S8300D and S8300E servers.

Procedure

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

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

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

   Note:

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

   Note:

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

Validating the migration

1. Verify that the ping to virtual machine is successful.
2. Verify that the you can log on to each virtual machine.
3. Verify that the customer configuration is restored correctly.
4. Verify that applications are licensed.

5. Verify that endpoints are registered.
6. Perform the postmigration validation steps that are specific to each application.

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

Chapter 7: Upgrade process

Upgrading Avaya Aura® System Manager

System Manager upgrade management

Upgrading virtualized environment-based System Manager by using the Solution Deployment Manager client

About this task

The procedure describes the steps to upgrade virtualized environment-based System Manager Release 7.0.x to System Manager Release 7.1.

Note:

If you are upgrading System Manager Release 7.0.x to Release 7.1.3 by using the Solution Deployment Manager client then post upgrade no need to reinstall the license file for the elements that are acquiring licenses from the old System Manager Release 7.0.x system. However, you need to install the license file for System Manager Release 7.1 and later.

Before you begin

- Install the Solution Deployment Manager client.
- Add a location.
- Add the ESXi, vCenter, or Appliance Virtualization Platform host from the VM Management page.
- Select the System Manager 7.0.x virtual machine and click **More Actions** > **Re-establish connection** to establish the trust. For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
- Obtain the System Manager software. See “Software details of System Manager”

Procedure

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

4. On the Upgrade Management page, select the System Manager 7.0.x virtual machine.
5. Click **Upgrade**.
6. **(Optional)** In **Host FQDN**, select the host.

   On the SMGR Upgrade dialog box, the system preselects and disables **Host FQDN**.
7. Select the datastore on the host.
8. Click **Next**.
9. 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 System Manager OVA file, and click **Submit**.
   - Click **S/W Library**, in **File Name**, select the System Manager OVA file.
   - Click **Browse**, select the required OVA file from a location on the computer, and click **Submit File**.
10. In **Choose Deployment Type**, select **ME Deployment**, if required.
11. From **Flexi Footprint**, select the flexi footprint.
12. Click the Data Migration tab, do one of the following:
    - Click **URL**, and provide the absolute path to the latest data migration utility file.
    - Click **S/W Library**, and select the latest data migration utility file.
    - Click **Browse**, and select the latest data migration utility file.
13. Click the Service or Feature Pack tab, do one of the following:
    - 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.
14. Click **Next**.
15. In the Config Parameters section, provide FQDN, Timezone, SNMP passwords, SMGR CLI User parameters, and EASG details.

    Note:

    Use the same FQDN as that on the old System Manager.
16. In the Network Parameters section, provide the Public and Out of Band Management details.

    Note:

    Use the same FQDN as that on the old System Manager.
17. Click **Upgrade** and accept the license terms.

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

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

    The complete process takes about 180–200 minutes depending on the data on System Manager.

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

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

20. Do one of the following:

    a. If the upgrade is successful, click **Commit**.

       The system deletes the old virtual machine.

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

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

Next steps

Install the valid license file for System Manager Release 7.1 and later.

Upgrading System Platform-based System Manager to Release 7.1.3 on a different server by using the Solution Deployment Manager client

About this task

The procedure describes the steps to upgrade System Manager on a different server.

Before you begin

- Install the Solution Deployment Manager client. See “Software details of System Manager”.
- Add a location.
- Upgrade the Appliance Virtualization Platform or the ESXi host.
- Add the Appliance Virtualization Platform or the ESXi host from the VM Management page.
- Obtain the System Manager software. See “Software details of System Manager”.

Procedure

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

   The system displays the Upgrade Elements page

4. If the System Manager element is not present on the Upgrade Elements page, do the following:

   a. Click **Add Elements**, add the System Manager element and console domain information.

b. Click **Save**.

5. If System Manager element is present, select the required element.
6. Click **Upgrade**.
7. **(Optional)** In **Host FQDN**, select the host.

   On the SMGR Upgrade dialog box, the system preselects and disables **Host FQDN**.
8. Select the datastore on the host.

   The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
9. Click **Next**.
10. 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 System Manager OVA file, and click **Submit**.
    - Click **S/W Library**, in **File Name**, select the System Manager OVA file.
    - Click **Browse**, select the required OVA file from a location on the computer, and click **Submit File**.
11. In **Choose Deployment Type**, select **ME Deployment**, if required.
12. From **Flexi Footprint**, select the flexi footprint.
13. Click the Data Migration tab, do one of the following:
    - Click **URL**, and provide the absolute path to the latest data migration utility file.
    - Click **S/W Library**, and select the latest data migration utility file.
    - Click **Browse**, and select the latest data migration utility file.
14. Click the Service or Feature Pack tab, do one of the following:
    - 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.
15. Click **Next**.
16. In the Config Parameters section, provide FQDN, Timezone, SNMP passwords, SMGR CLI User parameters, and EASG details.

    Note:

    Use the same FQDN as that on the old System Manager.
17. In the Network Parameters section, provide the Public and Out of Band Management details.

Note:

Use the same FQDN as that on the old System Manager.

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

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

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

    The complete process takes about 180–200 minutes depending on the data on System Manager.

Next steps

Install the valid license file for System Manager Release 7.1 and later.

Related links

Installing the Solution Deployment Manager client on your computer on page 39
Upgrade Management field descriptions on page 153
Add Element field descriptions on page 154
Install on Same ESXi field descriptions on page 160

Upgrading System Platform-based System Manager on the same server by using Solution Deployment Manager client

Before you begin

- Install the Solution Deployment Manager client.
- Add a location.
- Obtain the System Manager software. See Software details of System Manager.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. If the System Manager element is not present on the Upgrade Elements page, do the following:
   a. Click **Add Elements**, add the System Manager element and console domain information.
   b. Click **Save**.
5. If System Manager element is present, select the required element.
6. Click **Upgrade**.
7. On the Upgrade Management page, select the **Install on Same Host** check box.

8. Click **Continue**.

   The virtual machine shuts down and goes to the paused state.

   You must add the Appliance Virtualization Platform host from VM Management.

9. Install the Appliance Virtualization Platform host on the server on which System Platform was running.
10. To resume the upgrade operation, click **Upgrade Elements** > **Resume from Upgrade elements**.
11. In **Host FQDN**, select the host.
12. Select the datastore on the host.

    The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.

13. Click **Next**.
14. 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 System Manager OVA file, and click **Submit**.
    - Click **S/W Library**, in **File Name**, select the System Manager OVA file.
    - Click **Browse**, select the required OVA file from a location on the computer, and click **Submit File**.
15. In **Choose Deployment Type**, select **ME Deployment**, if required.
16. From **Flexi Footprint**, select the flexi footprint.
17. Click the Data Migration tab, do one of the following:
    - Click **URL**, and provide the absolute path to the latest data migration utility file.
    - Click **S/W Library**, and select the latest data migration utility file.
    - Click **Browse**, and select the latest data migration utility file.
18. Click the Service or Feature Pack tab, do one of the following:
    - 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.
19. Click **Next**.
20. In the Config Parameters section, provide FQDN, Timezone, SNMP passwords, SMGR CLI User parameters, and EASG details.

    Note:

    Use the same FQDN as that on the old System Manager.

21. In the Network Parameters section, provide the Public and Out of Band Management details.

Note:

Use the same FQDN as that on the old System Manager.

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

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

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

    The complete process takes about 180–200 minutes depending on the data on System Manager.

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

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

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

    After the rollback operation, you need to re-install System Platform and System Manager, and then restore the backup.

Related links

Installing the Solution Deployment Manager client on your computer on page 39
Upgrade Management field descriptions on page 153
Add Element field descriptions on page 154
Install on Same ESXi field descriptions on page 160

Upgrading System Manager Release 7.0 in Virtualized Environment

About this task

Use this procedure to upgrade System Manager Release 7.0 to Release 7.1.

Before you begin

- If the System Manager element is not present on the Upgrade Management page, do the following:
  1. Re-establish trust with the virtual machine using **Re-establish Connection**.
  2. Refresh the virtual machine using **Refresh VM**.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. On the Upgrade Elements page, select the required System Manager element.
5. Click **Upgrade**.
6. **(Optional)** In **Host FQDN**, select the host.

On the SMGR Upgrade dialog box, the system preselects and disables **Host FQDN**.

7. Select the datastore on the host.

   The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.

8. Click **Next**.
9. 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 System Manager OVA file, and click **Submit**.
   - Click **S/W Library**, in **File Name**, select the System Manager OVA file.
   - Click **Browse**, select the required OVA file from a location on the computer, and click **Submit File**.
10. From **Flexi Footprint**, select the flexi footprint.
11. Click the Data Migration tab, do one of the following:
    - Click **URL**, and provide the absolute path to the latest data migration utility file.
    - Click **S/W Library**, and select the latest data migration utility file.
    - Click **Browse**, and select the latest data migration utility file.
12. Click the Service or Feature Pack tab, do one of the following:
    - 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.
13. Click **Next**.
14. In the Configuration Parameters section, provide the System Manager CLI user details.
15. In the Network Parameters section, provide the Public and Out of Band Management details.

    Note:

    Use the same FQDN as that on the old System Manager.

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

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

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

    The complete process takes about 180–200 minutes depending on the data on System Manager.

Next steps

Verify that the upgrade is successful.

Upgrading to System Manager Release 7.1.3 from CLI

About this task

Use the procedure to upgrade System Manager vAppliance from Release 6.2.x or 6.3.x to Release 7.1.3 running on an Avaya-provided server with Appliance Virtualization Platform or on VMware in customer-provided Virtualized Environment by using Command Line Interface.

When you upgrade System Manager to Release 7.1 by using the data migration utility from CLI, the system performs the patch installation along with the data migration. Therefore, do not perform the patch installation.

Before you begin

- Ensure that System Manager is running.
- Download the `SMGR-7.1.0.0.1125193-e65-50.ova` file, `datamigration-146.bin` file, and `System_Manager_7.1.3.0_r713007763.bin` file from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the old System Manager web console.
2. Record the software version of old System Manager from the **About** link.

   For information, see “Verifying the current software version”.
3. Create a backup of System Manager and copy to the remote server by using System Manager web console.

   Note:

   For upgrades by using data migration utility, use only the backup that you created from the System Manager web console.
4. Log in to the System Manager command line interface of the existing system.
5. Shut down System Manager.
6. Deploy the `SMGR-7.1.0.0.1125193-e65-50.ova`.

   Important:

   You can use the same network parameters and system parameters that you recorded on the existing system or you can use the different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the existing system.
7. Copy `datamigration-146.bin`, the Release 7.1.3 bin file, and System Manager backup file to the `/swlibrary` location on System Manager.
8. Log in to the new System Manager virtual machine.
9. On System Manager Release 7.1.3, at the prompt, perform the following:
   a. Create a snapshot of the System Manager system.

b. To run the data migration utility, type the following command:

```
upgradeSMGR /swlibrary/<DMUtility_bin file name>.bin -m -v
```

You must provide the absolute path of the data migration utility.

c. In **Enter the location of backup file (full path)**, type the absolute path of the backup file.

```
/swlibrary/<backupfile name.*>
```

The system validates the backup file and displays the parameters.

d. In **Enter the patch file**, type the following command:

```
/swlibrary/<patch file name>.bin
```

For example, `swlibrary/System_Manager_R7.1.0.0.xxxxxxxxx.bin`.

The system validates the patch file and displays the following message:

```
You are about to run the System Manager Data Migration utility.
The System Manager will be inaccessible for approximately 60
minutes, depending on the resources available on the system.
```

e. To continue, type `Y`.

The system displays the following message:

```
WARNING:- The system is now going down for a halt and will be
inaccessible for some time.
Remote broadcast message (Tue Apr 5 21:06:27 2017):
INFO:- System Manager Data Migration would now be executed in
background process. For details, see System Manager Data
Migration logs in the /var/log/Avaya/datamigration/
data_migration.log.
```

10. Log on to System Manager and verify that the upgrade is successful.

The upgrade takes about 80 to 90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.

As part of running the data migration utility, the system performs the patch installation in the background that takes about 60–90 minutes.

You can verify the execution of System Manager:

- Data Migration Utility from the `/var/log/Avaya/datamigration/data_migration.log` file.
- Patch from the `/var/log/Avaya/SMGR_Patch.log` file.

Next steps

- If the upgrade or patch installation is successful, log off from the system, and remove the snapshot.

Note:

Snapshots occupy the system memory and degrades the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

- If the upgrade or patch installation fails, use the snapshot to restore the system to the original state.

  To collect logs, run the **collectLogs** command. The system creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

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

About this task

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

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click on **Refresh VM**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
6. Click **More Actions** > **Update VM**.

   The system displays the System Manager Update dialog box.
7. In **Select bin file from Local SDM Client**, provide the absolute path to the software patch or service pack.

Note:

The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.

8. **(Optional)** Click the **Auto commit the patch** check box.
9. Click **Install**.

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

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

       The system installs the patch, service pack or feature pack that you selected.
    b. Click **Get Info**.
    c. Select the patch, service pack or feature pack, and click **Commit**.

Related links

Update VM field descriptions on page 101

Upgrade Management field descriptions

Upgrade Elements

Name	Description
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
SMGR Name	System Manager name.
Upgrade Status	The status of the upgrade process. The status can be **Upgrading**, **Completed**, or **Failed**. The **Status Details** link provides more information about the System Manager upgrade.
Last Action	The last upgrade action.

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

Add Element field descriptions

Required Element information

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

Required C-DOM information

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

Button	Description
Save	Saves the element that you added

Edit Elements field descriptions

Required Element information

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

Required C-DOM information

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

Button	Description
Update	Updates the changes to the element.

Upgrade Management field descriptions

Name	Description
Install on Same Host	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update.
Host FQDN	The Host FQDN to which you want to update. The system displays the CPU and memory details of the host in the Capacity Details section.
VM Name	The virtual machine name displayed on the Add Element page.

