



Upgrading and Migrating Avaya Aura[®] applications to Release 7.0

Release 7.0
Issue 1
December 2015

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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 a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING 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. 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 Designated Processor that hosts 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. 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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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 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 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](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](http://WWW.MPEGLA.COM).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya and Avaya Aura® are registered trademarks of Avaya Inc.

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

Contents

Chapter 1: Introduction	9
Purpose	9
Intended audience	9
Change history	9
Prerequisites	9
Related resources	10
Documentation	10
Training	12
Viewing Avaya Mentor videos	13
Support	13
Chapter 2: Upgrade overview and considerations	15
Upgrade Management overview	15
Automated upgrades and migrations of Avaya Aura® applications	16
Upgrade automation support by Solution Deployment Manager	17
Upgrade modes using System Manager Solution Deployment Manager	17
Supported upgrades and migrations	19
Supported 7.0 servers	20
Server hardware and resources	20
Communication Manager migration considerations	20
Communication Manager Messaging migration considerations	20
Chapter 3: Planning for upgrade	22
Documentation map for Avaya Aura® application upgrade tasks	22
Supported upgrade paths to Avaya Aura® Release 7.0	23
Upgrades from System Platform on 6.x to Appliance Virtualization Platform on Avaya Aura® Release 7.0	35
Utility Services in the Avaya-appliance model	36
Avaya Aura® solution upgrade sequence	37
Required permissions	38
Deployment options for Avaya Aura® Release 7.0 applications	39
Software library options	39
Manual addition of elements	39
Profile mapping for Communication Manager 6.x upgrades	40
Licensing upgrades	41
Authentication files for application	42
Chapter 4: Preupgrade tasks	43
Preupgrade tasks overview	43
Key tasks for upgrading Avaya Aura® applications to Release 7.0	43
Installing the Solution Deployment Manager client on your computer	46
Upgrade target release selection	48

Selecting the target release for upgrade.....	48
Preupgrade checklist for Linux [®] Operating System upgrades.....	49
Pre-upgrade checklist for System Platform upgrades.....	50
Virtual machine management.....	50
Virtual machine management.....	50
Managing the location.....	51
Managing the host.....	56
Downloading the OVA file to System Manager.....	65
Managing the virtual machine.....	66
Monitoring a host and virtual machine.....	79
Chapter 5: Common procedures for deployment, upgrades, and migrations.....	81
Creating a backup of the existing configuration.....	81
Configuring servers preinstalled with Appliance Virtualization Platform.....	82
Activating SSH from Utility Services.....	84
Upgrade job status.....	85
Upgrade job status	85
Viewing the Upgrade job status.....	85
Deleting the Upgrade jobs.....	85
Upgrade Job Status field descriptions.....	86
Utility Services field descriptions.....	86
Recovering a Linux-based application from disaster.....	87
Recovering a System Platform-based application from disaster.....	88
Chapter 6: Migration from System Platform to Appliance Virtualization Platform.....	89
Migration checklist.....	89
System Platform and template values worksheet.....	90
IP address mapping.....	91
Appliance Virtualization Platform configuration spreadsheet field descriptions.....	92
Configuring the Appliance Virtualization Platform USB drive.....	93
Installing Appliance Virtualization Platform.....	94
Enabling IP forwarding using Services Port VM for Utility Services.....	96
Appliance Virtualization Platform networking.....	97
Teaming NICs from CLI.....	99
Setting the Ethernet port speed.....	100
Loading a customer-specific authentication file.....	101
Validating the migration.....	102
Chapter 7: Upgrade process.....	103
Upgrading Avaya Aura [®] System Manager.....	103
System Manager upgrade management.....	103
Verifying the installation of System Manager.....	114
Upgrading Avaya Aura [®] applications.....	114
Checklist for upgrading Avaya Aura [®] applications to Release 7.0	114
Upgrading Avaya Aura [®] applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0.....	115
Installing software patches.....	117

Installed Patches field descriptions.....	119
Upgrade Management field descriptions.....	120
Upgrade Configuration field descriptions.....	122
Edit Upgrade Configuration field descriptions.....	123
Upgrading Avaya Aura® Communication Manager.....	127
Upgrading Communication Manager 6.x to Release 7.0.....	127
Preparing duplex Communication Manager for migration.....	129
Migrating duplex Communication Manager on the same server.....	130
Migrating duplex Communication Manager on a different server.....	132
Upgrading Avaya Aura® Session Manager.....	134
Upgrading Session Manager or Branch Session Manager from Release 6.x to 7.0.....	134
Upgrading Avaya Aura® applications using Solution Deployment Manager in the Geographic Redundancy setup.....	136
Upgrading Avaya Aura® applications when the primary System Manager is operational and the secondary System Manager is in standby mode.....	136
Upgrading Avaya Aura® applications when the primary System Manager is nonoperational and secondary System Manager is in active standby mode.....	137
Upgrading Avaya Aura® applications when the primary System Manager is operational, and the secondary in standby and pause state.....	138
Chapter 8: Avaya Aura 7.0 migration scenarios.....	140
Avaya Aura® 7.0 migration scenarios.....	140
Avaya Aura® application upgrade and migration considerations.....	140
Deploying 6.x applications to Avaya Aura® Release 7.0 by using the Solution Deployment Manager client.....	141
Upgrading Avaya Aura® 6.x applications in a customer-provided Virtualized Environment to Avaya Aura® Release 7.0.....	143
Migrating System Platform-based Communication Manager 6.x to Avaya Aura® Release 7.0 on Appliance Virtualization Platform.....	145
Migrating Communication Manager 6.x S8300D or CM Simplex on survivable remote template to Avaya Aura® Release 7.0.....	149
Migrating Communication Manager 6.x duplex for main and standby, survivable core, Session Manager 6.x, System Manager 6.3.x, and Gateways.....	152
Migrating Communication Manager 6.x or 5.2.1 on S8800 duplex main or S8800 simplex survivable core with S8300D survivable remote.....	158
Migrating System Manager to Release 7.0.....	159
Migrating Midsize Enterprise to Release 7.0.....	161
System Platform to Appliance Virtualization Platform migration scenarios.....	163
Appliance Virtualization Platform installation scenarios.....	163
Deploying Utility Services and virtual machines when Out of Band Management is enabled.....	164
Deploying Utility Services and virtual machines on the services port.....	164
Chapter 9: Postmigration tasks.....	167
Postmigration tasks for Communication Manager.....	167
Postmigration tasks for Communication Manager Messaging.....	167

Downloading and installing an authentication file on the Avaya Aura® application.....	167
Chapter 10: Post Installation Verification.....	169
Verifying the installation of System Manager.....	169
Post installation checklist.....	169
Verifying the connections.....	170
Chapter 11: Rollback process.....	171
Upgrade rollback.....	171
Rolling back an upgrade.....	171
Glossary.....	172

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.

Intended audience

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.

Change history

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

Issue	Date	Summary of changes
2.0	May 2016	• Added procedure for installing custom patches for Avaya Aura® applications. • Added flexibility to select application and data port numbers during the Solution Deployment Manager client installation. • Added Out of Band Management configuration chapter.

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

Related 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
<i>Avaya Aura® System Manager Overview and Specification</i>	Understand the high-level solution features and functionality	Customers and sales, services, and support personnel
Administering		
<i>Administering Avaya Aura® System Manager</i>	Perform administration tasks	System administrators
<i>Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504</i>	Administer the network components of Communication Manager.	System administrators
<i>Administering Avaya Aura® Communication Manager, 03-300509</i>	Administer Communication Manager components, such as trunks, signalling groups, and dial plans. Set up telephony features, such as conferencing,	System administrators

Table continues...

Title	Use this document to:	Audience
	transfer, and messaging.Communication Manager.	
Implementing		
<i>Upgrading Avaya Aura® System Manager in Virtualized Environment</i>	Install and configure Avaya applications	Implementation personnel
<i>Migrating and Installing Avaya Appliance Virtualization Platform</i>	Install Appliance Virtualization Platform on Avaya-provided servers, and migrate the data from System Platform to Appliance Virtualization Platform.	Implementation personnel
Troubleshooting		
<i>Troubleshooting Avaya Aura® System Manager</i>	Perform troubleshooting tasks	System administrators and IT personnel

Related links

[Finding documents on the Avaya Support website](#) on page 11

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at <http://support.avaya.com/>.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.
For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

[Documentation](#) on page 10

Training

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

Course code	Course title
Avaya Aura® core implementation	
1A00234E	Avaya Aura® Fundamental Technology
4U00040E	Avaya Aura® Session Manager and System Manager Implementation
4U00030E	Avaya Aura® Communication Manager and Communication Manager Messaging Implementation
10U00030E	Avaya Aura® Application Enablement Services Implementation
8U00170E	Avaya Aura® Presence Services Implement and Support
AVA00838H00	Avaya Aura® Media Server and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Aura® Media Server and Gateways Implementation Workshop Labs
Avaya Aura® core support	
5U00050E	Session Manager and System Manager Support
5U00060E	ACSS - Avaya Aura® Communication Manager and CM Messaging Support
4U00115I	Avaya Aura® Communication Manager Implementation Upgrade (R5.x to R6.x)
4U00115V	
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

Table continues...

Course code	Course title
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.

Procedure

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

 Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Upgrade overview and considerations

Upgrade Management overview

Solution Deployment Manager > Upgrade Management, a centralized upgrade solution of System Manager, provides an automatic upgrade of Communication Manager and associated devices, such as Gateways, TN boards, and media modules from a single view. You can upgrade Communication Manager Release 5.2.1 and 6.x to Release 7.0, and Session Manager and Branch Session Manager to Release 7.0. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

 Important:

System Manager Release 7.0 also supports using System Manager Release 6.3.8 to upgrade Communication Manager, gateways, media modules, and TN boards to Release 6.3.8. However, the Release 6.3.8 user interface is available only when you select **Release 6.3.8** as target version on the **Solution Deployment Manager > Upgrade Release Setting** page.

Using System Manager Solution Deployment Manager, perform the following in the given sequence

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 elements and components.
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, if the new release supports the hardware, the RAID battery is sufficient, the bandwidth is sufficient, and if the files are downloaded.
5. Install software patches and service packs.

Upgrades of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVAs, but involve some manual operations for creating backup and restoring the backup data for all other applications manual process. The upgrade of Communication Manager,

Session Manager, Branch Session Manager and Utility Services to Release 7.0 is automated. The upgrade process includes creating backup, deploying OVA, upgrading, and restoring the backup.

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 elements combined together in an upgrade or update job is considered as a group.
- 20 elements in a job group: Maximum elements that can be combined in an upgrade or update group is 20. You can combine any element type for upgrade in a group.

Elements in paused state are also included in the capacity. If 5 upgrade job groups are running or in a paused state, you cannot upgrade the sixth group.

Automated upgrades and migrations of Avaya Aura® applications

From System Manager, 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.

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 Release 7.0 OVA, installing the patches, feature packs, or service pack, and restoring the backup on the Release 7.0 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 Release 7.0 OVA. You must manually create a backup of the existing system, install the Release 7.0 patches, service packs, or feature packs, and restore the data on the Release 7.0 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 Release 7.0 OVA by using the vSphere client, System Manager Solution Deployment Manager, or the Solution Deployment Manager client, install the Release 7.0 patches, and restore the data on the Release 7.0 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 7.0>* document.

Upgrade modes using System Manager Solution Deployment Manager

During migration, System Manager upgrade, System Manager updates, and Appliance Virtualization Platform host updates are performed by using the Solution Deployment Manager client only.

Modes of upgrading Avaya Aura® applications using Solution Deployment Manager

Operation	Avaya Aura® application	Tool or application supported
Fresh deployments	Communication Manager	• System Manager Solution Deployment Manager • Solution Deployment Manager client
Avaya-provided appliance on Appliance Virtualization Platform	Session Manager	
	Branch Session Manager	

Table continues...

