Upgrading Avaya Aura® Communication Manager

Release 7.0.1
Issue 3
August 2017

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. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

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

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

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

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from the earlier releases to Release 7.0.1 on Appliance Virtualization Platform. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.

The document is intended for people who perform upgrades.

Change history

Issue	Date	Summary of changes
3	August 2017	• Added the "Upgrading Communication Manager using full backup" section. • Added the "Upgrading Communication Manager 6.x to VMware" section.
2	May 2016	• Added the Installing software patches on page 62 section for installing the 7.0.1 software patch on Release 7.0. • Added support for Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers. • Added the Backup and restore on page 88 section. • Updated the Communication Manager upgrades on page 9 section. • Updated the Communication Manager OVA and server compatibility on page 13 section. • Updated the information about upgrade hardware requirements in the section "Preupgrade requirements on page 17".
1	August 2015	Initial release

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Upgrade overview and considerations

Communication Manager upgrades

The guide provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 7.0 and later.

Upgrades by using System Manager

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 the following releases:

- Release 6.x to Release 7.0 and later
- Release 5.2.1 to Release 7.0 and later

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

Supported platforms

- Appliance Virtualization Platform: Communication Manager runs as OVA on Avaya-provided server with Appliance Virtualization Platform.
- VMware: Communication Manager runs on the VMware 5.0, 5.1, 5.5, or 6.0 in Virtualized Environment as OVA.

  For instructions to upgrade Communication Manager to Release 7.0 and later in the Avaya Aura® Virtualized Environment, see *Deploying Avaya Aura® Communication Manager*.

Supported upgrade paths

Avaya supports the software-only upgrade of Communication Manager from Release 6.0 or later to Release 7.0 and later.

Supported migration paths

Avaya supports the following platform, and hardware and software upgrades:

- For systems on release earlier than 7.0, upgrading from Release 6.3.x to Release 7.0 and then apply the 7.0.1 patch.
- For systems on Release 5.2.1, upgrading from Release 5.2.1 to Release 7.0 and then apply the 7.0.1 patch.

- For systems between Release 5.0 and Release 5.2:
    1. Upgrading from Communication Manager Release 5.2.1 to Release 7.0 and then apply the 7.0.1 patch.
- For systems on a release earlier than 5.2.1:
    1. Upgrading from the existing release to Release 5.2.1
    2. Upgrading from Communication Manager Release 5.2.1 to Release 7.0 and then apply the 7.0.1 patch.

You can replace the existing server with the server that Communication Manager Release 7.0 and later supports and migrate to Communication Manager Release 7.0 and later on Appliance Virtualization Platform.

For procedures to migrate Communication Manager on System Platform to Appliance Virtualization Platform, see Migrating the data from System Platform to Appliance Virtualization Platform.

Supported servers

You can upgrade Communication Manager from Release 5.2.1 or Release 6.3.x to Release 7.0 and later on the following servers:

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

Note the following upgrade considerations:

- Upgrade the servers on Communication Manager Release 5.2.1 or later to Release 7.0 and later on the existing servers.
- Upgrade the servers on Communication Manager release earlier than 5.2.1 to Release 5.2.1 before you upgrade the servers to Release 7.0 and later, unless otherwise noted.

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 7.0 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 7.0 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
   - The files are downloaded
5. Upgrade applications: To upgrade Avaya Aura® applications to Release 7.0.1.
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 Utility Services to Release 7.0.1 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.

Communication Manager deployment options

Communication Manager installation on Appliance Virtualization Platform

The Communication Manager installation process consists of:

- Identifying or procuring necessary hardware, software, and other equipment
- Installing the necessary hardware and equipment
- Installing Appliance Virtualization Platform, that is Avaya-provided server running ESXi host.
- Deploying the appropriate Communication Manager OVA on the server
- Configuring the applications, including Communication Manager, Communication Manager Messaging, and Branch Session Manager
- Completing the post installation verification tasks

If Communication Manager is not running as an application in your enterprise, perform the installation. You must also install Communication Manager if one or more of your current Communication Manager executable files are corrupted.

You must upgrade Communication Manager when a new release is available. To start using the new release, shut down Communication Manager, replace the executable files with the new files, and restart Communication Manager.

For information about the upgrade process, see *Upgrading Servers to Avaya Aura® Communication Manager*.

