Upgrading Avaya Aura® Communication Manager

Release 8.0.x
Issue 6
July 2020

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License type(s)

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

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

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

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. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction 8
Purpose 8
Prerequisites 8
Change history 9
Chapter 2: Upgrade overview and considerations 10
Communication Manager upgrades 10
Supported upgrade paths for Communication Manager 10
Supported servers 12
Software requirements 12
Communication Manager upgrades from System Manager 13
Supported servers 14
License file for Communication Manager 15
Use of third-party certificates 16
Latest software updates and patch information 16
Solution Deployment Manager 16
Solution Deployment Manager client capabilities 19
Chapter 3: Planning for upgrade 21
Prerequisites 21
Software details of Communication Manager 22
Support for SIP Enablement Services 23
Special circumstances 23
Supported browsers 24
Profile mapping for Communication Manager 6.x upgrades 24
Upgrade order 25
Upgrade process 25
Chapter 4: Preupgrade 29
Preupgrade tasks 29
Preupgrade tasks overview 29
Key tasks for upgrading Avaya Aura® applications to Release 8.0.1 29
Installing the Solution Deployment Manager client on your computer 32
Upgrade target release selection 35
Preupgrade checklist for Linux® Operating System upgrades 36
Pre-upgrade checklist for System Platform upgrades 36
Virtual machine management 37
Backup and restore 104
Creating a backup 104
Changing the hostname 105
Restoring backup 105
Chapter 5: Upgrading the application to Software-only environment 107

Migration path 107
Upgrading the application to Release 8.0.1 on Software-only environment using SMI 107
Upgrading the application to Release 8.0.1 on Software-only environment using System Manager Solution Deployment Manager 109
Chapter 6: Upgrading the application to Virtual Appliance or VMware environment 111
Considerations for upgrading Communication Manager using full backup 111
Upgrading Communication Manager using full backup 112
Upgrading Avaya Aura® applications 113
Upgrade checklist for Avaya Aura® Virtual Appliance 113
Upgrading Avaya Aura® applications to Release 8.0.1 115
Upgrading duplex Communication Manager 117
Upgrading ESS and LSP servers 123
Installing software patches 124
Installing custom software patches 126
Installed Patches field descriptions 129
Upgrade Management field descriptions 130
Upgrade Configuration field descriptions 133
Edit Upgrade Configuration field descriptions 134
Uploading a custom patch 142
Uploading custom patch field descriptions 142
Upgrading Communication Manager using System Management Interface 143
Upgrading Communication Manager from pre–5.2.1 to Release 8.0.1 143
Migrating from Communication Manager Release 5.2.1 using SMI 145
Upgrading Communication Manager 6.x to VMware 146
Migrating from Communication Manager Release 6.3 using SMI 148
Upgrade job status 149
Upgrade job status 149
Viewing the Upgrade job status 150
Editing an upgrade job 150
Deleting the Upgrade jobs 150
Upgrade Job Status field descriptions 151
Support for Enhanced Access Security Gateway 151
Enabling or disabling EASG through the CLI interface 152
Enabling or disabling EASG through the SMI interface 152
Viewing the EASG certificate information 153
EASG product certificate expiration 153
EASG site certificate 154
Chapter 7: Upgrading the application to KVM environment 156
Migration path 156
Upgrading the application to Release 8.0.1 on KVM 156
License management 158
Chapter 8: Upgrading the application to IaaS environment 159
Upgrade path for AWS 159

Upgrade path for Google Cloud Network 159
Upgrade path for Microsoft Azure 160
Upgrading the application to Release 8.0.1 on IaaS 160
License management 161
Chapter 9: Postupgrade process 163
Connecting the services computer to the server 163
Accessing the System Management Interface 163
Busying out previously busied out equipment 164
Enabling the scheduled maintenance 164
Entering initial system translations 164
Saving translations 165
Resolving alarms 165
Logging off from all administration applications 166
Disconnecting from the server 166
Deleting the virtual machine snapshot 166
Deleting the virtual machine snapshot from the Appliance Virtualization Platform host 166
Deleting the virtual machine snapshot from the vCenter managed host or standalone host 167
Chapter 10: Rollback process 168
Upgrade rollback 168
Rolling back an upgrade 168
Chapter 11: Resources 169
Communication Manager documentation 169
Finding documents on the Avaya Support website 171
Accessing the port matrix document 171
Avaya Documentation Portal navigation 172
Training 173
Viewing Avaya Mentor videos 173
Support 174
Using the Avaya InSite Knowledge Base 174
Appendix A: OS-level logins for Communication Manager 176
Glossary 177

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from Release 5.2.1 or earlier (including Release 3.x and 4.x), Release 6.x, Release 7.x to Release 8.0.1 on:

- Avaya provided server in Avaya Aura® Virtualized Appliance environment.
- VMware in customer-provided Virtualized Environment.
- Kernel-based Virtual Machine (KVM) in customer-provided Virtualized Environment.
- Amazon Web Services (AWS), Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS).
- Customer provided Software-only environment.

This document:

- Includes upgrade checklists and maintenance procedures.
- Does not include optional or customized aspects of a configuration.

The primary audience for this document is anyone who upgrades, configures, and verifies Communication Manager upgrade at a customer site.

Prerequisites

Before upgrading the Avaya Aura® application, ensure that you have the following knowledge, skills and tools:

Knowledge

- **For Appliance Virtualization Platform:** Appliance Virtualization Platform virtualized environment
- **For VMware:** VMware® vSphere™ virtualized environment
- **For Kernel-based Virtual Machine (KVM):** KVM hypervisor set up
- **For Amazon Web Services(AWS):** AWS environment
- **For Google Cloud:** Google Cloud environment

- **For Azure:** Microsoft Azure environment
- Linux® Operating System
- System Manager

Skills

To administer:

- Solution Deployment Manager
- VMware® vSphere™ virtualized environment
- KVM hypervisor
- AWS Management Console
- Google cloud
- Microsoft Azure

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

Change history

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

Issue	Date	Summary of changes
6	July 2020	Updated the “License file for Communication Manager” section.
5	June 2020	Added “Changing the hostname” section.
4	September 2019	“Accessing the port matrix document” section is added.
3	August 2019	“Upgrading Communication Manager 6.x to VMware” section is updated.
2	December 2018	For Release 8.0.1, made the following changes: • Updated the target version of the Communication Manager application to Release 8.0.1, wherever applicable. • Added the content on how to apply the Release 8.0.1 patch on all the supported target platforms. • Added the “OS-level logins for Communication Manager” section under the Appendix chapter. • Added the “Considerations for upgrading Communication Manager using full backup” section under the Upgrading the application to Virtual Appliance or VMware environment chapter. • Added the “Entering initial system translations” section under the Postupgrade process chapter.
1	July 2018	Release 8.0 document.

Chapter 2: Upgrade overview and considerations

Communication Manager upgrades

You can use System Manager Solution Deployment Manager, the centralized upgrade solution, to upgrade Communication Manager and the associated devices, such as Gateways, TN boards, and media modules.

With Solution Deployment Manager, you can upgrade Communication Manager from:

- Release 7.x to Release 8.0.1
- Release 6.x to Release 8.0.1
- Release 5.2.1 to Release 8.0.1

Note:

- If your server release version is earlier than Release 5.2.1, ensure to upgrade servers to Release 5.2.1 first before you start upgrading to Release 8.0.1.
- To upgrade Communication Manager by using Solution Deployment Manager, you must have System Manager.
- In case the offer does not support Communication Manager upgrade by using System Manager Solution Deployment Manager, you must upgrade the application manually.

Supported upgrade paths for Communication Manager

If the Communication Manager version is earlier than Release 8.0, you must upgrade to Release 8.0 first before you can upgrade or migrate the Communication Manager to Release 8.0.1. Ensure that you take the backup of your system before proceeding with the upgrade process. After you upgrade the application to Release 8.0, apply the Release 8.0.1 patch file.

Note:

To upgrade from Release 8.0 to Release 8.0.1 on the same environment, you must update the application by applying the latest patch.

To migrate from Release 8.0 to Release 8.0.1 on a different environment, you must separately deploy the target environment specific Release 8.0 application, and then apply the Release 8.0.1 patch.

The following table displays all the upgrade paths from earlier releases to Release 8.0.1:

From offer	From Release	To Software-only 8.0.1	To AVP 8.0.1	To VMware/ KVM 8.0.1	To AWS 8.0.1	To Google Cloud/ Azure 8.0.1
AVP	7.0.x	Migration	Fully automated upgrade	Migration	Migration	Migration
	7.1.x	Migration	Fully automated upgrade	Migration	Migration	Migration
VMware/ KVM	6.x	Migration	Migration	VMware-to-VMware: Fully automated upgrade VMware-to-KVM: Migration	Migration	Migration
	7.0.x	Migration	Migration	VMware-to-VMware: Fully automated upgrade VMware-to-KVM: Migration	Migration	Migration
	7.1.x	Migration	Migration	VMware-to-VMware: Fully automated upgrade VMware-to-KVM and vice-versa: Migration	Migration	Migration
AWS	7.1.x	Migration	Migration	Migration	Upgrade	Migration
System Platform	6.x	Migration	Migration	Migration	Migration	Migration
Bare Metal	5.2.1	Migration	Migration	Migration	Migration	Migration
Any	3.x	Migration	Migration	Migration	Migration	Migration
	4.x	Migration	Migration	Migration	Migration	Migration
	Pre-release 5.2.1	Migration	Migration	Migration	Migration	Migration

Note:

- Communication Manager Release 8.0.1 supports upgrade on Hyper-V systems as one of the Software-only offers. For details, see “Upgrading Communication Manager to Release 8.0.1 on Software-only environment”.

- You can replace the existing server with the server that Communication Manager Release 8.0.1 supports and migrate to Communication Manager Release 8.0.1 on Appliance Virtualization Platform.
- You must upgrade to Release 5.2.1 or 6.3.x on a supported server before you complete the Communication Manager upgrade to Release 8.0.1.
- For releases earlier than 5.2.x, you can take "translation-only" backup and restore that data on the Release 8.0.1 system.
- Fully automated upgrade can be performed either by the Solution Deployment Manager client or by the System Manager Solution Deployment Manager depending on the Avaya Aura® application that you want to upgrade.
- Migration involves manual upgrade process using backup and restore method where server hardware (upgrade platform or environment) or operating system or hypervisor is changed.

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 8.0 and later:

- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9
- S8300E, for Communication Manager and Branch Session Manager
- Avaya Converged Platform 120 Server: Dell PowerEdge R640

Note:

- Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.
- Release 7.0 and later does not support S8510 and S8800 servers.

For fresh installations, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 7.1.2 and later on a customized version of VMware® ESXi 6.0.

- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 6.0, 6.5, or 6.7
  - VMware® vCenter Server 6.0, 6.5, or 6.7

  To view compatibility with other solution releases, see VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

Note:

- Avaya Aura® Release 8.0 and later does not support vSphere ESXi 5.0 and 5.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.

Communication Manager upgrades from System Manager

Upgrade Management in Solution Deployment Manager is a centralized upgrade solution of System Manager, provides an automatic upgrade of Avaya Aura® applications. You can upgrade Communication Manager, Session Manager, and Branch Session Manager directly to Release 8.0.1 from a single view. Communication Manager includes associated devices, such as Gateways, TN boards, and media modules. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

Important:

System Manager Release 7.x and later also support the System Manager Release 6.3.8 flow to upgrade Communication Manager, gateways, media modules, and TN boards to Release 6.3.100. However, the Release 6.3.8 user interface is available only when you select **Release 6.3.8** as the target version on the Upgrade Release Selection page.

With Upgrade Management, you can perform the following:

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

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

- The bandwidth is sufficient

  Note:

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

- The files are downloaded

5. Upgrade applications: To upgrade Avaya Aura® applications to Release 8.0.1.
6. Install patches: To install the software patches, service packs, and feature pack.

Upgrade automation level

- The upgrade of Communication Manager, Session Manager, Branch Session Manager, and AVP Utilities to Release 8.0.1 is automated. The upgrade process includes creating a backup, deploying OVA, upgrading, installing software patches, feature packs, or service packs, and restoring the backup.
- Upgrade of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVA files.

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

Upgrade job capacity

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

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

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

Supported servers

You can deploy Communication Manager using the following OVA types:

- **Simplex:** If you want to have only one Communication Manager server in your environment, then you can use simplex OVA.
- **Duplex:** If you want to have a standby Communication Manager server, then you can use duplex OVA. The standby server becomes active when the main server goes down. To deploy the Duplex OVA, install the Duplex OVA on two different hosts. Ensure that the hosts reside on two different clusters.

The following table provides the information about servers compatible with each OVA.

OVA type	Server configuration	Supported server
Simplex	• Main • Survivable Core • Survivable Remote	• S8300E • Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360p G8 • HP ProLiant DL360 G9 • Avaya Converged Platform 120 Server
Duplex	• Main • Survivable Core	• Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360p G8 • HP ProLiant DL360 G9 • Avaya Converged Platform 120 Server

For information about capacities, see *Avaya Aura® Communication Manager System Capacities Table*.

For information about hardware specifications, see *Avaya Aura® Communication Manager Hardware Description and Reference*.

License file for Communication Manager

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager.

PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

After you obtain the license file, use System Manager WebLM to install the license file. System Manager WebLM is a Web-based application for managing licenses and is installed as part of System Manager.

The license file is an Extensible Markup Language (XML) file. The license file has the information regarding the product, major release, and license features and capacities.

You must install license files for the Communication Manager main server, but not for survivable servers. Survivable servers receive licensing information from the main server.

A 30-day grace period applies to new installations or upgrades to Communication Manager, Collaboration Server, and Solution for Midsize Enterprise. You have 30 days from the day of installation to install a license file.

Duplicated server licensing

For a Communication Manager duplex configuration, install the Communication Manager license file on WebLM, assign the same license file to both active and standby servers on WebLM, and then configure the same WebLM URL on both servers.

Note:

One centralized license file should not be mapped to more than one Communication Manager. In case of duplex Communication Manager, both active and standby Communication Manager from that pair should be mapped to same centralized license file.