Operation	Avaya Aura® application	Tool or application supported
	Utility Services System Manager Application Enablement Services Presence Services on Engagement Development Platform WebLM Communication Manager Messaging Media Server	
Deployment during migration	Upgrade System Manager Update System Manager Update Appliance Virtualization Platform	Solution Deployment Manager client
Automated upgrade	Communication Manager Session Manager Branch Session Manager Utility Services	System Manager Solution Deployment Manager
Semi-automated upgrade	Communication Manager Messaging	• System Manager Solution Deployment Manager • Solution Deployment Manager client
Manual upgrade	Application Enablement Services Presence Services on Engagement Development Platform WebLM Media Server SAL or Services VM	

Supported upgrades and migrations

Supported upgrades

With Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.0:

- Linux-based Communication Manager and the associated devices, such as media gateways, TN boards, and media modules.
- System Platform-based Communication Manager
 - Duplex CM Main / Survivable Core with Communication Manager
 - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
 - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
 - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
 - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- Branch Session Manager associated with Communication Manager
- Linux-based Session Manager
- 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 7.0.

Supported updates

With Solution Deployment Manager, you can install service packs, feature packs, and software patches for the following Avaya Aura® Release 7.0 applications:

- Communication Manager and the associated devices, such as media modules, TN boards, and media gateways
- Session Manager
- Branch Session Manager
- Communication Manager Messaging
- Utility Services
- Appliance Virtualization Platform, the ESXi host running on Avaya-provided appliance

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 and service packs on System Manager

Supported 7.0 servers

In the Avaya appliance model, the customer can deploy or upgrade to Avaya Aura® Release 7.0 applications on the following Avaya-provided servers:

- Dell™ PowerEdge™ R610 2CPU MID2
- HP ProLiant DL360 G7 2CPU MID4
- Dell™ PowerEdge™ R620 1CPU MID3
- HP ProLiant DL360p G8
- S8300D, for Communication Manager and Branch Session Manager
- S8300E, for Communication Manager and Branch Session Manager

Related links

[Server hardware and resources](#) on page 20

Server hardware and resources

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see <http://www.vmware.com/resources/guides.html>.

Related links

[Supported 7.0 servers](#) on page 20

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 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 7.0, check for any additional languages. The languages must be restored on the Release 7.0 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 7.0 OVA, and manually restoring the data. For example, Application Enablement Services. For more information, see the *Upgrading and migrating to <Avaya Aura application 7.0>* document.

Task	Document
Obtaining the supported server and installing the server for Avaya-provided appliance deployments.	Installation procedures for servers supported in Release 7.0.
Installing Appliance Virtualization Platform.	This document
Installing the Solution Deployment Manager client if System Manager is unavailable.	<i>Deploying Avaya Aura[®] applications from Avaya Aura[®] System Manager</i>
Ensuring that System Manager is installed and operational.	<i>Deploying Avaya Aura[®] applications from Avaya Aura[®] System Manager</i>
Upgrading System Manager if required using the Solution Deployment Manager client.	<i>Upgrading Avaya Aura[®] System Manager in Virtualized Environment</i>
Configuring SNMP for successful discovery of elements, such as Communication Manager and Session Manager.	"Managing inventory" in <i>Administering Avaya Aura[®] System Manager</i>
Adding elements or automatically discovering applications and associated devices.	"Managing inventory" in <i>Administering Avaya Aura[®] System Manager</i>
Setting up PLDS or alternate source.	"Solution deployment and upgrades" in <i>Administering Avaya Aura[®] System Manager</i>
Setting up the software library.	"Solution deployment and upgrades" in <i>Administering Avaya Aura[®] System Manager</i>
Refreshing software.	"Solution deployment and upgrades" in <i>Administering Avaya Aura[®] System Manager</i>
Analyzing the software.	"Solution deployment and upgrades" in <i>Administering Avaya Aura[®] System Manager</i>

Table continues...

Task	Document
Downloading the entitled software.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>
Running the preupgrade check.	This document
Upgrading the application.	This document
Checking preupgrade or upgrade job status	This document
Post upgrade tasks. For example: • Creating a backup of new system. • Installing ASG file.	Upgrading <Avaya Aura application>. For example, for postupgrade tasks for Communication Manager, see <i>Upgrading to Avaya Aura® Communication Manager</i> .
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 <i>Upgrading Avaya Aura® Session Manager</i> .

Supported upgrade paths to Avaya Aura® Release 7.0

Table 1: System Manager

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.3.x, 6.2.x, 6.1.x, or 6.0 Service Pack 1 and 2	System Platform	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Deploy Release 7.0 with Solution Deployment Manager client. 4. Restore the data with data migration utility by using System Manager command line interface or Solution Deployment Manager client.	1. Create a backup of 6.x with latest System Platform. 2. Deploy Release 7.0 on the customer-supplied server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data with data migration utility by using System Manager command line interface or Solution Deployment Manager client.

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.3 or 6.2	Virtualized Environment	1. Create a backup of 6.x 2. Install the server and Appliance Virtualization Platform 3. Deploy Release 7.0 with the Solution Deployment Manager client. 4. Restore the data with data migration utility by using System Manager command line interface.	1. Create a backup of 6.x 2. Deploy Release 7.0 on the customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data with data migration utility by using System Manager command line interface.
5.2	Appliance	1. Create a backup of the existing System Manager 5.2 system.  Note: You can use the back later to restore the system to the original state in disaster recovery. 2. Export the NRP data. 3. Install Appliance Virtualization Platform. 4. Install System Manager Release 7.0 Solution Deployment Manager client. 5. Ensure that the same IP address and hostname as the original System	1. Create a backup of the existing System Manager 5.2 system.  Note: You can use the back later to restore the system to the original state in disaster recovery. 2. Export the NRP data. 3. Install Appliance Virtualization Platform. 4. Install System Manager Release 7.0 Solution Deployment Manager client or vCenter. 5. Ensure that the same IP address and hostname as the original System

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
		Manager 5.2 server is used. 6. Import the NRP data.	Manager 5.2 server is used. 6. Import the NRP data.
Release earlier than 5.0		No upgrade or migration. A new System Manager install with day 1 configuration.	No upgrade or migration. A new System Manager install with day 1 configuration.

Table 2: Application Enablement Services

You cannot upgrade Application Enablement Services by using Solution Deployment Manager. You can use Solution Deployment Manager only to deploy Application Enablement Services 7.0 on the new system.

From		To: Release 7.0		
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare	Release 7.0 Software Only
6.x, 5.2.x, 4.x, or 3.x	Software only	1. Create a backup of Application Enablement Services. 2. Replace the server if required. 3. Install Appliance Virtualization Platform. 4. Deploy Release 7.0 with Solution Deployment Manager 5. Restore the data.	1. Create a backup of Application Enablement Services. 2. Deploy Release 7.0 with vCenter 3. Restore the data.	1. Create a backup of Application Enablement Services. 2. Replace the server if required. 3. Install Release 7.0 4. Restore the data.
6.x or 5.2.x	• System Platform • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7	1. Create a backup of 6.x or 5.2.x 2. Replace server if required.	1. Create a backup of 6.x. 2. Deploy Release 7.0 on the customer-supplied server	1. Create a backup of 6.x or 5.2.x. 2. Replace server if required.

Table continues...

From		To: Release 7.0		
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare	Release 7.0 Software Only
	• Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • The IBM x3550 M2 not supported with Application Enablement Services Release 7.0	3. Install Appliance Virtualization Platform 4. Deploy Release 7.0 with Solution Deployment Manager 5. Restore the data.	or VMware infrastructure with vCenter. 3. Restore the data.	3. Install Release 7.0 4. Restore the data.
6.x	Virtualized Environment	1. Create a backup of 6.x. 2. Install server if required. 3. Install Appliance Virtualization Platform. 4. Deploy Release 7.0 with Solution Deployment Manager 5. Restore the data.	1. Create a backup of 6.x. 2. Deploy Release 7.0 with vCenter 3. Restore the data.	1. Create a backup of 6.x. 2. Install server if required. 3. Install Release 7.0 4. Restore the data.
6.x	• Non-System Platform • Bundled server • S8510 not supported with Application Enablement Services Release 7.0	1. Create a backup of 6.x. 2. Replace server. 3. Install Appliance Virtualization Platform 4. Deploy Release 7.0 with Solution Deployment Manager	1. Create a backup of 5.2.x. 2. Deploy Release 7.0 on customer-supplied server or VMware infrastructure with vCenter 3. Restore the data.	1. Create a backup of 6.x. 2. Replace the server. 3. Install Release 7.0 4. Restore the data.

Table continues...

From		To: Release 7.0		
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare	Release 7.0 Software Only
		5. Restore the data.		
5.2.x	• Non-System Platform • Bundled server • S8500C or S8510	1. Create a backup of 5.2.x. 2. Install Appliance Virtualization Platform. 3. Deploy Release 7.0 with Solution Deployment Manager 4. Restore the data	1. Create a backup of 5.2.x. 2. Deploy Release 7.0 on customer-supplied server or Vmware infrastructure with vCenter 3. Restore the data	1. Upgrade to 6.3. 2. Create a backup of 6.x 3. Replace the server. 4. Install Linux operating system 6.5. 5. Install Release 7.0. 6. Restore the data.
4.x or 3.x	• Bundled server S8500B, S8500C. • S8510 • IBM x3550 M2 not supported with Application Enablement Services Release 7.0	1. Upgrade to 6.3.3. 2. Create a backup of 6.3.3. 3. Replace the server. 4. Install Appliance Virtualization Platform. 5. Deploy Release 7.0 with Solution Deployment Manager 6. Restore the data.	1. Upgrade to 6.3.3. 2. Create a backup of 6.3.3. 3. Deploy Release 7.0 on customer-supplied server or Vmware infrastructure with vCenter 4. Restore the data.	1. Upgrade to 6.3.3. 2. Create a backup of 6.3.3. 3. Replace the server. 4. Install Linux operating system 6.5. 5. Install Release 7.0. 6. Restore the data.

Table 3: Communication Manager

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
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	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Perform the upgrade from Solution Deployment Manager.	1. Create a backup of 6.x. 2. Perform the upgrade from with Solution Deployment Manager.
6.3.x, 6.2.x, or 6.0.1	System Platform on unsupported servers. For example, S8800 and S8510.	1. Create a backup of 6.x. 2. Install the new server. 3. Install Appliance Virtualization Platform. 4. Deploy Release 7.0 with Solution Deployment Manager 5. Restore the data.	1. Create a backup of 6.x. 2. Deploy Release 7.0 on the customer-supplied server or VMware infrastructure with Solution Deployment Manager or vCenter 3. Restore the data.
6.3.x, 6.2.x, or 6.0.1	Virtualized Environment	1. Create a backup of 6.3.x. 2. Install the new supported server and Appliance Virtualization Platform. 3. Deploy Release 7.0 with Solution Deployment Manager. 4. Restore the data.	1. Create a backup of 6.x. 2. Deploy Release 7.0 with Solution Deployment Manager or vCenter 3. Restore the data.

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
5.2.1	Appliance	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Perform Upgrade with Solution Deployment Manager.	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Perform Upgrade with Solution Deployment Manager.
Release earlier than 5.0	any	1. Create a backup of 6.3.x. 2. Install new supported server and virtualization platform. 3. Deploy Release 7.0 with Solution Deployment Manager. 4. Restore the data.	1. Create a backup of 6.3.x. 2. Install new supported server and virtualization platform. 3. Deploy Release 7.00 with Solution Deployment Manager. 4. Restore the data.

Table 4: Communication Manager Messaging

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.3	System Platform embedded with Communication Manager 6.3	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Perform Upgrade with Solution Deployment Manager. 4. Restore the Communication Manager Messaging data.	1. Create a backup of 6.x. 2. Deploy Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data.

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.3	Virtualized Environment	1. Create a backup of 6.3.x. 2. Install new supported server and virtualization platform 3. Deploy Release 7.0 with Solution Deployment Manager. 4. Restore the data.	1. Create a backup of 6.x. 2. Deploy Release 7.0 with Solution Deployment Manager or vCenter. 3. Restore the data.