Deploy OVA

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is ✓.
SMGR Datamigration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest data migration bin that is available for the System Manager release.

Table continues…

Name	Description
Backup file	The absolute path to the backup of System Manager virtual machine.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see the latest System Manager release notes.

Note:

- For upgrades from System Manager Release 6.3.15 or later, the bin file is mandatory.
- For upgrades from System Manager from 6.3.14 or earlier, the service pack, feature pack or patch file is optional.

  If you provide the service pack or feature pack, the data migration utility automatically deploys the service pack or feature pack on System Manager Release 7.0.0.0 after data migration.

Configuration Parameters

The system populates most of the fields depending on the OVA file. You must provide information, such as password, FQDN, and timezone.

Management Network Settings

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager 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.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.
Management Gateway	The gateway IPv4 address to assign to the System Manager virtual machine.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager virtual machine. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager virtual machine for out of band management. The field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager virtual machine. The field is optional.

Table continues…

Name	Description
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.

Public Network Settings

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

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • Do not add VFQDN entries in the DNS configuration. • Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to the System Manager virtual machine with administrator privilege credentials. 2. Run the following command, `changeVFQDN`.
Virtual Domain	The virtual domain name of the System Manager virtual machine.

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

SMGR CLI USER

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

Table continues…

Name	Description
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. The system generates an alarm if you do not schedule a System Manager backup every seven days.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.

Table continues…

Name	Description
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Network Parameters

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

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

Install on Same ESXi field descriptions

Name	Description
Install on Same Host	The option to select the same or a different server during the upgrade. The options are: • Select: To upgrade on same server. • Clear: To upgrade on a different server.
HOST FQDN	The fully qualified domain name. For example, platform.mydomain.com.

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 7.1.3 and configure System Manager.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`, and ensure that the system displays the System Manager web console.
2. On the upper-right corner, click  and click **About**.

   The system displays the About SMGR window with the build details.
3. Verify the System Manager version number.

Upgrading Avaya Aura® applications

Checklist for upgrading Avaya Aura® applications to Release 7.1.3

No.	Task	References	✔
1	Download the OVA files and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at http://support.avaya.com. **Note:** For information about the upgrade sequence and the required patches, see the latest *Avaya Aura® Release Notes* for the specific release on the Avaya Support website.	-	
2	Download the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip` file from the Avaya Support website at http://support.avaya.com.		

Table continues…

No.	Task	References	✔
3	Install the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe` file.	Installing the Solution Deployment Manager client on your computer on page 39	
4	To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.		
5	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.1 OVA file, and install the Release 7.1.3 bin file by using the Solution Deployment Manager client. • Available: Upgrade System Manager to 7.1 and install the Release 7.1.3 bin file.		
6	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	“Discovering elements” in *Administering Avaya Aura® System Manager*	
7	Configure user settings.	“User settings” in *Administering Avaya Aura® System Manager*	
8	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for TN Boards and media gateway upgrades is not supported.	“User settings” in *Administering Avaya Aura® System Manager*	
9	Refresh the elements in the inventory.	“Refreshing elements” in *Administering Avaya Aura® System Manager*	
10	Analyze the software.	“Analyzing software” in *Administering Avaya Aura® System Manager*	
11	Download the required firmware for the Avaya Aura® application upgrade.	“Downloading the software” in *Administering Avaya Aura® System Manager*	
12	Analyze the software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*	
13	Perform the preupgrade check.	“Performing the preupgrade check” in *Administering Avaya Aura® System Manager*	

Table continues…

No.	Task	References	✔
14	Perform the upgrade.	Upgrading Avaya Aura applications to Release 7.1.3 on page 163	
15	Verify that the upgrade is successful.	-	

Upgrading Avaya Aura® applications to Release 7.1.3

About this task

The procedure covers upgrades on the same server and on a different server. Use the procedure to upgrade the supported Avaya Aura® applications from

- 6.x running on Avaya Aura® to Release 7.1.3
- 7.0.x running on virtualized environment to Release 7.1.3

Before you begin

- From the Roles page, ensure that you set permissions that are required to perform all upgrade-related operations.
- Configure user settings.
- Complete all required operations up to the preupgrade check.
- To migrate the Avaya Aura® application from old server to ESXi host, add the new host in to VM Management.
- To migrate the Avaya Aura® application to a different server, add the Appliance Virtualization Platform host from the VM Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. To view and select the dependent elements:
   a. Click the element.
   b. On the Displaying Communication Manager Hierarchy page, select an element in the hierarchy.

      When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy. The page displays TN boards and media modules details in a table.

   c. Click **Done**.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

   When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

6. To provide the upgrade configuration details, click **Edit**.
7. On the Edit Upgrade Configuration page, and perform the following:
   a. In **Service/Feature Pack for auto-install after migration**, provide the Release 7.1.3 patch file.
   b. Complete the details, and click **Save**.
8. 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.
9. Click **Save**.
10. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.
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. Click **Upgrade**.
15. On the Upgrade Management page, click .

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

    For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, the field displays . This icon indicates that the upgrade is successful and awaiting commit or rollback.
16. For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, do the following:
    a. On the Upgrade Management page, select the element.
    b. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.

       The system displays the Job Schedule page.
    c. Select the action to be performed under the **Upgrade Action** column.
    d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.
    e. Click **Schedule**.
17. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.

b. In the **Job Type** field, click **Upgrade**.

c. Click the upgrade job that you want to view.

18. Verify that the upgrade of the application is successful.

    For upgrades on the same server, the system goes to the pause state.

19. For upgrades on the same server, perform 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.

Related links

Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 173
Edit Upgrade Configuration field descriptions on page 174

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”.

Related links

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 233
Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 234
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 173
Edit Upgrade Configuration field descriptions on page 174
Installed Patches field descriptions on page 169

Installing custom software patches

About this task

With this procedure, you can install a single software file, such as software patch, service pack, or a feature pack to an Avaya Aura® application. With the custom patch deployment, you do not require the System Manager automation and analyze functions, so that the advanced administrators can fully control the deployment of hot fixes, patches, service pack, and feature packs.

You can install custom patches for the following Avaya Aura® applications:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- Communication Manager Messaging

- WebLM
- Application Enablement 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 an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Custom Patching**.
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.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. 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.
13. Click **Upgrade**.
14. 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.
15. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
16. 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 .
17. Click **Upgrade Actions** > **Installed Patches**.

18. 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.

19. 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.

20. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.

21. 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”.

Next steps

To display the latest values in the **Entitled Update Version** column on the Upgrade Management page, click **Pre-upgrade Actions** > **Analyze**. If applied patch is:

- Uploaded as a custom patch in software library, the system does not change the value of the **Entitled Update Version** column.
- Downloaded in software library through the Download Manager page from PLDS or an Alternate source, the system displays the latest entitlement values in the **Entitled Update Version** column.

Related links

Uploading a custom patch on page 183
Uploading custom patch field descriptions on page 183

Installed Patches field descriptions

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

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.
Patch Type	The type of the software patch. The options are: • service pack or software patch • Kernel
Patch State	The state of the software patch. The options are: • Installed • Activated • Deactivated • Removed • Uninstall • Pending

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.

Upgrade Management field descriptions

You can apply filters and sort each column in the devices list.

Name	Description
Name	The name of the device that you want to upgrade.
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board.
Sub-Type	The sub type of the device. For example, TN2302AP.
IP Address	The IP address of the device.
Release Status	The release status of the device. The upgrade status can be: For upgrade: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed
Update Status	The update status of the device. The upgrade status can be: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed

Table continues…

Name	Description
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • : Mandatory checks and recommended checks passed • : Mandatory checks are successful, but recommended checks failed. • : Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
Location	The location of the device.

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/Rolback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.

Table continues…

Button	Description
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, CommunicationManager_123.
Type	The device type.
IP Address	The IP Address of the device.
Current Version	The release status of the device.
Override Preupgrade Check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.

Table continues…

Name	Description
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system ignores any recommendations during upgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. • : Configuration incomplete. • : Configuration complete.

Button	Description
Import AVP Configuration(s)	Imports the `AVP_Bulk import spread sheet.xlsx` spreadsheet. The system displays the Upload AVP Xlsx File Configuration dialog box to upload the `AVP_Bulk import spread sheet.xlsx` spreadsheet.
Save Configuration	Saves the upgrade configuration. **Note:** The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page.
Upgrade	Commits the upgrade operation.

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

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

Element Configuration: General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.

Table continues…

Name	Description
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host	The ESXi host on which you want to run the device. The options are: • Same Box • List of hosts that you added from VM Management
Migrate With AVP Install	The option to migrate System Platform-based system and Communication ManagerRelease 5.2.1 bare metal system to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.
Service/Feature Pack for auto-install after upgrade/migration	The service pack or feature pack that you want to install.

Element Configuration: Upgrade Configuration Details

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

Name	Description
Auto Commit	The option to automatically commit the upgrade.
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.

Table continues…

Name	Description
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. For Communication Manager Messaging, the button is unavailable and you must fill in all details. For Communication Manager Messaging you must provide a new IP address.
CM IPv4 Address	The IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	The network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine.
CM IPv6 Gateway	The IPv6 default gateway of the Communication Manager virtual machine.
Out of Band Management IPv4 Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnetwork mask of the virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv6 network prefix of the virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the virtual machine.

Table continues…

Name	Description
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.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Services	The port number that is assigned to the services port. The system displays this field when Utility Services is available.
Duplication link	The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process. The field is available only for the Communication Manager duplex configuration and when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

The page displays the following fields when you upgrade Session Manager.

Name	Description
Existing Administrative User	The user name of the administrator.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields.
IP Address	The IP address of the virtual machine.
Short Hostname	The hostname of the virtual machine. The hostname of the server and is often aligned with the DNS name of the server.
Network Domain	The domain name of the virtual machine.
Netmask	The network mask of the virtual machine.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Timezone	The timezone of the virtual machine.
Login Name	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Enter Customer Account Password	Password to log on to the system.
Primary System Manager IP	The IP address of System Manager.
Enrollment Password	The password that is required to establish trust between System Manager and Session Manager.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: End User License Agreement

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

AVP Configuration: Existing Machine Details

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

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses.
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.

Table continues…

Name	Description
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.
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.

Table continues…

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

Table continues…

Name	Description
Enhanced Access Security Gateway (EASG)	**Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. **Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled. Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Save	Saves the changes that you made to the Edit Upgrade Configuration page.
Cancel	Cancels the changes that you made to the Edit Upgrade Configuration page.

Uploading a custom patch

About this task

If the file size exceeds 300 MB, the upload operation fails.

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.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Download Manager**.
3. In **Select Software/Hardware Types**, select the firmware you want to download.

   You can choose either **Tree View** or **List View** to view the software, hardware types.
4. Click **Show Files**.
5. In the **Select Files Download Details** section, enter **My Computer**.
6. Click **Download**.
7. On the Upload File page, enter the details of the patch file you want to upload.
8. Click **Commit**.
9. On the Upload Remote Warning page, perform one of the following actions:
   - Click **Now** to upload the file to the remote software library.
   - Click **Schedule** to upload the file at the scheduled time.
   - Click **Cancel** to cancel the upload file operation and return to the previous page.

Uploading custom patch field descriptions

Name	Description
Software Library	The remote software library where you want to upload the custom patch file.
Product Family	The product family to which the file belongs. In a product family, the number of devices are listed.
Device Type	The device type that you can upgrade using the software library file. For example, B5800 and IP Office are the device types for IP Office.
Software Type	The type of software file which includes firmware and images.

Table continues…

Name	Description
File Version	The software file version that you want to upload. For example, OVA, service pack, and feature pack. Version number is mandatory if you are uploading files, such as OVA, service pack, and feature pack because analyze operation works on version number and the system might have to install the version of the file. Custom patching does not require the analyze operation, and therefore, the file version number is optional.
Hardware Compatibility	The hardware compatibility for the file you upload. For IP Office, this field can be null.
File Size (in bytes)	The file size of the patch file you want to upload.
File	The patch file you want to upload to the remote software library. Click **Choose File** to browse to the file you want to upload.

Button	Description
Commit	Click to go to the upload file scheduler page.
Cancel	Click to cancel the upload operation and return to the Download Manager page.

Upgrading Avaya Aura® Communication Manager

Upgrading Communication Manager 6.x to Release 7.1.3

About this task

Use the procedure to upgrade System Platform-based simplex Communication Manager, Branch Session Manager, and associated devices to Release 7.1.3. The process automatically updates to Release 7.1.3 when you provide the Release 7.1.3 patch file. The procedure covers upgrades on the same server and on a different server.

Before you begin

- From the Roles page, ensure that permissions to perform all upgrade-related operations are set.
- Configure user settings.
- Complete all required operations up to the preupgrade check.
- From the Manage Elements link on System Manager, add Communication Manager, Utility Services, and System Platform that is associated with Communication Manager if you are migrating from Release 6.x.

- If you are migrating Communication Manager to a different server:
  - Install the Appliance Virtualization Platform host.
  - Add the Appliance Virtualization Platform host from the VM Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Communication Manager server that you want to upgrade.

   The system selects any dependent element for upgrade during the upgrade operation.

   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message `Selected System Platform or child of System Platform, and System Platform and all child applications.`

   If parent-child relation is not established, run **Refresh Elements** again for child elements to associate with the parent.
4. To view and select the dependent elements:
   a. Click the element.
   b. On the Displaying Communication Manager Hierarchy page, select an element in the hierarchy.

      When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy. The page displays TN boards and media modules details in a table.
   c. Click **Done**.
5. Click **Upgrade Actions** > **Upgrade/Update**.
6. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

   When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.
7. To provide the upgrade configuration details, click **Edit**.
8. On the Edit Upgrade Configuration page, and perform the following:
   a. In **Service/Feature Pack for auto-install after migration**, provide the Release 7.1.3 patch file.
   b. Complete the details, and click **Save**.
9. 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.
10. Click **Save**.