Communication Manager installation in VMware environment

You can install Communication Manager Release 6.3 and later as an Open Virtualization Program (OVA) on VMware vSphere ESXi 5.0, 5.1, 5.5, or 6.0. The Communication Manager VMware virtualization environment is packaged as a virtual appliance ready for deployment on VMware certified hardware.

For more information about deploying Communication Manager on VMware, see *Deploying Avaya Aura® Communication Manager*.

Communication Manager OVA and server compatibility

Communication Manager is an OVA that can be deployed on Appliance Virtualization Platform. The Communication Manager OVA has all the features that Communication Manager supports, whether the OVA is on a duplicated server or a branch server.

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

OVA type	Server configuration	Supported server
Simplex	• Main • Survivable Core • Survivable Remote	• S8300D • S8300E • Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G7 • HP ProLiant DL360 G9
Duplex	• Main • Survivable Core	• Dell™ PowerEdge™ R610 • Dell™ PowerEdge™ R620 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G7 • HP ProLiant DL360 G9

For information about capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.

For information about hardware specifications, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

The S8300E server is based on a 2.0 GHz, dual core Intel Ivy Bridge processor. The S8300E server is supported in the G430 Branch Gateway and G450 Media Gateway. The S8300E server supports Appliance Virtualization Platform and Communication Manager Release 6.3.8 and later. The S8300E server is certified by VMware as VMware Ready.

License file for Communication Manager

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later. Earlier versions of Communication Manager, except Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template, continue to use the Remote Feature Activation (RFA) online tool for license files. Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template uses PLDS to manage licenses.

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.

For Communication Manager 6.0 and later, 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 7.0 and later, 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 System Manager WebLM or WebLM virtual application for licensing a duplicated pair configuration, you need to install the license file on the main Communication Manager server. To activate a Communication Manager license file for a duplicated pair, you do not need to provide host IDs on both servers.

For a duplicated pair configuration on System Manager WebLM, you must install the license file on both servers. The system does not synchronize the license file from active server with standby server. To activate a Communication Manager license file for a duplicated pair, provide the WebLM host ID for both servers. The license file that the system generates includes both host IDs. You must install that license file on both servers in the duplicated pair.

Authentication files for Communication Manager

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

Appliance Virtualization Platform and Communication Manager share the same authentication file. The system installs a default authentication file with Appliance Virtualization Platform. However, you must replace the default file with a unique file. The Authentication File System (AFS) creates unique authentication files. AFS is an online application that you can download from http://rfa.avaya.com.

Authentication files for duplicated servers and survivable servers

For duplicated pair configurations, you must install the same authentication file on both the active server and standby server. The system does not automatically synchronize the authentication file from active server to standby server.

Each survivable server must have its own unique authentication file. You must install a unique file from the System Manager Web Console of each server.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies the file. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Security enhancements

With the Communication Manager Release 6.3.6 security service patch, you can receive and validate the certificate that uses the SHA-2 signing algorithm and 2048 bit RSA keys. Using Communication Manager System Management Interface, you can import the third-party trusted certificate that uses the SHA-2 signing algorithm.

Note:

To obtain the security service pack details, go to the Avaya Support website at http://support.avaya.com.

For information about certificates, see *Avaya Aura® Communication Manager Security Design*, 03-601973 and *Administering Avaya Aura® Communication Manager*, 03-300509.

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.

Chapter 3: Planning for upgrade

Upgrade paths

The table provides the supported upgrade paths from various releases of Communication Manager to Release 7.0 and later.

Note:

- You cannot upgrade some servers to Release 5.2.1 or 6.3.x directly. 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 7.0 and later.
- You can also upgrade Communication Manager from earlier releases to Release 7.0 and later on VMware vSphere™ 5.0, 5.1, 5.5, or 6.0 Virtualized Environment.

  For instructions to upgrade Communication Manager to Release 7.0 and later in the Avaya Aura® Virtualized Environment, see *Deploying Avaya Aura® Communication Manager*.

Release	Requirement
5.0.x and 5.1.x	Back up translations and restore to the Release 7.0 and later supported server
5.2.1	Migrate to 6.x by using the migration patch installed on 5.2.1 then migrate from 6.x to 7.0 or later by using System Manager Solution Deployment Manager.
6.0.x, 6.2	Upgrade or migrate to Release 7.0 and later supported server by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.
6.3.x	Upgrade the supported hardware remotely to Release 7.0 and later by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.
7.0.x	Upgrade the supported hardware remotely to Release 7.0 and later by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Support for SIP Enablement Services

SIP Enablement Services is not compatible with Communication Manager Release 7.0.1. If you upgrade Communication Manager with SIP Enablement Services Release 5.2.1 or earlier to

Release 7.0.1, 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 Communication Manager to Release 7.0.1.