Table 5: Session Manager

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
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	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Perform Upgrade with Solution Deployment Manager.	1. Create a backup of 6.x. 2. Deploy Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data.
6.3, 6.2, 6.1, or 6.0	Appliance— older servers	1. Create a backup of 6.x. 2. Install server. 3. Install Appliance Virtualization Platform. 4. Perform Upgrade with Solution Deployment Manager.	1. Create a backup of 6.x. 2. Deploy Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter 3. Restore the data.
6.3 or 6.2	Virtualized Environment	1. Create a backup of 6.x. 2. Install server.	1. Create a backup of 6.x. 2. Deploy Release 7.0 with Solution

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
		3. Install Appliance Virtualization Platform. 4. Deploy Release 7.0 with Solution Deployment Manager. 5. Restore the data.	Deployment Manager or vCenter. 3. Restore the data.
5.2	Appliance on unsupported servers	• Create a backup of 6.3.x • Install Appliance Virtualization Platform	1. Upgrade to 6.3.x, then Deploy Release 7.0 to customer provided VE through Solution Deployment Manager or vCenter. 2. Restore the data.
Release earlier than 5.0	Appliance —unsupported servers	1. Create a backup of 6.x. 2. Install server. 3. Install Appliance Virtualization Platform. 4. Restore the data.	1. Upgrade to 6.3.x. 2. Deploy Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data.

Table 6: Presence Services

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
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	1. Create a backup of 6.x. 2. Install Appliance Virtualization Platform. 3. Install Engagement Development Platform OVA using Solution Deployment Manager. 4. Install Presence Services onto	1. Create a backup of 6.x. 2. Deploy Engagement Development Platform Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Install Presence Services onto

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
		Engagement Development Platform 5. Replicate data from System Manager.	Engagement Development Platform. 4. Replicate data from System Manager.
6.2.6 or 6.2.5	Software only	1. Create a backup of 6.x. 2. Install the server. 3. Install Appliance Virtualization Platform. 4. Install Engagement Development Platform OVA using Solution Deployment Manager. 5. Install Presence Services onto Engagement Development Platform 6. Replicate data from System Manager.	1. Create a backup of 6.x. 2. Deploy Engagement Development Platform Release 7.0 onto customer server/VMware infrastructure with Solution Deployment Manager or vCenter. 3. Install Presence Services onto Engagement Development Platform, replicate data from System Manager.
6.2.6 or 6.2.5	Virtualized Environment	1. Create a backup of 6.x. 2. Install the server. 3. Install Appliance Virtualization Platform. 4. Install Engagement Development Platform OVA using Solution Deployment Manager. 5. Install Engagement Development Platform OVA using Solution Deployment Manager. 6. Install Presence Services onto	1. Create a backup of 6.x. 2. Deploy Engagement Development Platform Release 7.0 onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Install Presence Services onto Engagement Development Platform. 4. Replicate data from System Manager.

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
		Engagement Development Platform 7. Replicate data from System Manager.	
Release earlier than 6.2.5	System Platform	Upgrade to 6.2.4, then follow process for 6.2.4	Upgrade to 6.2.4, then follow process for 6.2.4
Release earlier than 6.2.5	Software Only	Upgrade to 6.2.4, then follow process for 6.2.4	Upgrade to 6.2.4, then follow process for 6.2.4

Table 7: Utility Services

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.2 or 6.3	System Platform	1. Create a backup of 6.x. 2. Install server if needed. 3. Install Appliance Virtualization Platform, deploy US OVA with Solution Deployment Manager client. 4. Restore the data. 5. Rehost licenses.	1. Create a backup of 6.x. 2. Deploy US Release 7.0 OVA onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data.
6.2 or 6.3	Virtualized Environment	1. Create a backup of 6.x. 2. Install Server Install Appliance Virtualization Platform. 3. Deploy US OVA with Solution Deployment Manager client. 4. Restore the data. 5. Rehost licenses.	1. Create a backup of 6.x. 2. Deploy US Release 7.0 OVA onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data.

Table 8: WebLM

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
6.2.x	System Platform	1. Create a backup of 6.2.x. 2. Install server if needed. 3. Install Appliance Virtualization Platform. 4. Deploy WebLM Release 7.0 OVA with Solution Deployment Manager client. 5. Restore the data. 6. Rehost licenses.	1. Create a backup of 6.2.x. 2. Deploy WebLM Release 7.0 OVA onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data. 4. Rehost licenses.
6.2.x or 6.3.0	Virtualized Environment	1. Create a backup of 6.2.x or 6.3. 2. Install server. 3. Install Appliance Virtualization Platform 4. Deploy WebLM Release 7.0 OVA with Solution Deployment Manager client. 5. Restore the data. 6. Rehost licenses.	1. Create a backup of 6.2.x or 6.3. 2. Deploy WebLM Release 7.0 OVA onto customer server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data. 4. Rehost licenses.
Release earlier than 6.0	System Platform, standalone WebLM deployed with adopting products.	1. Create a backup of pre 6.x. 2. Install the server. 3. Install Appliance Virtualization Platform. 4. Restore the data. 5. Rehost licenses. 6. Update logs and usage history	1. Create a backup of pre 6.x. 2. Deploy WebLM Release 7.0 OVA onto customer's server or VMware infrastructure with Solution Deployment Manager or vCenter. 3. Restore the data. 4. Rehost licenses.

Table continues...

From		To: Release 7.0	
Release	Offer and Deployment	Avaya-provided Virtual Appliance	Customer-provided VMWare
		configurations, if they were changed from default values.	5. Update logs and usage history configurations if they were changed from default values.

Upgrades from System Platform on 6.x to Appliance Virtualization Platform on Avaya Aura® Release 7.0

In Release 7.0, you can select the applications that are installed on a server. Therefore, when planning for upgrade to Release 7.0, 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 in Release 7.0, 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 being supported as a snap-in on Engagement Development Platform, so that OVA needs to be installed on the server in Release 7.0.

System Platform Template	Applications Included in template on System Platform 6.x	OVA's needed in Release 7.0 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	Communication Manager, Communication Manager	Since WebLM is part of System Manager, no

Table continues...

System Platform Template	Applications Included in template on System Platform 6.x	OVA's needed in Release 7.0 for upgrade to Appliance Virtualization Platform	Notes
	Messaging, Utility Services, with SAL and WebLM as part of System Platform CDOM.	Messaging, Utility Services, SAL	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	
Midsized 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, Engagement Development Platform, 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, Engagement Development Platform, Utility Services	Since WebLM is part of System Manager, no separate WebLM OVA is required.

Related links

[Utility Services in the Avaya-appliance model](#) on page 36

Utility Services in the Avaya-appliance model

In Avaya Aura® Release 7.0, 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. As a

result, Utility Services with the Services Port virtual machine becomes a key component, and must be deployed on all virtual machines in Avaya-appliance offer in Release 7.0.

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, Services Port is on the front plate. The Services Port virtual machine also supports ASG logins and install of a customer ASG file on to the system. By default, a generic ASG file is available on the system.

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

From Avaya Aura® Release 7.0, 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 Avaya-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 Linux® server: Utility Services is mandatory for migration of systems running on 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 Release 7.0](#) on page 35

Avaya Aura® solution upgrade sequence

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

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

Note:

Use the Solution Deployment Manager client to upgrade System Manager.

2. Session Manager. If available in the solution, upgrade in the following order:
 - a. All Session Manager servers
 - b. All Branch Session Manager servers
3. G650 or H.248 gateways if IPSI firmware needs to be updated.

H.248 gateways include G250, G350, G430, G450, and G700.

4. Communication Manager. If available in the solution, upgrade in the following order:
 - a. Survivable remote server
 - b. Main server that is in the standby state
 - c. Main server that is in the active state
5. WebLM
6. SAL
7. Application Enablement Services

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 7.0 applications

During upgrades, you can deploy Avaya Aura® Release 7.0 applications by using the following:

- System Manager deployment by using the Solution Deployment Manager client only.
- All other Avaya Aura® Release 7.0 applications:
 - The centralized Solution Deployment Manager that System Manager provides.
 - The Solution Deployment Manager client when System Manager is unavailable.

In Avaya-appliance model, for fresh deployments, Avaya Aura® is available to end-users through a set of Avaya-supplied common servers. Avaya appliances are 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 39

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 39

[Discovery of Avaya Aura applications and associated devices](#) on page 40

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 39

Profile mapping for Communication Manager 6.x upgrades

Before you upgrade Communication Manager from Release 6.x to Release 7.0 ensure the correct footprints.

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 7.0 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	2 vCPUs, 4400 MHz, 4.0 Gb RAM

Table continues...

Communication Manager 6.x template	Communication Manager Release 7.0 deployment option	Resources
	Medium Main only supporting up to 2400 users This profile is targeted as a migration path for Communication Manager on Midsize Enterprise.	
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
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 7.0 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 7.0 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 7.0 license file.
- On centralized WebLM, install the Communication Manager 7.0 and Session Manager 7.0 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.

Authentication files for application

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for the application. With the ASG keys, Avaya Services can gain secure access to the customer system.

The application installs a default authentication file. You must replace the default file using the Authentication File System (AFS) to create a unique authentication file. AFS is an online application available at [RFA](#).

Each authentication file contains an authentication file ID (AFID) to identify the file. You use the AFID to create a new authentication file to replace the current authentication file on the server.

 Note:

Installation of the unique authentication file is essential. Failure to install the unique authentication file results in receiving an alarm that retransmits daily until you install the authentication file.

Chapter 4: Preupgrade tasks

Preupgrade tasks overview

To successfully upgrade the system to Release 7.0, you must perform all tasks listed in the Preupgrade tasks section.

Key tasks for upgrading Avaya Aura® applications to Release 7.0

The table contains the key tasks that are required to upgrade Avaya Aura® applications to Release 7.0.

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 Release 7.0.	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 <i>Administering Avaya Aura® System Manager</i>
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

Table continues...

Task	Note
Option 2: Set up the PLDS access through an alternate source.	
Set up the software library.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>

Performing the upgrade process

Task	Note
Refresh the elements in inventory.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>
Perform the analyze software operation for the Avaya Aura® application that you selected.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>
Download the software.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>
Perform the preupgrade check.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>
Run the upgrade operation.	Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0 on page 115 Checklist for upgrading Avaya Aura applications to Release 7.0 on page 114  Note: The system takes about 2.5 hours to complete the upgrade process.

Installing the service packs

Task	Note
Installing the service pack or software patches on the Avaya Aura® application.	Installing software patches on page 117
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-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.

! Important:

For deployments through service port by using the Solution Deployment Manager client, get the Solution Deployment Manager client software from the Avaya support site at <http://support.avaya.com>. The Solution Deployment Manager client software version available in the media does not support the service port deployment.

Before you begin

1. Ensure that Windows 7.0 or 8.1 operating system is installed on the computer.

+ Tip:

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

2. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

+ Tip:

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

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

+ Tip:

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

4. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
5. Ensure that 443 and 1527 ports are available.
6. Close all applications that are running on your computer.
7. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

+ Tip:

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

- a. In the left navigation pane, click **Advanced system settings**.

- b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.
 - c. Verify the system variables.
8. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

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

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.0.1.17824_7.zip` file from the Avaya PLDS website at <https://plds.avaya.com/>.

On the Avaya PLDS website, you can provide the application name as **System Manager**, and version as **7.0**.

2. Copy the zip file, and extract to a location on your computer by using the WinZip application.
3. Using the **Run as administrator** option, run the `Avaya_SDMClient_win64_7.0.0.1.17824_7.exe` file.

The system displays the Avaya Solution Deployment Manager screen.

4. On the Welcome page, click **Next**.
5. On the License Agreement page, click **I accept the terms of the license agreement** and click **Next**.
6. On the Install Location page, perform one of the following:
 - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
 - To specify a different location for installation, click **Choose** and browse to an empty folder.
7. Click **Next**.
8. On the Preinstallation Summary page, review the information, and click **Next**.
9. On the Summary and Validation 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 system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.

- c. 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.

! Important:

If port 443 is unavailable, verify if the Skype application is running on the computer, and quit the application. If you close Skype, the application continues to run in the background. For more information, see “Solution Deployment Manager client installation fails” in *Troubleshooting Avaya Aura® System Manager*.

10. Click **Install**.

11. To exit the installer, on the Install Complete page, click **Delete**.

The installer creates a shortcut on the desktop.