11. On the Upgrade Configuration page, click **Upgrade**.
12. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.
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**.
15. Click **Upgrade**.
16. On the Upgrade Management page, click  .

    Last Action column displays **Upgrade**, and **Last Action Status** column displays  .
17. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
18. Verify that the upgrade of Communication Manager is successful.

    For upgrades on the same server, the system goes to the pause state.
19. For upgrades on the same server, perform 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.
20. On Communication Manager Release 7.1.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

Next steps

On Communication Manager 7.0, click **Administration** > **Server (Maintenance)**, and reconfigure SNMP parameters.

After migration the system does not populate old SNMP values. Therefore, you need to reconfigure SNMP parameters.

Preparing duplex Communication Manager for migration

About this task

To migrate the duplex Communication Manager system, prepare Communication Manager, migrate the standby Communication Manager, interchange the roles of Communication Manager systems, and migrate the active Communication Manager, change the roles of two Communication Manager systems to the original state.

Before you begin

Perform all preupgrade operations, such as refresh elements, analyze software, download software, perform preupgrade check, and ensure that all operations are successful.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. Add the following applications if not already available:
   - Two Communication Manager systems. Select the **Add to Communication Manager** check box for only primary server, and ensure that the check box is cleared for the secondary server.

     Add only primary Communication Manager. In primary Communication Manager, mention the IP address of secondary standby Communication Manager as the alternate IP address.
   - System Platform that is associated with Communication Manager systems, if Communication Manager is System Platform-based.

     The system starts the second level discovery. The process adds System Platform in the system and creates the parent association with System Platform and Communication Manager.
3. To ensure that the changes made to the translation are saved, log in to the active Communication Manager server, and perform the following:
   a. Start a SAT session.
   b. Type `save translation`
4. In the command line interface of the active Communication Manager server, type `server -u`.

Migrating duplex Communication Manager on the same server

Before you begin

Prepare duplex Communication Manager for migration.

For more information, see Preparing duplex Communication Manager for migration.

Procedure

1. Start the upgrade for the standby Communication Manager:
   a. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   b. In the left navigation pane, click **Upgrade Management**.
   c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

      After the second analyze operation, the status column displays **Ready for Upgrade**.
   d. Select the standby Communication Manager or System Platform and click **Upgrade Actions** > **Upgrade/Update**.
   e. On the Upgrade Configuration page, click **Edit**.
   f. Schedule the upgrade of the standby Communication Manager.
   g. On the Upgrade Management page, in the **Release Status** column, verify that the status is **Paused**.
   h. Ensure that you install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from VM Management.
   i. To resume the upgrade process, click **More Actions** > **Resume**.
   j. On the Resume Configuration, select the Appliance Virtualization Platform host and datastore.
   k. On the Upgrade Job Status page, check the upgrade job status.

      If the upgrade is successful, proceed with the next step.
2. Configure the newly upgraded standby Communication Manager server by performing the following:
   a. Log on to the software management interface of the standby Communication Manager.
   b. On Communication Manager Release 7.1.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
      - **Network Configuration**
      - **Duplication Parameters**
      - **Server role**
   c. From the command line interface of the standby Communication Manager, perform the following:
      a. To release the server from the busy out state, type `server -r`.
      b. Type `server`, and ensure that the duplication link is active and the standby server refreshes.

3. From the command line interface, on the active Communication Manager, interchange the standby and active Communication Manager, type `server -if`.

   Upgrade to Communication Manager Release 7.1.3 is not connection preserving.

4. Start the upgrade of the current standby Communication Manager server:
   a. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   b. In the left navigation pane, click **Upgrade Management**.
   c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

      After the second analyze operation, the status column displays **Ready for Upgrade**.

   d. Click **Upgrade Actions** > **Upgrade/Update**.
   e. On the Upgrade Configuration page, click **Edit**.
   f. Schedule the upgrade of Communication Manager.
   g. On the Upgrade Management page, in the **Release Status** column, verify that the status is **Paused**.
   h. Ensure that you install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from VM Management.
   i. To resume the upgrade process, click **Upgrade Actions** > **Resume** to resume the upgrade process.
   j. On the Resume Configuration, select the Appliance Virtualization Platform host and datastore.
   k. Check the job status for upgrade job.

      At this point, the two Communication Manager systems get upgraded.

5. Configure the newly upgraded active Communication Manager server by performing the following:
   a. Log on to the software management interface of the active Communication Manager.
   b. On Communication Manager Release 7.1.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
      - **Network Configuration**
      - **Duplication Parameters**
      - **Server role**
   c. Type `server`, and ensure that the duplication link is active and the standby server refreshes.
   d. **(Optional)** To interchange the roles of standby and active Communication Manager servers, from the command line interface of the active Communication Manager server, type `server -i`.

The duplication link becomes active and the standby Communication Manager server refreshes.

Migrating duplex Communication Manager on a different server

Before you begin

Prepare duplex Communication Manager for migration.

For more information, see Preparing duplex Communication Manager for migration.

Procedure

1. Start the upgrade for the standby Communication Manager:
   a. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   b. In the left navigation pane, click **Upgrade Management**.
   c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

      After the second analyze operation, the status column displays **Ready for Upgrade**.
   d. Select the standby Communication Manager or System Platform, and click **Upgrade Actions** > **Upgrade/Update**.
   e. On the Upgrade Configuration page, click **Edit**.
   f. Schedule the upgrade of the standby Communication Manager.
   g. Check the job status for upgrade job.

      The system upgrades the standby Communication Manager to 7.0, and restores the data on the Communication Manager 7.0 system.
2. Configure the newly upgraded standby Communication Manager server by performing the following:
   a. Log on to the software management interface of the standby Communication Manager.
   b. On Communication Manager Release 7.1.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
      - **Network Configuration**
      - **Duplication Parameters**
      - **Server role**
   c. To release the server busy out state, from the command line interface of the standby Communication Manager, type `server -r`.

      The standby server becomes active because no duplication link is available between the active Communication Manager and the new standby Communication Manager.

3. To busy out the server, from the active Communication Manager command line interface, type `server -if`.
4. Verify that all elements associated with Communication Manager, such as TN Boards, media gateways, and media modules gets registered with the new active server and the calls get processed with the new active server.
5. Start the upgrade for the Communication Manager that was earlier active:
    a. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
    b. In the left navigation pane, click **Upgrade Management**.
    c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the Communication Manager server.

       After the second analyze operation, the status column displays **Ready for Upgrade**.
    d. Select the active Communication Manager or System Platform, and click **Upgrade Actions** > **Upgrade/Update**.
    e. On the Upgrade Configuration page, click **Edit**.
    f. Schedule the upgrade of the active Communication Manager.
    g. Check the job status for upgrade job.

       The system upgrades the active Communication Manager to 7.0, and restores the data on the Communication Manager 7.0 system, and installs the Release 7.1.1 feature pack.
6. Configure the newly upgraded active Communication Manager server by performing the following:
    a. Log on to the software management interface of the active Communication Manager.
    b. On Communication Manager Release 7.1.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
       - **Network Configuration**
       - **Duplication Parameters**
       - **Server role**
    c. To release the server busy out state, from the command line interface of the standby Communication Manager, type `server -r`.

       The standby server becomes active because no duplication link is available between the active Communication Manager and the new standby Communication Manager.
    d. To interchange the roles of standby and active Communication Manager servers, from the command line interface of the active Communication Manager server, type `server -i`.

       The standby server becomes the main Communication Manager server, and starts processing calls.

Upgrading Avaya Aura® Session Manager

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 Avaya Aura® applications using Solution Deployment Manager in the Geographic Redundancy setup

Upgrading Avaya Aura® applications when the primary System Manager is operational and the secondary System Manager is in standby mode

Before you begin

- Enable the Geographic Redundancy replication.

  For all Geographic Redundancy-related procedures, see “Geographic Redundancy” in *Administering Avaya Aura® System Manager*.
- Ensure that all Avaya Aura® applications are connected to the primary System Manager server.
- Ensure that the primary System Manager server manages Session Manager and Communication Manager from **Inventory** > **Manage Elements**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. For each Avaya Aura® application, select the application, and perform the following:
   a. To refresh elements, click **Pre-upgrade Actions** > **Refresh Elements**.
   b. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   c. To download the OVA file to the software library, click **Solution Deployment Manager** > **Download Management**.
   d. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   e. To perform the preupgrade check, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   f. To perform the upgrade, click **Upgrade Actions** > **Upgrade/Update**.

Upgrading Avaya Aura® applications when the primary System Manager is nonoperational and secondary System Manager is in active standby mode

Before you begin

- Disable the Geographic Redundancy replication.

- Ensure that all Avaya Aura® applications are connected to the secondary System Manager server.
- Ensure that the secondary System Manager server manages Session Manager and Communication Manager from **Inventory** > **Manage Elements**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. To delete the current application OVA files that need to migrate from the secondary System Manager, perform the following:
   a. In the left navigation pane, click Software Library Management.
   b. Click **Manage Files**, and select the application OVA files that you want to delete.
   c. Click **Delete**.
3. For each Avaya Aura® application, select the application, and perform the following:
   a. To refresh elements, click **Pre-upgrade Actions** > **Refresh Elements**.
   b. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   c. To download the OVA file to the software library, click **Solution Deployment Manager** > **Download Management**.
   d. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   e. To perform the preupgrade check, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   f. To perform the upgrade, click **Upgrade Actions** > **Upgrade/Update**.

Upgrading Avaya Aura® applications when the primary System Manager is operational, and the secondary in standby and pause state

Before you begin

- Ensure that all Avaya Aura® applications are connected to the secondary System Manager server.

  For all Geographic Redundancy-related procedures, see “Geographic Redundancy” in *Administering Avaya Aura® System Manager*.
- Ensure that the secondary System Manager server manages Session Manager and Communication Manager from **Inventory** > **Manage Elements**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. To delete the current application OVA files that need to migrate from the secondary System Manager, perform the following:
   a. In the left navigation pane, click Software Library Management.

b. Click **Manage Files**, and select the application OVA files that you want to delete.
c. Click **Delete**.

3. For each Avaya Aura® application, select the application, and perform the following:
   a. To refresh elements, click **Pre-upgrade Actions** > **Refresh Elements**.
   b. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   c. To download the OVA file to the software library, click **Solution Deployment Manager** > **Download Management**.
   d. To analyze software, click **Pre-upgrade Actions** > **Analyze**.
   e. To perform the preupgrade check, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   f. To perform the upgrade, click **Upgrade Actions** > **Upgrade/Update**.
   g. In the **Target Host** field, select **Same Box**.

      All applications come to the **Pause** state.
4. When the primary System Manager is operational, to upgrade from the primary System Manager server, for each application, copy backup files from the secondary System Manager to the primary System Manager server.
   - For System Platform, copy the full path `/swlibrary/orchestrator/backup/System_Platform/<System_platform_IP>` from secondary System Manager to primary System Manager.

     For example, `scp -r System_Platform admin@<Primary SMGR IP>:/swlibrary/orchestrator/backup/.`
   - For System Platform, copy the full path `/swlibrary/orchestrator/backup/Session_Manager/<Session_Manager_IP>` from secondary System Manager to primary System Manager with the same path.

     For example, `scp -r Session_Manager admin@<Primary SMGR IP>:/swlibrary/orchestrator/backup/.`
5. Deactivate the secondary System Manager server.
6. On the primary System Manager server, click **Services** > **Geographic Redundancy**, and restore the data from the secondary server.

   The system restores the secondary System Manager server database.
7. From Solution Deployment Manager, download the application OVAs if not previously downloaded.
8. On the primary System Manager, click **Services** > **Solution Deployment Manager** > **Upgrade Management**.
9. Select the applications, and click **Upgrade Actions** > **Resume**.

   The system starts the virtual machine deployment and restore operation from the primary System Manager server.

Chapter 8: Avaya Aura® 7.1 migration scenarios

Avaya Aura® 7.1.x migration scenarios

This section covers various migration scenarios that customers might use, and provides required and recommended steps for migrating to Avaya Aura® Release 7.1.3. The scenarios provide only high-level procedures.

For detailed instructions to perform each procedure, see *Migrating and Installing Avaya Aura® Appliance Virtualization Platform* and *Upgrading and Migrating Avaya Aura® applications from System Manager* to Release 7.1.3.

Avaya Aura® application upgrade and migration considerations

- Update the IPSI firmware in G650 and H.248 gateways first from the System Manager Solution Deployment Manager if the IPSI firmware must communicate with Communication Manager Release 7.1.3 systems.
- You require to generate new licenses for Avaya Aura® Release 7.1.3 for each application. System Manager WebLM is used as the licensing server in Avaya Aura® Release 7.1.3 environment. For the customer-provided Virtualized Environment solution, you can continue to use standalone WebLM as the licensing server.
- You require a separate instance of WebLM for Application Enablement Services to support Enterprise Licensing with allocation mode which uses a master and local WebLM.
- If the Avaya Aura® application that you want to deploy on an Avaya-provided appliance does not already have Utility Services, deploy Utility Services before you deploy the Avaya Aura® application Release 7.1.3.
- Manually migrate SAL or Services VM if needed. You require one SAL or Services VM per enterprise to support a Avaya Services offer.
- If you require SAL on S8300D, replace the server with one of the following servers that Release 7.1.3 supports:
  - Dell™ PowerEdge™ R610 2CPU MID2

  - HP ProLiant DL360 G7 2CPU MID4
  - Dell™ PowerEdge™ R620 1CPU MID3
  - HP ProLiant DL360p G8
  - S8300E
- If number of users exceed 700 on S8300D, replace server with one of the servers that Release 7.1.3 supports.
- In the Avaya-provided appliance deployments of Avaya Aura® Release 7.1.3 applications on Dell™ PowerEdge™ R620 and HP ProLiant DL360e G8 contain Appliance Virtualization Platform. For the new S8300E server, Appliance Virtualization Platform must be installed in the field.
- During migrations or upgrades from System Platform to Avaya Aura® Release 7.1.3 on the Avaya-provided appliance, you must install Appliance Virtualization Platform on the existing servers.
- Automated migration and upgrade process:
  - Migration and upgrade process for Communication Manager, Session Manager, and Branch Session Manager to Avaya Aura® Release 7.1.3 from System Manager Solution Deployment Manager are automated. The only manual step is the installation of Appliance Virtualization Platform.
  - For customer-provided Virtualized Environment solutions, System Manager Solution Deployment Manager and the Solution Deployment Manager client does not support upgrade and migration from Release 6.x to Avaya Aura® Release 7.1.3.
- Applications that use S8800 servers must replace the server with the server that Avaya Aura® Release 7.1.3 supports.