- 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) coresident on the S8300 Server, you cannot restore SES on the new server because Communication Manager Release 7.0.1 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.

Preupgrade requirements

Ensure that you:

- Place an order for all the hardware, and ensure that the hardware is available onsite.

- Download all the software and service packs.
- Copy the applications on the computer that you later use to perform the upgrade.
- Identify a server with adequate disk space to store the datasets.

Hardware requirements

- HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, or Dell™ PowerEdge™ R630 Server to replace an existing standalone server that does not support Release 7.0.1 or later.
- S8300D or S8300E server to replace an existing embedded server that you cannot upgrade to Release 7.0.1.
- Required Ethernet CAT5 cables

Note:

For adopting Communication Manager with a High Performance Duplex template, HP DL360 G7 or Dell R610 with a 2.93 Ghz processor is recommended. The HP DL360 G7 and Dell R610 server can be used for Avaya Aura® 7 deployment with the existing applications installed. For example, if the earlier HP DL360 G7 or Dell R610 server supported Communication Manager Simplex Release 6.x, then the upgrade is possible for Communication Manager Simplex Release 7.x on AVP. Only servers with identical hardware can be used for duplex configuration. Also see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Software requirements

Download the following software from the appropriate website:

- System Manager OVA from PLDS
- DVDs for the Solution Deployment Manager client and Appliance Virtualization Platform from PLDS
- Utility Services and Communication Manager OVA files from PLDS
- The license file from PLDS
- The authentication or password file from the Authentication File System (AFS)
- Preupgrade and postupgrade service packs from the Avaya Support website at http://support.avaya.com.

Application requirements

Install the following applications on your computer:

- Internet Explorer 9.x, 10.x, or 11.x browser
- Firefox 37, 38, or 39 browser.
- A Secure Shell application such as PuTTY.

Profile mapping for Communication Manager 6.x upgrades

Before you upgrade Communication Manager from Release 6.x to Release 7.0.1 ensure the correct footprints.

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

Table 1: Summary of profile mapping

Communication Manager 6.x template	Communication Manager Release 7.0.1 deployment option	Resources
CM_onlyEmbed on S8300D and S8300E	CM Main Max users 1000 Small Main supporting up to 1000 users	2vCPUs, 3900 MHz, 3.5 Gb RAM
CM_SurvRemoteEmbed on S8300D and S8300E	CM Survivable Max users 1000 Small Survivable supporting up to 1000 users	1vCPU, 1950 MHz, 3.5 Gb RAM
CM as part of Midsize_Ent	CM Main Max users 2400 Medium Main only supporting up to 2400 users This profile is targeted as a migration path for Communication Manager on Midsize Enterprise.	2 vCPUs, 4400 MHz, 4.0 Gb RAM
CM_Simplex	CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_SurvRemote	CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users	2 vCPUs, 4400 MHz, 4.5 Gb RAM
CM_Duplex	CM Duplex Max users 30000 Standard Duplex 30,000 users	3 vCPUs, 6600 MHz, 5.0 Gb RAM
CM_Duplex high capacity	CM High Duplex Max users 36000 High Duplex 36,000 users	3 vCPUs, 7800 MHz, 5.0 Gb RAM

Upgrade order

If Communication Manager 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.		
Record the IP addresses and other data of the existing System Platform and Communication Manager that you later configure on the Release 7.0.1 system.	Use the worksheets provided in appendices to make sure that you capture all the required information.	

Table continues…

Task	Notes	√
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.		
Install one of the following servers in the rack and connect the power cord and cables: • HP DL360 G7, HP DL360 G8, or HP DL360 G9 server • Dell R610, Dell R620 or Dell R630 server • S8300D or S8300E server. Install this embedded server in a branch gateway.	You can install a new server before completing the tasks on the existing server.	

Table continues…

Task	Notes	√
Get the System Manager and Communication Manager OVA files.	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.	
Obtain the authentication file from AFS and install the file.	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, virtual machine, and deploy the System Manager and Communication Manager Release 7.0.1OVA files on the server.	On the new server, you can perform the step before completing the tasks on the existing server.	
Deploy the Communication Manager Messaging OVA 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.		
Complete the postupgrade administration.		
Create a backup of the system.		
Register the upgraded system.		

Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

Note:

Click **Next** only once, and wait for the installer to load the next screen.

Before you begin

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

   If you are unable to uninstall, see *Uninstalling the Solution Deployment Manager client*.
2. Ensure that Windows 7, Windows 8.1 64-bit, or Windows 10 64-bit operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.
3. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

   Tip:

   Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space available.
4. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.
5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
6. Ensure that ports support Avaya Aura® 7.0.1 supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

Tip:

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

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

b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.

c. Verify the system variables.

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

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

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

   On the Avaya PLDS website, at https://plds.avaya.com/, click **Support by Products** > **Downloads**, and provide the product **System Manager**, and version as **7.0.x**.

2. Copy 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`.

3. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

4. On the Welcome page, click **Next**.

5. 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**.

6. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.

7. Click **Next**.

8. On the Preinstallation Summary page, review the information, and click **Next**.

9. On the User Input page, perform the following:

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

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

      The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.

   c. In **Data Port No**, select the appropriate port from the range 1527 through 1627.

   d. In **Application Port No**, select the appropriate port from the range 443 through 543.

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

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

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

11. Click **Install**.

12. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.

13. To start the client, click the Solution Deployment Manager client icon,SDM.

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 more information, see “Methods to connect Solution Deployment Manager client to Appliance Virtualization Platform”.

Related links

Preupgrade tasks on page 26

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

Chapter 4: Preupgrade tasks

For the appropriate Communication Manager release and the server on which Communication Manager is deployed, use the procedures in *UpgradingAvaya Aura® Communication Manager to Release 6.3 6* to perform the preupgrade tasks.

Related links

Preupgrade checklist for Linux Operating System upgrades on page 26

Pre-upgrade checklist for System Platform upgrades on page 27

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.	

Related links

Preupgrade tasks on page 26
Preupgrade tasks on page 26

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.	
3	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all the elements.	
4	On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.	
5	After you perform the **Analyze** operation, verify on the Upgrade Job Status page that the operation that you performed is successful.	
6	Download the OVA file for the element that you want to upgrade.	
7	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
8	On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as **Successful**.	
9	In the **Upgrade Job Status** section, on the Pre-upgrade Configuration page, verify the configuration values are correct.	

Related links

Preupgrade tasks on page 26
Preupgrade tasks on page 26

Preupgrade tasks

Preupgrade tasks overview

To successfully upgrade the system to Release 7.0.1, you must perform all tasks listed in the Preupgrade tasks section.

Related links

Preupgrade tasks on page 26

Key tasks for upgrading Avaya Aura® applications to Release 7.0.1

The table contains the key tasks that are required to upgrade Avaya Aura® applications to Release 7.0.1.

Performing the preconfiguration steps

Task	Note
For Communication Manager, click **Save Trans** to save the changes that you have made. For Session Manager, using command line interface, create a backup of the system.	
Ensure that sufficient disk space is available for the server that you have attached with the software library.	
Create a user with administrator credentials to gain access for the applications using HTTP, FTP, SCP or SFTP services.	
For the Avaya Aura® application instance that you have created, create a user and the user profile.	
Configure SNMP for the user.	
For the Communication Manager instance, create the EPW file for the following templates: • Embedded CM Main • Embedded Survivable Remote	
Add the Avaya Aura® application 6.x license file.	
Ensure that you have the PLDS access credentials and Company ID.	
Administer Branch Session Manager in System Manager.	

Performing the initial setup

Task	Note
1. Install the physical or virtual servers that support the Avaya Aura® applications that you want to deploy. 2. Deploy System Manager Release 7.0Release 7.0.1. 3. For Release 7.0 system, install the Release 7.0.1 feature pack to upgrade to Release 7.0.1.	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 Release 7.0.1*
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 for Release 7.0.1*

Performing the upgrade process

Task	Note
Refresh the elements in inventory.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager for Release 7.0.1*
Perform the analyze software operation for the Avaya Aura® application that you selected.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager for Release 7.0.1*
Download the software.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager for Release 7.0.1*
Perform the preupgrade check.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager for Release 7.0.1*
Run the upgrade operation.	Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0.1 on page 95 Checklist for upgrading Avaya Aura applications to Release 7.0.1 on page 94 **Note:** The system takes about 2.5 hours to complete the upgrade process.