Use of third-party certificates

Many companies use third-party certificates for security. You cannot retain the third-party certificates as a part of the upgrade dataset, you must reinstall the third-party certificates after the upgrade. If you use third-party certificates, keep a copy or download new third-party certificates before you start the upgrade process.

Latest software updates and patch information

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

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

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

Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

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

- AVP Utilities 8.0.1
- System Manager 8.0.1
- Session Manager 8.0.1
- Branch Session Manager 8.0.1

- Communication Manager 8.0.1
- Application Enablement Services 8.0.1
- WebLM 8.0.1
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  Note:

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.

- Hardware-based Session Manager 6.x
- 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
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

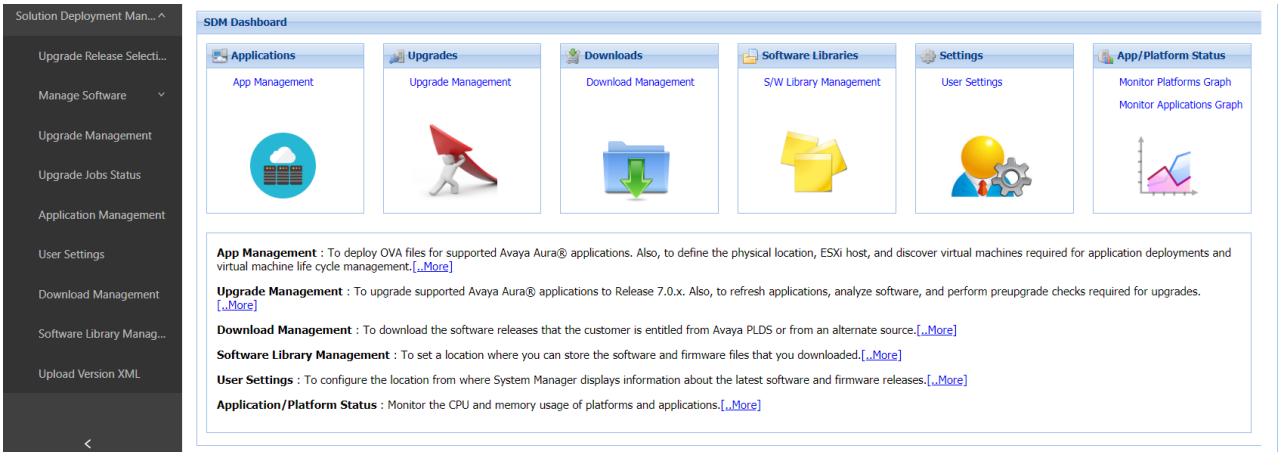
Note:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 8.0.1. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.x Onwards** or **6.3.8** as the target upgrade. Release 8.0.1 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Kickstart file.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, and WebLM to Release 8.0.1.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the `version.xml` file to perform upgrades.

Related links

Solution Deployment Manager client capabilities on page 19

Solution Deployment Manager client capabilities

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

- Runs on the following operating systems:
  - Windows 7, 64-bit Professional or Enterprise
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deploying the System Manager OVA. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports the Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of the Avaya Aura® applications.
- 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 Appliance Virtualization Platform or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.

  Note:

  - System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 7.1.3.2 before you upgrade Communication Manager to 7.1.3.2.

    All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.
  - Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 7.1.3 OVA, Solution Deployment Manager Client version must be on Release 7.1.3, 7.1.3.1, 7.1.3.2, or 8.0. Solution Deployment Manager Client cannot be on Release 7.1.
- Configures application and networking parameters required for application deployments.

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

  Note:

  To install the patch on System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 7.1.1, you must use Solution Deployment Manager Client Release 7.1.1 or higher.

  However, to install the patch on System Manager Release 7.0.x, Solution Deployment Manager Client must be on Release 7.0.x.

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

  For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.
- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.

Related links

Solution Deployment Manager on page 16

Chapter 3: Planning for upgrade

Prerequisites

Serial Number	Prerequisites	Tasks/ Notes
1	Download the Avaya Aura® application software from the Avaya Support website at http://support.avaya.com. Copy the applications on the computer that you later use to perform the upgrade. If you placed an order for the hardware, ensure that the hardware is available onsite.	Download the following files: • OVA files of System Manager, Communication Manager and Utility Services from PLDS • DVDs for the Solution Deployment Manager client and Appliance Virtualization Platform from PLDS • The license file from PLDS • Preupgrade and postupgrade service packs from the Avaya Support website at http://support.avaya.com.
2	Verify that the existing server is compatible with Release 8.0.1 version of the application. If the existing server is incompatible, change the server accordingly.	See, Supported servers on page 12.
3	Keep the following checklists: • The application specific Release 8.0.1 installation checklist • Upgrade checklist	-
4	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	-

Table continues…

Serial Number	Prerequisites	Tasks/ Notes
5	Ensure that Appliance Virtualization Platform host and all virtual machines running on the host are on the same subnet mask. If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need two subnet masks based on following requirements: • Public or signaling traffic: To route signaling traffic of Appliance Virtualization Platform, and all virtual machines. • Management traffic: To route management traffic of Appliance Virtualization Platform, and all virtual machine.	-

Software details of Communication Manager

The following table lists the software details of all the supported platform for the application. You can download the softwares from the Avaya PLDS website at http://plds.avaya.com/.

Table 1: Communication Manager build details

Release	Bundle offer type	Installer files
8.0	OVA	• **AVP and VMware Simplex:** `CM-Simplex-08.0.0.0.822-e67-1.ova` • **AVP and VMware Duplex:** `CM-Duplex-08.0.0.0.822-e67-1.ova` • **KVM Simplex:** `CMKVM-Simplex-08.0.0.0.822-e67-1.ova` • **KVM Duplex:** `CMKVM-Duplex-08.0.0.0.822-e67-1.ova` • **AWS Simplex:** `CMAWS-Simplex-08.0.0.0.822-e67-1.ova` • **AWS Duplex:** `CMAWS-Duplex-08.0.0.0.822-e67-1.ova`
8.0	ISO	**Simplex or Duplex:** `CM-08.0.0.0.822-e67-0.iso`
8.0.1	Patch file	**Simplex or Duplex:** `8.0.1.0.0.25031.tar`
8.0.1	Solution Deployment Manager Client	`Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip` contains the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe` file.

Support for SIP Enablement Services

SIP Enablement Services is not compatible with Communication Manager Release 7.1.1 and later. If you upgrade Communication Manager with SIP Enablement Services Release 5.2.1 or earlier to Release 7.1.1 and later, you must install Avaya Aura® Session Manager for continued support of SIP stations and adjuncts. For Session Manager options, contact an Avaya salesperson.

Special circumstances

Consider the following special situations when upgrading to latest version of Communication Manager.

- If you have Communication Manager Messaging or Intuity Audix 770 enabled on the existing system, backup and restore that dataset separately on the upgraded system.
- If you have Communication Manager and SIP Enablement Services (SES) co-resident on the S8300 Server, you cannot restore SES on the new server because latest version of Communication Manager does not support SES.
- When you upgrade Communication Manager with Communication Manager Messaging, deploy Communication Manager Messaging OVA with a new IP address along with Communication Manager migration.

  You must create a backup for messaging translations, names, and messages, and create a separate backup of announcements if Communication Manager Messaging contains custom announcements recorded. The procedures are available in this document. The maximum limit for backup size is about 50 GB.
- If you have SES on the existing system and want to use the same SIP signaling group for Session Manager:
  - To edit the **Peer Server** field, set the **Peer Detection Enabled** field to `n`. By default, the system sets the **Peer Detection Enabled** field to `y` .
  - In the **Peer Server** field, enter `SM` or `Others`.
- If the existing system has SIP integrated Modular Messaging, the upgrade process automatically prefixes a + character to the phone number.

  Important:

  You must remove the + character manually from the phone number. For instructions, see *Messaging Application Server (MAS) Administration Guide*.
- If you use Unicode phone messages on the existing system, reinstall the Unicode phone messages file after the upgrade.

Supported browsers

The Avaya Aura® applications support the following web browsers:

- Internet Explorer 11
- Mozilla Firefox 59, 60, and 61

Profile mapping for Communication Manager 6.x upgrades

Before you upgrade Communication Manager from Release 6.x to Release 8.0.1 ensure the correct footprints are available.

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

Table 2: Summary of profile mapping

Communication Manager 6.x template	Communication Manager Release 8.0.1 deployment option	Resources
CM_onlyEmbed on S8300E	CM Main Max users 1000 Small Main supporting up to 1000 users	2vCPUs, 3900 MHz, 3.5 Gb RAM
CM_SurvRemoteEmbed on S8300E	CM Survivable Max users 1000 Small Survivable supporting up to 1000 users	1vCPU, 1950 MHz, 3.5 Gb RAM
CM as part of Midsize_Ent	CM Main Max users 2400 Medium Main only supporting up to 2400 users This profile is targeted as a migration path for Communication Manager on Midsize Enterprise.	2 vCPUs, 4400 MHz, 4.0 Gb RAM
CM_Simplex	CM Main/Survivable Max users 41000 Large Main/Survivable supporting up to 41000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_SurvRemote	CM Main/Survivable Max users 41000 Large Main/Survivable supporting up to 41000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_Duplex	CM Duplex Max users 41000 Standard Duplex 41000 users	3 vCPUs, 6600 MHz, 5.0 Gb RAM
CM_Duplex high capacity	CM High Duplex Max users 41000 High Duplex 41000 users	3 vCPUs, 7650 MHz, 5.0 Gb RAM

Upgrade order

If the application is part of the Avaya Aura® solution, perform the upgrade in the following order:

1. Endpoints
2. Avaya Aura® System Manager
3. Avaya Aura® Session Manager
4. Branch gateways
5. Media modules
6. Survivable remote servers (Communication Manager and Branch Session Manager)
7. TN boards
8. Survivable core servers
9. Primary Communication Manager, configured as feature servers and evolution servers

Upgrade process

The following list provides the key upgrade sequence for upgrade paths that start with a server running Communication Manager Release 5.2.1.

1. Communication Manager on any survivable remote server
2. Latest firmware on all Avaya H.248 Branch Gateway
3. Latest firmware on the media modules within the H.248 Branch Gateway
4. Communication Manager on any survivable core server
5. Latest firmware on all TN circuit packs if you are using port networks
6. Communication Manager on the main server
7. Latest firmware on all telephones

When you replace the server, verify the following general tasks that you complete on a simplex server:

Task	Notes	√
Ensure that the site has the server and other hardware.		
Get the required software and preupgrade and postupgrade service packs.		
Ensure that you have the server and disk space available to back up the upgrade data set.		
Keep the required documentation and release notes handy.		

Table continues…

Task	Notes	√
Record the IP addresses and other data of the existing System Platform and Communication Manager that you later configure on the Release 8.0.1 system.	Use the worksheets provided in appendices to make sure that you capture all the required information.	
Convert private control networks to the corporate LAN.	Release 6.x does not support private networks (CNA and CNB). For instructions, see Converting private control networks to corporate LAN.	
Complete the routine preupgrade tasks on the existing server.		
If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system. If Communication Manager Messaging or Messaging is enabled on the system, that is, if Audix is set to yes in the `ecs.conf` file, disable or configure Messaging or Communication Manager Messaging before you upgrade the system. The upgrade fails if you do not disable or configure Messaging or Communication Manager Messaging.		
Back up all files on the existing server if you need to roll back to the original release.	• For release earlier than 5.2.1, obtain TMT from the STS team. • For Release 5.2.1 or later, back up the migration data set	
Install the preupgrade service pack on the existing server.	**Important:** To roll back the upgrade, you must deactivate the preupgrade patch.	
Create the backup of the Communication Manager data set to be restored on the new server.		
Create the backup of the Communication Manager Messaging data set that you will restore on the new server if messaging is enabled.		
For a standalone server, shut down the existing server and remove all power cords and cables. For an embedded server, remove all cables from the faceplate, shut down the existing server, and remove the server from the H.248 Branch Gateway.		

Table continues…

Task	Notes	√
Install one of the following servers in the rack and connect the power cord and cables: • HP DL360 G8, or HP DL360 G9 server • Dell R620 or Dell R630 server • S8300E server. Install this embedded server in a branch gateway.	You can install a new server before completing the tasks on the existing server. **Note:** Release 8.0 and later does not support the following servers: • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R610 • Avaya S8300D Microsoft Azure Google Cloud Platform	
Get the System Manager and Communication Manager applications.	On the new server, you can install the ESXi host before completing the tasks on the existing server.	
Get the license file from the PLDS website at https://plds.avaya.com. Install the file on the WebLM server.	On the new server, you can perform the step before completing the tasks on the existing server.	
Using central Solution Deployment Manager or the Solution Deployment Manager client, add an ESXi host and virtual machine. Then, deploy the latest application and patch or feature pack or service pack files of System Manager and Communication Manager.	On the new server, you can perform the step before completing the tasks on the existing server.	
Deploy the Communication Manager Messaging application file if the existing system contains Communication Manager Messaging.		
Restore the Communication Manager dataset.		
Using System Management Interface, configure Communication Manager		
Restart the server by using System Management Interface. **Important:** Check the status of other devices and applications that depend on Communication Manager, such as Call Management System (CMS) and Call Center. After you complete the Communication Manager upgrade, reboot the applications if required.		
Using System Management Interface, restore the Communication Manager Messaging data set.		
Configure Communication Manager Messaging.		

Table continues…

Task	Notes	√
Complete the post-upgrade operations.		
Create a backup of the system.		
Register the upgraded system.		

Chapter 4: Preupgrade

Preupgrade tasks

Preupgrade tasks overview

To successfully upgrade the system to Release 8.0.1, you must perform all tasks listed in the Preupgrade tasks section.

Key tasks for upgrading Avaya Aura® applications to Release 8.0.1

The table contains the key tasks that are required to upgrade Avaya Aura® applications to Release 8.0.1.

Performing the pre-configuration 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.	