Deploying 6.x applications to Avaya Aura® Release 7.1.3 by using the Solution Deployment Manager client

About this task

The section provides the procedure to deploy Avaya Aura® Release 7.1.1 application OVA files during migration of Avaya Aura® 6.x by using the Solution Deployment Manager client when System Manager is unavailable.

Also, you can install System Manager by using the Solution Deployment Manager client, and use the centralized Solution Deployment Manager to deploy other Avaya Aura® Release 7.1.3 application OVA files.

Before you begin

- Read the Avaya Aura® application upgrade and migration considerations.
- Obtain the OVA files for Utility Services, System Manager, and other applications.

Procedure

1. Using the backup and restore capability of the application, create a full backup of the Avaya Aura® 6.x application.

   For a System Platform-based application, additionally, create a System Platform backup to get back the system to the original state during disaster recovery.

2. Record the following network parameters for the 6.x application:

   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server

   You can use the information later in situations such as performing disaster recovery.

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

3. Install the Solution Deployment Manager client on the computer of the technician if not already installed.

   Avaya provides the Solution Deployment Manager client DVD with the Appliance Virtualization Platform order. DVD is available on the PLDS website at https://plds.avaya.com/

4. On the existing server that you want to migrate to Avaya Aura® Release 7.1.1, install Appliance Virtualization Platform from DVD and thumb drive.

   The installation process takes about 30 minutes.

5. For the Solution Deployment Manager client to communicate with the Appliance Virtualization Platform services port on the same network, set the IP address of the computer to 192.168.13.5.

6. On the VM Management page, create a location, host, and a virtual machine.

7. If Utility Services is not already deployed, on Appliance Virtualization Platform, perform the following to deploy and configure Utility Services:

   a. Deploy the Utility Services OVA file.

   b. During the deployment, select one of the following footprints:

      - **Small S8300D**: To reduce the memory allocated for Utility Services virtual machine on S8300D that has limited resources. With the default footprint on S8300D, the system might not run all required virtual machines.
      - **Default** : For all other server platforms.

   c. Select one of the following Utility Services modes:

      - **Services Port Only**: Deploys Services Port only. You can use this mode when the customer already has Utility Services running on another virtual machine and providing the services.

- **Utility Servers Only**: Routing Disabled. You can use this mode when the customer wants to disallow routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the Services port becomes non-operational.
- **Full Functionality**: Utility Services and Services Port enabled. The default mode for Appliance Virtualization Platform.

d. 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. The Utility Services application provides application routing between the physical port and virtual applications.

8. Configure the required settings for Avaya Aura® application, accept the license agreement terms and deploy other Avaya Aura® Release 7.1.3 application OVA to the virtual machine.

   With the Solution Deployment Manager client, you can deploy one application OVA at a time. You can use this process to deploy OVA ddfor all applications that Avaya Aura® Release 7.1.3 supports.

9. With the patch installation capability of the application, install the required software patches for the application.
10. With the restore capability of the application, restore the backup of the application that you created in Step 1.
11. For each application that you installed and Appliance Virtualization Platform, log in to the command line interface and install the Avaya Secure Gateway (ASG) file.
12. With the backup and restore capability, create a backup of the Avaya Aura® Release 7.1.3 application.

Upgrading Avaya Aura® 6.x applications in a customer-provided Virtualized Environment to Avaya Aura® Release 7.1.3

About this task

The section provides the procedure to migrate Avaya Aura® 6.x applications to Avaya Aura® Release 7.1.3:

- Avaya Aura® applications include Communication Manager, System Manager, Session Manager, Application Enablement Services, WebLM, Communication Manager Messaging, and Avaya Breeze™.
- Avaya Aura® Release 7.1.3 does not support automated upgrade from Virtualized Environment to Virtualized Environment.

- Upgrade Avaya Aura® applications to Release 7.1.1 in the following order:
  - System Manager
  - Session Manager
  - Communication Manager
  - WebLM
  - SAL
  - Application Enablement Services

Before you begin

Read the Avaya Aura® application upgrade and migration considerations.

- Ensure that required space is available on the disk for the existing Avaya Aura® 6.x applications and Avaya Aura® Release 7.1.1 applications.
- Obtain the OVA files for Utility Services, System Manager, and other Avaya Aura® Release 7.1.3 applications.

Procedure

1. Using the backup and restore capability of the application, create a full backup of the Avaya Aura® 6.x application.

   For a System Platform-based application, additionally, create a System Platform backup to get back the system to the original state during disaster recovery.

2. Record the following network parameters for the 6.x application:

   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server

   You can use the information later in situations such as performing disaster recovery.

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

3. Using vSphere Client, perform the following to prepare the existing Virtualized Environment for upgrade:

   a. Shutdown the Release 6.x virtual machine if sufficient disk resources are available to run the Avaya Aura® 6.x and 7.0 applications.

      The new and existing applications cannot see each other on the network during and after the deployment of the Release 7.1.1 application.

   b. Delete the existing Avaya Aura® 6.x application image on the customer-provided VMware host to create sufficient disk resources to deploy the Avaya Aura® Release 7.1.1 application.

4. Using vSphere Client, deploy the new Avaya Aura® Release 7.1.1 application OVA and provide the required application-level configuration settings for using the existing customer-provided VMware tools to the VMware host.

   For more information to deploy the application, see *Deploying <Avaya Aura application> on VMware*. You can also deploy OVA files to a customer Virtualized Environment solution by using the Solution Deployment Manager client.

5. With the patch installation capacity of the application, install the Release 7.1.3 patch for the application.

   You can use the command line interface or the System Manager Solution Deployment Manager in Virtualized Environment solution if System Manager Solution Deployment Manager is configured to support software upgrades. For example, setting up the software library and user settings to gain access to PLDS.

6. With the restore capability of the application, restore the backup of the application that you created in Step 1.
7. Verify that the application is running Release 7.1.1.
8. For each application that you installed, log in to the command line interface and install the Avaya Secure Gateway (ASG) file.
9. With the backup and restore capability, create a backup of the Avaya Aura® Release 7.1.3 application.

Migrating System Platform-based Communication Manager 6.x to Avaya Aura® Release 7.1.3 on Appliance Virtualization Platform

About this task

The section provides the procedure to migrate Communication Manager running on System Platform to Avaya Aura® Release 7.1.3:

- Communication Manager Release 6.x Embedded CM Main template on S8300D and Gateway

  Survivable remote template does not contain Communication Manager Messaging and WebLM.
- Communication Manager Release 6.x Simplex template on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, HP ProLiant DL360p G8 or Dell™ PowerEdge™ R630 HP ProLiant DL360 G9.

Before you begin

- Read the Avaya Aura® application upgrade and migration considerations.
- Obtain the OVA files for Utility Services, System Manager, and other Avaya Aura® applications.

Procedure

1. Obtain a new Avaya-provided server that runs on Appliance Virtualization Platform with System Manager OVA.
2. Download the Solution Deployment Manager client DVD from the PLDS website at https://plds.avaya.com.

   Avaya provides the Solution Deployment Manager client DVD with the Appliance Virtualization Platform order.
3. Type `192.168.13.5` as the IP address of the computer.

   When you set this IP address, the Solution Deployment Manager client communicates with the Appliance Virtualization Platform services port on the same network.
4. Install the Solution Deployment Manager client on your computer.
5. On the server that you want to migrate to Release 7.1.3, install Appliance Virtualization Platform.
6. Perform the following to prepare Utility Services OVA for deployment:
   a. Select a footprint.
   b. Select a mode.
7. Deploy the Utility Services OVA file.
8. Type `192.11.13.5` as the IP address of the computer.

   The Solution Deployment Manager client can communicate with the hypervisor and all virtual machines. After Utility Services OVA is setup, Utility Services can gain access to the entire virtual machine. Utility Services provides application routing between the physical port and virtual applications.
9. Using the Solution Deployment Manager client, perform the following:
   a. Configure the required System Manager settings.
   b. Accept the licence terms.
   c. Deploy System Manager Release 7.1.1 on the virtual machine.
10. Log in to the command line interface of the application and install the Avaya Secure Gateway (ASG) file for each installed application and Appliance Virtualization Platform.

    For example, Utility Services and System Manager.

    System Manager is operational at this point.
11. To save the files required for upgrade, click **Solution Deployment Manager** > **Software Library Management**, and configure an external server as a remote System Manager software library.

    You can save about 30 GB on System Manager. Therefore, configure external server as remote software library.
12. Click **Services** > **Inventory** > **Manage Elements**, and run the discovery operation.

You can use the SNMP discovery or manually add the Communication Manager system on the Manage Elements page with the appropriate configuration.

The system discovers the Communication Manager, S8300D or simplex server.

After successful discovery, the Manage Elements page displays the Communication Manager Release 6.x system.

When the initial discovery is complete, the system starts the second level inventory. System Manager then displays the S8300D or the simplex server and associated devices, such as TN Boards, media modules, media gateways on the Upgrade Management page.

13. On the Solution Deployment Manager page, perform the initial Solution Deployment Manager setup and entitlement analysis.
    a. Configure PLDS or an alternate source for System Manager-Solution Deployment Manager to perform the analysis of the a discovered Communication Manager 6.x application software, and the software version to which the customer is entitled for the discovered Communication Manager 6.x application.
    b. Perform the analyze operation on the selected Communication Manager 6.x element.

       The Upgrade Management page displays the current state.

       When analysis is complete, the system provides an option to download entitlements for elements that are entitled to a software or firmware versions. For example, OVA, `version.xml`, firmware for media modules, TN boards, gateways, and software patches.
    c. On the Download Management page, download the entitlements to the external software library.
    d. On VM Management, create a location that defines where the Communication Manager 6.x resides in the VM hierarchy.
14. Perform the following to prepare Communication Manager 6.x for migration to Release 7.1.3.
    a. From System Manager, get the primary host ID WebLM that is required to generate Communication Manager Release 7.1.3 licence files.
    b. Install license files on System Manager WebLM.
    c. Install the preupgrade patch on Communication Manager manually.
    d. Create the following backup for Communication Manager Release 6.x and Communication Manager Messaging Release 6.x:
       - Full backup of Communication Manager for disaster recovery.
       - Backup from System Platform for disaster recover and to migrate SAL or the Services VM data.

         The backup does not include Communication Manager Messaging.
       - Backup of announcement and configuration files from the Communication Manager Messaging web console. The maximum size is 280 GB, on S8300D or S8300E the size is about 80 GB.

- Backup of SAL or the Services VM data.

e. Record the following network parameters for embedded main Communication Manager Release 6.x:

- All IP addresses
- Subnetwork mask
- Gateway
- DNS
- NTP Server

You might require the values after the migration.

15. On the Upgrade Management page, select the Communication Manager Release 6.x system, and click **Pre-upgrade Actions** > **Pre-upgrade Check**.

    You do not require to provide the footprint size, the value is already provided in OVA.

    Preupgrade check validates the hardware requirements for applications being migrated, and also checks if Utility Services is running in the virtual machine. If Utility Services is running, you must remove Utility Services.

16. Select the Communication Manager Release 6.x system, and click **Upgrade Actions** > **Upgrade/Update**.

    Solution Deployment Manager performs the following:

    - Imports the required network setting from System Platform.
    - Prompts you to fill the new attributes that are required from OVA for the deployment.
    - Creates a backup of the Communication Manager embedded template.

      Note:

      Solution Deployment Manager does not backup Communication Manager Messaging.

    After successful backup, the upgrade process moves to the pause state.

17. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, click the 7.1.3 feature pack.

18. Install Appliance Virtualization Platform on the server that was earlier running System Platform and Communication Manager 6.3.x.

    The installation process takes about 30 minutes.

19. Select the same system, and click **Upgrade Actions** > **Resume**.

    - During the upgrade, the system prompts you to select host on which the OVA is deployed.
    - The process continues and the system automatically deploy all OVAs that are part of the Communication Manager embedded template. For example, Communication Manager, Utility Services, and Communication Manager Messaging.

You can monitor the migration job status from the Upgrade Job Status page.

- Restores all applications such as Communication Manager and Utility Services.

20. Restore Communication Manager Messaging using the Communication Manager Messaging backup and restore capability.
21. Update the trunk configuration for establishing connection between Communication Manager Messaging and Communication Manager.
22. On VM Management, deploy the SAL or Services VM OVA if required.

    Deploy one SAL or Services VM per customer solution.

    You might require to update IP address during the migration from SAL or Services VM in System Platform to VMware™. The best practice is to maintain the SAL IP address.

    Adequate space is unavailable to load on S8300D.
23. Restore SAL or Services VM by using the SAL restore capability.
24. From SAL web console, update SAL with the new models, such as DOM0 to Appliance Virtualization Platform, and add Communication Manager Messaging and Utility Services.
25. Log in to the command line interface or the web console of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform, Communication Manager, Communication Manager Messaging, Utility Services, and SAL or Services VM.
26. Create a backup of the Communication Manager Release 7.1.3 S8300D or Communication Manager Release 7.1.3 simplex server.