Installing feature packs and service packs

Task	Note
Install the Release 7.0.1 feature pack and any required software patches on the Avaya Aura® application.	Installing software patches on page 62
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.

Related links

Preupgrade tasks on page 26

Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

Note:

Click **Next** only once, and wait for the installer to load the next screen.

Before you begin

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

   If you are unable to uninstall, see *Uninstalling the Solution Deployment Manager client*.

2. Ensure that Windows 7, Windows 8.1 64-bit, or Windows 10 64-bit operating system is installed on the computer.

   Tip:

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

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

   Tip:

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

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

   Tip:

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

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
6. Ensure that ports support Avaya Aura® 7.0.1 supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

Tip:

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

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

b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.

c. Verify the system variables.

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

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

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

   On the Avaya PLDS website, at https://plds.avaya.com/, click **Support by Products** > **Downloads**, and provide the product **System Manager**, and version as **7.0.x**.

2. Copy 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`.

3. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

4. On the Welcome page, click **Next**.

5. 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**.

6. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.

7. Click **Next**.

8. On the Preinstallation Summary page, review the information, and click **Next**.

9. On the User Input page, perform the following:

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

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

   The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.

   c. In **Data Port No**, select the appropriate port from the range 1527 through 1627.
   d. In **Application Port No**, select the appropriate port from the range 443 through 543.
   e. **(Optional)** Click **Reset All to Default**.

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

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

11. Click **Install**.
12. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.

13. To start the client, click the Solution Deployment Manager client icon,SDM.

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 more information, see “Methods to connect Solution Deployment Manager client to Appliance Virtualization Platform”.

Related links

Preupgrade tasks on page 26

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

Preupgrade tasks on page 26
Selecting the target release for upgrade on page 33

Selecting the target release for upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.

3. In the **Upgrade to release** field, select one of the following:
    - **SMGR 7.0**: To upgrade Avaya applications to Release 7.0 or later from the Upgrade Management page.
    - **SMGR 6.3.8**: To upgrade Communication Manager and the associated applications to Release 6.3.6 or later from the **Upgrade Management** > **Software Inventory** page.

    Important:

    By default, the target version is set to Release 7.0.
4. Click **Commit**.
5. Click **OK**.
6. To perform the upgrade, click **Upgrade Management**.

Related links

Upgrade target release selection on page 33

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.	

Related links

Preupgrade tasks on page 26

Preupgrade tasks on page 26

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.	
3	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all the elements.	
4	On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.	
5	After you perform the **Analyze** operation, verify on the Upgrade Job Status page that the operation that you performed is successful.	
6	Download the OVA file for the element that you want to upgrade.	
7	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
8	On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as **Successful**.	
9	In the **Upgrade Job Status** section, on the Pre-upgrade Configuration page, verify the configuration values are correct.	

Related links

Preupgrade tasks on page 26

Preupgrade tasks on page 26

Virtual machine management

Virtual machine management

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

VM Management provides the following capabilities:

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

You can deploy the OVA file on the virtual machine by using the System Manager Solution Deployment Manager and the Solution Deployment Manager client.

Related links

Preupgrade tasks on page 26
Certification validation on page 78

Managing the location

Viewing a location

Procedure

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

   The Locations section lists all locations.

Related links

Preupgrade tasks on page 26

Adding a location

About this task

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

Procedure

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

2. On the Location tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
    a. In the Required Location Information section, type the location information.
    b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

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

Related links

Preupgrade tasks on page 26
New and Edit location field descriptions on page 42

Editing the location

Procedure

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

Related links

Preupgrade tasks on page 26
New and Edit location field descriptions on page 42

Deleting a location

Procedure

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

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

Related links

Preupgrade tasks on page 26

VM Management field descriptions

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

Locations

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

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

Hosts

Name	Description
Host Name	The name of the ESXi host.
Host IP	The IP address of the ESXi host.
Host FQDN	FQDN of the ESXi host.
vCenter IP/FQDN	The IP address or FQDN of vCentre.
Current Action	The operation that is currently being performed on the ESXi host.
Last Action	The last completed operation on the ESXi host.
License Status	The status of the license.
Host Version	The ESXi host version. The options are 5.5, 5.1, and 5.0. 6.0 only for VMware ESXi host.
Offer Type	The ESXi host type. The options are: • **AVP**: Appliance Virtualization Platform host • **Customer VE**: customer-provided VMware ESXi host