Table continues…

Task	Note
For the Communication Manager instance, create the EPW file for the following templates: • Embedded CM Main • Embedded Survivable Remote	
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 8.0. 3. For Release 8.0 system, install the Release 8.0 OVA file to upgrade to Release 8.0.	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 *Administering Avaya Aura® System Manager*
For Communication Manager, configure the access for the **H.248 Gateway** device.	

Performing the configuration settings required for upgrade

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

Performing the upgrade process

Task	Note
Refresh the elements in inventory.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Perform the analyze software operation for the Avaya Aura® application that you selected.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Download the software.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Perform the preupgrade check.	“Solution deployment and upgrades” in *Administering Avaya Aura® System Manager*
Run the upgrade operation.	Upgrading Avaya Aura applications to Release 8.0.1 on page 115 Upgrade checklist for Avaya Aura Virtual Appliance on page 113 **Note:** The system takes about 2.5 hours to complete the upgrade process.

Installing feature packs and service packs

Task	Note
Install the Release 8.0.1 feature pack and any required software patches on the Avaya Aura® application.	Installing software patches on page 76
For Communication Manager, updating the H.248 media gateway device.	1. In the alternate source location, download the patch file `g450_sw_36.x.bin`. 2. For the gateway that you have selected, perform the Analyze job. 3. On the Select Gateway (G) panel, select **Library and download protocol**. 4. Click **Download**. 5. Click on active status link to observe the progress of upgrade.

Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

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

Procedure

1. Download the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products** > **Downloads**, and type the product name as **System Manager**, and Release as **8.0.x**.
3. Click the **Avaya Aura® System Manager Release 8.0.x SDM Client Downloads, 8.0.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

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

4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

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

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.

8. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:

   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

   b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

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

      You can save the artifacts in the specified directory.

   c. In **Data Port No**, select the appropriate data port.

      The default data port is 1527. The data port range is from 1527 through 1627.

   d. In **Application Port No**, select the appropriate application port.

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

      Note:

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

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

10. Click **Next**.

11. On the Summary and Validation page, verify the product information and the system requirements.

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

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

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

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

Next steps

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

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

Related links

Accessing the Solution Deployment Manager client dashboard on page 34
Accessing Solution Deployment Manager on page 35

Accessing the Solution Deployment Manager client dashboard

About this task

Note:

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

Procedure

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

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

Related links

Installing the Solution Deployment Manager client on your computer on page 32

Accessing Solution Deployment Manager

About this task

You require to start Solution Deployment Manager to deploy and upgrade virtual machines, and install service packs or patches.

Procedure

Perform one of the following:

- If System Manager is not already deployed, double-click the Solution Deployment Manager client.

  Note:

  All the management operation related to System Manager, such as, deployment, patching, or upgrade can only be done by using Solution Deployment Manager Client.

- If System Manager is available, on the web console, click **Services** > **Solution Deployment Manager**.

Related links

Installing the Solution Deployment Manager client on your computer on page 32

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 35

Selecting the target release for upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select one of the following:
   - **SMGR 7.x**: To upgrade Avaya applications to Release 7.0 or later from the Upgrade Management page.
   - **SMGR 6.3.8**: To upgrade Communication Manager and the associated applications to Release 6.3.6 or later from the **Upgrade Management** > **Software Inventory** page.

   Important:

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

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

Related links

Upgrade target release selection on page 35

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:

You must perform these tasks on the System Manager web console.

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:

You must perform these tasks on the System Manager web console.

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. Elements include Communication Manager Utility Server, CDOM, System Platform and the Communication Manager itself that will be upgraded to Avaya Aura® Virtualized Appliance or VMware in customer-provided Virtualized Environment.	
3	After you perform the **Refresh Element(s)** operation, ensure that your system contains the current 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

Application management

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

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

- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

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

Managing the location

Viewing a location

Procedure

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

   The Locations section lists all locations.

Adding a location

About this task

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

Procedure

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

Related links

New and Edit location field descriptions on page 39

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, select a location that you want to edit.

3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 39

Deleting a location

Procedure

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

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

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.

Table continues…

Name	Description
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnetwork mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).

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

Managing the platform

Adding an Appliance Virtualization Platform or ESXi host

About this task

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

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

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

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

Before you begin

Add a location.

Procedure

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

5. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

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

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

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

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

   Important:

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

Next steps

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

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

Related links

Add and Edit platform field descriptions on page 68

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 8.0.1, the system supports the Red Hat Enterprise Linux Release 7.5 64-bit operating system.

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the platform or the base operating system.
5. In **User Name**, type the user name of the platform.

   For a software-only deployment, the user name must be a direct access admin user. If the software-only application is already deployed, provide the application cli user credentials.
6. In **Password**, type the password of the platform.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

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

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

   The system displays the added platform on the **Platforms** tab.

Editing a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.

3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select a platform that you want to update.
4. Change the platform information.
5. Click **Save**.

   The system updates the platform information.

Related links

Add and Edit platform field descriptions on page 68

Upgrading Appliance Virtualization Platform from Solution Deployment Manager

About this task

Upgrade Appliance Virtualization Platform from Release 7.0.x, 7.1.x, or 8.0 to Release 8.0.1 by using the upgrade bundle from the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Note:

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

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

  If you are installing a patch on a virtual machine, then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.
- If you are using services port to update or upgrade Appliance Virtualization Platform, connect the system directly with the Appliance Virtualization Platform services port (Gateway 192.168.13.1). If you connect the system using the AVP Utilities services port (Gateway 192.11.13.6), the Appliance Virtualization Platform update or upgrade fails.

Before you begin

1. Add a location.
2. Select Location and add an Appliance Virtualization Platform host.

To upgrade from Appliance Virtualization Platform Release 7.x or 8.0 to Release 8.0.1, ensure that:

- AVP Utilities is deployed on Release 8.0.
- Utility Services 7.x is deployed on Appliance Virtualization Platform Release 7.x and trust is established with the application.

- Appliance Virtualization Platform 7.x is not deployed on S8300D, Dell™ PowerEdge™ R610, or HP ProLiant DL360 G7 as the upgrade to Appliance Virtualization Platform 8.0 and later is not supported on these servers.

Note:

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

Procedure

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

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

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

4. If you are using System Manager Solution Deployment Manager, on the Update Host page, click **Select Patch from Local SMGR**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.

   For Solution Deployment Manager Client, the patch file must be available on windows machine where the Solution Deployment Manager client is hosted.

   For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-8.0.0.0.0.xx.zip`.

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

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

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

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

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

   Enable: (Recommended)

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

   Disable:

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

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

      Avaya recommends to enable EASG.

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

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

8. If Utility Services is deployed on Appliance Virtualization Platform Release 7.x, the system upgrades Appliance Virtualization Platform to Release 8.0, and then updates Utility Services to AVP Utilities.

   This step is applicable when you upgrade from Release 7.x to Release 8.0.1.

   The system displays the Utility Services Upgrade window.

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

   a. In Platform Details, the data store is auto-selected as server-local-disk, and then click **Next**.

   b. In **OVA**, provide the AVP Utilities OVA file details, and then click **Next**.

      For AVP Utilities OVA, the system automatically performs the resource check and disables the **Flexi Footprint** field.

   c. In Config Parameters, provide the network and configuration parameters details, and click **Update**.

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

    This step is applicable when you upgrade from Release 7.x to Release 8.0.1.

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

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

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

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

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

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

Next steps

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

Related links

Update Host field descriptions on page 71

Upgrading Utility Services 7.x to AVP Utilities Release 8.0.1 in bulk during Appliance Virtualization Platform upgrade

About this task

Use this procedure to upgrade Utility Services 7.x to AVP Utilities Release 8.0.1 in bulk when you are upgrading one or more Appliance Virtualization Platform to Release 8.0.1.

Before you begin

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

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

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

  Note:

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

Procedure

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

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

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

4. If you are using System Manager Solution Deployment Manager, on the Update Host page, click **Select Patch from Local SMGR**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **AVPU Configuration Import**.

   For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-8.0.0.0.0.xx.zip`.

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

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

   c. Click **Submit File**.
7. Click **Update Host** and accept the EULA.
8. To view the details, in the **Current Action** column, click **Status Details**.

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

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

Rolling back to Utility Services

About this task

Use this procedure to rollback Utility Services to 7.x if the upgrade from Utility Services to AVP Utilities fails from Release 7.x to Release 8.0 and later.

Before you begin

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

Procedure

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

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

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

   The system displays the confirmation message to accept the rollback.

Retrying Utility Services to AVP Utilities upgrade

About this task

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

Before you begin

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

  Note:

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

Procedure

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

   If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions** > **Rollback/Retry** after selecting the Utility Services application.

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

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

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

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

Changing the network parameters for an Appliance Virtualization Platform host

About this task

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

Note:

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, 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, do the following:
   a. Click **Change Gateway**.

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

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

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 68

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

About this task

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

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

Note:

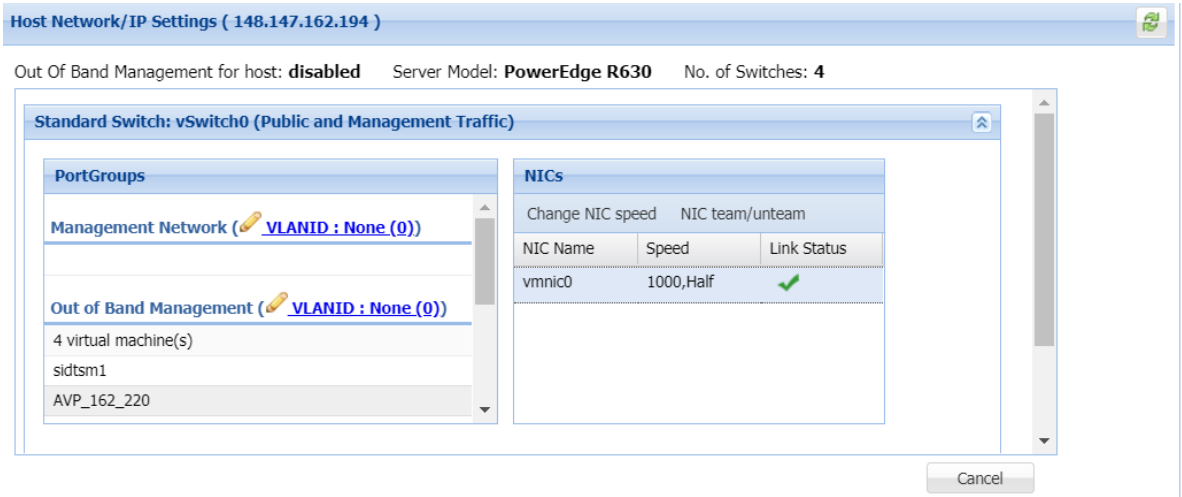
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fail because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

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.

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



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

You can configure port groups for the following switches:

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

5. To change VLAN ID, do the following:
   a. Expand the Standard Switch: vSwitch<n> section by clicking the downward arrow .

      The section displays the vSwitch details.

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

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

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

      For more information about the value, see NIC teaming.

   d. Click **OK**.

   The system displays the new VLAN ID.

6. To change the NIC speed, do the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.

      The system displays the selected vmnic dialog box.

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

d. Click **OK**.

For more information, see VLAN ID assignment.

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

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

Note:

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

7. To change the NIC teaming, do the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.

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

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

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

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for the S8300E server.

Related links

Host Network / IP Settings field descriptions on page 69

Changing the password for an Appliance Virtualization Platform host

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.

3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, do the following:
   a. Select a host.
   b. Click **More Actions** > **Change Password**.
4. In the Change Password section, type the current password and the new password.

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

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

Related links

Password policy on page 53
Change Password field descriptions on page 70

Password policy

The password must meet the following requirements:

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

Note:

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

Example of a valid password is *myPassword$*.

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

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

Related links

Changing the password for an Appliance Virtualization Platform host on page 52

Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Generate AVP Kickstart**.
3. On Create AVP Kickstart, do the following:
   a. Select **8.0.x**.
   b. Enter the appropriate information in the fields.

c. Click **Generate Kickstart File**.

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

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

For Appliance Virtualization Platform Release 8.0 and later, the kickstart file name must be `avp80ks.cfg`.

Related links

Create AVP Kickstart field descriptions on page 54

Create AVP Kickstart field descriptions

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

Table continues…

Name	Description
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Out of Band Management Setup	The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • **yes**: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • **no**: To disable Out of Band Management. The default option.
OOBM vLAN ID (Used on S8300E only)	• For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Confirm Password	Admin password for Appliance Virtualization Platform.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

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

Related links

Generating the Appliance Virtualization Platform kickstart file on page 53

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

About this task

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

Procedure

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

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

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

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

Activating SSH from AVP Utilities

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 AVP Utilities.

Before you begin

Start an SSH session.

Procedure

1. Log in to the AVP Utilities virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type the following:

   ```
   AVP_SSH enable
   ```

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

   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.
3. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
4. To disable SSH, type `AVP_SSH disable`.

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

About this task

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

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

Before you begin

Start an SSH session.

Procedure

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

   The system displays the following options:

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

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

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

For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.

5. To disable SSH, perform the following:
   a. At the prompt, type `2` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is already disabled, the system displays `False` and the message `SSH is already disabled. No operation performed. Exiting`.
6. **(Optional)** To view the status of SSH, perform the following:
   a. At the prompt, type `3` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.

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

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

Changing the IP address and default gateway of the host

About this task

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

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

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

Before you begin

Connect the computer to the services port.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. At the command prompt of the host, do the following:
   a. To change the IP address, type the following:

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

For example:

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

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

For example:

```
esxcfg-route 135.27.162.1
```

4. Enable SSH on Appliance Virtualization Platform and run the **`/opt/avaya/bin/./serverInitialNetworkConfig`** command.

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

Appliance Virtualization Platform license

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

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

To configure the Appliance Virtualization Platform license file:

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

Note:

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

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

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

- **Normal:** If the Appliance Virtualization Platform host has acquired a license, the **License Status** column displays **Normal**.
- **Error:** If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day

grace period. The **License Status** column displays **Error - Grace period expires: <DD/MM/YY> <HH:MM>**.