12. To start the client, click .

Next steps

To enable the Solution Deployment Manager client to communicate with the services port of Appliance Virtualization Platform, set the following on the technician computer:

- IP address: 192.168.13.5
- Netmask: 255.255.248
- Gateway: 192.168.13.1

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 48

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 7.0**: 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 48

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.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, and reset virtual machines.

- Deploy Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya-provided appliance environments.
- Remove 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 virtual machine by using the System Manager Solution Deployment Manager and the Solution Deployment Manager client.

Managing the location

Viewing a location

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. Click the Locations tab.

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. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () 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 55

Editing the location

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () 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 55

Deleting a location

Procedure

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

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 ESXi host.
Host IP	The IP address of the ESXi host.
Host FQDN	FQDN of the ESXi host.
Current Action	The operation that is currently being performed on the ESXi host.
Last Action	The last completed operation on the ESXi host.
Data Store	The data store with the available size.
License Status	The status of the license.
ESXi Version	The VMware ESXi version. The options are 5.5, 5.1, and 5.0.
AVP	The ESXi host type. The options are: • true: Appliance Virtualization Platform host • false: VMware ESXi host

Button	Description
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.

Table continues...

Button	Description
Remove	Removes the hosts that you select. The system moves the hosts associated with the deleted locations to unknown location.
Change Network Params	Displays the Network Parameters section where you can change the network parameters for the Appliance Virtualization Platform host.
Change Password	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
Update	Displays the Update Host page where you can select the file for updating the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.

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 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, 7.0.0.0.
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 virtual machine
Trust Status	The trust status of the connection between System Manager and the virtual machine. The status can be Success or Failed .

Table continues...

Name	Description
	When the connection between System Manager and the virtual machine establishes, the Trust Status changes to Success . Only when the trust status is Success , you can perform other operations.
Data Store	The data store.

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 machines.
Start	Starts the selected virtual machines.
Stop	Stops the selected virtual machines.
Restart	Starts the selected virtual machines that were stopped earlier.
Refresh VM	Updates the status of the virtual machines.
Show Selected	Displays only the selected virtual machines.
More Actions > Reestablish 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 VM	Displays the System Manager VM section where you can install the software patches and service packs for System Manager virtual machine.
More Actions > Installed Patches	Refreshes and displays the latest information of the software patch.
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.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number.

Table continues...

Name	Description
	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/PostalCode	The zip code of the host location.
Country	The country where the host is located.
Time Zone	The timezone of the host location.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The 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 operation, and returns to the Locations section.

Managing the host

Adding an 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.

Before you begin

A location must be available.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, click **New**.
4. In the New Host section, provide the ESXi host information.
5. Click **Save**.

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

6. To view details of the discovered applications, establish trust between the application and System Manager using the following:
 - a. Click **More Actions > Re-establish connection**.
 - b. Click **Refresh VM**.

Important:

When you change the IP address or FQDN of the Appliance Virtualization Platform host from 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.

Related links

[New and Edit host field descriptions](#) on page 63

Editing an ESXi host

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host 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 63

Updating the Appliance Virtualization Platform host from Solution Deployment Manager

About this task

You can update only the Appliance Virtualization Platform host using this procedure.

* Note:

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

Before you begin

1. Install the Solution Deployment Manager client on your computer.
2. Add a location.
3. Add a host.
4. Enable the SSH service on the Appliance Virtualization Platform host.
5. Stop all virtual machines that are running on the Appliance Virtualization Platform host.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
 - On the desktop, click the SDM icon ()
 - Click **Start > All Programs > Avaya**, and click **SDM Client > Avaya SDM Client**.
2. In VM Management Tree, select a location.
3. On the **Host** tab, in the Host for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions > Update**.
4. On the Update Host page, select the file from the local System Manager or software library.
5. Click **Update Host**, and copy the Appliance Virtualization Platform host with the absolute path to the file.

In the Host for Selected Location <location name> section, the system displays the update status.

6. To view the details, in the **Current Action** column, click **Patching**.

Host Patching 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

Start the virtual machines that were running on the Appliance Virtualization Platform host.

Related links

[Update Host field descriptions](#) on page 65

Changing the network parameters for an ESXi 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. When the IP address changes, you must reconnect by using the new IP address.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, select an ESXi host and click **Change Network Params**.
4. In the Network Parameters 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 63

Changing the password for an ESXi host

About this task

You can change password only for the Appliance Virtualization Platform host.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () , and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, select an ESXi host and click **Change Password**.
4. In the Change Password section, enter the current password and the new password, and reenter the 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 64

Password policy

The password must meet the following requirements:

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

Examples for invalid password:

- 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 for 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 root password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting in future.

Related links

[Changing the password for an ESXi host](#) on page 60

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 as root.
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 reenables SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenables 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`.

Deleting an ESXi host

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. On the Host tab, in the Host for Selected Location <location name> section, select one or more hosts that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation page, click **Yes**.

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. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.

- For the Solution Deployment Manager client, on the desktop, click the SDM icon () 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.

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. For example, smgrdev.
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 root login and password that you configured in the spreadsheet.
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 Host 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.
IP	The IP address of the Appliance Virtualization Platform host

Table continues...

Name	Description
Subnet Mask	The subnet mask the Appliance Virtualization Platform host
Host Name	The host name the Appliance Virtualization Platform host
Domain Name	The domain name the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
Gateway	The gateway IP address. The field is available only when you click Change Gateway .

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

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

Change Password field descriptions

Name	Description
Current Password	The current password
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 that is available. The options are: • Select Patch from Local SMGR: The Appliance Virtualization Platform patch is available on the local System Manager. • Select Patch from software library: The Appliance Virtualization Platform patch that is available in the software library.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Updates 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 Files Download Details section, in the **Source** field, select **My Computer**.
 - b. 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.

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

Managing the virtual machine

Deploying the Utility Services OVA 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 the System Manager Solution Deployment 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

- Ensure you complete the Deployment checklist

For information about the Deployment checklist, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to a location.
- Download the required OVA files to System Manager.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () , and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, click **New**.
The system displays the VM Deployment section.
4. In the Select Location and Host section, perform the following:
 - a. In **Select Location**, select a location.
 - b. In **Select Host**, select a host.
 - c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.
The page displays the capacity details.
6. 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 by using 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 **Select Flexi Footprint**, select the footprint size that the application supports.
 - **S8300D**: To reduce the memory allocated for Utility Services virtual machine on S8300D that has limited resources. With the minimal footprint on S8300D, the system might not run all required virtual machines.
 - **Default**: For all other server platforms.

In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

7. In the Network Parameters section, ensure that the following fields are preconfigured:
 - **Public**
 - **Services**: Only for Utility Services
 - **Out of Band Management**: Only if Out of Band Management is enabled

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

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

9. Click **Deploy**.

10. Click **Accept the license terms**.

In the Host 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 Host <host name> page.

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

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

Related links

[VM Deployment field descriptions](#) on page 72

[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 the System Manager Solution Deployment 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 a location.
- Download the required OVA files to System Manager.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, click **New**.
The system displays the VM Deployment section.
4. In the Select Location and Host section, perform the following:
 - a. In **Select Location**, select a location.
 - b. In **Select Host**, select a host.
 - c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.
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 by using 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.
8. Click **Next**.
In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
9. In the Network Parameters section, ensure that the following fields are preconfigured:
 - **Public**
 - **Services**: Only for Utility Services
 - **Out of Band Management**: Only if Out of Band Management is enabled

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

For each application that you deploy, fill the appropriate fields.

11. Click **Deploy**.

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

In the Host 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 Host <host name> page.

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

Next steps

- Install the Release 7.0 patch file for the Avaya Aura® application.
- After you deploy the virtual machine, manually update the user password for the system to synchronize data from applications.

Note:

If you fail to update the password after the deployment, for applications such as Communication Manager, synchronization operation fails.

Related links

[VM Deployment field descriptions](#) on page 72

[Downloading the OVA file to System Manager](#) on page 65

Editing a virtual machine

Before you begin

- 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 **Refresh VM**.

Procedure

1. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () , and then click **VM Management**.
2. In VM Management Tree, select a host.

3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, select a host and click **Edit**.

The system displays the Edit VMs section.

4. **(Optional)** Click **Change flexi footprint value** and perform the following:
 - a. In the **Select Flexi Footprint** field, select a value that the application supports.
 - b. Click **Change flexi foot print value**.

! Important:

Each application must ensure that only the supported flexible footprint is selected.

5. To update the IP address and FQDN, perform the following:
 - a. Click **Update IP/FQDN in Local Inventory**.

The **Update IP/FQDN in Local Inventory** option 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.

- b. Click **Update VM IP/FQDN**.
- c. Provide the IP address and FQDN of the virtual machine.

Update IP/FQDN 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**.

Starting a virtual machine from Solution Deployment Manager

Procedure

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

VM Deployment field descriptions

Select Locations and Hosts

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.
VM Name	The name of the virtual machine.
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Select Resource Pool and Data Store

Button	Description
Resource Pool	The login to the resources. The field is display-only.
Datacentre/Cluster	The data centre or the cluster. The field is display-only.
AVP host	The host type. The values are: • Yes: An Appliance Virtualization Platform host • No: An ESXi host The field is display-only.
Model	The server model. For example, ProLiant DL360 G8 and PowerEdge™ R620.
Data Store	The data store with the available size.

Capacity Details

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

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

Deploy OVA

Name	Description
Select the OVA from Local SMGR	The option to select a .ova file of the virtual machine that is available on System Manager.
Select OVA File	The absolute path to the .ova file of the virtual machine that you must provide. The field is available only when you click Select the OVA from Local SMGR .
Submit	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 .
Select OVA from software library	The option to get the .ova file of the virtual machine from the software library.
Select Software Library	The software library where the .ova file is available. The field is available only when you click Select OVA from software library .
Select OVAs	The .ova file that you want to deploy. The field is available only when you click Select OVA from software library .
Select 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.

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 75.

Table 10: Configuration Parameters for Communication Manager simplex OVA deployment

Name	Description
CM IPv4 Address	The IP address of the Communication Manager virtual machine.

Table continues...

Name	Description
CM IPv4 Netmask	The network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The default gateway of the Communication Manager virtual machine.
Out of Band Management IPv4 Address	The IP 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 Netmask	The subnetmask of the Communication Manager 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 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 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.
Confirm Password	The password required to be confirmed.

Network Parameters

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Services	The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication.

Table continues...

Name	Description
	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.
Cancel	Cancels the deploy operation and returns to the VMs for Selected Host <host name> section.

Related links

[VM Deployment Configuration and Network Parameters field descriptions](#) on page 75

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.
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 (,).

Table continues...

Name	Description
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
Configuration Parameters	
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.
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine.
Timezone setting	The selected timezone setting for the Utility Services virtual machine.
NTP Server IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
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.
Utility Services Mode	The mode in which you want to 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.

Table continues...

Name	Description
	• 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 non-operational. • 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.  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. Utility Services provides application routing between the physical port and virtual applications.
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.
Confirmation password	The confirmation password.
Network Parameters	
Default Gateway	The IP address of the default gateway. Required field unless you use DHCP.
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.
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.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.

Update Static Routing field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The VM IP/FQDN
Utility Services IP	The utility services IP

Button	Description
Update	Updates the VM static routing address.

Installed Patches field descriptions

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

Button	Description
Get Patch Info	Displays the information about the software patch.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

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

Table continues...

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

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

Reestablish Connection field descriptions

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

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

Monitoring a host and virtual machine

Monitoring a host

Procedure

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

2. Click the Monitor Hosts tab.
3. In 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. Perform one of the following:
 - For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
 - For the Solution Deployment Manager client, on the desktop, click the SDM icon () 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

You can obtain the root password for the Appliance Virtualization Platform system from the USB configuration file. The file must be kept secure. After installation, you must change the root password for the Appliance Virtualization Platform host to a different value with the password change option from Solution Deployment Manager.

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.

Note:

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

Procedure

1. Turn on the power to 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 as root, and type `Avaya123$` as password.

The system prompts to change the password immediately.

6. To change the root password, perform the following:
 - a. At the prompt, type the current UNIX password.
 - 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. Read and accept the license terms.
8. 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 will not enable Out of Band Management. Use the `set_oobm` command only if you want to enable Out of Band Management for the host and all virtual machines.