Table continues…

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

Note:

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

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

Table continues…

Button	Description
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **Update**	Displays the Update host page where you can select the file for updating the Appliance Virtualization Platform host.
More Actions > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays `SSH enabled successfully`.
More Actions > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.
More Actions > **Host Restart**	Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Host Shutdown**	Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Generate/Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the host. Depending on the host type, the options are: • **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only. • **Accept Certificate**: To accept a valid certificate for the host or vCenter. • **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.0.0.0.
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the VMware host or Appliance Virtualization Platform host
Trust Status	The status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store with the available size.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machines.
Start	Starts the selected virtual machines.

Table continues…

Button	Description
Stop	Stops the selected virtual machines.
Show Selected	Displays only the selected virtual machines.
More Actions > **Restart**	Starts the selected virtual machines that were stopped earlier.
More Actions > **Refresh VM**	Updates the status of the virtual machines.
More Actions > **Reestablish Connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.

Related links

Preupgrade tasks on page 26

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 operation, and returns to the Locations section.

Related links

Preupgrade tasks on page 26

Managing the host

Adding an ESXi host

About this task

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

Before you begin

A location must be available.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, click **New**.
4. In the New Host section, provide the following:

   Host name, IP address, user name, and password.
5. Click **Save**.
6. On the Certificate dialog box, click **Accept Certificate**.

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

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

7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
    a. Click **More Actions** > **Re-establish connection**.
    b. Click **Refresh VM**.

    ❗ **Important:**

    When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.

Related links

Preupgrade tasks on page 26
New and Edit host field descriptions on page 54
Generating and accepting certificates on page 79

Editing an ESXi host

Procedure

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

    The system updates the ESXi host information.

Related links

Preupgrade tasks on page 26
New and Edit host field descriptions on page 54

Installing the Appliance Virtualization Platform patch from Solution Deployment Manager

About this task

Install the Release 7.0.1 feature pack on the existing Appliance Virtualization Platform Release 7.0 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Note:

From System Manager Solution Deployment Manager, you cannot update an Appliance Virtualization Platform that hosts this System Manager.

Do not use this procedure for installing the Appliance Virtualization Platform patch on an S8300D server.

Before you begin

1. Add a location.
2. Add a host.
3. Enable the SSH service on the Appliance Virtualization Platform host.
4. Stop all virtual machines that are running on the Appliance Virtualization Platform host.

Note:

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

Procedure

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

   For example, the absolute path on your computer can be `/tmp/avp/avaya-avp-7.0.0.1.0.5.zip`.

   In the Hosts for Selected Location <location name> section, the system displays the update status in the **Current Action** column.
6. To view the details, in the **Current Action** column, click **Patching**.

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

Next steps

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

Related links

Preupgrade tasks on page 26
Update field descriptions on page 57

Changing the network parameters for an Appliance Virtualization Platform host

About this task

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

Note:

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnetmask, and other parameters as appropriate.
5. To change the gateway IP address, perform the following:
   a. Click **Change Gateway**.

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

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

   The system updates the Appliance Virtualization Platform host information.