- **Restricted:** If the 30-day grace period of the Appliance Virtualization Platform license expires, Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The **License Status** column displays **Restricted**. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

  Note:

  Restricted administrative actions for:

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

Appliance Virtualization Platform licensing alarms

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

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

Before you begin

1. Add an Appliance Virtualization Platform host.

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions** > **WebLM Configuration**.

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

For WebLM configuration, if you select:

- Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.
- Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.

5. In **Port Number**, type the port number of WebLM Server.

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

6. Click **Submit**.

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

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

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

WebLM Configuration field descriptions

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

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

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Shutting down the Appliance Virtualization Platform host

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Lifecycle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

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

Procedure

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

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

Removing an Appliance Virtualization Platform or ESXi host

Procedure

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

Configuring the login banner for the Appliance Virtualization Platform host

About this task

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

Procedure

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

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

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

Mapping the ESXi host to an unknown location

About this task

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

Procedure

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

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

   The system displays the ESXi host in the selected location.

Applying third-party AVP certificates

Applying third-party certificates to Appliance Virtualization Platform

About this task

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

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

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

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

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

      The system generates CSR for the Appliance Virtualization Platform host.
   f. In the **Current Action** column, click **Status Details** to view the status.
6. To download CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Download CSR**.

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

      In the Download CSR Status dialog box, the system displays the path of the downloaded `CSR.zip` file.
7. Extract the downloaded certificates, and ensure that the third-party signs them.
8. To upload and push the signed certificate from a third-party CA, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.

b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
c. Click **Browse** and select the required certificates from the local computer.
d. Click **I Agree to accept to add the same certificate in SDM**.
e. Click **Push Certificate**.
f. In the **Current Action** column, click **Status Details** to view the status.

Creating or editing generic CSR

About this task

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

Procedure

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

Next steps

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

Load Certificate field descriptions

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

Button	Description
View/Generate CSR	Displays the View/Generate CSR dialog box to generate CSR.
Download CSR	Downloads CSR for the selected host.

Table continues…

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

Create or edit CSR field descriptions

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

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

Virtual Machine snapshot on Appliance Virtualization Platform

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

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

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 67
Snapshot Manager field descriptions on page 67

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

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

Procedure

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

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

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

   The system deletes the selected snapshots.

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 66

Snapshot Manager field descriptions

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

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

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 66

Add and Edit platform field descriptions

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

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

Change Network Parameters field descriptions

Network Parameters

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

Table continues…

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

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

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

Host Network / IP Settings field descriptions

Port Groups

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

Name	Description
or **VLAN ID** link	Displays the Port Group Properties page where you configure VLAN ID.

Table continues…

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

NIC speed

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

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

NIC teaming

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

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

Change Password field descriptions

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

Table continues…

Name	Description
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Update Host field descriptions

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

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

Downloading the OVA file to System Manager

About this task

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

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.

3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. Click **Download**.

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

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

   Note:

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

Managing the application

Deploying AVP Utilities

About this task

Use this procedure to deploy AVP Utilities on Appliance Virtualization Platform Release 8.0.1.

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

Before you begin

- Add a location.

  See “Adding a location” in *Administering Avaya Aura® System Manager*.
- Add Appliance Virtualization Platform.

  See “Adding an Appliance Virtualization Platform or ESXi host” in *Administering Avaya Aura® System Manager*.
- Download the AVP Utilities OVA file.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ().

2. In **Application Management Tree**, select a platform.
3. On the Applications tab, in the Applications for Selected Location <location name> section, click **New**.

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

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

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

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

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

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

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

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

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

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

Next steps

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

Related links

Application Deployment field descriptions on page 82

Deploying an OVA file for an Avaya Aura® application

About this task

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

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

Deploy AVP Utilities first, and then deploy all other applications one at a time.

Before you begin

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

Procedure

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

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

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

   The page displays the capacity details.
6. Click **Next**.

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

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

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

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

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

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

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

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

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

Next steps

Perform the following for Communication Manager:

1. From the Manage Elements link on System Manager, update the credentials corresponding to the element that you added.
2. Before the synchronization and after deployment, add an SMNP profile on Communication Manager.

Note:

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

Related links

Installing software patches on page 76
Application Deployment field descriptions on page 82

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application using the Solution Deployment Manager client.

Before you begin

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

Procedure

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

Installing software patches

About this task

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

Note:

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

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

Before you begin

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

Procedure

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

   Note:

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

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

Note:

- For Communication Manager, if you are editing the Utility Services for System Platform based system, then you must select the details as per the Utility Services. If you are upgrading Communication Manager which is not on System Platform, then select the details for the Communication Manager only.
- To upgrade Communication Manager having duplex configuration, you must select the duplex related details.

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

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

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

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

    The page displays all software patches that you can commit.

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

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

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

    Note:

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

Related links

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 166

Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 167
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 133
Edit Upgrade Configuration field descriptions on page 134
Installed Patches field descriptions on page 129

Editing an application

Before you begin

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

Procedure

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

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

      Note:

      To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.
   b. Click **More Actions** > **Refresh App**.

      Note:

      To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.
   c. Click **Update IP/FQDN in Local Inventory**.
   d. Click **Update App IP/FQDN**.
   e. Provide the IP address and FQDN of the application.

      Update IP/FQDN in Local Inventory updates the IP address or FQDN of the application only in the local database in System Manager. The actual IP address or

FQDN of the host does not change. Use **Update Network Params** in the **Platforms** tab to update the IP address or FQDN of the host.

5. Click **Save**.

Deleting an application

Procedure

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

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

Updating Services Port Static Routing on an Avaya Aura® application

About this task

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

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

Before you begin

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

Procedure

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

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

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

Related links

Update Static Routing field descriptions on page 91

Starting an application from Solution Deployment Manager

Procedure

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

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

Stopping an application from Solution Deployment Manager

About this task

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

Procedure

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

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

Restarting an application from Solution Deployment Manager

Before you begin

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

Procedure

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

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

Common causes for application deployment failure

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

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

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

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

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

Application Deployment field descriptions

Select Location and Platform

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

Capacity Details

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

Note:

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

Name	Description
Name	The name

Table continues…

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

Provide admin and root Credentials

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

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

Deploy OVA using System Manager Solution Deployment Manager

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

Deploy OVA using the Solution Deployment Manager client

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

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

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

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

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

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

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

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

The system displays the following common fields.

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

Configuration Parameters

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

Note:

For configuration parameter fields, for Communication Manager Messaging and AVP Utilities, see Configuration and Network Parameters field descriptions on page 88.

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

Communication Manager Configuration Parameters

Name	Description
CM IPv4 Address	The IPv4 address of the Communication Manager virtual machine.
CM IPv4 Netmask	The IPv4 network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The IPv4 default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine. The field is optional.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine. The field is optional.
CM IPv6 Gateway	The IPv6 gateway of the Communication Manager virtual machine. The field is optional.

Table continues…

Name	Description
Out of Band Management IPv4 Address	The IPv4 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv4 Netmask	The IPv4 subnetwork mask of the Communication Manager virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv4 subnetwork mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Server(s)	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). You can type up to three NTP servers.
DNS Server(s)	The DNS IP address of the Communication Manager virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IPv4 address of WebLM. The field is mandatory.
EASG User Access	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.
Confirm Password	The password required to be confirmed. The field is mandatory.

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

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

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 AVP Utilities is deployed in the solution. AVP Utilities provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Private	The field is available only when you deploy Application Enablement Services.
Create Port Group	The field to create new port group for interface.
Out of Band Management	The port number that is mapped to the out of band management port group.

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

Related links

Configuration and Network Parameters field descriptions on page 88

Configuration and Network Parameters field descriptions

Table 3: Configuration Parameters for Communication Manager Messaging deployment

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

Configuration and Network Parameters for AVP Utilities deployment

Name	Description
Networking Properties	

Table continues…

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

Table continues…

Name	Description
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirm Password	The confirmation password.
Application Properties	
AVP Utilities Mode	The mode in which you want to deploy AVP Utilities. You can set the mode during the deployment only. You cannot change the mode after the virtual machine is deployed. The options are: • **standard_mode**: AVP Utilities and services port enabled. The default mode for Appliance Virtualization Platform. • **hardened_mode**: Sets up the system for commercial hardening. • **hardened_mode (dod)**: Sets up the system for military hardening.
Admin User Password	The admin user password.
Confirm Password	The confirmation password.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management. **Note:** **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

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

Update Static Routing field descriptions

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

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

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

Table continues…

Button	Description
Get Patch Info	Displays software patches, service packs, and feature packs that you installed.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

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

Update App field descriptions

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

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

Reestablish Connection field descriptions

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

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

Virtual machine report

You can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

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

Important:

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

generate_report.sh command

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

Syntax

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

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

Generating a virtual machine report

Before you begin

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

Procedure

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

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

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

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

   Note:

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

Viewing the status of the virtual machine report

Procedure

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

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

Aborting the virtual machine report generation

About this task

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

Procedure

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

   The system aborts the virtual machine report generation process.

Certificate validation

Certification validation

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

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

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

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

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

For the correct certificate:

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

If the certificate is incorrect:

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

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

Note:

Solution Deployment Manager:

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

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

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

Generating and accepting the Appliance Virtualization Platform host certificates

About this task

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

If the certificate is invalid:

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

Before you begin

Get permissions to add a host to generate certificates.

Procedure

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

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

   b. **Accept Certificate**

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

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

Generating and updating the certificate on the ESXi host from VMware

About this task

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

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

Procedure

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

Next steps

Note:

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

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

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

Managing certificates for existing hosts

About this task

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

Before you begin

Gain permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions** > **Generate/ Accept Certificate**, and click **Accept Certificate**.

- If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

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

Managing vCenter

Creating a role for a user

About this task

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

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

Procedure

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

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

      Note:

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

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

Note:

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

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

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager.

To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

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

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

Before you begin

Ensure that you have the required permissions.

Procedure

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

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

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

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

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

      PSC must have a valid certificate.

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

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

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

   The system generates the certificate and adds vCenter.

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

Related links

Editing vCenter on page 100
Map vCenter field descriptions on page 101
New vCenter and Edit vCenter field descriptions on page 102

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ( ).
   - Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.
7. Click **Commit** to get an updated list of managed and unmanaged hosts.

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

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

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

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

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

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

Button	Description
Add	Displays the New vCenter page where you can add a new ESXi host.

Table continues…

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

New vCenter and Edit vCenter field descriptions

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

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

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Edit	The option to edit the location and host.

Table continues…

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

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** For Release 8.0.1, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.

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

Monitoring a host and virtual machine

Monitoring a platform

Procedure

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

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

Monitoring an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

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

Backup and restore

Creating a backup

Before you begin

Before creating a backup, ensure that the hostname string does not contain '_' (underscore) character in it. If the hostname with '_' character already exists, then change the hostname.

For more information about changing the hostname, see Changing the hostname on page 105.

Procedure

1. Log in to theCommunication Manager System Management Interface with administrator privilege user credentials.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Data Backup/Restore** > **Backup Now**.

   The system displays the Backup Now page.
4. Click **Full Backup**.
5. In the **Network Device** section, select the backup method and type the user name, password, hostname, and path of the directory in which you stored the data.
6. Click **Start Backup**.

   On the Backup Now Results page, the system displays the message `Backup Successfully Completed`.

Changing the hostname

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server Configuration** > **Network Configuration**. The system displays the Network Configuration page.
3. Enter the hostname and click **Change**.

Note:

If a backup is created with hostname containing '_' (underscore) character, then that backup will not get restored on any Communication Manager. Make sure, you have a valid hostname before creating a backup.

Restoring backup

Procedure

1. Log in to Communication Manager System Management Interface with admin credential.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Data Backup/Restore** > **View/Restore Data**.

   The system displays the View/Restore Data page.
4. In the **Network Device** section, perform the following to restore the data:
   a. Select the method to restore the data.
   b. In the **User Name** field, enter the user name.
   c. In the **Password** field, enter the password
   d. In the **Host Name** field, enter the host name.
   e. In the **Directory** field, enter the path for the directory.
5. Click **View**.

   The system displays the View/Restore Data Results page.
6. Click the `tar.gz` file.
7. Select **Force restore if server name mismatch**.
8. Click **Restore**.

   On the View/Restore Data Results page, the system displays the message `Restore Successfully Completed`.

Note:

As a result of full backup and restore, SSH Connectivity might be lost for cloud Instances and network configuration such as IP Address, Gateway, FQDN and, NAT in the IP link. Thus, full backup and restore is not recommended for Communication Manager cloud instances.

Chapter 5: Upgrading the application to Software-only environment

Migration path

You can migrate the application to Release 8.0.1 on Software-only environment from the following:

- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment or AWS.
- Release 6.x on VMware in customer-provided Virtualized Environment.
- Release 6.x on System Platform.
- Release 5.2.1 on Bare Metal (Appliance).
- Pre–5.2.1 Release on any offer.

Upgrading the application to Release 8.0.1 on Software-only environment using SMI

About this task

Use the procedure to upgrade the application from any earlier releases to Release 8.0.1 on Software-only environment by using the manual Backup-Restore process.

Before you begin

Ensure that you have,

- Installed the Red Hat Linux Version 7.4 on the target host. For more information, refer the "*Deploying Avaya Aura® Communication Manager* on Software-only environment" document.
- Run "Save Trans" utility using Communication Manager CLI before taking the backup.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.

2. Record the network parameters and system parameters, such as virtual FQDN (vFQDN), IP Address, and Netmask of the old system.
3. Create a backup of the system and copy to the remote server.
4. Deploy the Release 8.0 application on the Software-only environment.

   For information, see the "*Deploying Avaya Aura® Communication Manager* on Software-only environment" document.