9. **(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.

10. At the prompt, perform the following:

- a. Type `./serverInitialNetworkConfig`.

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
```

11. 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

12. Add a host on the Solution Deployment Manager client as 192.168.13.6.
13. On Solution Deployment Manager, click **Change Network Params**, and change the IP address to the customer IP address.
14. Click **Change Password**, and change the password.
15. Register the host on the main System Manager.
16. Deploy Utility Services.
17. Deploy other application OVA files on the system.

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 an admin account.
2. Type `/opt/avaya/common_services`.
3. Perform one of the following:
 - To enable SSH, type `AVP_SSH enable`.
 - To disable SSH, type `AVP_SSH disable`.
 - To find the status of SSH, type `AVP_SSH status`.
4. Type `# AVP_SSH enable`.

Within 3 minutes, 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.

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.

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
Stop	Stops the upgrade job.
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.

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

Table continues...

Name	Description
	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.

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 with System Platform service packs and software patches. • Linux live CD-ROM Download any missing components from the PLDS website.	
2	Get the migration media.	The following components are required to migrate to Appliance Virtualization Platform: • The Appliance Virtualization Platform DVD • USB in FAT32 format • OVA files	
3	Create a local backup of System Platform and the template data.	Creating a backup of the existing configuration on page 81	
4	Create a back up all virtual machines.	Create a backup of every virtual machine. For more information, see the documentation of the application templates.  Note: If you have System Platform Release 6.0, perform the following: • Log in to System Platform console.	

Table continues...

No.	Task	Description	✓
		• Navigate to the SAL gateway. • Note the values that you need to enter into the new SAL that you create.	
5	Record System Platform and template values.	Record the data on the System Platform and template values worksheet on page 90 1. On the Main Console page, note the IP addresses. 2. On the 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 the Server Management > SNMP Trap Receiver Configuration tab, note the SNMP settings.	
6	Configure the USB drive.	Configuring the Appliance Virtualization Platform USB drive on page 93	
7	Insert the USB drive and Appliance Virtualization Platform DVD into the server.		
8	Install Appliance Virtualization Platform.	Installing Appliance Virtualization Platform on page 94	
9	Verify the Appliance Virtualization Platform installation.		
10	Load the authentication file.	Loading a customer-specific authentication file on page 101	

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	

Table continues...

Reference	Name	Value
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

Table continues...

Release	IP address mapping	
6.0	System Console Domain	Utility Services virtual machine
	Services VM	SAL virtual machine
	System Platform Domain 0	Appliance Virtualization Platform host
	System Console Domain	SAL virtual machine
	Utility Services	New Utility Services IP address

Appliance Virtualization Platform configuration spreadsheet field descriptions

Name	Description
AVP management IP address	Customer IP address for Appliance Virtualization Platform host. Format is x.x.x.x.
AVP netmask	Customer subnet mask for the Appliance Virtualization Platform host. Format is x.x.x.x.
AVP gateway IP address	IP address of the customer default gateway on the network. Must be on the same network as the Host IP address. Format is x.x.x.x.
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.
NTP server	IP address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary NTP server	IP address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main DNS server	IP address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.

Table continues...

Name	Description
Secondary DNS server	IP address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
Public VLAN ID	VLAN ID for the S8300D and S8300E. If the customer does not use VLANs, leave as 1. For any other server type, leave as 1. The range is 1 through 4095. Use Public VLAN ID only on S8300D and S8300E servers.
Out of Band Management setup	The option to install Appliance Virtualization Platform with Out of Band Management enabled. 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	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 user root Password	Root password for Appliance Virtualization Platform. This field is hidden. The password must contain 8 characters and can include alphanumeric characters and @\$. You must make a note of the password because you require to register to System Manager.

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. Download a copy of Avaya Aura® Appliance Virtualization Platform 7.0 Kick Start Generator from Avaya PLDS at <https://plds.avaya.com/> or from Avaya support site at <https://support.avaya.com>.

The kick start generator is also available from the 700510424 media kit on the USB stick.

2. Type the required details in the spreadsheet.
3. Click **Generate AVP installation configuration file**.
4. Save a copy of `ks.cfg` on the USB drive.

Next steps

Install Appliance Virtualization Platform.

Installing Appliance Virtualization Platform

About this task

Warning:

You can obtain the root password for the Appliance Virtualization Platform system from the USB configuration file. The file must be kept secure. After installation, you must change the root password for the Appliance Virtualization Platform host to a different value with the password change option from Solution Deployment Manager.

Install Appliance Virtualization Platform on one of the following servers:

- Dell™ PowerEdge™ R610 2CPU MID2
- HP ProLiant DL360 G7 2CPU MID4
- Dell™ PowerEdge™ R620 1CPU MID3
- HP ProLiant DL360p G8
- S8300D for Communication Manager
- S8300E for Communication Manager

Release 7.0 does not support S8150 and S8800 servers.

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 install 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 installation process stops. You must remove the duplicate IP address, and restart the installation.

Procedure

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

Use an external Avaya-approved USB and CD-ROM drives for installing 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 installed, and all existing data on the server is lost.

The system installs Appliance Virtualization Platform and ejects CD-ROM. The installation process might takes about 30 minutes to complete.

 Note:

If using a monitor, the screen changes to black before the installation 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. Alternatively, you can connect to the public network address that was configured during the installation from a computer on the customer network.

5. Log in to Appliance Virtualization Platform as root and provide the password that is configured in the spreadsheet.

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. Perform one of the following:

- For System Manager Solution Deployment Manager, on the web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
- For the Solution Deployment Manager client, on the desktop, click the SDM icon () , and then click **VM Management**.

8. 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 Avaya Aura® System Manager*.

9. 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

You can access virtual machines on Utility Services by connecting a laptop to the Services Port VM. By default, the system enables IP forwarding. To configure IP forwarding manually, use the Services Port VM.

 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 networking

Overview

When you install Appliance Virtualization Platform, the public network of virtual machines is assigned to NIC1 of the server.

In the installation spreadsheet, if Out of Band Management is:

- Disabled: 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.
- Enabled: The public interfaces of virtual machines are assigned to NIC1, and the Out of Band Management interfaces are assigned to NIC3. Assign separate network ranges to the public and management interfaces of virtual machines.

When Out of Band Management is:

- Disabled: The management port of Appliance Virtualization Platform is assigned to the public interface.
- Enabled: The management port of Appliance Virtualization Platform is assigned to the Out of Band Management network. The management port must be given an appropriate IP address of the public and Out of Band Management network.

The NIC2 of the server is assigned to the services port.

The hypervisor is 192.168.13.6 on the services port network.

After Utility Services is deployed, you can gain access to Utility Services with the services port virtual machine with 192.11.13.6 as the IP address.

With eth1 or NIC2, the IP address of the hypervisor is 192.168.13.6.

*** 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, the first Ethernet port of the server called NIC1 is assigned to the public interface of virtual machines.

When deploying or reconfiguring Appliance Virtualization Platform, if Out of Band Management is:

- Disabled: The public and Out of Band Management ports are assigned to the public interface and must remain on the same network. The Appliance Virtualization Platform management interface is on NIC1.
- Enabled: The public interfaces of virtual machines are assigned to NIC1, and Out of Band Management interfaces are assigned to NIC3. Assign separate network ranges to the public and Out of Band Management interfaces. The Appliance Virtualization Platform management interface is on NIC3.

S8300D

When Appliance Virtualization Platform installs the connection through the media gateway, Ethernet ports are assigned to the public interface of virtual machines. This can be on a VLAN or independent of the network setup within the G4x0 gateway.

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 gateway, Ethernet ports are the public interface of virtual machines. This can be on a VLAN or independent of the network setup within the G4x0 gateway.

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

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”.

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 vSwitch, 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 they are connected must be set to autonegotiate on both the server and the customer network switch.

Use the procedure if you must change the Ethernet port speeds.

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.

Loading a customer-specific authentication file

About this task

Avaya provides the default authentication file for Appliance Virtualization Platform. You must download the customer-specific authentication file from the Authentication File System website.

Procedure

1. To gain access to the Avaya RFA Home page, type <http://rfa.avaya.com> in the web browser.
2. Log on to the RFA Home page.
3. Click **Start the AFS Application**.
4. On the license page, click **I Agree**.
5. In the **Product** field, select **Appliance Virtualization Platform**.
6. In the **Release** field, click **7.x**.
7. Click **Next**.
8. On the Deliver an Authentication File page, perform one of the following:
 - To create an authentication file for a new system, click **New System - Product: <Appliance Virtualization Platform Release: 7.x>**.
 - To create an authentication file for an upgrade or re-delivery for an existing system, click **Upgrade or Re-deliver for Existing System or re-deliver for existing system - Product: <Appliance Virtualization Platform Release: 7.x>**, and type the authentication file ID.
9. Click **Next**.

10. Ensure that SSH is running on the Appliance Virtualization Platform host, and if required, activate through Utility Services.
For more information, see “Activating SSH” to Appliance Virtualization Platform.
11. Click **Download file to my PC**.
12. Using WinSCP or a similar application, copy the authentication file on to the Appliance Virtualization Platform system by using the root account and the password set at installation.
13. Using PuTTY or a similar SSH client, log in to Appliance Virtualization Platform by using the root account and the password set at installation.
14. Type `/opt/avaya/bin/loadauth -l AF-7001064472-150430-131707.xml -o /etc/asg/lacfile`

Where `AF-7001064472-150430-131707.xml`, is the authentication file name and `-l` is the location where the system downloaded the `xml` file. Always include the `-o` option as `-o /etc/asg/lacfile`.
15. Using the SSH client, log in to Appliance Virtualization Platform as `sroot`, and view the updated product ID displayed with the ASG challenge.

Validating the migration

1. Verify that the ping to virtual machine is successful.
2. Verify that 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 System Manager on a different server by using Solution Deployment Manager client

About this task

You can upgrade System Manager on the same server or a different server.

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

Before you begin

- Add a location.
- Install the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host from the VM Management page.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
 - OVA file, SMGR-7.0.0.0.16266-e55-43-29-II.ova
 - Data migration utility, Data_Migration_Utility_7.0.1.0_r94.bin
- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
 - On the desktop, click the SDM icon .
 - Click **Start > All Programs > Avaya**, and click **SDM Client > Avaya SDM Client**.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.

4. Click **Add Elements**, add the details of System Manager such as IP address, login credentials of System Manager and login credentials of the console domain.
5. Click **Save**.
6. On the Upgrade Elements page, select the System Manager that you added.
7. Click **Upgrade**.

The system displays the Upgrade Management page.

8. Clear the **Install on Same ESXi** check box.
9. In **Host FQDN**, select the host that you added.

The system populates details such as resources and memory.

10. Select the datastore on the host.
11. In the **Deploy OVA** section, perform the following:
 - a. In **Select OVA** file, type the absolute path to the System Manager OVA file, and click **Submit File**.

The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
 - b. Select the flexi footprint.
 - c. Provide the absolute path to the data migration utility.
 - d. Provide absolute path to the System Manager backup file.
12. In the Configuration Parameters section, provide FQDN, Timezone, and SNMP passwords.
13. In the Network Parameters section, provide the Public and Out of Band Management details.