    You must create a separate backup for each deployed application.

Migrating Communication Manager 6.x S8300D or CM Simplex on survivable remote template to Avaya Aura® Release 7.1.3

About this task

The section provides the procedure to migrate Communication Manager Release 6.x on System Platform to Avaya Aura® Release 7.1.3 in the following configuration:

- Embedded remote template on S8300D or CM Simplex with survivable remote template running on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, or HP ProLiant DL360p G8 server

  Survivable remote template does not contain Communication Manager Messaging and WebLM, and bulk of the Communication Manager configuration data is transferred from the Communication Manager main server.

- Communication Manager, Utility Services, Branch Session Manager, and SAL or Services VM

Before you begin

- Ensure that System Manager Solution Deployment Manager is available in the solution with appropriate Communication Manager licenses.
- Read the Avaya Aura® application upgrade and migration considerations.
- Ensure that the applications that you want to migrate must be available in the inventory and discovered before the migration.

Procedure

1. Create a backup of the following Communication Manager and the associated applications in the survivable remote template:
   a. Communication Manager
   b. SAL or Services VM backup by using SAL or Services VM application utility.
   c. Branch Session Manager
2. Create a System Platform-based backup.

   You require the System Platform backup for disaster recovery purposes and to migrate the SAL Services VM data.
3. Record the following Communication Manager embedded main settings for Release 6.x:
   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server
4. On the System Manager Web console, click **Solution Deployment Manager** > **Upgrade Management**, select the Communication Manager 6.x element, and perform the following upgrade-related tasks:
   a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.

      The preupgrade check provides the hardware requirements for Communication Manager 6.x and associated devices that you migrate and checks if Utility Services is running on the virtual machine. If Utility Services is running, remove from migration.
   b. Select the Communication Manager Release 6.x system and click **Upgrade Actions** > **Upgrade/Update**.

      Solution Deployment Manager performs the following:
      - Imports the required network settings from System Platform.
      - Prompts you to fill the new attributes from OVA that are required for the deployment.

- Creates a backup of Communication Manager Survivable remote template.

  Note:

  Solution Deployment Manager does not backup Communication Manager Messaging.

- After successful backup, the upgrade process moves to the pause state.

5. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.
6. Install Appliance Virtualization Platform on the server over System Platform on Communication Manager 6.3.x hardware.

   The installation process takes about 30 minutes.
7. Select the same Communication Manager and click **Upgrade Actions** > **Resume**.
   - During the upgrade, the system prompts you to select host on which the OVA is deployed.
   - The process continues and the system automatically deploy all OVAs that are required to run Communication Manager automatically. For example, Communication Manager, Utility Services and Branch Session Manager.

     You can monitor the migration job status from the Upgrade Job Status page.
   - Restores Communication Manager and provides status of the upgrade.
8. Using System Manager Solution Deployment Manager deploy the SAL or Services VM OVA if needed.
   - You require one SAL or Services VM for each customer solution. You require to make changes to the IP address configuration when you migrate from SAL or Services VM in System Platform to VMware. The best practice is to maintain the same SAL IP address.
   - There is not enough space to load on S8300D.
9. Restore SAL or Services VM by using SAL restore capability.

   Update SAL with the new models, for example mapping Dom–0 to Appliance Virtualization Platform and adding Communication Manager Messaging and Utility Services.
10. Log in to the command line interface or the web console of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform , Communication Manager, Branch Session Manager, Utility Services, and SAL or Services VM.

Next steps

On the Communication Manager web console, create a backup of Communication Manager Release 7.1.3 running on S8300D or Communication Manager Survivable Remote Server.

Note:

You require to create a separate backups for each deployed application.

Migrating Communication Manager 6.x duplex for main and standby, survivable core, Branch Session Manager 6.x, System Manager 6.3.x, and Gateways

About this task

The section provides the procedure to migrate the following servers running on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, HP ProLiant DL360p G8, Dell™ PowerEdge™ R630, or HP ProLiant DL360 G9 server to Release 7.1.3 on Avaya-provided server:

- Communication Manager 6.x duplex main and standby
- Communication Manager 6.x survivable core
- G650, G450, G430, G350, G250, or G700 Gateways on Communication Manager 6.x
- Branch Session Manager 6.x
- System Manager 6.3.x

Before you begin

- Read the Avaya Aura® application upgrade and migration considerations.
- Upgrade the applications and the associated devices in the order defined in Avaya Aura® upgrade sequence.

Procedure

1. Migrate System Manager 6.3.x from System Platform to Appliance Virtualization Platform Release 7.1.3.

   For more information, see Migrating System Manager to Release 7.1.3 on page 218.

2. Generate new Communication Manager Release 7.1.3 and Branch Session Manager Release 7.1.3 license files from Avaya:

   a. From System Manager WebLM get the Primary Host ID that is required to generate the Release 7.1.3 license file.

   b. Install Communication Manager and Branch Session Manager license files on System Manager WebLM.

3. Click **Services** > **Inventory** > **Manage Elements** and perform the discovery operation to discover Communication Manager 6.x and Branch Session Manager 6.x.

4. On System Manager, click **Solution Deployment Manager** > **Software Library Management**, and configure an external server as a remote System Manager software library to save the files required for upgrade.

   You can save about 30 GB on System Manager. Therefore, configure external server as remote software library.

5. On the Solution Deployment Manager page, perform the following initial Solution Deployment Manager setup and entitlement analysis:

   a. Configure PLDS or an alternate source for System Manager-Solution Deployment Manager to perform the analysis of the a discovered Communication Manager 6.x and

Branch Session Manager 6.x applications software and software versions a customer is entitled to for the discovered 6.x applications.

b. Run the analyze operation on the selected Communication Manager 6.x and Branch Session Manager 6.x.

The Upgrade Management page displays the current state.

When analysis is complete, the system provides an option to download entitlements for elements that are entitled to a software or firmware versions. For example, OVA, `version.xml`, firmware for media modules, TN boards, gateways, and software patches.

c. On the Download Management page, download the entitlements to the external software library.

d. On VM Management, create a location that defines where the Communication Manager 6.x and Branch Session Manager 6.x reside in the VM hierarchy.

6. Perform the following to prepare Branch Session Manager 6.x for migration to Release 7.1.3:

a. From the command line interface create a backup of Branch Session Manager for disaster recovery.

b. Record the following network parameters for Branch Session Manager Release 6.x that you later require:

- All IP addresses
- Subnetwork mask
- Gateway
- DNS
- NTP Server

7. On Upgrade Management, select the Branch Session Manager 6.x element, perform the following upgrade-related tasks:

a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.

b. Select the Branch Session Manager Release 6.x system and click **Upgrade Actions** > **Upgrade/Update**.

Solution Deployment Manager:

- Imports required network setting from Branch Session Manager.
- Prompts you to fill the new attributes that are required from OVA for the deployment.
- Creates a backup of Branch Session Manager.
- After successful backup, the upgrade process moves to the Pause state.

8. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.

9. Install Appliance Virtualization Platform on the server that was earlier running Linux® Operating System.

   The installation process takes about 30 minutes.

10. Select the same Branch Session Manager and click **Upgrade Actions** > **Resume**.

    - During the upgrade, the system prompts you to select host on which the OVA is deployed.
    - The process continues and the system automatically deploy all OVAs that are required to run Branch Session Manager automatically. For example, Branch Session Manager and Utility Services.

      You can monitor the migration job status from the Upgrade Job Status page.
    - Restores Branch Session Manager and provides status of the upgrade.

11. Configure Branch Session Manager to point to System Manager WebLM that has the new Release 7.1.3 license files.
12. Verify that Branch Session Manager is operational.
13. Log in to command line interface or the web console of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform, Branch Session Manager, Utility Services, and SAL or Services Virtual Machine.

14. On the Branch Session Manager web console, create a backup of Branch Session Manager Release 7.1.3.

    You require to create a separate backups for each deployed application.

15. Perform the following to prepare Communication Manager 6.x survivable core server for migration to Release 7.1.3:

    a. Create a backup of Communication Manager 6.x for disaster recovery.

       - Communication Manager
       - System Platform

    b. Record the following network parameters for Communication Manager Release 6.x that you later require:

       - All IP addresses
       - Subnetwork mask
       - Gateway
       - DNS
       - NTP Server

16. On Upgrade Management, select the Communication Manager survivable core 6.x element, perform the following upgrade-related tasks:
    a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
    b. Select the Communication Manager Release 6.x system and click **Upgrade Actions** > **Upgrade/Update**.

       Solution Deployment Manager performs the following:

       - Imports required network setting from Communication Manager
       - Prompts you to fill the new attributes from OVA that are required for deployment.
       - Creates a backup of Communication Manager.
       - After successful backup, the upgrade process moves to the Pause state.
17. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.
18. Install Appliance Virtualization Platform on the server that was earlier running System Platform on Communication Manager 6.x element.

    The installation process takes about 30 minutes.
19. Select the same Communication Manager, and click **Upgrade Actions** > **Resume**.
    - During the upgrade, the system prompts you to select host on which OVA must be deployed.
    - The process continues and the system automatically deploy all OVAs that are required to run Communication Manager automatically. For example, Communication Manager and Utility Services.

      You can monitor the migration job status from the Upgrade Job Status page.
    - Restores Communication Manager and provides status of the upgrade.
20. Select the ESXi host on which you want to deploy OVA.
21. Configure Communication Manager to point to System Manager WebLM that has the new Release 7.1.3 license files.
22. Log in to command line interface of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform, Communication Manager, Utility Services, and SAL or Services Virtual Machine.
23. On the Communication Manager web console, create a backup of Communication Manager Release 7.1.3.

    You require to create a separate backups for each deployed application.
24. Perform the following to prepare Communication Manager 6.3.x main standby server for migration to Communication Manager Release 7.1.3:
    a. Create a backup of Communication Manager 6.3.x for disaster recovery.

b. Record the following network parameters for Communication Manager Release 6.3.x that you later require:

- All IP addresses
- Subnetwork mask
- Gateway
- DNS
- NTP Server

25. On Upgrade Management, select the Communication Manager 6.x element, and perform the following upgrade-related tasks:
    a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
    b. Select the Session Manager Release 6.x system and click **Upgrade Actions** > **Upgrade/Update**.

    Solution Deployment Manager performs the following:

    - Imports required network setting from Communication Manager
    - Prompts you to fill the new attributes that are required from OVA for the deployment
    - Creates a backup of Communication Manager
    - After successful backup, the upgrade process moves to the pause state
26. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.
27. Install Appliance Virtualization Platform on the server that was earlier running System Platform on the Communication Manager 6.x element.

    The installation process takes about 30 minutes.
28. Select the same Communication Manager and click **Upgrade Actions** > **Resume**.

    - During the upgrade, the system prompts you to select host on which the OVA is deployed.
    - The process continues and the system automatically deploy all OVAs that are required to run Communication Manager automatically. For example, Communication Manager and Utility Services.

      You can monitor the migration job status from the Upgrade Job Status page.
    - Restores Communication Manager and provides status of the upgrade.
29. Configure Communication Manager to point to System Manager WebLM that has the new Release 7.1.3 license files.
30. Log in to command line interface or the web console of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform, Communication Manager, Utility Services, and SAL or Services Virtual Machine.

31. On the Communication Manager web console, create a backup of Communication Manager Release 7.1.3.

    You require to create a separate backups for each deployed application.

32. Perform the following to prepare Communication Manager 6.3.x Main Active for migration to Communication Manager Release 7.1.3:

    a. From the command line interface, create a backup of Communication Manager 6.3.x for disaster recovery.

    b. Record the following network parameters for Communication Manager Release 6.3.x that you later require:

    - All IP addresses
    - Subnetwork mask
    - Gateway
    - DNS
    - NTP Server

33. On Upgrade Management, select the Communication Manager 6.3.x element, perform the following upgrade-related tasks:

    a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.

    b. Select the Communication Manager Release 6.3.x system and click **Upgrade Actions** > **Upgrade/Update**.

    Solution Deployment Manager

    - Imports required network setting from Communication Manager
    - Prompts you to fill the new attributes that are required from OVA for the deployment.
    - Creates a backup of Communication Manager.
    - After successful backup, the upgrade process moves to the Pause state.

34. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.

35. Install Appliance Virtualization Platform on the server that was earlier running System Platform on the Communication Manager 6.x element.

    The installation process takes about 30 minutes.

36. Select the same Communication Manager and click **Upgrade Actions** > **Resume**.

    - During the upgrade, the system prompts you to select host on which the OVA is deployed.
    - The process continues and the system automatically deploy all OVAs that are required to run Communication Manager automatically. For example, Communication Manager Utility Services, SAL or Services Virtual Machine.

You can monitor the migration job status from the Upgrade Job Status page.

- Restores Communication Manager and provides status of the upgrade.

37. Configure Branch Session Manager to point to System Manager WebLM that has the new Release 7.1.3 license files.
38. Log in to command line interface or the web console of the application, and install the Avaya Secure Gateway (ASG) file for each application OVA that you installed.

    For example, Appliance Virtualization Platform, Communication Manager, Utility Services, and SAL or Services Virtual Machine.
39. On the Communication Manager web console, create a backup of Communication Manager Release 7.1.3.

    You require to create a separate backups for each deployed application.

Migrating Communication Manager 6.x or 5.2.1 on S8800 duplex main or S8800 simplex survivable core with S8300D survivable remote

About this task

The section provides the procedure to migrate Communication Manager 6.x or 5.2.1 to Release 7.1.3 on Appliance Virtualization Platform:

- S8800 on CM duplex main, simplex survivable core or duplex simplex survivable core with S8300D survivable remote
- With S8300D survivable remote or Branch Session Manager
- System Manager 6.x installed on a Dell™ PowerEdge™ R610 or HP ProLiant DL360 G7 server

However, you can also migrate Communication Manager to Release 7.1.3 in customer-provided Virtualized Environment. You must purchase the required VMware hardware and virtual resources and licenses to run the duplex and simplex remote Communication Manager systems in a customer-provided Virtualized Environment. Get the new S8300E server or use the existing S8300D server. Communication Manager Release 7.1.3 survivable remote does not support the S8300C server.