   Important:

   You can use same network parameters and system parameters that you recorded on the older system or you can use different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the older system.
5. Log in to the new Communication Manager System Management Interface with admin credential.
6. Click **Administration** > **Server (Maintenance)**.
7. On the navigation bar, click **Miscellaneous** > **Download Files**.
8. Download the patch file using any of the following options:
   - File(s) to download from the machine I'm using to connect to the server: Select the desired patch file(s) from your local computer.
   - File(s) to download from the LAN using URL: Type the file names to download from the LAN and the **Proxy Server**.
9. Click **Download**.
10. Click **Server Upgrades** > **Manage Updates**.
11. Select the downloaded patch file(s) appearing in the **Update ID** column and click **Unpack**.
12. After unpacking, select the patch file(s) and click **Activate**.
13. To remove unnecessary files, select the required file(s) and click **Remove**.
14. Select the activated patch files and click **Commit**.

    The **Status** column of the selected patch files display as **activated**.
15. Configure the server.
16. Restore the data backup on the new system.
17. Verify the software version of the new system.

Upgrading the application to Release 8.0.1 on Software-only environment using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade the application from any earlier releases to Release 8.0.1 on Software-only environment by using System Manager Solution Deployment Manager.

Before you begin

Ensure that you have installed the Red Hat Linux Version 7.4 on the target host. For more information, refer the "*Deploying Avaya Aura® Communication Manager* on Software-only environment" document.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. On the navigation pane, click **Application Management**.
3. Add the host on which the old Communication Manager system is located.
4. Select the added host on the **Application Management Tree**, and select the Communication Manager application or any other element available on that host.
5. To establish trust, click **More Actions** > **Re-establish Connection**.

   Note:

   If there are multiple elements available on the host, you must repeat this step to establish trust for each of these elements.
6. On the navigation bar, click **Upgrade Management**.
7. Select the element(s) that you want to upgrade and perform the following steps:
   a. Click **Pre-upgrade Actions** > **Refresh Element(s)** and click **Schedule**.
   b. Click **Pre-upgrade Actions** > **Analyze** and click **Schedule**.
   c. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
   d. On the **Pre-upgrade Configuration** page, select **Target Platform** as Software Only and select the **Upgrade Source** where the application source file is located.

      Note:

      If you are upgrading to a different box, then select the relevant option available under **New Target Platform**.
8. Select the element(s) that you want to upgrade and click **Upgrade Actions** > **Upgrade/Update**.
9. On the **Upgrade Configuration** page, click **Edit** next to the element that you want to upgrade.

10. On the **Edit Upgrade Configuration** page, configure following options:
    - Select **ESXI/AVP host/Platform** as Software only.
    - Select **New Target ESXI/AVP host/Platform** if upgrading to a different box.
    - Select **Upgrade Source** which is the location where the application source file is located.
    - Select **Upgrade To**.
    - Select **Service/Feature Pack for auto-install after upgrade/migration** and provide the Release 8.0.1 patch file.
    - Enter details of **Existing Administrative User** and **Existing Administrative Password** and click **Pre-populate Data**.
    - Configure **Enhanced Access Security Gateway (EASG)**.
    - Enter details of **CM Privileged Administrator User Login** and **CM Privileged Administrator User Password** and click **Pre-populate Data**.
    - Select the **Enable Customer Root Account for this Application** check box.
    - Select the **Flexi Footprint**, **Datastore** and **End User License Agreement**.
    - Click **Save**.
11. Click **Upgrade**.

    The **Upgrade Job Details** page appears.
12. On the **Upgrade Job Details** page when the system displays the notification to install the platform/ host, configure the RHEL RPM on the target system.
13. On the navigation pane, click **Application Management**.
14. Add the host on which the new Communication Manager system should be located. If upgrading to the same box, then do not add the host.
15. On the **Add Platform** page, enter the **User Name**, **Password** and select the **Platform Type** as OS.
16. Click **Save**.
17. On the navigation bar, click **Upgrade Management**.
18. Select the element(s) that you want to upgrade and click **Upgrade Actions** > **Resume**.
19. On the **Resume Configuration** page, select **Target Platform**, **Upgrade Source**, **Upgrade/Update To**.
20. Click **Edit Credential** and provide the required credentials.
21. Click **Done** and **Schedule**.

Chapter 6: Upgrading the application to Virtual Appliance or VMware environment

Considerations for upgrading Communication Manager using full backup

Important:

When performing the full Backup on the existing Communication Manager server, write down the existing Communication Manager host name, DNS information, and the information listed below that you need to manually enter after restoring the backup.

1. When upgrading Communication Manager from 6.x or 7.x to 8.x, using the full backup, the system restores the configuration for the following:
   - **Accounts** (Logins, Profiles)
   - **Translations**
2. After a full backup upgrade of Communication Manager, the following must be manually configured using the Communication Manager System Management Interface:
   - **SNMP**
   - **Schedule Backup**
   - **Web Access Mask**
3. Manually configure the **SID** and **MID** fields of the server after the restore process. This is needed for the file sync to work between the Survivable Remote server, Survivable Core server and the Main server.
4. The **MID** field on the Survivable Remote server should be same as the Main server for the Survivable Remote server to register with the Main server.
5. For the Survivable Core server, both the **SID** and **MID** fields must be same as the Main server.
6. Manually configure the Customer options form on the SAT for:
   - **Multiple Location**
   - **Media Encryption**

- **Business Advocate**
- **Dynamic Advocate**

Note:

You also need to enable the above options in Communication Manager System Management Interface **License** page.

Upgrading Communication Manager using full backup

About this task

Use the following procedure to upgrade the new Communication Manager VMware virtual machine by taking a full backup of an existing Communication Manager VMware virtual machine.

Procedure

1. Deploy the new Communication Manager virtual machine on a host server.
2. Start the new Communication Manager virtual machine.
3. Take the full backup of the existing Communication Manager virtual machine.
4. Shutdown the existing Communication Manager virtual machine.
5. Log in to the new Communication Manager virtual machine console with admin credentials.
6. Administer the new Communication Manager virtual machine:
   a. Administer the network parameters.

      Note:

      Ensure that the host name and DNS information of the new Communication Manager is same as it was on the existing Communication Manager virtual machine.

   b. Apply the Communication Manager patch.
   c. Set the time zone.
   d. Set up the network time protocol.
   e. Add an suser account.
7. Restore the full backup on the new Communication Manager virtual machine.
8. Reboot the new Communication Manager virtual machine.
9. Log in to Communication Manager System Management Interface and configure the following if applicable:
   - SNMP
   - Schedule Backup

- Web Access Mask
- WebLM Server
- License Feature enablement
- SID/MID configuration

Note:

If required, at this point, the Communication Manager host name and DNS may be changed. This may require modification in WebLM if utilizing Centralized licensing.

Upgrading Avaya Aura® applications

Upgrade checklist for Avaya Aura® Virtual Appliance

This is a reference checklist for Virtual Appliance. For detailed steps, see the application specific upgrading guides.

Nos.	Tasks	Notes	✔
1	Download the OVA files, ISO files, and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at http://support.avaya.com. **Note:** For information about the upgrade sequence and the required patches, see the latest *Avaya Aura® Release Notes* for the specific release on the Avaya Support website.	-	
2	If you need to deploy or upgrade the System Manager, do the following: Download the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip` file from the Avaya Support website at http://support.avaya.com.	-	
3	Install the `Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe` file.	-	

Table continues…

Nos.	Tasks	Notes	✔
4	To upgrade on an Avaya-provided server, use Solution Deployment Manager client for Appliance Virtualization Platform.	-	
5	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 8.0 OVA file, and install the Release 8.0.1 bin file by using the Solution Deployment Manager client. • Available: Upgrade System Manager to 8.0 and install the Release 8.0.1 bin file.	-	
6	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	For more information, see “Discovering elements” in *Administering Avaya Aura® System Manager*	
7	Configure user settings.	For more information, see “User settings” in *Administering Avaya Aura® System Manager*	
8	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for TN Boards and media gateway upgrades is not supported.	For more information, see “User settings” in *Administering Avaya Aura® System Manager*	
9	Refresh the elements in the inventory.	For more information, see “Refreshing elements” in *Administering Avaya Aura® System Manager*	
10	Analyze the software.	For more information, see “Analyzing software” in *Administering Avaya Aura® System Manager*	
11	Perform the preupgrade check.	For more information, see “Performing the preupgrade check” in *Administering Avaya Aura® System Manager*	
12	Download the required firmware for the Avaya Aura® application upgrade.	For more information, see “Downloading the software” in *Administering Avaya Aura® System Manager*	
13	Perform the upgrade.	-	
14	Verify that the upgrade is successful.	-	

Upgrading Avaya Aura® applications to Release 8.0.1

About this task

The procedure covers upgrades on the same server and on a different server. Use the procedure to upgrade the supported Avaya Aura® applications to Release 8.0.1 from the following:

- Release 6.x running on System Platform or VMware-based virtualized environment.
- Release 7.x running on Appliance Virtualization Platform or VMware-based virtualized environment.
- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.

Before you begin

- From the Roles page, ensure that you set permissions that are required to perform all upgrade-related operations.
- Configure user settings.
- Complete all required operations up to the preupgrade check.
- To migrate the Avaya Aura® application from old server to ESXi host, add the new host in to Application Management.
- To migrate the Avaya Aura® application to a different server, add the Appliance Virtualization Platform host from the Application Management page.
- To upgrade from Release 6.x, ensure to add all elements in Manage Elements page available under **Inventory** tab. For example, if the Communication ManagerRelease 6.x server is on System Platform, add the System Platform, Utility Services and Communication Manager server.
- Ensure that elements that you want to upgrade are in sync with the elements displayed on the Upgrade Management page.
- Ensure to add old as well as the new server to start upgrading using System Manager Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the 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.
    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, perform the following:
   a. In **Service/Feature Pack for auto-install after migration**, provide the Release 8.0.1 patch file.
   b. Complete the details, and click **Save**.
8. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

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

   Note:

   - For Communication Manager, if you are editing the Utility Services for System Platform based system, then you must select the details as per the Utility Services. If you are upgrading Communication Manager which is not on System Platform, then select the details for the Communication Manager only.
   - To upgrade Communication Manager having duplex configuration, you must select the duplex related details.

9. Click **Save**.
10. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.

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

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

    For upgrades from Release 7.0.x running on a virtualized environment to Release 8.0.1, the field displays . This icon indicates that the upgrade is successful and awaiting commit or rollback.

16. For upgrades from Release 7.0.x running on a virtualized environment to Release 8.0.1, do the following:
    a. On the Upgrade Management page, select the element.
    b. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.

       The system displays the Job Schedule page.
    c. Select the action to be performed under the **Upgrade Action** column.
    d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.
    e. Click **Schedule**.
17. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
18. Verify that the upgrade of the application is successful.

    For upgrades on the same server, the system goes to the pause state.
19. For upgrades on the same server, perform the following:
    a. Install the Appliance Virtualization Platform host.
    b. From the Application 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 133
Edit Upgrade Configuration field descriptions on page 134

Upgrading duplex Communication Manager

About this task

You can migrate duplex Communication Manager system using these steps.

Procedure

1. Prepare the Communication Manager server.

2. Migrate the standby Communication Manager server.

   Note:

   For migration to software-only environment, refer the section “Upgrading the application to Software-only environment”.

3. Interchange the roles of Communication Manager systems.
4. Migrate the active Communication Manager.
5. Change the roles of two Communication Manager systems to the original state.

Related links

Preparing the duplex Communication Manager server on page 118
Migrating duplex Communication Manager on the same server on page 119
Migrating duplex Communication Manager on a different server on page 121

Preparing the duplex Communication Manager server

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 the 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 the Communication Manager systems, if the 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`.

Related links

Upgrading duplex Communication Manager on page 117

Migrating duplex Communication Manager on the same server

Before you begin

Ensure that:

- The duplex Communication Manager is prepared for migration.
- The server that you are going to upgrade is in maintenance mode. For that, log in to the command line interface of the server, and then type the command `server –b`.

Procedure

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

      After the second analyze operation, the status column displays **Ready for Upgrade**.
   d. Select the standby Communication Manager or System Platform and click **Upgrade Actions** > **Upgrade/Update**.
   e. On the Upgrade Configuration page, click **Edit**.
   f. Schedule the upgrade of the standby Communication Manager.
   g. On the Upgrade Management page, in the **Release Status** column, verify that the status is **Paused**.

      Note:

      This step is applicable for System Platform to Appliance Virtualization Platform migration until you ‘Resume’ the upgrade process.
   h. For Avaya provided server in Avaya Aura® Virtualized Appliance environment, install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from Application 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 to 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 SMI, 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 8.0.1 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 navigation pane, click **Upgrade Management**.
    c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

        After the second analyze operation, the status column displays **Ready for Upgrade**.
    d. Click **Upgrade Actions** > **Upgrade/Update**.
    e. On the Upgrade Configuration page, click **Edit**.
    f. Schedule the upgrade of Communication Manager.
    g. On the Upgrade Management page, in the **Release Status** column, verify that the status is **Paused**.
    h. For Avaya provided server in Avaya Aura® Virtualized Appliance environment, install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from Application 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 SMI, 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.

Related links

Upgrading duplex Communication Manager on page 117

Migrating duplex Communication Manager on a different server

Before you begin

Ensure that:

- The duplex Communication Manager is prepared for migration.
- The server that you are going to upgrade is in maintenance mode. For that, log in to the command line interface of the server, and then type the command `server –b`.

Procedure

1. Start upgrading the standby Communication Manager using following steps:

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

   b. In the navigation pane, click **Upgrade Management**.

   c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

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

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

e. On the Upgrade Configuration page, click **Edit**.

f. On the Edit Upgrade Configuration page, provide the mandatory parameters along with target host information, latest patch file and credentials.

g. Complete the details, and click **Save**.

h. Schedule the upgrade of the standby Communication Manager.

i. Check the job status for upgrade job.

The system upgrades the standby Communication Manager to the latest release, and restores the data on the same Communication Manager 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 SMI, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

- **Network Configuration**
- **Duplication Parameters**
- **Server role**

c. To release the server busy out state, from the command line interface of the standby Communication Manager, type `server -r`.

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

3. To busy out the server, from the active Communication Manager command line interface, type `server -if`.

4. Verify that all elements associated with Communication Manager, such as TN Boards, media gateways, and media modules get registered with the new active server and the calls get processed with the new active server.