14. Click **Upgrade** and accept the license terms.

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

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

The complete process takes about 3 hours depending on the data on System Manager.

Related links

[Installing the Solution Deployment Manager client on your computer](#) on page 46

[Upgrade Management field descriptions](#) on page 107

[Add Element field descriptions](#) on page 108

[Install on Same ESXi field descriptions](#) on page 113

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

About this task

You can upgrade System Manager on the same server or a different server.

The procedure describes the steps to upgrade System Platform-based System Manager on the same server.

Before you begin

- Add a location.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
 - OVA file, SMGR-7.0.0.0.16266-e55-43-29-II.ova
 - Data migration utility, Data_Migration_Utility_7.0.1.0_r94.bin
- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
 - On the desktop, click the SDM icon ().
 - Click **Start > All Programs > Avaya**, and click **SDM Client > Avaya SDM Client**.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. Click **Add Elements**, add the details of System Manager such as IP address, login credentials of System Manager and login credentials of the console domain.
5. Click **Save**.
6. On the Upgrade Elements page, select the System Manager that you added.
7. Click **Upgrade**.

The system displays the Upgrade Management page.

8. Select the **Install on Same ESXi** check box.
9. Click **Continue**.

The system shuts down the virtual machine and reaches a paused state.

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

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

The system populates details such as resources and memory.
13. Select the datastore on the host.

14. In the **Deploy OVA** section, perform the following:
 - a. In **Select OVA** file, type the absolute path to the System Manager OVA file, and click **Submit File**.

The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
 - b. Select the flexi footprint.
 - c. Provide the absolute path to the data migration utility.
 - d. Provide absolute path to the System Manager backup file.
15. In the Configuration Parameters section, provide FQDN, Timezone, and SNMP passwords.
16. In the Network Parameters section, provide the Public and Out of Band Management details.
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 3 hours depending on the data on System Manager.

Related links

- [Installing the Solution Deployment Manager client on your computer](#) on page 46
- [Upgrade Management field descriptions](#) on page 107
- [Add Element field descriptions](#) on page 108
- [Install on Same ESXi field descriptions](#) on page 113

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

About this task

Use this procedure for updating System Manager that was deployed using the same Solution Deployment Manager client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
 - On the desktop, click the SDM icon ().
 - Click **Start > All Programs > Avaya**, and click **SDM Client > Avaya SDM Client**.
2. Click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Host <host 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 SMGR**, 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. Click the **Auto commit the patch** check box.

To install the patches manually, click **More Actions > Installed Patches**.

9. Click **Install**.

In the VMs for Selected Host <host 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 patch installation takes some time.

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.

Table continues...

Button	Description
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 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 ESXi	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.

Select Resource Pool and Data Store

Button	Description
Resource Pool	The login to the resources. The field is display-only.
Datacentre/Cluster	The data centre or the cluster. The field is display-only.
AVP host	The host type. The values are: • Yes: An Appliance Virtualization Platform host • No: An ESXi host The field is display-only.
Model	The server model. For example, ProLiant DL360 G8 and PowerEdge™ R620.
Data Store	The data store with the available size.

Capacity Details

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

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

Deploy OVA

Name	Description
Select the OVA	The option to select a .ova file of the virtual machine that is available on System Manager.
Select 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.
Select 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  .
Select bin file	The absolute path to the System Manager data migration bin file.
Select backup file	The absolute path to the backup of System Manager virtual machine.

Configuration Parameters

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

Name	Description
Management IP Address (Out of Band Management IP Address)	The IP 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 IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
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 (.). For example, 172.16.1.2, 172.16.1.4.
Management Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP or 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 can select the continent and the country.

Public Network Settings

Name	Description
Public IP Address	The IP address to enable public access to different interfaces.
Public Netmask	The subnetwork mask to assign to System Manager virtual machine.
Public Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
Public Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. For example, grsmgr.
Virtual Domain	The virtual domain name of the System Manager virtual machine. For example, dev.com.

SNMPv3 Parameters

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.

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

Table continues...

Name	Description
	Monthly
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 6 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.

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 where you must click Accept to start the upgrade.

Install on Same ESXi field descriptions

Name	Description
Install on Same ESXi	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 7.0 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 7.0

No.	Task	References	✓
1	Install Solution Deployment Manager client on your computer.	Installing the Solution Deployment Manager client on your computer on page 46	
2	To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.		
3	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.0 OVA file by using the Solution Deployment Manager client • Available: Upgrade System Manager to Release 7.0		
4	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 <i>Administering Avaya Aura® System Manager</i>	

Table continues...

No.	Task	References	✓
5	Configure user settings.	"User settings" in <i>Administering Avaya Aura® System Manager</i>	
6	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 <i>Administering Avaya Aura® System Manager</i>	
7	Refresh the elements in the inventory.	"Refreshing elements" in <i>Administering Avaya Aura® System Manager</i>	
8	Analyze the software.	"Analyzing software" in <i>Administering Avaya Aura® System Manager</i>	
9	Download the required firmware for the Avaya Aura® application upgrade.	"Downloading the software" in <i>Administering Avaya Aura® System Manager</i>	
10	Analyze the software.	"Solution deployment and upgrades" in <i>Administering Avaya Aura® System Manager</i>	
11	Perform the preupgrade check.	"Performing the preupgrade check" in <i>Administering Avaya Aura® System Manager</i>	
12	Perform the upgrade.	Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0 on page 115	
13	Verify that the upgrade is successful.	-	

Upgrading Avaya Aura® applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0

About this task

Use the procedure to upgrade Communication Manager, Session Manager, Branch Session Manager, Utility Services to Release 7.0. The procedure covers upgrades on the same server and on a different server.

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.
- If you are migrating from old server to ESXi host, add the new host in to VM Management.

- If migrating 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, complete the details and click **Save**.
8. Ensure that the **Configuration Status** field displays .

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

9. Click **Save**.
10. On the Upgrade Configuration page, click **Upgrade**.
11. 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.

12. Click **Schedule**.

13. Click **Upgrade**.

14. On the Upgrade Management page, click .

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

15. 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.

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

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

17. 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 122

[Edit Upgrade Configuration field descriptions](#) on page 123

Installing software patches

About this task

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

Before you begin

- Perform the preupgrade check.
- If you upgrade an application that was not deployed from Solution Deployment Manager, perform the following:
 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 the **Upgrade Source** field, select the software library where you have downloaded the patch.

In the Select patches for update section, the page displays the available patches.

8. Select the patch that you want to install.
9. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
10. In the Upgrade Configuration Details section, select the software patch that you want to install.
11. Click **Save**.
12. Ensure that the **Configuration Status** field displays .
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 latter time by using the **Schedule later** option.
20. Click **Schedule**.

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

21. Ensure that the **Update status** and **Last Action Status** fields display .

Related links

[Preupgrade Configuration field descriptions](#)

[Upgrade Configuration field descriptions](#) on page 122

[Edit Upgrade Configuration field descriptions](#) on page 123

[Installed Patches field descriptions](#) on page 119

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.

Table continues...

Name	Description
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

Table continues...

Name	Description
	❌: 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
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.

Table continues...

Button	Description
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	Displays the Upgrade Configuration page where you can configure the upgrade.
Upgrade Actions > Install 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 > 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 Platformhost.
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.
Release 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 .
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.

Table continues...

Name	Description
Configuration Status	An icon that defines the configuration status. ✖: Configuration incomplete. ✔: Configuration complete.

Button	Description
Upgrade	Commits the upgrade operation.

Edit Upgrade Configuration field descriptions

General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: - Upgrade - Update
ESXI Host	The ESXi host on which you want to run the device. The options are: - Same host - List of hosts that you added from VM Management
VM Name	The name of the virtual machine.
Upgrade Source	The source where the installation files are available. The options are: - Local machine - Software library
Upgrade To	The Release 7.0 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.

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 Communication Manager user name with appropriate privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. 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 Managervirtual machine.
CM IPv4 Netmask	The network mask of the Communication Managervirtual machine.
CM IPv4 Gateway	The default gateway of the Communication Managervirtual 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.
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.
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

Table continues...

Name	Description
	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.

Table continues...

Name	Description
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.

Button	Description
End User License Agreement	The end user license agreement. You must select the check box to accept the license agreement.

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

Upgrading Avaya Aura® Communication Manager

Upgrading Communication Manager 6.x to Release 7.0

About this task

Use the procedure to upgrade System Platform-based simplex Communication Manager, Branch Session Manager, and associated devices to Release 7.0. The procedure covers upgrades on the same server and on a different server.

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.
- 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, complete the details and click **Save**.
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. Click **Upgrade**.
15. On the Upgrade Management page, click .

Last Action column displays **Upgrade**, and **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 the **Job Type** field, click **Upgrade**.
 - c. Click the upgrade job that you want to view.
17. Verify that the upgrade of Communication Manager is successful.

For upgrades on the same server, system goes to the pause state.
18. 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.
19. On Communication Manager 7.0, 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** and complete the upgrade configuration of Communication Manager.
 - 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 7.0, 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 7.0 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** and complete the upgrade configuration of Communication Manager.
 - 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 7.0, 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** and complete the upgrade configuration of Communication Manager.
 - 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 7.0, click **Administration > Server (Maintenance) > Server Configuration**, and configure the following parameters:

- **Network Configuration**

- **Duplication Parameters**

- **Server role**

- 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.

- To busy out the server, from the active Communication Manager command line interface, type `server -if`.
- 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.
- Start the upgrade for the Communication Manager that was earlier active:

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

- In the left navigation pane, click Upgrade Management.