Before you begin

Read the Avaya Aura® application upgrade and migration considerations.

- Order three new Communication Manager servers with preloaded Appliance Virtualization Platform that replaces the duplex main and simplex survivable core.
- Order an S8300E server or use an existing S8300D server. Communication Manager Release 7.1.3 survivable remote does not support the S8300C server. Appliance Virtualization Platform is not preloaded on S8300E.

Procedure

1. Migrate System Manager 6.x from System Platform to Appliance Virtualization Platform Release 7.1.3.

   For more information, see Migrating System Manager to Release 7.1.3 on page 218.

2. Install the new Communication Manager servers that are preloaded with Appliance Virtualization Platform
3. On System Manager, perform the discovery of the existing Communication Manager 6.x systems.
4. On Solution Deployment Manager, perform the following premigration tasks:
   a. From Software Library Management, configure the external or internal software library.
   b. From User Settings, configure to gain access to PLDS or an alternative source.

      System Manager Solution Deployment Manager uses the settings to perform the analysis of the a discovered Communication Manager element software and determines the software version a customer is entitled to for the discovered CM 6.x elements.

   c. On selected the Communication Manager 6.x elements, run the analyze operation.

      The Upgrade Management page displays the current state.

      When the Analyze operation is complete, the system displays an option to download entitlements elements that are required and entitled to a software or firmware version upgrade. The software files include OVA, `version.xml`, firmware for media modules, TN boards, gateways, and software patches.

   d. From Download Management, download the entitlements to the external or the internal library.
5. On VM Management, create a location where Communication Manager 5.2.1 and 6.x elements resides in the VM hierarchy.
6. From System Manager Solution Deployment Manager, ensure the second level discovery is successful for the existing Communication Manager 5.2.1 and 6.x servers.
7. Select the Communication Manager 5.2.1 and 6.x server to upgrade.

   During the upgrade configuration, do not select the same server option because Release 7.1.3 does not support upgrades to S8800.

8. Select one of the new ESXi VMware hosts where you want to migrate the existing Communication Manager 5.2.1 or 6.x.
9. Select the Communication Manager 5.2.1 or 6.x server, and click **Pre-upgrade Actions** > **Pre-upgrade Check**.

   The **Last Action Status** column displays the preupgrade status. Click the icon to view the complete status.

10. Select the Communication Manager 5.2.1 or 6.x server, and click **Upgrade Actions** > **Upgrade/Update**.

    The **Last Action Status** column displays the upgrade status. Click the icon to view the complete status.

    The system displays the migration status on the Upgrade Job Status page.

Related links

Migrating System Manager to Release 7.1.3 on page 218

Migrating System Manager to Release 7.1.3

About this task

During the migration of Avaya Aura® solution to Release 7.1.3, you must first migrate System Manager 6.x to Release 7.1.3.

Procedure

1. Create a backup of System Manager from the following:
   - System Manager web console
   - System Platform web console
2. Record the following System Platform and System Manager 6.x settings:
   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server
3. With the DVD that comes with Appliance Virtualization Platform, install the Solution Deployment Manager client on the computer of the technician if not already installed.

   Avaya provides the DVD with Solution Deployment Manager client and Appliance Virtualization Platform.
4. Set the IP address of the computer to 192.168.13.5.

   When you set the IP address to 192.168.13.5, the Solution Deployment Manager client can communicate with the Appliance Virtualization Platform services port on same network.
5. Install Appliance Virtualization Platform on the existing System Manager Release 6.x.
6. Using the Solution Deployment Manager client, in the VM Management section, create a location, host, and virtual machine that you require for deployment of OVA files.
7. Perform the following to prepare Utility Services if Utility Services is not already installed:
   a. Select the footprint size of the Utility Services virtual machine.

b. Select the Utility Services mode.

8. Deploy the Utility Services OVA file.
9. Install the Utility Services 7.1.3 feature pack.
10. On the computer of the technician, change the IP address to 192.11.13.5.

    The Solution Deployment Manager client can now communicate with Appliance Virtualization Platform and all virtual machines. When Utility Services OVA is setup, Utility Services can gain access to the entire virtual machine. Utility Services provides application routing between physical port and virtual applications.
11. Using the Solution Deployment Manager client, set any System Manager configuration settings that the system prompts, accept the licence terms, and deploy System Manager Release 7.1.3 OVA to the virtual machine.

    System Manager OVA deployment takes about 30 minutes.

Related links

Migrating Communication Manager 6.x or 5.2.1 on S8800 duplex main or S8800 simplex survivable core with S8300D survivable remote on page 216

Migrating Midsize Enterprise to Release 7.1.3

About this task

The section provides the procedure to migrate System Platform-based on Linux-based template to Appliance Virtualization Platform on Avaya common servers.

Before you begin

- Read the Avaya Aura® application upgrade and migration considerations.
- For Communication Manager 6.0 through 6.2 to Release 7.1.3 migration, you must manually upgrade from Communication Manager 6.x to 6.3.x by using System Manager, System Platform, and Communication Manager command line interface options. When the upgrade is complete, use the following procedure to migrate Communication Manager 6.3.x to Release 7.1.3.
- Deploy Utility Services if not already available.

Procedure

1. Create a backup of each Midsize Enterprise application running on the Midsize Enterprise 6.2.2 template by using:
   - The backup and restore capability of each application
   - System Platform

   System Platform backup can be used for disaster recovery.

2. Record the following network parameters for Midsize Enterprise Release 6.x that you later require:
   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server
3. Install the Solution Deployment Manager client on the computer of the technician.
4. Download all Avaya Aura® Release 7.1.3 Midsize Enterprise application OVAs on computer of the technician.
5. Install Appliance Virtualization Platform on the Midsize Enterprise Release 7.1.3 server to remove the Midsize Enterprise System Platform.
6. Using the Solution Deployment Manager client, create a location, host, and virtual machine on which the Midsize Enterprise application must run.
7. Deploy the following OVAs one at a time:
   - Utility Services
   - System Manager
   - Session Manager
   - Communication Manager
   - Application Enablement Services
   - SAL
   - Communication Manager Messaging
   - Presence Services

   Enable the option to override the footprint resource reservation when you deploy the OVA files on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, or HP ProLiant DL360p G8 servers.
8. Install the required software patches by using command line interface or System Manager Solution Deployment Manager.
9. With the restore capability of the application, restore the backup of the application that you created in Step 1.
10. Make any networking configuration change that is required for migrating from System Platform to Virtualized Environment.

    The network configuration is required for the applications such as Utility Services, Appliance Virtualization Platform, Communication Manager, Communication Manager Messaging to communicate with each other.

11. Generate new Communication Manager Release 7.1.3 license files from Avaya:
    a. From System Manager WebLM get the Primary Host ID that is required to generate the Release 7.1.3 license file.
    b. Install Communication Manager license files on System Manager WebLM.
12. On each Avaya Aura® application, install the Avaya Secure Gateway file.
13. Verify that the system is migrated to Release 7.1.3.

Migrating System Platform-based elements or bare metal-based Communication Manager elements to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager

Migrating Communication Manager 6.x or CM Simplex on survivable remote template or Communication Manager 5.2.1 on S8330D to Avaya Aura® Release 7.1.3 with Appliance Virtualization Platform remote deployment

About this task

The section provides the procedure to migrate Communication Manager Release 5.2.1 on S8300D or 6.x on System Platform to Avaya Aura® Release 7.1.3 in the following configuration:

- Embedded remote template on S8300D or CM Simplex with survivable remote template running on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, or HP ProLiant DL360p G8 server.

  Survivable remote template does not contain Communication Manager Messaging and WebLM, and bulk of the Communication Manager configuration data is transferred from the Communication Manager main server.
- Communication Manager, Utility Services, Branch Session Manager, and SAL or Services VM.

Note:

You must have the minimum network speed of 2Mbps with up to 100ms delay (WAN).

Before you begin

- Ensure that System Manager Solution Deployment Manager is available in the solution with appropriate Communication Manager licenses.
- Read the Avaya Aura® application upgrade and migration considerations.

- Ensure that the applications that you want to migrate must be available in the inventory and discovered before the migration.

Procedure

1. Create a backup of the following Communication Manager Release 6.x and the associated applications in the survivable remote template:
   a. Communication Manager
   b. SAL or Services VM backup by using SAL or Services VM application utility.
   c. Branch Session Manager
2. Create a System Platform-based backup.

   You require the System Platform backup for disaster recovery purposes and to migrate the SAL Services VM data.
3. Record the following Communication Manager embedded main settings for Release 6.x:
   - All IP addresses
   - Subnetwork mask
   - Gateway
   - DNS
   - NTP Server
4. On the System Manager Web console, click **Solution Deployment Manager** > **Upgrade Management**, select the Communication Manager 6.x element, and perform the following upgrade-related tasks:
   a. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.

      The preupgrade check provides the hardware requirements for Communication Manager 6.x and associated devices that you migrate and checks if Utility Services is running on the virtual machine. If Utility Services is running, remove from migration.
   b. Select the Communication Manager Release 5.2.1 or 6.x system and click **Upgrade Actions** > **Upgrade/Update**.

      Solution Deployment Manager performs the following:
      - Imports the required network settings from System Platform.
      - Prompts you to fill the new attributes from OVA that are required for the deployment.
      - Creates a backup of Communication Manager Survivable remote template.

        Note:

        Solution Deployment Manager does not backup Communication Manager Messaging.
5. On the Upgrade Configuration page, click **edit**.

6. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 7.1.3 feature pack.
7. On the **Element Configuration** tab, fill the required fields, and click **Migrate to AVP install**.

   The system displays the **AVP Configuration** tab.
8. On the **AVP Configuration** tab, provide the required details.
   - If you are migrating from Communication Manager Release 5.2.1 bare metal LSP to Appliance Virtualization Platform, you must configure the following fields:
     - **Source Root User**
     - **Source Root Password**
     - **AVP management IPv4 Address** (completely new IP address to be assigned to Appliance Virtualization Platform)
   - If you are migrating from Communication Manager Release 6.x, the system displays the above fields preconfigured and prepopulated.
9. Click **Save**.
10. To save the configuration, click **Save Configuration**.

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

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

Next steps

Note:

- For migrating Communication Manager 6.x S8300D or CM Simplex on survivable remote template to Appliance Virtualization Platform, Utility Services element is also automatically migrated to Release 7.1.2 or later.
- For migrating bare metal LSP (Communication Manager 5.2.1 on 8300D/E) to Appliance Virtualization Platform, only Communication Manager element is automatically migrated to Release 7.1.2 or later. When the migration of bare metal LSP Communication Manager 5.2.1 on 8300D/E) to Appliance Virtualization Platform is successfully completed, you must deploy Utility Services Release 7.1.0 separately and then update it to Release 7.1.2.0 or later using Solution Deployment Manager.

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

About this task

Use this procedure to remotely migrate System Platform-based system and elements in bulk to Appliance Virtualization Platform Release 7.1.3. You can remotely migrate:

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

Before you begin

- On the Manage Elements page, add the System Platform system and required elements. For information about adding a new element, see *Administering Avaya Aura® System Manager*.
- Refresh the element.
- Analyze the software.
- Perform the pre-upgrade check.
- Download a copy of the `AVP_Bulk import spread sheet.xlsx` spreadsheet from Avaya PLDS website at https://plds.avaya.com/or from Avaya Support website at https://support.avaya.com. Fill the required system details in the spreadsheet.

  Note:

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

Procedure

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

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

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

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

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

7. On the Upgrade Management page, click  .

   The **Configuration Status** column displays  .

8. To save the configuration, click **Save Configuration**.

   The update configuration is saved as a job in the Upgrade Jobs Status page.

9. On the Upgrade Configuration page, click **Upgrade**.

10. To view the upgrade status, perform the following:

    a. In the navigation pane, click **Upgrade Job Status**.

    b. In the **Job Type** field, click **Upgrade**.