5. Start upgrading the Communication Manager that was active earlier using following steps:

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

b. In the navigation pane, click **Upgrade Management**.

c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the Communication Manager server.

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

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

e. On the Upgrade Configuration page, click **Edit**.

f. On the Edit Upgrade Configuration page, provide the mandatory parameters along with target host information, latest patch file and credentials.

g. Complete the details, and click **Save**.

h. Schedule the upgrade of the active Communication Manager.

i. Check the job status for upgrade job.

The system upgrades the active Communication Manager to the latest release, restores the data, and installs the feature pack file that you uploaded corresponding to the latest feature pack release.

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

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

b. On Communication Manager SMI, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

- **Network Configuration**
- **Duplication Parameters**
- **Server role**

c. To release the server busy out state, from the command line interface of the standby Communication Manager, type `server -r`.

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

d. To interchange the roles of standby and active Communication Manager servers, from the command line interface of the active Communication Manager server, type `server -i`.

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

Related links

Upgrading duplex Communication Manager on page 117

Upgrading ESS and LSP servers

About this task

You can upgrade ESS and LSP servers using the following steps.

Procedure

1. Prepare the Communication Manager server.

Note:

For server preparation related steps, refer the section on duplex Communication Manager.

2. Migrate the standby Communication Manager server.

Note:

For migration steps, refer the section ”Upgrading Avaya Aura applications to Release 8.0.1”.

3. Interchange the roles of Communication Manager systems.
4. Migrate the active Communication Manager.
5. Change the roles of two Communication Manager systems to the original state.

Installing software patches

About this task

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

Note:

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

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

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.

6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

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

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

    Note:

    - For Communication Manager, if you are editing the Utility Services for System Platform based system, then you must select the details as per the Utility Services. If you are upgrading Communication Manager which is not on System Platform, then select the details for the Communication Manager only.
    - To upgrade Communication Manager having duplex configuration, you must select the duplex related details.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

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

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

    When the update is complete, the **Update status** and **Last Action Status** fields displays .
16. Click **Upgrade Actions** > **Installed Patches**.

17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

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

19. Click **Schedule**.

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

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

    Note:

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

Related links

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 166
Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 167
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 133
Edit Upgrade Configuration field descriptions on page 134
Installed Patches field descriptions on page 129

Installing custom software patches

About this task

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

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

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

- WebLM
- Application Enablement Services

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

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

    Note:

    - For Communication Manager, if you are editing the Utility Services for System Platform based system, then you must select the details as per the Utility Services. If you are upgrading Communication Manager which is not on System Platform, then select the details for the Communication Manager only.
    - To upgrade Communication Manager having duplex configuration, you must select the duplex related details.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .

16. To view the update status, click .

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

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

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

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

19. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

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

20. Click **Schedule**.

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

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

    Note:

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

Next steps

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

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

Related links

Uploading a custom patch on page 142
Uploading custom patch field descriptions on page 142

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.

Table continues…

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

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

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.

Table continues…

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

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/Rollback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download > **Download**	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Download > **AVP Bulk Import Template**	Downloads the `AVP_Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.

Table continues…

Button	Description
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, CommunicationManager_123.
Type	The device type.
IP Address	The IP Address of the device.
Current Version	The release status of the device.
Override Preupgrade Check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system ignores any recommendations during upgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. • : Configuration incomplete. • : Configuration complete.

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

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

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

Element Configuration: General Configuration Details

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

Table continues…

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

Element Configuration: Upgrade Configuration Details

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

Name	Description
Auto Commit	The option to automatically commit the upgrade.
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. For Communication Manager Messaging, the button is unavailable and you must fill in all details. For Communication Manager Messaging you must provide a new IP address.
CM IPv4 Address	The IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	The network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The default gateway of the Communication Manager virtual machine.

Table continues…

Name	Description
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine.
CM IPv6 Gateway	The IPv6 default gateway of the Communication Manager virtual machine.
Out of Band Management IPv4 Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnetwork mask of the virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management IPv6 Network Prefix	The IPv6 network prefix of the virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.

Table continues…

Name	Description
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Services	The port number that is assigned to the services port. The system displays this field when Utility Services is available.
Duplication link	The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process. The field is available only for the Communication Manager duplex configuration and when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

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

Name	Description
Existing Administrative User	The user name of the administrator.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields.
IP Address	The IP address of the virtual machine.
Short Hostname	The hostname of the virtual machine. The hostname of the server and is often aligned with the DNS name of the server.
Network Domain	The domain name of the virtual machine.
Netmask	The network mask of the virtual machine.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.

Table continues…

Name	Description
Timezone	The timezone of the virtual machine.
Login Name	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Enter Customer Account Password	Password to log on to the system.
Primary System Manager IP	The IP address of System Manager.
Enrollment Password	The password that is required to establish trust between System Manager and Session Manager.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: End User License Agreement

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

AVP Configuration: Existing Machine Details

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

Table continues…

Name	Description
Source Root User	The source user name with appropriate root privileges.
Source Root Password	The source password of the root.

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com

Table continues…

Name	Description
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

Table continues…

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

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

Uploading a custom patch

About this task

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

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

Procedure

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

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

Uploading custom patch field descriptions

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

Table continues…

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

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

Upgrading Communication Manager using System Management Interface

Upgrading Communication Manager from pre–5.2.1 to Release 8.0.1

About this task

This procedure is applicable if you are upgrading from Communication Manager 3.x or 4.x or 5.0.x or 5.1.x to Communication Manager Release 8.0.1.

Procedure

1. Log in to the existing Communication Manager web console.
2. In the **Disk Backup/Restore** section, click **Backup Now**.
3. Select **Specify Data Sets**, and choose **Avaya Call Processing (ACP) Translations** and **Save ACP translations prior to backup**.

4. Under **Backup Method**, enter the login credentials, and IP address of the server where you want to backup the data.
5. Click **Start Backup**, and wait until the backup successful message appears.
6. Deploy Communication Manager Release 8.0 application on the new system.

   For instructions, see *Deploying Avaya Aura® Communication Manager* document.
7. If you are using the same Hostname and IP address of the previous system, shut down the previous system and start the new system.
8. Log in to the new Communication Manager SMI.
9. Click **Administration** > **Server (Maintenance)**.
10. On the navigation bar, click **Miscellaneous** > **Download Files**.
11. Download the patch file using any of the following options:
    - File(s) to download from the machine I'm using to connect to the server: Select the desired patch file(s) from your local computer.
    - File(s) to download from the LAN using URL: Type the file names to download from the LAN and the **Proxy Server**.
12. Click **Download**.
13. Click **Server Upgrades** > **Manage Updates**.
14. Select the downloaded patch file(s) appearing in the **Update ID** column and click **Unpack**.
15. After unpacking, select the patch file(s) and click **Activate**.
16. To remove unnecessary files, select the required file(s) and click **Remove**.
17. Select the activated patch files and click **Commit**.

    The **Status** column of the selected patch files display as **activated**.
18. Click **Administration** > **Server (Maintenance)**.
19. In the **Data Backup/Restore** section, click **View/Restore Data**.
20. Select the restore method and provide the server details where the backup is stored, as mentioned in step 4.
21. Click **View** and verify that the system displays the backup tar.gz file.
22. If the host name is different on the new system than that of the old system, select **Force restore if there is a server name mismatch or the server migration**.
23. Click Restore, and wait for the Restore Successful message.
24. Restart Communication Manager.
25. Access the Communication Manager System Access Terminal (SAT).
26. Verify that expected Communication Manager translations are present.

Next steps

You must configure the following Operating System related data on the new Communication Manager system:

- All customer created Linux users can be noted or copied from the old system and must be recreated manually (the /etc/passed file lists all logins) on the new system. The user login details are available at `/etc/passed` file.
- Manually copy all cron jobs by using the **`crontabl -l`** CLI command on the old system and reconfigure them on the new system using the **`crontabl -l`** CLI command.
- Since 6.3.1xx and 7.x systems use Net-SNMP, you must re-configure SNMP.
- All other customizations.

Note:

- Ensure that a new license file is installed.
- Communication Manager 7.1 and above does not require an authentication file.
- If using a different IP Address, all of the Media Gateways need to be reconfigured with the new MGC IP. This applies to other integrating products as well.
- Communication Manager 7.1 and above includes EASG.

Migrating from Communication Manager Release 5.2.1 using SMI

About this task

Use this procedure to migrate from the Communication Manager Release 5.2.1 to Communication Manager Release 8.0.1.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.
2. Take full backup from the Communication Manager Release 5.2.1 System Management Interface page.
3. Deploy and apply the patch to upgrade AVP and AVP Utilities to Release 8.0.1.

   For detailed description, see the deploying and upgrading documents of corresponding products.
4. Deploy the Communication Manager Release 8.0 application on the new system.
5. Log in to the new Communication Manager SMI.
6. Install and activate the Release 8.0.1 patch on the new system.
7. Restore the full backup data on the new Communication Manager system.
8. Open a SAT session and restart the new Communication Manager server.

Next steps

Ensure that you run the post upgrade process after the above steps are performed.

Upgrading Communication Manager 6.x to VMware

Before you begin

VMware is not supported on the S8300D server if migrating to the Avaya Aura® Virtualized Appliance environment. Therefore, you must upgrade to Communication Manager on System Platform. You must upgrade survivable remote servers to System Platform 6.2.1.0.9 or later before you can upgrade the Communication Manager template to the survivable embedded remote template. Survivable servers must have the same version or later than the main server.

Important:

Ensure the survivable remote server has the same version as the Communication Manager virtual application version. The survivable remote version must remain at Release 6.2. Use the 6.2 media if you must update the version.

Procedure

1. Go to http://support.avaya.com and search for the *Migrating from Avaya Aura® Communication Manager 6.x to VMware® Workbook* and download it. In the Security Warning dialog box, click **Enable Macros**.
2. Record the required Communication Manager data in the workbook.
3. Navigate to the Communication Manager SMI page of the existing main Communication Manager server.
4. Backup the existing translations from the SMI page:
   - Communication Manager 6.x translation files
   - Utility Services translations files if applicable. Utility Services is only available in 6.2 and later. For instructions to create a backup, see the Utility Services deployment guide.
5. If using Utility Services 6.1:
   a. Note the DHCP server settings if in use.
   b. Note any special firmware that has been loaded and ensure that you have a copy of the firmware that you must upload to the new server. The firmware includes Branch Gateway, ADVD, and IP phone firmware.
   c. Note the Communication Manager server IP address, login, and password so Utility Services can interrogate the system to understand the IP phone firmware.
6. Download and install the following virtual application OVA files.
   - Communication Manager

     See the appropriate deployment guide for downloading and installing the virtual application OVA file.
   - Utility Services if applicable
   - WebLM if applicable

- Secure Access Link. You do not require if a standalone SAL Gateway exists

Note:

Do not turn on the applications.

7. If SAL is in use on System Platform:
   a. Log in to the SAL Gateway.
   b. Capture settings using screen capture.
8. Turn off the existing server.
9. If a Standalone SAL Gateway is *not* in place, turn on and configure the SAL virtual application. Reuse the details on the screen captures from the existing SAL Gateway.
10. Turn on the following virtual applications:
    - Communication Manager. Provision the initial IP address as required by the deployment guide.
    - Utility Services if applicable
    - WebLM if applicable
11. Download and activate the latest Communication Manager service pack.
12. Navigate to SMI of Communication Manager and perform the following:
    a. Set the date and time.
    b. Set the NTP. You must reboot to synchronize all processes to NTP.
    c. Add a superuser login.
    d. Restore existing Communication Manager call processing translations (XLN file only). Re-enter the SNMP data if required.
    e. Click **Administration** > **Licensing** > **WebLM Configuration,** and retranslate the WebLM server destination if applicable.
13. Restore Utility Services 6.2 and later or retranslate Utility Services as applicable.
14. Retranslate the Utility Services server destination if applicable.
15. Set up System Manager or WebLM as applicable to provide licensing support for Communication Manager.

    You cannot use the MAC address from the previously used server. See the appropriate deployment guide for the licensing procedures. You require a new PLDS license. Log in to WebLM and click **Properties** to get the MAC address information or equivalent.
16. Complete the SAL registration spreadsheet in the migration workbook.
17. Reregister Communication Manager as a virtual application.
18. Avaya Registration Team must perform the following:
    a. Remove records for Communication Manager as System Platform.

b. Add records.

19. Verify the SAL connectivity after the new SAL Gateway starts communicating with the data center.
20. Test an alarm and verify that the alarming is working properly.
21. Verify the survivability with existing survivable servers.
22. If System Platform used multiple SAL Gateways before the upgrade, and you require to consolidate SAL Gateways into a single SAL Gateway virtual application, perform the following steps:
    a. Choose settings for one SAL Gateway virtual application that carries forward. Make a screen capture of the administration settings and export managed elements for the primary SAL Gateway.
    b. Export managed elements for each existing System Platform-based SAL Gateway to the virtual application-based SAL Gateway.
    c. Update the virtual SEID and Product IDs for each System Platform-based SAL Gateway that is no longer used.
23. Remove the Ethernet cables from the decommissioned server as a network safety measure.

    If IP addresses were reused, the pre-VMware Communication Manager environment cannot be running on the customer's network at the same time as the VMware-based Communication Manager.
24. Determine the disposition of the server on which applications were previously running. The server cannot be reused for any other Avaya applications unless the server has the same comcode as the Communication Manager server. If the server will not be used, submit the appropriate forms to the Avaya Customer Care Center to remove the server from the installed base record.
    - For Avaya personnel, the forms can be found at Avaya Personnel Forms.
    - For Business Partners, the forms can be found at Business Partner Forms.
25. Remove the physical server from the maintenance contract if it is no longer utilized. The customer contacts the Avaya Customer Care Center and requests removal from the installed base record of the Functional Location (FL). The adjustment becomes effective with the next contract renewal or true-up because the contract is prepaid by the customer.

    For Duplex Communication Manager, configure Duplication parameters using Communication Manager System Management Interface.