- 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**.

- Select the active Communication Manager or System Platform, and click **Upgrade Actions > Upgrade/Update**.

- On the Upgrade Configuration page, click **Edit** and complete the upgrade configuration of Communication Manager.

- Schedule the upgrade of the active Communication Manager.

- 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.

- Configure the newly upgraded active Communication Manager server by performing the following:

- Log on to the software management interface of the active Communication Manager.

- On Communication Manager 7.0, click **Administration > Server (Maintenance) > Server Configuration**, and configure the following parameters:

- **Network Configuration**

- **Duplication Parameters**

- **Server role**

- 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 7.0

About this task

Use the procedure to upgrade Session Manager or Branch Session Manager to Release 7.0.

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.

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 LSP, separately.

8. On the Edit Upgrade Configuration page, perform one of the following:

- 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.
- 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.

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 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 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 7.0 migration scenarios

Avaya Aura® 7.0 migration scenarios

This section covers various migration scenarios that customers might use, and provides required and recommended steps for migrating to Avaya Aura® Release 7.0. The scenarios provide only high-level procedures.

For detailed instructions to perform each procedure, see *Migrating and Installing Avaya Appliance Virtualization Platform* and *Upgrading and Migrating Avaya Aura® applications from Avaya Aura® System Manager* to Release 7.0.

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 7.0 systems.
- You require to generate new licenses for Avaya Aura® Release 7.0 for each application. System Manager WebLM is used as the licensing server in Avaya Aura® Release 7.0 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 7.0.
- 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 7.0 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 7.0 supports.
- In the Avaya-provided appliance deployments of Avaya Aura® Release 7.0 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 7.0 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 7.0 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 7.0.
- Applications that use S8800 servers must replace the server with the server that Avaya Aura® Release 7.0 supports.

Deploying 6.x applications to Avaya Aura® Release 7.0 by using the Solution Deployment Manager client

About this task

The section provides the procedure to deploy Avaya Aura® Release 7.0 application OVA files during migration of Avaya Aura® 6.x by using the Solution Deployment Manager client when System Manager is unavailable.

You can also install System Manager by using the Solution Deployment Manager client, and use the centralized Solution Deployment Manager to deploy other Avaya Aura® Release 7.0 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.

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/](https://PLDS.AVAYA.COM/)

4. On the existing server that you want to migrate to Avaya Aura® Release 7.0, 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 7.0 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 for all applications that Avaya Aura® Release 7.0 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 7.0 application.

Upgrading Avaya Aura® 6.x applications in a customer-provided Virtualized Environment to Avaya Aura® Release 7.0

About this task

The section provides the procedure to migrate Avaya Aura® 6.x applications to Avaya Aura® Release 7.0:

- The Avaya Aura® applications include Communication Manager, System Manager, Session Manager, Application Enablement Services, WebLM, Communication Manager Messaging, and Engagement Development Platform.
- Release 7.0 does not support automated upgrade from Virtualized Environment to Virtualized Environment in Avaya Aura® Release 7.0.

- Upgrade Avaya Aura® applications to Avaya Aura® Release 7.0 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 7.0 applications that you want to upgrade to.
- Obtain the OVA files for Utility Services, System Manager, and other Avaya Aura® Release 7.0 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.

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 7.0 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 7.0 application.
4. Using vSphere Client, deploy the new Avaya Aura® Release 7.0 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 required software patches 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 7.0.
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 7.0 application.

Migrating System Platform-based Communication Manager 6.x to Avaya Aura® Release 7.0 on Appliance Virtualization Platform

About this task

The section provides the procedure to migrate Communication Manager running on System Platform to Avaya Aura® Release 7.0:

- 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, or HP ProLiant DL360p G8

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® Release 7.0 applications.

Procedure

1. Obtain a new Avaya-provided server that is based on Appliance Virtualization Platform with System Manager OVA.

The new Avaya-provided server contains preinstalled Appliance Virtualization Platform.

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 7.0, 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 the System Manager Release 7.0 OVA 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 7.0.

- a. From System Manager, get the primary host ID WebLM that is required to generate Communication Manager Release 7.0 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. 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.

18. 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.

19. Restore Communication Manager Messaging using the Communication Manager Messaging backup and restore capability.

20. Update the trunk configuration for establishing connection between Communication Manager Messaging and Communication Manager.
21. 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.
22. Restore SAL or Services VM by using the SAL restore capability.
23. 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.
24. 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.
25. Create a backup of the Communication Manager Release 7.0 S8300D or Communication Manager Release 7.0 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 7.0

About this task

The section provides the procedure to migrate Communication Manager Release 6.x on System Platform to Avaya Aura® Release 7.0 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**, and select the Communication Manager 6.x element, 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 7.0 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 7.0 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, 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, or HP ProLiant DL360p G8 server to Release 7.0 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
- 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 7.0.

For more information, see [Migrating System Manager to Release 7.0](#) on page 159.

2. Generate new Communication Manager Release 7.0 and Session Manager Release 7.0 license files from Avaya:
 - a. From System Manager WebLM get the Primary Host ID that is required to generate the Release 7.0 license file.
 - b. Install Communication Manager and 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 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

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 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 Session Manager 6.x reside in the VM hierarchy.
6. Perform the following to prepare Session Manager 6.x for migration to Release 7.0:
- a. From the command line interface create a backup of Session Manager for disaster recovery.
 - b. Record the following network parameters for Session Manager Release 6.x that you later require:
 - All IP addresses
 - Subnetwork mask
 - Gateway
 - DNS
 - NTP Server
7. On Upgrade Management, select the Session Manager 6.x element, 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:

- Imports required network setting from Session Manager.
 - Prompts you to fill the new attributes that are required from OVA for the deployment.
 - Creates a backup of Session Manager.
 - After successful backup, the upgrade process moves to the Pause state.
8. Install Appliance Virtualization Platform on the server that was earlier running Linux® Operating System.

The installation process takes about 30 minutes.

9. Select the same 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 Session Manager automatically. For example, Session Manager and Utility Services.

You can monitor the migration job status from the Upgrade Job Status page.
 - Restores Session Manager and provides status of the upgrade.
10. Configure Session Manager to point to System Manager WebLM that has the new Release 7.0 license files.
11. Verify that Session Manager is operational.
12. 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, Session Manager, Utility Services, and SAL or Services Virtual Machine.
13. On the Session Manager web console, create a backup of Session Manager Release 7.0.

You require to create a separate backups for each deployed application.
14. Perform the following to prepare Communication Manager 6.x survivable core server for migration to Release 7.0:
 - 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
15. 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.
16. 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.
17. 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.
18. Select the ESXi host on which you want to deploy OVA.
19. Configure Communication Manager to point to System Manager WebLM that has the new Release 7.0 license files.
20. 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.
21. On the Communication Manager web console, create a backup of Communication Manager Release 7.0.
- You require to create a separate backups for each deployed application.
22. Perform the following to prepare Communication Manager 6.3.x main standby server for migration to Communication Manager Release 7.0:
- 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
23. 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

24. 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.

25. 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.

26. Configure Communication Manager to point to System Manager WebLM that has the new Release 7.0 license files.

27. 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.

28. On the Communication Manager web console, create a backup of Communication Manager Release 7.0.

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

29. Perform the following to prepare Communication Manager 6.3.x Main Active for migration to Communication Manager Release 7.0:
 - 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

30. 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.

31. 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.

32. 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.
33. Configure Session Manager to point to System Manager WebLM that has the new Release 7.0 license files.
34. 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.

35. On the Communication Manager web console, create a backup of Communication Manager Release 7.0.

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 7.0 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 7.0 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 7.0 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 7.0 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 7.0.

For more information, see [Migrating System Manager to Release 7.0](#) on page 159.

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 7.0 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 7.0](#) on page 159

Migrating System Manager to Release 7.0

About this task

During the migration of Avaya Aura® solution to Release 7.0, you must first migrate System Manager 6.x to Release 7.0.

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. On the compute 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.

10. 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 7.0 OVA to the virtual machine.

System Manager Release 7.0 OVA deployment takes about 30 minutes.

11. Log in to the command line interface or the web browser of the application, and install the Avaya Secure Gateway file for each application OVA that you installed and Appliance Virtualization Platform.

You installed Appliance Virtualization Platform, System Manager, and Utility Services on the virtual machine.

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 158

Migrating Midsize Enterprise to Release 7.0

About this task

The section provides the procedure to migrate System Platform-based on Linux-based template to Appliance Virtualization Platform on Dell™ PowerEdge™ R610, HP ProLiant DL360 G7, Dell™ PowerEdge™ R620, and HP ProLiant DL360p G8 servers.

Before you begin

- Read the Avaya Aura® application upgrade and migration considerations.
- For Communication Manager 6.0 through 6.2 to Release 7.0 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 7.0.
- 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 7.0 Midsize Enterprise application OVAs on computer of the technician.
5. Install Appliance Virtualization Platform on the Midsize Enterprise Release 7.0 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 7.0
 - System Manager 7.0

- Session Manager 7.0
- Communication Manager 7.0
- Application Enablement Services 7.0
- SAL 2.5
- Communication Manager Messaging 7.0
- 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.

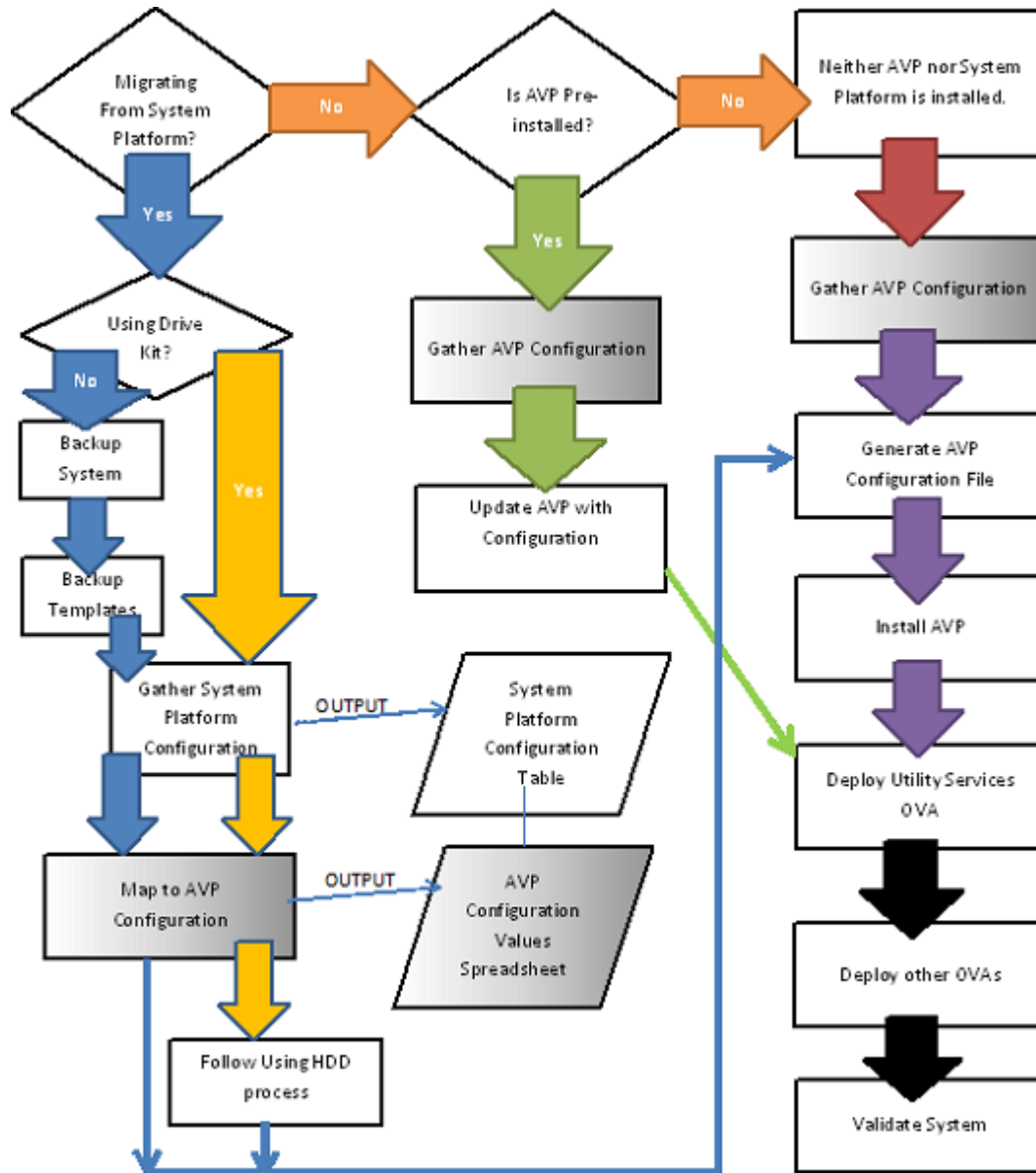
8. Install the required software patches by using command line interface or System Manager Solution Deployment Manager.
9. With the restore capability of the application, restore the backup of the application that you created in Step 1.
10. Make any networking configuration change that is required for 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 7.0 license files from Avaya:
 - a. From System Manager WebLM get the Primary Host ID that is required to generate the Release 7.0 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 7.0.

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 public 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 all OVA files of 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. Deploy all other virtual machines in the solution one after the other.
10. Validate the system.

Related links

[Enabling IP forwarding using Services Port VM for Utility Services](#) on page 96

Deploying Utility Services and virtual machines on the services port

Before you begin