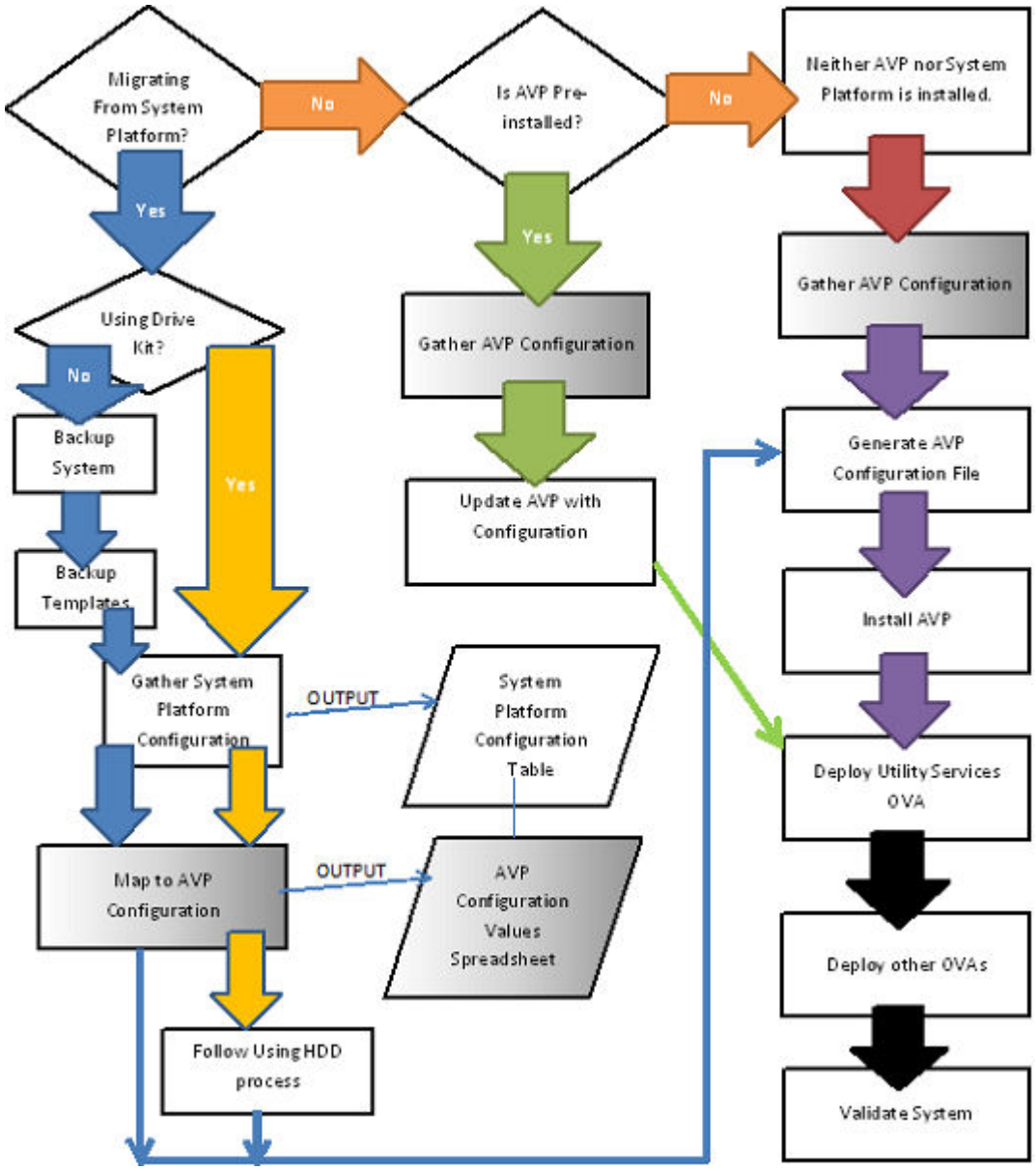
    c. Click the upgrade job that you want to view.

11. On the Upgrade Management page, click  .

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

System Platform to Appliance Virtualization Platform migration scenarios

Appliance Virtualization Platform installation scenarios



Deploying Utility Services and virtual machines when Out of Band Management is enabled

Before you begin

Install the Solution Deployment Manager client on your computer.

Procedure

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

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

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

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

   If Out of Band Management is enabled, provide information in the Out of Band Management-related fields. If Out of Band Management is disabled, leave the fields blank.
8. Deploy Utility Services, and wait for the virtual machine to deploy successfully.
9. Install the Utility Services 7.1.3 feature pack.
10. Deploy all other virtual machines in the solution one after the other.
11. Install the feature pack for Avaya Aura® applications.
12. Validate the system.

Related links

Enabling IP forwarding using Services Port VM for Utility Services on page 135

Deploying Utility Services and virtual machines on the services port

Before you begin

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

Procedure

1. Using the Solution Deployment Manager client, create a location.
2. To connect the computer to the services port on the server, configure the following:
   - **IP address**: 192.168.13.5
   - **Netmask**: 255.255.255.248
   - **Gateway**: 192.168.13.6

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

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

   In the Configuration Parameters section, the page displays parameters that are specific to Utility Services.
7. Enter the IP address details for Utility Services, deploy Utility Services, and wait for the virtual machine to deploy successfully.
8. Install the Utility Services 7.1.3 feature pack.
9. Change the Utility Services configuration parameters to the following:
   - **IP address**: 192.11.13.5
   - **Netmask**: 255.255.255.252
   - **Gateway**: 192.11.13.6

   On the Solution Deployment Manager client, in the Appliance Virtualization Platform host, leave the IP address as 192.168.13.6.
10. Ensure that the IP forwarding feature is enabled on Utility Services.

11. Deploy all other virtual machines in the solution one after the other.
12. **(Optional)** During the deployment, if the sanity check fails, verify the host network configuration.

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

Related links

Enabling IP forwarding using Services Port VM for Utility Services on page 135

Chapter 9: Post-upgrade tasks

Rehosting license files

Procedure

1. On the WebLM console, click **Server Properties**.
2. On the Server Properties page, note the WebLM server host ID.
3. Go to the PLDS website regenerate the license file for your product using the same host ID.
4. Install the license file that you generated on the WebLM server.

   For more information on installing a license file, see “Installing the license file” in *Administering Avaya WebLM*.

Related links

Rehost of license files on page 34

Postmigration tasks for Communication Manager

Before you begin

Log on to the software management interface of Communication Manager Release 7.1.1.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. On the left navigation pane, click **Server Configuration** and reconfigure the SNMP parameters.

   You require to configure the SNMP parameters because after migration, the values from existing system are not populated in System Manager.

Postmigration tasks for Communication Manager Messaging

Procedure

1. For migration from Communication Manager 5.2.1 with Communication Manager Messaging, restore the Communication Manager Messaging 5.2.1 data that you saved on a remote server after migration.
2. Restore any additional languages that you backed up.

Enhanced Access Security Gateway (EASG) overview

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

Managing EASG from CLI

About this task

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

Before you begin

Log in to the application CLI interface.

Procedure

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

   The system displays the status of EASG.
2. To enable EASG, do the following:
   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message.

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

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      ```

```
eligible for Avaya remote connectivity. Please see the Avaya
support site (https://support.avaya.com/ registration) for
additional information for registering products and
establishing remote access and alarming.
```

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

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

3. To disable EASG, do the following:

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

The system displays the following message.

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

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

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

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **`EASGProductCert --certInfo`**.

The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.

2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
2. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
3. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Deleting the virtual machine snapshot

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`

2. To log in to the Appliance Virtualization Platform host, provide the credentials.
3. In the left navigation pane, click **Virtual Machines**.
4. Select the virtual machine, click **Actions** > **Snapshots** > **Manage snapshots**.

   The system displays the Manage snapshots - <Virtual machine name> dialog box.
5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.

Deleting the virtual machine snapshot from the vCenter managed host or standalone host

Procedure

1. Log in to the vSphere client for the vCenter managed host or the standalone host.
2. Depending on the host, perform one of the following
   a. On the vCenter managed host, select the host, and then select the virtual machine.
   b. On the Standalone host, select the virtual machine.
3. Right-click the selected virtual machine, click **Snapshot** > **Snapshot Manager**.

   The system displays the Snapshot for the <Virtual machine name> dialog box.
4. Select the snapshot and click **Delete**.

   The system deletes the selected snapshot.

Chapter 10: Rollback process

Removing the Appliance Virtualization Platform patch from the ESXi host CLI

About this task

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

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

Note:

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

Before you begin

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

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

Procedure

1. To stop all virtual machines that are running on the Appliance Virtualization Platform host, at the prompt, type `/opt/avaya/bin/stopallvms.py`.
2. To rollback from Appliance Virtualization Platform Release 7.1.3 to any of the previous releases, perform the following:
   a. Type the `/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<complete path name of the rollback patch>` command.

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

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

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

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

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

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

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

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

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

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

   Issue the following commands after reboot:

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

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

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

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

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

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

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

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

Issue the following commands after reboot:

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

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

Next steps

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

Upgrade rollback

If the upgrade process of an element fails:

- If the admin does not specify rollback all, when the element upgrade fails, the system stops the entire upgrade process and display the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- If the admin specifies rollback all, when the element upgrade fails, the system stops the upgrade and rolls back the overall upgrade process. The system rolls back only the successfully upgraded elements.

Rolling back an upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.

   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message `Selected System Platform or child of System Platform, and System Platform and all child applications`.
4. Click **Upgrade Actions** > **Rollback**.

Chapter 11: Resources

Documentation

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

Title	Use this document to:	Audience
Overview		
Avaya Aura® Virtualized Environment Solution Description	Understand the high-level solution features and functionality	Customers and sales, services, and support personnel
Avaya Aura® System Manager Overview and Specification	Understand the high-level solution features and functionality	Customers and sales, services, and support personnel
Administering		
Administering Avaya Aura® System Manager	Perform administration tasks	System administrators
Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Administer the network components of Communication Manager.	System administrators
Administering Avaya Aura® Communication Manager, 03-300509	Administer Communication Managercomponents, such as trunks, signalling groups, and dial plans. Set up telephony features, such as conferencing, transfer, and messaging.	System administrators
Using		
Using the Solution Deployment Manager client	Deploy Avaya Aura® applications and install patches on Avaya Aura® applications.	System administrators
Implementing		
Upgrading Avaya Aura® System Manager	Install and configure Avaya applications	Implementation personnel
Migrating and Installing Avaya Appliance Virtualization Platform	Install Appliance Virtualization Platform on Avaya-provided servers, and migrate the data from System Platform to Appliance Virtualization Platform.	Implementation personnel
Troubleshooting		

Table continues…

Title	Use this document to:	Audience
Troubleshooting Avaya Aura® System Manager	Perform troubleshooting tasks	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 239

Finding documents on the Avaya Support website

Procedure

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

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

Related links

Documentation on page 238

Training

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

Course code	Course title
Avaya Aura® core implementation	
1A00234E	Avaya Aura® Fundamental Technology
4U00040E	Avaya Aura® Session Manager and System Manager Implementation
4U00030E	Avaya Aura® Communication Manager and Communication Manager Messaging Implementation

Table continues…

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

Viewing Avaya Mentor videos

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

About this task

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

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

Note:

Videos are not available for all products.

Support

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

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.

Glossary

Appliance Virtualization Platform	Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.
Migration	The migration process includes changing the server hardware, change the operating system, and reinstallation of software that includes hypervisor. During migration, you might need to perform backup and restore operations outside the normal upgrade process. You cannot rollback the upgrade easily.
Update	The update process includes installing patches of an application. For example, kernel patches, security patches, hotfixes, service packs, and feature packs.
Upgrade	The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor. The process is triggered through the normal process without requiring additional backup and restore operations. You can rollback an upgrade.

Index

Special Characters

/sbin/generate-certificates 109

Numerics

7.0 ..... 171, 173

A

aborting
virtual machine report generation 104
activate SSH from Utility Services 120
add
virtual machine 96
Add elements
manual 32
adding
Appliance Virtualization Platform host 52
AVP host 52
ESXi host 52
location 44
vCenter to SDM 110
adding certificates
available hosts 108
existing hosts 108
migrated hosts 108
adding ESXi host 52
adding location 44
adding location to host 111
adding vCenter to SDM 110
add virtual machine 96
analyze job status 120
Appliance Virtualization Host
configure login banner 70
push login banner 70
Appliance Virtualization Platform 57, 63, 64, 76, 117, 144
change password 60
deploy 133
generating kickstart file 61, 130
license file 66
networking 136
NIC teaming 138
remove patch 235
restarting 69
shutting down 69
update 54, 78
WebLM Configuration 66
Appliance Virtualization Platform and Utility Services 27
Appliance Virtualization Platform host Gateway
change 56
edit 56
Appliance Virtualization Platform host IP address
change 56
edit 56
Appliance Virtualization Platform host IP address *(continued)*
change 56
edit 56
Appliance Virtualization Platform host password
changing 60
Appliance Virtualization Platform installation scenarios 226
Appliance Virtualization Platform network parameters 56
Appliance Virtualization Platform USB drive
configure 133
Application Enablement Services 15
application upgrade tasks 20
applying
third-party AVP certificates 71
automated
Avaya Aura application upgrades 13
Avaya Aura 201, 203
Avaya Aura application
Services Port static routing update 89
upgrade order 28
Avaya Aura application migration 16
Avaya Aura applications
migrations 13
Network Parameters change 102
upgrades 13
Avaya Aura application upgrade 171
Avaya Aura application upgrade tasks 20
Avaya-provided appliance
Avaya Virtualized Platform 15
AVP license status 69

B

backup connection 138
backup existing configuration 116
Branch Session Manager 15
Branch Session Manager upgrade 163, 192

C

certificates
accepting 106
generating 106
certificate update
ESXi host 107
vCenter 107
VMware documentation 107
Certification
validation 105
Certification validation 105
change
Appliance Virtualization Platform host IP address 56
Host/ IP Settings 57
network settings 76

change *(continued)*
Network Settings 57
Change Gateway 75
change IP address for AVP host 56
Change IP FQDN 86
change Netmask for Appliance Virtualization Platform host 56
Change Network Params 56
changing
IP address and default gateway 65
changing Appliance Virtualization Platform host password . 60
changing Network Parameters for Avaya Aura 102
checklist
Branch Session Manager upgrade 161
Communication Manager 7.x upgrade 161
Session Manager upgrade 161
common causes
VM deployment failure 91
Communication Manager 15
Application Enablement Services 201
Communication Manager Messaging 201
Engagement Development Platform 201
Session Manager 201
System Manager 201
upgrade 36
WebLM 201
Communication Manager 6.x on S8800 duplex main 216
Communication Manager Messaging 15
backup 18
migration 18
post migration tasks 231
restore 231
Communication Manager update 84, 165, 167
Communication Manager upgrade 163, 184
Communication Manager upgrade considerations 18
Communication Manager upgrade from Software Management 12
Communication Manager upgrade from System Manager .. 12
Communication Manager upgrades
footprints 33
profile map 33
Configuration Parameters 91, 96
configure
Ethernet port speed 140
login banner on host 70
port speed 140
configure Appliance Virtualization Platform USB drive 133
configure server preinstalled with Appliance Virtualization Platform 117
configuring
WebLM Server on Appliance Virtualization Platform 68
considerations
Avaya Aura application migration 198
migration 198
upgrade 198
correcting ESXi host certificate 107
create
virtual machine 81
create discovery profiles 32
creating
generic CSR 72
CSR
create field description 73
edit field description 73
custom patch
upload 183