Migrating from Communication Manager Release 6.3 using SMI

About this task

Use this procedure to migrate from the Communication Manager Release 6.3 to Communication Manager Release 8.0.1.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.
2. Take full backup of Communication Manager Release 6.3 from the System Management Interface page.
3. Deploy and apply the patch to upgrade AVP and AVP Utilities to Release 8.0.1.

   For detailed description, see the deploying and upgrading documents of corresponding products.
4. Deploy the Communication Manager Release 8.0 application on the new system.
5. Log in to the new Communication Manager SMI.
6. Install and activate the Release 8.0.1 patch on the new system.
7. Restore the full backup on the Communication Manager system.
8. Open a SAT session and restart the new Communication Manager server.

Next steps

Ensure that you run the post upgrade process after the above steps are performed.

Upgrade job status

Upgrade job status

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

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

Viewing the Upgrade job status

Procedure

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

   The system displays the Upgrade Job Status page.

Editing an upgrade job

Before you begin

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

Procedure

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

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

Deleting the Upgrade jobs

Procedure

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

   The system updates the Upgrade Job Status page.

Upgrade Job Status field descriptions

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

Button	Description
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Support for Enhanced Access Security Gateway

Communication Manager supports Enhanced Access Security Gateway (EASG). EASG is a certificate based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provides support and troubleshooting.

EASG provides a secure method for Avaya services personnel to access the Communication Manager remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to

enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck. EASG must be enabled for Avaya Services to perform the required maintenance tasks.

You can enable or disable EASG through Communication Manager.

EASG only supports Avaya services logins, such as init, inads, and craft.

Discontinuance of ASG and ASG-enabled logins

EASG in Communication Manager 7.1.1 and later replaces Avaya's older ASG feature. In the older ASG, Communication Manager allowed the creation of ASG-enabled user logins through the SMI Administrator Accounts web page. Such logins are no longer supported in Communication Manager 7.1.1 and later. When upgrading to Communication Manager 7.1.1 or later from older releases, Communication Manager does not support ASG-enabled logins.

For more information about EASG, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Enabling or disabling EASG through the CLI interface

About this task

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

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

Procedure

1. Log in to the Communication Manager CLI interface as an administrator.
2. To check the status of EASG, run the following command: `EASGStatus`.
3. To enable EASG (Recommended), run the following command: `EASGManage --enableEASG`.
4. To disable EASG, run the following command: `EASGManage --disableEASG`.

Enabling or disabling EASG through the SMI interface

About this task

By enabling Avaya Services Logins you are granting Avaya access to your system. This setting is required to maximize the performance and value of your Avaya support entitlements, allowing

Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com for Avaya remote connectivity. See the Avaya support site support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Services Logins you are denying Avaya access to your system. This setting is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

Procedure

1. Log on to the Communication Manager SMI interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the **Security** section, click **Server Access**.
4. In the **Avaya Services Access via EASG** field, select:
   - **Enable** to enable EASG.
   - **Disable** to disable EASG.
5. Click **Submit**.

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Communication Manager CLI interface.
2. Run the following command: `EASGProductCert --certInfo`.

EASG product certificate expiration

Communication Manager raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. Log in to the CLI interface as an administrator.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.

- `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Chapter 7: Upgrading the application to KVM environment

Migration path

You can migrate the application to Release 8.0.1 on KVM from the following:

- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- Release 6.x on VMware in customer-provided Virtualized Environment.
- Release 6.x on System Platform.

Upgrading the application to Release 8.0.1 on KVM

About this task

Use the procedure to upgrade the application from any earlier releases to Release 8.0.1 on KVM.

Before you begin

Ensure that you have,

- Downloaded the required software files.
- Run “Save Trans” utility using Communication Manager CLI before taking the backup.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.
2. Record the network parameters and system parameters, such as virtual FQDN (vFQDN), IP Address, and Netmask of the old system.
3. Create a backup of the system and copy to the remote server.
4. Deploy the Release 8.0 application on KVM environment.

If you are using the Release 8.0 OVA application for KVM environment, see the "*Deploying Avaya Aura® Communication Manager* on Virtualized Environment" document.

If you are using the Release 8.0 ISO application for KVM environment, see the "*Deploying Avaya Aura® Communication Manager* on Software-only Environment" document.

Important:

You can use the same network parameters and system parameters that you recorded on the old system or you can use the different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the old system.

5. Log in to the new Communication Manager System Management Interface with admin credential.
6. Click **Administration** > **Server (Maintenance)**.
7. On the navigation bar, click **Miscellaneous** > **Download Files**.
8. Download the patch file using any of the following options:
   - File(s) to download from the machine I'm using to connect to the server: Select the desired patch file(s) from your local computer.
   - File(s) to download from the LAN using URL: Type the file names to download from the LAN and the **Proxy Server**.
9. Click **Download**.
10. Click **Server Upgrades** > **Manage Updates**.
11. Select the downloaded patch file(s) appearing in the **Update ID** column and click **Unpack**.
12. After unpacking, select the patch file(s) and click **Activate**.
13. To remove unnecessary files, select the required file(s) and click **Remove**.
14. Select the activated patch files and click **Commit**.

    The **Status** column of the selected patch files display as **activated**.
15. Configure the server.
16. Restore the data backup on the new system.
17. Verify the software version of the new system.

License management

Following are the use cases for managing licenses when a KVM supported application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 7.1.1 and later, KVM supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, but only the KVM supported applications move to KVM, then you do not have to regenerate the license for those applications that move to KVM.
- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to KVM, then all the licenses need to migrate to the centralized System Manager Release 7.1.1 and later with integrated WebLM in KVM and the supported KVM applications that move need to regenerate the license files.

Chapter 8: Upgrading the application to IaaS environment

Upgrade path for AWS

You can upgrade to Communication Manager Release 8.0.1 on AWS from the following:

- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on AWS.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- Release 6.x on VMware in customer-provided Virtualized Environment.
- Release 6.x on System Platform.
- Release 5.2.1 on Bare Metal (Appliance).
- Pre–5.2.1 Release on any offer.

Upgrade path for Google Cloud Network

You can upgrade to Communication Manager Release 8.0.1 on Google Cloud Network from the following:

- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on AWS.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- Release 6.x on VMware in customer-provided Virtualized Environment.
- Release 6.x on System Platform.

- Release 5.2.1 on Bare Metal (Appliance).
- Pre–5.2.1 Release on any offer.

Upgrade path for Microsoft Azure

You can upgrade to Communication Manager Release 8.0.1 on Microsoft Azure from the following:

- Release 8.0 on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- Release 7.x on AWS.
- Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- Release 6.x on VMware in customer-provided Virtualized Environment.
- Release 6.x on System Platform.
- Release 5.2.1 on Bare Metal (Appliance).
- Pre–5.2.1 Release on any offer.

Upgrading the application to Release 8.0.1 on IaaS

About this task

Use the procedure to upgrade the application from any earlier releases to Release 8.0.1 on IaaS.

Before you begin

Ensure that you have,

- Downloaded the required software files.
- Run “Save Trans” utility using Communication Manager CLI before taking the backup.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.
2. Create a backup of the system and copy to the remote server.
3. Deploy the Release 8.0 application on the IaaS environment that you are using as the target platform.

   If you are using the OVA application to deploy on AWS, see AWS specific section in the “*Deploying Avaya Aura® Communication Manager* on Infrastructure as a Service environment” document.

If you are using the ISO application, see the relevant environment specific section in "*Deploying Avaya Aura® Communication Manager* on Software-only environment" document.

4. Log in to the new Communication Manager System Management Interface with admin credentials.
5. Click **Administration** > **Server (Maintenance)**.
6. On the navigation bar, click **Miscellaneous** > **Download Files**.
7. Download the patch file using any of the following options:
   - File(s) to download from the machine I'm using to connect to the server: Select the desired patch file(s) from your local computer.
   - File(s) to download from the LAN using URL: Type the file names to download from the LAN and the **Proxy Server**.
8. Click **Download**.
9. Click **Server Upgrades** > **Manage Updates**.
10. Select the downloaded patch file(s) appearing in the **Update ID** column and click **Unpack**.
11. After unpacking, select the patch file(s) and click **Activate**.
12. To remove unnecessary files, select the required file(s) and click **Remove**.
13. Select the activated patch files and click **Commit**.

    The **Status** column of the selected patch files display as **activated**.
14. Configure the server.
15. Restore the data backup on the new system.
16. Verify the software version of the new system.

License management

Following are the use cases for managing licenses when an AWS supported application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 8.0, AWS supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, but

only the AWS supported applications move to AWS, then you do not have to regenerate the license for those applications that move to AWS.

- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to AWS, then all the licenses need to migrate to the centralized System Manager Release 8.0 with integrated WebLM in AWS and the supported AWS applications that move need to regenerate the license files.

Chapter 9: Postupgrade process

Connecting the services computer to the server

Procedure

Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible web browser.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Enhanced Access Security Gateway (EASG), you must have an EASG tool to generate a response for the challenge that the Logon page generates.

5. Click **Continue**.
6. Type the password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

Enabling the scheduled maintenance

About this task

Use the procedure to schedule daily maintenance.

Procedure

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

Entering initial system translations

Before you begin

- Prepare the initial translations offsite and save the translations in the translation file.
- Store the translation file in the `/etc/opt/defty` folder with *xln1* and *xln2* file names.

  Alternatively, you can save the full backup of a system in a translation file, and restore the files on another system.

Procedure

1. Log in to the Communication Manager CLI as a root user.

2. If the system translations are prepared offsite, install the prepared translations, and reset Communication Manager using the command **`reset system 4`** or **`drestart 1 4`**.
3. If translations are not prepared offsite:
   a. Type **`save translation`** and press `Enter` to save the translations to the hard disk drive.
   b. Type **`reset system 4`** or **`drestart 1 4`** and press `Enter`.
4. Enter minimal translations to verify connectivity to the port networks or media gateway.
5. After you enter the translations, type **`save translation`**, and press `Enter` to save the translations to the hard disk drive.

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

1. Enter `save translation all`.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.
2. At the command prompt, enter `filesync -Q all`.

   Verify that the system displays the filesync errors, if any.

Resolving alarms

Before you begin

Log on to System Management Interface.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
3. In the **Server Alarms** section, select the alarms that you must clear.

4. Click **Clear**.
5. To resolve new alarms after the server upgrade, use a SAT session.

   For more information, see:

   - *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431
   - *Avaya Aura® Communication Manager Server Alarms*, 03-602798

Logging off from all administration applications

Procedure

When you complete all administration activities, log off from all applications that you used.

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Deleting the virtual machine snapshot

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`
2. To log in to the Appliance Virtualization Platform host, provide the credentials.
3. In the left navigation pane, click **Virtual Machines**.
4. Select the virtual machine, click **Actions** > **Snapshots** > **Manage snapshots**.

   The system displays the Manage snapshots - <Virtual machine name> dialog box.
5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.

Deleting the virtual machine snapshot from the vCenter managed host or standalone host

Procedure

1. Log in to the vSphere Web client for the vCenter managed host or the standalone host.
2. Depending on the host, perform one of the following
   a. On the vCenter managed host, select the host, and then select the virtual machine.
   b. On the Standalone host, select the virtual machine.
3. Right-click the selected virtual machine, click **Snapshot** > **Snapshot Manager**.

   The system displays the Snapshot for the <Virtual machine name> dialog box.
4. Select the snapshot and click **Delete**.

   The system deletes the selected snapshot.

Chapter 10: Rollback process

Upgrade rollback

The Admin specifies the rollback in two cases:

- Upgrade process of an element fails: Admin need not rollback upgrade of all the elements. When the element upgrade fails, the system stops the entire upgrade process and displays the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- Upgrade process of the entire system fails: Admin specifies rollback all when the system upgrade fails. The system stops the upgrade and rolls back the overall upgrade process.

Rolling back an upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.

   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message `Selected System Platform or child of System Platform, and System Platform and all child applications.`
4. Click **Upgrade Actions** > **Rollback**.

Chapter 11: Resources

Communication Manager documentation

The following table lists the documents related to Communication Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers, and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware and Kernel-based Virtual Machine (KVM).	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Virtual Appliance	Describes the implementation instructions while deploying Communication Manager on Appliance Virtualization Platform.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment	Describes the implementation instructions while deploying Communication Manager on Amazon Web Services, Microsoft Azure, Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only Environment	Describes the implementation instructions while deploying Communication Manager on a software-only environment.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that are requested by specific customers for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

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

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

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.

4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

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

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/.

Important:

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

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

Navigate to the **My Content** > **Watch list** menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

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

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

Note:

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

Training

The following courses are available on the Avaya Learning website at 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
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura® Release 8.0
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.0
21450V	Administering Avaya Aura® Communication Manager Release 8.0

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos` 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 do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click 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 https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

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

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

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

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

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

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

Appendix A: OS-level logins for Communication Manager

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

- **root:** A default user login that cannot be removed . By default, a root user has complete access.
- **sroot:** A root-level user login that is used by Avaya Services. The init, inads, craft, and rasaccess users are also Avaya services logins that are equivalent to customer super-users in CM. These logins (including sroot) can be removed if desired, but that does make the system difficult for services to troubleshoot should the need the arise.

  Note:

  Sroot and root cannot login directly from either SSH or the web GUI.
- **acpsnmp:** acpsnmp user is used internally by Communication Manager to handle SNMP-related tasks. As you can see, it has a shell of /sbin/nologin and cannot login on the Web or via SSH. It has customer super-user access because it needs to perform administration operations. This user cannot be deleted, nor can the password be changed (it doesn't have a password anyway).
- **csadmin:** csadmin is used by the System Manager orchestration software in Solution Deployment Manager to perform upgrades and other maintenance that is required. This login is a customer super-user that should not be removed in order to allow Solution Deployment Manager to continue working.
- **init, inads, rasaccess, craft, and csadmin:** Users with these users logins cannot change their passwords. The csadmin login user will use keys, and the other users are protected by EASG challenge-response logins.