- Download the Solution Deployment Manager client from the PLDS website.

The DVD version must use the public IP address on Appliance Virtualization Platform.

- 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 all OVA files of 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. Change the Utility Services configuration parameters to the following:
 - **IP address:** 192.11.13.5
 - **Netmask:** 255.255.255.252
 - **Gateway:** 192.168.13.6

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

9. Ensure that the IP forwarding feature is enabled on Utility Services.
10. Deploy all other virtual machines in the solution one after the other.
11. **(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.

12. Validate the system.

Related links

[Enabling IP forwarding using Services Port VM for Utility Services](#) on page 96

Chapter 9: Postmigration tasks

Postmigration tasks for Communication Manager

Before you begin

Log on to the software management interface of Communication Manager 7.0.

Procedure

Click **Administration > Server (Maintenance) > 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.

Downloading and installing an authentication file on the Avaya Aura[®] application

About this task

Avaya provides the default authentication file for an application. You must download the customer-specific authentication file from the AFS website.

Procedure

1. To gain access to the Avaya RFA Home page, type <http://rfa.avaya.com> in the web browser.

2. Log on to the RFA Home page.
3. Click **Start the AFS Application**.
4. On the license page, click **I Agree**.
5. In the **Product** field, click **<Avaya Aura application name>**.
Where <Avaya application> is the application that you want to deploy or upgrade.
6. In the **Release** field, click 7.x.
7. Perform one of the following:
 - To create new authentication file for new installation, click **New System - Product: <Avaya Aura application name Release: 7.x>**.
 - To create new authentication file for an upgrades system, click **Upgrade or Re-deliver for Existing System or re-deliver for existing system - Product: <Avaya Aura application name Release: 7.x>**, and type the authentication file ID.
8. In the **Enter the fully qualified domain name** field, type FQDN or retain the default value.
9. Click **Download file to my PC** or **Download file via email**.
Depending on the selection, the system downloads the authentication file on your computer or sends the file through email.
10. Using WinSCP or similar application, copy the authentication file on to the <Avaya Aura application> by using the root account and the password set at installation.
11. Using PuTTY or similar SSH client, log in to the <Avaya Aura application> by using the root account and the password set at installation.
12. Type `./opt/avaya/bin/loadauth -l AF-7001064472-150430-131707.xml -o /etc/asg/lacfile`.
Where AF-7001064472-150430-131707.xml is the authentication file name –l is the location where the system downloaded the xml file. Always include –o option as –o /etc/asg/lacfile.
13. Using the SSH client, log in to the application, and view the updated product ID displayed with the ASG challenge.

Chapter 10: Post Installation Verification

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 7.0 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.

Post installation checklist

Perform the following steps to verify the Session Manager OVA installation.

No.	Task	Description
1	Verify the connections of the deployed Session Manager.	
2	Upgrade Session Manager to the latest release.	<i>Deploying Session Manager on VMWare</i>
3	Run the maintenance tests on the deployed Session Manager.	<i>Administering Avaya Aura® Session Manager</i>
4	Verify data replication.	
5	Upgrade the Session Manager VMware tools.	<i>Deploying Session Manager on VMWare</i>

Verifying the connections

Verify the connections of the deployed Session Manager and Branch Session Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. Verify **Security Module state** is **Up** for Session Manager and Branch Session Manager.
3. Verify the Service State of the Session Manager or Branch Session Manager instance is **Accept New Service**. If the service state is not **Accept New Service**:
 - a. Select the Session Manager or Branch Session Manager instance.
 - b. Click **Service State > Accept New Service**.

Chapter 11: Rollback process

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**.

Glossary

Appliance Virtualization Platform

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. 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

Numerics

7.0 [120](#), [122](#)

A

activate SSH from Utility Services [84](#)
add
 Appliance Virtualization Platform host [56](#)
 AVP host [56](#)
 ESXi host [56](#)
 location [51](#)
 virtual machine [72](#), [75](#)
Add elements
 manual [39](#)
add ESXi host [56](#)
add location [51](#)
add virtual machine [72](#), [75](#)
analyze job status [85](#)
Appliance Virtualization Platform [61](#), [82](#), [101](#)
 change password [60](#)
 install [94](#)
 networking [97](#)
 NIC teaming [99](#)
Appliance Virtualization Platform and Utility Services [36](#)
Appliance Virtualization Platform configuration
 spreadsheet [92](#)
Appliance Virtualization Platform host password
 change [60](#)
Appliance Virtualization Platform installation scenarios [163](#)
Appliance Virtualization Platform network parameters [59](#)
Appliance Virtualization Platform USB drive
 configure [93](#)
Application Enablement Services [17](#)
application upgrade tasks [22](#)
ASG file [101](#)
ASG file installation on Appliance Virtualization Platform .. [101](#)
ASG file installation on Avaya Aura application [167](#)
authentication file
 ASG file [167](#)
 download [101](#), [167](#)
 install [101](#), [167](#)
automated
 Avaya Aura application upgrades [16](#)
Avaya Aura [143](#), [145](#)
Avaya Aura application migration [19](#)
Avaya Aura applications
 migrations [16](#)
 upgrades [16](#)
Avaya Aura application upgrade [120](#)
Avaya Aura application upgrade tasks [22](#)
Avaya-provided appliance
 Avaya Virtualized Platform [17](#)

B

backup connection [99](#)
backup existing configuration [81](#)
Branch Session Manager [17](#)
Branch Session Manager upgrade [115](#), [134](#)

C

change
 ESXi host IP address [59](#)
change ESXi host password [60](#)
Change Gateway [63](#)
change IP address for ESXi host [59](#)
Change IP FQDN [69](#)
change Netmask for Appliance Virtualization Platform host [59](#)
Change Network Params [59](#)
checklist
 Branch Session Manager upgrade [114](#)
 Communication Manager 6.x upgrade [114](#)
 Session Manager upgrade [114](#)
Communication Manager [17](#)
 Application Enablement Services [143](#)
 Communication Manager Messaging [143](#)
 Engagement Development Platform [143](#)
 Session Manager [143](#)
 System Manager [143](#)
 upgrade [43](#)
 WebLM [143](#)
Communication Manager 6.x on S8800 duplex main [158](#)
Communication Manager Messaging [17](#)
 backup [20](#)
 migration [20](#)
 post migration tasks [167](#)
 restore [167](#)
Communication Manager update [117](#)
Communication Manager upgrade [115](#), [127](#)
Communication Manager upgrade considerations [20](#)
Communication Manager upgrade from Software
 Management [15](#)
Communication Manager upgrade from System Manager .. [15](#)
Communication Manager upgrades
 footprints [40](#)
 profile map [40](#)
Configuration Parameters [75](#)
configure
 Ethernet port speed [100](#)
 port speed [100](#)
configure Appliance Virtualization Platform USB drive [93](#)
configure server preinstalled with Appliance Virtualization
 Platform [82](#)
connections
 verifying [170](#)

Index

considerations		
Avaya Aura application migration	140	
migration	140	
upgrade	140	
create		
virtual machine	67	
create discovery profiles	40	
creating authentication file	101	
D		
delete		
ESXi host	62	
location	52	
delete ESXi host	62	
delete location	52	
deleting		
upgrade jobs	85	
delivering authentication file	101	
deploy		
Branch Session Manager	67	
Communication Manager	67	
product knowledge	9	
Session Manager	67	
skills	9	
System Manager	67	
tools	9	
Utility Services	67	
deploy application	50	
deploy Avaya Aura 7.0 application	67	
Deploy Avaya Aura applications		
Solution Deployment Manager client	141	
Deploying an OVA file		
utility services	66	
Deployment options for Avaya Aura applications	39	
deploy OVA	67	
deploy Utility Services and virtual machines		
services port	164	
deploy virtual machines on Appliance Virtualization Platform		
.....	164	
different server migration	132	
disabling SSH	61	
disaster recovery	87 , 88	
discover elements	40	
discovery		
profiles	40	
discovery profiles		
create	40	
documentation	10	
documentation map	22	
download		
ASG file	101	
authentication file	101	
download software	65	
duplex Communication Manager		
migration	129	
duplex system	130 , 132	
duplication parameters	129 , 130 , 132	
E		
edit		
ESXi host	57	
location	52	
virtual machine	69	
edit elements	108	
edit ESXi host	57	
Edit Host	63	
edit location	52	
Edit Location	55	
Edit Upgrade Configuration	123	
edit virtual machine	69	
element		
add	108	
elements		
discover	40	
elements upgrade		
target release	48	
element upgrade	120	
Enabling	96	
enabling SSH	61	
ESXi host		
add	56	
delete	62	
edit	57	
ESXi host Gateway		
change	59	
edit	59	
ESXi host IP address		
change	59	
edit	59	
ESXi host map to unknown location	62	
ESXi host password		
change	60	
Ethernet port speed	100	
existing configuration		
backup	81	
F		
field descriptions		
Appliance Virtualization Platform configuration	92	
change password	64	
Edit Host	63	
Edit Location	55	
Hosts	53	
Locations	53	
New Host	63	
New Location	55	
Upgrade Configuration	122	
upgrade management	120	
Virtual Machines	53	
VM Deployment	72 , 75	
footprint		

footprint (<i>continued</i>)	
Utility Services	86
footprint flexibility	40
for Communication Manager	
postmigration tasks	167

G

General Configuration Details	123
-------------------------------------	---------------------

H

hardware supported	20
host	
monitoring	79
Host	
update	65
Hosts	53

I

install	
Application Enablement Services	46
ASG file	101 , 167
authentication file	101 , 167
Avaya Aura applications	46
Avaya Aura Media Server	46
Branch Session Manager	46
Communication Manager	46
Engagement Deployment Platform	46
SAL	46
SDM	46
Session Manager	46
Solution Deployment manager client	46
System Manager	46
WebLM	46
install Appliance Virtualization Platform	94
Installed Patches	119
Installed Patches field descriptions	78
Install on Same server	113
install patches	117
install services packs	117
install software patches	117
Install System Manager patch	78
Install System Manager patches	107
interchange active and standby servers	132
interchange roles	132
IP address mapping	91
IP forwarding	96

L

legal notice	
licensing upgrades	41
Life cycle management	50
Linux-based application	

recovery	87 , 88
Linux Operating System upgrades	49
preupgrade check	49
location	
add	51
delete	52
edit	52
view	51
Locations	53

M

Manage	
System Manager upgrades	107
Manage Software	15
Manual addition of elements	39
map Dom-0 to Appliance Virtualization Platform	91
map ESXi host to unknown location	62
Media Server	17
Midsized Enterprise	
upgrade	161
migrate	145
migrate Communication Manager 6.x on survivable remote	
template	149
Migrate to Appliance Virtualization Platform	89
migrating	
Avaya Aura applications	140
Communication Manager	140
SAL	140
Session Manager	140
migrating	
Communication Manager 6.x on S8800 duplex main	158
S8800 simplex survivable core with S8300D survivable	
remote	158
migrating Avaya Aura applications	140
migrating Communication Manager	152
migrating duplex Communication Manager servers	129
migrating System Manager during Avaya Aura application	
migration	159
Migration	
System Platform	90
migration on different server	132
migration on same server	130
mode	
Utility Services	86
monitoring	
host	79
virtual machine	80
VM	80

N

network configurations	129 , 130 , 132
network parameters	
change	63
New Host	63
New Location	55

O

on System Platform	145
Options	
Avaya Aura applications deployments	39
Out of Band Management	
deploy virtual machines	164

P

password	
change	64
password change	
Appliance Virtualization Platform host	60
ESXi host	60
password policy	60
password rules	60
perform System Manager tests	114 , 169
permissions required	38
Post Installation Checklist	169
post migration tasks	
Communication Manager Messaging	167
postmigration tasks for Communication Manager	167
Postmigration validation	102
preinstall Appliance Virtualization Platform	82
Presence Services	17
preupgrade check	49
pre upgrade checks	
System Platform upgrades	50
preupgrade job status	85
Preupgrade tasks	43
primary server	136 , 137
primary System Manager operational	138
product knowledge	9
profile mapping for Communication Manager upgrades, ...	40
profiles	
discovery	40

R

recovering	
Linux-based application	87
System Platform-based application	88
reestablish	
connection	79
Reestablish Connection	53
refresh elements job status	85
related documentation	10
required	
credentials	38
permissions	38
required permissions	38
resources	
server	20
restart	
virtual machine	71
restart virtual machine from SDM	71

restore additional languages	167
rollback	
upgrade	171
rollback upgrade	171

S

same host installation	113
same server migration	130
scenario	
deploy Appliance Virtualization Platform on services port	164
deploy virtual machines on Appliance Virtualization Platform	164
scenario is enabled	
deploy virtual machines on Appliance Virtualization Platform when Out of Band Management	164
scenarios	
Appliance Virtualization Platform	163
SDM	
installation	46
SDM client	
Deploy Avaya Aura applications	141
secondary System Manager standby and pause	138
Select Flexi Footprint	69
select upgrade target release	48
sequence	
Avaya Aura upgrade upgrade	37
server hardware and resources	20
servers supported	20
services port	
deploy Utility Services	164
virtual machines	164
Services Port VM	96
Session Manager	17
Session Manager update	117
Session Manager upgrade	115 , 127 , 134
skills to deploy	9
software	
download	65
Software library options	39
Software Management	15
software management interface	130
Solution Deployment Manager	15 , 17 , 60
install	103 , 104
restart virtual machine	71
start virtual machine	70
stop virtual machine	71
upgrade automation	17
Solution Deployment Manager client	
install	46
spreadsheet	92
SSH from Utility Services	84
standby server	136 , 137
start	
virtual machine	70
start virtual machine from SDM	70

Index

validate migration (<i>continued</i>)	
System Platform to Appliance Virtualization Platform	102
validate System Platform migration	102
verify	
System Manager installation	114 , 169
verifying	
connections	170
videos	13
view	
location	51
view location	51
virtual appliance	23
virtualized environment	23
Virtualized Environment	143
virtual machine	
create	67
edit	69
monitoring	80
restart	71
start	70
stop	71
Virtual machine management	50
Virtual Machines	53
VM connection reestablish	79
VM Deployment	72 , 75
VM Management	103 , 104
VMware infrastructure	23

W

WebLM	17
-------------	--------------------