D

Data Migration utility 150
deleting
location 45
snapshot from standalone host 234
upgrade jobs 122
virtual machine 87
deleting location 45
deleting vCenter 111
deploy
Branch Session Manager 81
Communication Manager 81
product knowledge 9
Session Manager 81
skills 9
System Manager 81
tools 9
Utility Services 81
deploy Appliance Virtualization Platform 133
deploy application 43
deploy Avaya Aura 7.0 application 81
Deploy Avaya Aura applications
Solution Deployment Manager client 199
Deploying an OVA file
utility services 79
Deployment options for Avaya Aura applications 31
deploy OVA 81
deploy Utility Services and virtual machines
services port 228
deploy virtual machines on Appliance Virtualization Platform 227
different server migration 190
disabling
SSH on Appliance Virtualization Platform 63
disabling SSH 64
disaster recovery 124
discover elements 32
discovery
profiles 32
discovery profiles
create 32
documentation 238
documentation map 20
download manager
uploading custom patch 183
download software 78
duplex Communication Manager

duplex Communication Manager *(continued)*
migration ... 187
duplex system ... 187, 190
duplication parameters ... 187, 190

E

EASG
certificate information ... 232
disabling ... 231
enabling ... 231
status ... 231
EASG site certificate ... 232
edit
virtual machine ... 86, 87
Edit Host ... 75
editing
ESXi host ... 54
generic CSR ... 72
location ... 45
vCenter ... 111
editing ESXi host ... 54
editing location ... 45
editing upgrade configuration ... 121
editing vCenter ... 111
Edit Location ... 51
Edit Upgrade Configuration
AVP Configuration ... 174
Element Configuration ... 174
Edit vCenter ... 113
edit virtual machine ... 86
element
add ... 154
elements
discover ... 32
elements upgrade
target release ... 41
element upgrade ... 171
enabling
SSH on Appliance Virtualization Platform ... 63
Enabling ... 135
enabling SSH ... 64
Enhanced Access Security Gateway
EASG overview ... 231
esxcfg-route ... 65
esxcli network ip interface ipv4 set -i vmk0 -I ... 65
ESXi host
adding ... 52
editing ... 54
removing ... 70
restarting ... 69
ESXi host certificate addition ... 108
ESXi host certificate update ... 107
ESXi host map to unknown location ... 70
Ethernet port speed ... 140
existing configuration
backup ... 116
existing hosts
managing certificates ... 108
existing vCenter
managing certificates ... 108

F

field description
edit elements ... 154
field descriptions
change password ... 77
Create AVP Kickstart ... 61, 130
create CSR ... 73
edit CSR ... 73
Edit Host ... 75
Edit Location ... 51
Hosts ... 45
load AVP host certificate ... 73
Locations ... 45
Map vCenter ... 112
New Host ... 75
New Location ... 51
Upgrade Configuration ... 173
upgrade management ... 171
Virtual Machines ... 45
VM Deployment ... 96
WebLM Configuration ... 68
field descriptions, Snapshot Manager ... 74
footprint
Utility Services ... 123
footprint flexibility ... 33
for Communication Manager
postmigration tasks ... 230

G

General Configuration Details ... 174
generate_report.sh ... 103
generating
certificates ... 106
new self-signed certificates for ESXi host ... 109
virtual machine report ... 103
generic CSR
creating ... 72
editing ... 72

H

hardware supported ... 17
host ... 57, 76
generating kickstart file ... 61, 130
monitoring ... 114
Host
update ... 78
Hosts ... 45

I

InSite Knowledge Base 241
install
- Application Enablement Services 39
- Avaya Aura applications 39
- Avaya Aura Media Server 39
- Avaya Breeze 39
- Branch Session Manager 39
- Communication Manager 39
- SAL 39
- SDM 39
- Session Manager 39
- Solution Deployment Manager client 39
- System Manager 39
- WebLM 39

install AVP host patch
- Solution Deployment Manager 54

install custom patches 167
install custom software patches 167
Installed Patches 169
Installed Patches field descriptions 100
Install on Same ESXi 155
Install on Same server 160
install patches 84, 165
install services packs 84, 165, 167
install software patches 84, 165
Install System Manager patch 101
Install System Manager patches 153
interchange active and standby servers 190
interchange roles 190
invalid license 34
IP address and default gateway
- changing 65

IP address change
- license rehost 34

IP address mapping 130
IP forwarding 135

L

latest software patches 21
license files
- rehost 230

license rehost 34
licensing upgrades 34
Life cycle management 43
Linux-based application
- recovery 124

Linux Operating System upgrades 42
- preupgrade check 42

load AVP host certificate
- field descriptions 73

location
- adding 44
- deleting 45
- editing 45

location *(continued)*
- view 44

Locations 45

M

Manage
- System Manager upgrades 153

Manage Software 12
managing certificates migrated hosts 108
Manual addition of elements 32
map Dom-0 to Appliance Virtualization Platform 130
map ESXi host to unknown location 70
Map vCenter 110–113
Media Server 15
Midsize Enterprise
- upgrade 219

migrate 203
- System Platform-based system and elements in bulk to AVP remotely 224
- System Platform-based system and elements to AVP remotely 221

migrate Communication Manager 6.x on survivable remote template 207
migrated hosts
- managing certificates 108

migrate to Appliance Virtualization Platform 126
migratiing
- Avaya Aura applications 198
- Communication Manager 198
- SAL 198
- Session Manager 198

migrating
- Communication Manager 6.x on S8800 duplex main 216
- S8800 simplex survivable core with S8300D survivable remote 216

migrating Avaya Aura applications 198
migrating Communication Manager 210
migrating duplex Communication Manager servers 187
migrating System Manager during Avaya Aura application migration 218
Migration
- System Platform 128

migration on different server 190
migration on same server 187
mode
- Utility Services 123

monitoring
- host 114
- virtual machine 114
- VM 114

N

network configurations 187, 190
networking
- Appliance Virtualization Platform 136

network parameters
change 75
Network Parameters change 102
network parameters for AVP and virtual machines
change 87
New Host 75
New Location 51
New vCenter 113

O

on System Platform 203
Options
Avaya Aura applications deployments 31
Out of Band Management
deploy virtual machines 227
OVA
Release version 22

P

password
change 77
password change
Appliance Virtualization Platform host 60
password policy 60
password rules 60
patch information 21
perform System Manager tests 161
permissions required 31
post migration tasks
Communication Manager Messaging 231
postmigration tasks for Communication Manager 230
Postmigration validation 140
preinstall Appliance Virtualization Platform 117
Presence Services 15
preupgrade check 42
pre upgrade checks
System Platform upgrades 43
preupgrade job status 120
Preupgrade tasks 36
primary server 195
primary System Manager operational 196
product knowledge 9
profile mapping for Communication Manager upgrades, ... 33
profiles
discovery 32
push
login banner on host 70

R

recovering
Linux-based application 124
System Platform-based application 124
reestablish
reestablish *(continued)*
connection 101
Reestablish Connection 45
re-establishing trust
SDM elements 83
Solution Deployment Manager elements 83
virtual machine 83
re-establishing trust virtual machine 83
refresh elements job status 120
rehosting license files 230
rehost license 34
related documentation 238
release notes for latest software patches 21
remove AVP patch 235
remove patch
Appliance Virtualization Platform 235
removing
ESXi host 70
removing ESXi host 70
removing location from host 111
removing vCenter 111
required
credentials 31
permissions 31
required permissions 31
restart
virtual machine 90
restarting
Appliance Virtualization Platform 69
ESXi host 69
restart virtual machine from SDM 90
restore additional languages 231
rollback
upgrade 237
rollback upgrade 237
run
Data Migration utility 150

S

same host installation 160
same server migration 187
scenario
deploy Appliance Virtualization Platform on services port 228
deploy virtual machines on Appliance Virtualization Platform 228
scenario is enabled
deploy virtual machines on Appliance Virtualization Platform when Out of Band Management 227
scenarios
Appliance Virtualization Platform 226
SDM
installation 39
SDM client
Deploy Avaya Aura applications 199
SDM elements

SDM elements *(continued)*
re-establishing trust ... 83
secondary System Manager standby and pause ... 196
Select Flexi Footprint ... 86
select upgrade target release ... 41
self-signed certificates for ESXi host
generate ... 109
servers supported ... 17
services port
deploy Utility Services ... 228
virtual machines ... 228
Services Port static route update ... 89
Services Port VM ... 135
Session Manager ... 15
Session Manager update ... 84, 165, 167
Session Manager upgrade ... 163, 184, 192
shutting down
AVP ... 69
site certificate
add ... 232
delete ... 232
manage ... 232
view ... 232
skills to deploy ... 9
snapshot from Appliance Virtualization Platform
deleting ... 233
snapshot from vCenter managed host
deleting ... 234
Snapshot Manager
virtual machine snapshot ... 74
Snapshot Manager field descriptions ... 74
software
download ... 78
Software library options ... 32
Software Management ... 12
software management interface ... 187
software patches ... 21
Solution Deployment Manager ... 12, 15, 60, 63
install ... 144, 146
restart virtual machine ... 90
start virtual machine ... 90
stop virtual machine ... 90
update Appliance Virtualization Platform host ... 54
upgrade automation ... 14
Solution Deployment Manager elements
re-establishing trust ... 83
SSH from Utility Services ... 120
standby server ... 195
start
virtual machine ... 90
start virtual machine from SDM ... 90
static routing
changing ... 89
updating ... 89
status
Analyze ... 122
analyze job ... 120
status *(continued)*
Preupgrade check ... 122
preupgrade check job ... 120
Refresh elements job ... 120
upgrade job ... 120
upgrade jobs ... 122
stop
virtual machine ... 90
stop virtual machine from SDM ... 90
support ... 241
supported servers ... 17
supported upgrades and migrations ... 16
System Manager ... 15
7.0 ... 121
7.0 upgrade ... 148
installing patches ... 152
Solution Deployment Manager ... 152
upgrade ... 121, 144, 146
Virtual Machines ... 152
VM Management ... 152
System Manager documentation ... 238
System Manager during Avaya Aura application migration ... 218
System Manager installation
verify ... 161
System Manager upgrade ... 155
System Manager upgrade to Avaya-provided server ... 150
System Manager upgrade to VMware ... 150
System Manager VM management ... 100
System Manager VM update ... 101
System Platform ... 144, 146
System Platform-based Communication Manager ... 203
System Platform to Appliance Virtualization Platform migration ... 126
System Platform to Appliance Virtualization Platform upgrade ... 25
System Platform upgrades
preupgrade checks ... 43

T

target release ... 41
select ... 41
template values ... 128
third-party AVP certificates
applying ... 71
creating generic CSR ... 72
editing generic CSR ... 72
tools to deploy ... 9
training ... 239

U

Unknown location host mapping ... 70
update
Appliance Virtualization Platform ... 78
Appliance Virtualization Platform host ... 54

update *(continued)*
Branch Session Manager 167
Communication Manager 84, 165, 167
Session Manager 84, 165, 167
Utility Services 167
WebLM 167
updates 16
update software 84, 165, 167
update static routing 100
Update Static Routing 45
update System Manager VM 101
Update VM IP/FQDN 87
updating ESXi host or vCenter certificate 107
updating Services Port static routing 89
upgrade
Avaya Aura application 36, 163
Branch Session Manager 161, 163, 174, 184, 192
checklist 161
Communication Manager 36, 161, 163, 174
Communication Manager Messaging 163
elements 169
Midsize Enterprise 219
rehost license 34
rollback 237
Session Manager 36, 161, 163, 174, 184, 192
simplex Communication Manager 184
System Platform to Appliance Virtualization Platform 25
target release 41
WebLM 163
Upgrade 173
upgrade and migration considerations 198
Upgrade automation support by Solution Deployment Manager 14
Upgrade Configuration
field descriptions 173
Upgrade Configuration Details 174
upgrade considerations 18
upgrade jobs
deleting 122
editing 121
status 122
upgrade job status 120
Upgrade job status
Viewing 121
upgrade management
field descriptions 171
Upgrade Management 12, 155
upgrade order
Avaya Aura applications 28
Avaya Aura applications using the Solution Deployment Manager client 30
Upgrade Release Selection 41
upgrade rollback 237
upgrades
licensing 34
upgrades and migrations 16
Upgrade System Manager 153
upgrade System Manager using data migration utility 150
Upgrade to release 41
upgrading 201
upgrading Avaya Aura applications 195, 210
primary System Manager operational 196
secondary System Manager standby and pause 196
upgrading Avaya Aura applications in Geographic Redundancy setup 195
upgrading system manager
virtualized environment 148
upgrading System Manager 7.0 148
upload
custom patch 183
uploading a custom patch 183
uploading custom patch 183
uploading custom patch field description 183
Utility Services 15, 135, 203
Avaya Aura virtualized appliance offer 27
footprint 123
mode 123
Utility Services and Appliance Virtualization Platform 27
UUID change
license rehost 34

V

validate migration
System Platform to Appliance Virtualization Platform 140
validate System Platform migration 140
Validation
certificate 105
vCenter
add 113
adding 110
add location 111
deleting 111
edit 113
editing 111
manage 111
remove location 111
removing 111
unmanage 111
vCenter certificate update 107
vCentre 112
verify
System Manager installation 161
videos 240
view
location 44
viewing
virtual machine report status 104
Viewing AVP host
license status 69
view location 44
virtual appliance 22
virtualized environment 22
Virtualized Environment 201

virtualized environment-based System Manager
upgrade 142
virtual machine
create 81
deleting 87
edit 86
migration 125
monitoring 114
re-establishing trust 83
restart 90
start 90
stop 90
Virtual machine management 43
virtual machine report
aborting 104
overview 103
Virtual Machines 45
virtual machine snapshot using SDM
deleting 74
VM connection reestablish 101
VM Deployment 96
field descriptions 91
VM Management 144, 146, 148
VMware infrastructure 22

W

WebLM 15
WebLM Server on AVP host 68