Warning:

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

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

Glossary

Fully automated upgrade	The fully automated upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor by using either Solution Deployment Manager Client or System Manager Solution Deployment Manager. In fully automated upgrade all subsequent steps are executed as a single process, including tasks such as backup, upgrade, restore and post upgrade tasks such as applying patches or service packs.
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

7.0 133

A

aborting
  virtual machine report generation 94
accessing port matrix 171
access Solution Deployment Manager 35
access Solution Deployment Manager client 34
activate SSH from AVP Utilities 56
adding
  Appliance Virtualization Platform host 40
  AVP host 40
  ESXi host 40
  location 38
  software-only platform 42
  vCenter to SDM 99
adding certificates
  available hosts 97
  existing hosts 97
  migrated hosts 97
adding ESXi host 40
adding location 38
adding location to host 100
adding vCenter to SDM 99
Add Platform 68
AES upgrade 115
analyze job status 149
Appliance Virtualization Host
  configure login banner 62
  push login banner 62
Appliance Virtualization Platform 50, 57, 69
  change password 53
  generating kickstart file 53
  license file 59
  restarting 62
  shutting down 61
  update 43, 71
  WebLM Configuration 59
Appliance Virtualization Platform host Gateway
  change 49
  edit 49
Appliance Virtualization Platform host IP address
  change 49
  edit 49
Appliance Virtualization Platform host password
  changing 52
Appliance Virtualization Platform network parameters 49
application
  deleting 80
  edit 79
application *(continued)*
  monitoring 104
  re-establishing trust 76
  restart 81
  start 81
  stop 81
Application Deployment
  field descriptions 82
Application Enablement Services upgrade 115
Application management 37
applications
  log off 166
applying
  third-party certificates to Appliance Virtualization Platform 63
Avaya Aura application
  Services Port static routing update 80
Avaya Aura application upgrade 130
Avaya courses 173
Avaya support website support 174
AVP license status 61

B

backup
  restore 105
Branch Session Manager upgrade 115
browser requirements 24
bulk upgrade
  Utility Services to AVP Utilities 46
busying out
  busied-out equipment 164
busying out previously busied-out equipment 164

C

capabilities
  Solution Deployment Manager client 19
certificates
  accepting 96
  generating 96
certificate update
  ESXi host 97
  vCenter 97
  VMware documentation 97
Certification
  validation 95
Certification validation 95
change
  Appliance Virtualization Platform host IP address 49
  Host/ IP Settings 50
  hostname 105
  network settings 69

change *(continued)*
Network Settings ... 50
Change Gateway ... 68
change IP address for AVP host ... 49
Change IP FQDN ... 79
change Netmask for Appliance Virtualization Platform host 49
Change Network Params ... 49
changing
IP address and default gateway ... 58
changing the Appliance Virtualization Platform host password ... 52
checklist
Branch Session Manager upgrade ... 113
Session Manager upgrade ... 113
collection
delete ... 172
edit name ... 172
generating PDF ... 172
sharing content ... 172
common causes
application deployment failure ... 82
Communication Manager ... 22
license file ... 15
migrate to Virtualized Environment ... 146
upgrade ... 29
upgrades ... 10
Communication Manager update ... 76, 124, 126
Communication Manager upgrade ... 115
Communication Manager upgrade from Software Management ... 13
Communication Manager upgrade from System Manager ... 13
Communication Manager upgrade paths ... 10
Communication Manager upgrades
footprints ... 24
profile map ... 24
Configuration and Network Parameters
AVP Utilities ... 88
Communication Manager ... 82
Communication Manager Messaging ... 88
configure
login banner on host ... 62
configuring
WebLM Server on Appliance Virtualization Platform ... 60
connect service computer to server ... 163
considerations for upgrading Communication Manager using full backup ... 111
content
publishing PDF output ... 172
searching ... 172
sharing ... 172
watching for updates ... 172
correcting ESXi host certificate ... 97
create
virtual machine ... 74
creating
backup ... 104
generic CSR ... 65
creating a role in vCenter ... 98
CSR
create field description ... 66
edit field description ... 66
custom patch
upload ... 142

D

data migration prerequisites ... 21
deleting
application ... 80
location ... 39
snapshot from standalone host ... 167
upgrade jobs ... 150
deleting a location ... 39
deleting vCenter ... 100
deploy
Branch Session Manager ... 74
Communication Manager ... 74
Session Manager ... 74
System Manager ... 74
Utility Services ... 74
deploy application ... 37
deploy Avaya Aura application ... 74
deploying
AVP Utilities ... 72
deploy OVA ... 74
different server migration ... 121
disabling
SSH on Appliance Virtualization Platform ... 56
disabling SSH ... 57
disconnecting
from the server ... 166
documentation
Communication Manager ... 169
documentation portal ... 172
finding content ... 172
navigation ... 172
download manager
uploading custom patch ... 142
download software ... 71
duplex Communication Manager
migration ... 117, 118
preparation ... 117, 118
upgrading ... 117
duplex system ... 119, 121
duplication parameters ... 117–119, 121

E

EASG ... 151
disabling ... 152
enabling ... 152
SMI ... 152
EASG certificate information ... 153
EASG product certificate expiration ... 153

EASG site certificate 154
edit
application 79
edit application 79
editing
generic CSR 65
location 38
vCenter 100
editing a platform 42
editing the location 38
editing upgrade configuration 150
editing vCenter 100
Edit Location 39
Edit Platform 68
Edit Upgrade Configuration
AVP Configuration 134
Element Configuration 134
Edit vCenter 102
elements upgrade
target release 35
element upgrade 130
enable
scheduled maintenance 164
enabling
SSH on Appliance Virtualization Platform 56
enabling SSH 57
Enhanced Access Security Gateway 151
esxcfg-route 58
esxcli network ip interface ipv4 set -i vmk0 -I 58
ESXi host
adding 40
removing 62
restarting 62
ESXi host certificate addition 97
ESXi host certificate update 97
ESXi host map to unknown location 63
existing hosts
managing certificates 97
existing vCenter
managing certificates 97

F

field descriptions
Add Platform 68
Application Deployment 88
change password 70
Create AVP Kickstart 54
create CSR 66
edit CSR 66
Edit Location 39
Edit Platform 68
load AVP host certificate 65
Map vCenter 101
New Location 39
Upgrade Configuration 133
Upgrade Management 130
field descriptions *(continued)*
WebLM Configuration 61
field descriptions, Snapshot Manager 67
finding content on documentation portal 172
finding port matrix 171
footprint flexibility 24

G

General Configuration Details 134
generate_report.sh 93
generating
certificates 96
virtual machine report 94
generating kickstart file
Appliance Virtualization Platform 53
generic CSR
creating 65
editing 65

H

hardware supported
System Manager 12
host 50, 69
Host
update 71

I

inputting translations 164
InSite Knowledge Base 174
install
Application Enablement Services 32
Avaya Aura applications 32
Avaya Aura Media Server 32
Avaya Breeze 32
Branch Session Manager 32
Communication Manager 32
SAL 32
SDM 32
Session Manager 32
Solution Deployment Manager client 32
System Manager 32
WebLM 32
install AVP host patch
Solution Deployment Manager 43
install custom patches 126
install custom software patches 126
installed logins 176
Installed Patches 129
install patches 76, 124
install services packs 76, 124, 126
install software patches 76, 124
Install System Manager patch 92
interchange active and standby servers 121

interchange roles 121
IP address and default gateway
changing 58

L

latest software patches 16
legal notice .....
Licenses 158, 161
licensing
Communication Manager 15
Life cycle management 37
Linux Operating System upgrades 36
preupgrade check 36
load AVP host certificate
field descriptions 65
location
adding 38
deleting 39
editing 38
view 38
logins
installed 176
Log off
applications 166

M

Manage Software 13
managing certificates migrated hosts 97
map ESXi host to unknown location 63
Map vCenter 99–102
migrated hosts
managing certificates 97
migrating
Communication Manager to VMware 146
from Communication Manager Release 5.2.1 using SMI 145
from Communication Manager Release 6.3 using SMI 148
migration on different server 121
migration on same server 119
migration path
KVM 156
Software-only 107
monitoring
application 104
platform 103
My Docs 172

N

network configurations 117–119, 121
network parameters
change 68
New Location 39
New vCenter 102

P

password
change 70
password change
Appliance Virtualization Platform host 52
password policy 52, 53
password rules 53
patch information 16
PCN 16
platform
editing 42
monitoring 103
port matrix 171
preparing duplex Communication Manager servers 118
prerequisites
data migration 21
for upgrading application 8
upgrading 21
preupgrade check 36
pre upgrade checks
System Platform upgrades 36
preupgrade job status 149
Preupgrade tasks 29
profile mapping for Communication Manager upgrades, ... 24
PSN 16
push
login banner on host 62

R

reestablish
connection 93
re-establishing trust
application 76
SDM elements 76
Solution Deployment Manager elements 76
re-establishing trust application 76
refresh elements job status 149
release notes for latest software patches 16
removing
Appliance Virtualization Platform host 62
ESXi host 62
removing location from host 100
removing vCenter 100
Resolving
alarms 165
restart
application 81
restart application from SDM 81
restarting
Appliance Virtualization Platform 62
ESXi host 62
restoring
backup 105

retrying
Utility Services to AVP Utilities upgrade 48
rollback
upgrade 168
rollback upgrade 168
rolling back
Utility Services 47

S

same server migration 119
saving translations 164, 165
schedule daily maintenance 164
SDM
installation 32
SDM elements
re-establishing trust 76
searching for content 172
Select Flexi Footprint 79
select upgrade target release 35
servers
accessing System Management Interface 163
servers supported 12
Services Port static route update 80
SES 23
Session Manager update 76, 124, 126
Session Manager upgrade 115
sharing content 172
shutting down
AVP 61
SIP Enablement Services 23
site certificate
add 154
delete 154
manage 154
view 154
snapshot from Appliance Virtualization Platform
deleting 166
snapshot from vCenter managed host
deleting 167
Snapshot Manager
virtual machine snapshot 67
Snapshot Manager field descriptions 67
software
download 71
software details 22
Software Management 13
software management interface 119
software patches 16
software requirements 12
Solution Deployment Manager 13, 53
access 35
restart application 81
start 35
start application 81
stop application 81
supported applications 16
Solution Deployment Manager *(continued)*
update Appliance Virtualization Platform host 43
Solution Deployment Manager client dashboard 34
Solution Deployment Manager elements
re-establishing trust 76
Special
circumstances 23
Special circumstances 23
SSH from AVP Utilities 56
start
application 81
start application from SDM 81
start Solution Deployment Manager 35
static routing
changing 80
updating 80
status
Analyze 151
analyze job 149
Preupgrade check 151
preupgrade check job 149
Refresh elements job 149
upgrade job 149
upgrade jobs 151
stop
application 81
stop application from SDM 81
support 174
supported
servers 14
supported browsers 24
supported Communication Manager upgrade paths 10
supported servers 12
System Manager
7.0 150
upgrade 150
System Manager Application Management
Installed Patches field descriptions 91
System Manager VM update 92
System Platform upgrades
preupgrade checks 36

T

target release 35
select 35
third-party AVP certificates
creating generic CSR 65
editing generic CSR 65
third-party certificates 16
applying to Appliance Virtualization Platform 63
training 173
translations
inputting 164
saving 164
translations; save 165

U

Unknown location host mapping 63
update
  Appliance Virtualization Platform 71
  Appliance Virtualization Platform host 43
  Branch Session Manager 126
  Communication Manager 76, 124, 126
  Session Manager 76, 124, 126
  Utility Services 126
  WebLM 126
update software 76, 124, 126
update static routing 91
update System Manager VM 92
updating ESXi host or vCenter certificate 97
updating Services Port static routing 80
upgrade
  AES 115
  Application Enablement Services 115
  Avaya Aura application 29, 115
  Branch Session Manager 113, 115, 134
  checklist 113
  Communication Manager 29, 113, 115, 134
  Communication Manager Messaging 115
  elements 129
  order 25
  rollback 168
  sequence 25
  Session Manager 29, 113, 115, 134
  target release 35
  to IaaS 160
  to KVM 156
  WebLM 115
Upgrade 133
upgrade Communication Manager 10
Upgrade Configuration
  field descriptions 133
Upgrade Configuration Details 134
upgrade jobs
  deleting 150
  editing 150
  status 151
upgrade job status 149
Upgrade job status
  Viewing 150
Upgrade Management 13
upgrade order 25
upgrade path
  Amazon Web Services 159
  AWS 159
  Azure 160
  GCN 159
  Google Cloud 159
  Microsoft Azure 160
upgrade paths 10
upgrade process 25
Upgrade Release Selection 35
upgrade rollback 168
upgrade sequence 25
Upgrade to release 35
upgrading
  Communication Manager from pre-5.2.1 Release 143
  ESS servers 123
  LSP servers 123
  to Software-only using manual Backup-Restore method 107
  to Software-only using SMGR SDM 109
  to Software-only using SMI 107
  to Software-only using System Manager Solution Deployment Manager 109
Upgrading
  full backup 112
  virtual machine 112
upgrading duplex Communication Manager servers 117
upgrading prerequisites 21
upgrading to IaaS 160
upgrading to KVM 156
upload
  custom patch 142
uploading a custom patch 142
uploading custom patch 142
uploading custom patch field description 142
Utility Services
  rolling back 47
Utility Services bulk upgrade during AVP upgrade 46

V

Validation
  certificate 95
vCenter
  add 102
  adding 99
  add location 100
  deleting 100
  edit 102
  editing 100
  manage 100
  remove location 100
  removing 100
  unmanage 100
vCenter certificate update 97
vCentre
  field descriptions 101
videos 173
view
  location 38
viewing
  virtual machine report status 94
Viewing AVP host
  license status 61
view location 38
virtual machine
  create 74

virtual machine *(continued)*
snapshot on Appliance Virtualization Platform 66
virtual machine report
aborting 94
overview 93
virtual machine snapshot using SDM
deleting 67
VM connection reestablish 93
VMware software requirements 12

W

watch list 172
WebLM Server on AVP host 60