Related links

Preupgrade tasks on page 26

Change Network Parameters field descriptions on page 55

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

About this task

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

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

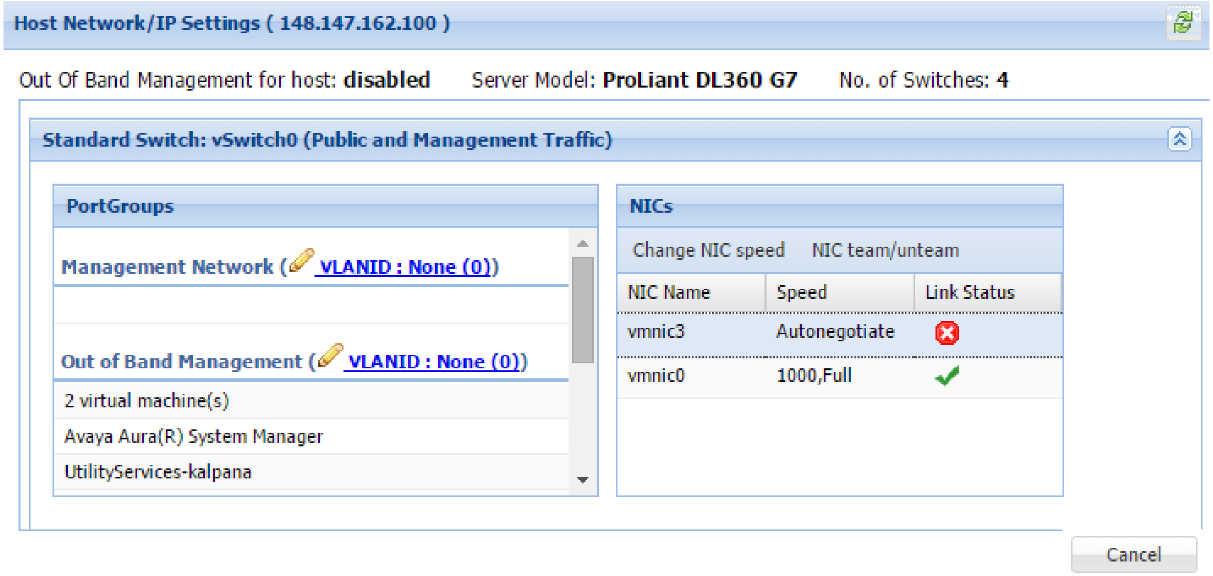
Note:

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

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

Procedure

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



Host Network/IP Settings (148.147.162.100)

Out Of Band Management for host: **disabled** Server Model: **ProLiant DL360 G7** No. of Switches: **4**

Standard Switch: vSwitch0 (Public and Management Traffic)

PortGroups

Management Network (VLANID : None (0))

Out of Band Management (VLANID : None (0))

2 virtual machine(s)

Avaya Aura(R) System Manager

UtilityServices-kalpana

NICs

NIC Name	Speed	Link Status
vmnic3	Autonegotiate	✗
vmnic0	1000,Full	✓

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

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.

- **vSwitch3**. No reservations.

5. To change VLAN ID, perform the following:

    a. To expand the Standard Switch: vSwitch<n> section, click ︾.

    The section displays the vSwitch details.

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

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

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

    For more information about the value, see NIC teaming.

    d. Click **OK**.

    The system displays the new VLAN ID.

    Note:

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

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

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

    b. Click **Change NIC speed**.

    The system displays the selected vmnic dialog box.

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

    d. Click **OK**.

    For more information, see VLAN ID assignment.

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

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

    Note:

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

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

    a. Select a vmnic.

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

    The system displays the Out of Band Management Properties page.

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

For more information, see NIC teaming modes.

d. Click **OK**.

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

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

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

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for S8300D and S8300E servers.

Related links

Preupgrade tasks on page 26
Host Network / IP Settings field descriptions on page 55

Changing the password for an Appliance Virtualization Platform host

About this task

You can change the password only for the Appliance Virtualization Platform host. This is the password for the user that you provide when adding the Appliance Virtualization Platform host.

Procedure

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

Preupgrade tasks on page 26
Password policy on page 49
Change Password field descriptions on page 57

Password policy

The password must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

- Must not contain an uppercase letter at the beginning and a digit or a special character at the end.

Examples of invalid passwords:

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

Example of a valid password: myPassword!1ok

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

Ensure that you keep the root 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 49

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

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, click **More Actions** > **Enable SSH**.

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

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

Related links

Preupgrade tasks on page 26

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

About this task

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

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

Before you begin

Start an SSH session.

Procedure

1. Log in to the System Manager command line interface as root.
2. Navigate to the `$MGMT_HOME/infra/bin/avpSSHUtility` location.
3. Type `./enableDisableSSHOnAVP.sh`.

   The system displays the following options:

   - Enable SSH on the Appliance Virtualization Platform host.
   - Disable SSH on the Appliance Virtualization Platform host.
   - Check the SSH status on the Appliance Virtualization Platform host.
4. To enable SSH, perform the following:
   a. At the prompt, type `1` and press `Enter`.

   b. Type the IP address of the Appliance Virtualization Platform host.

   c. Type the time in minutes.

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

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

   For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you 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`.

Related links

Preupgrade tasks on page 26

Changing the IP address and default gateway of the host

About this task

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

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

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

Before you begin

Connect the computer to the services port.

Procedure

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

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

   For example:

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

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

   For example:

   ```
   esxcfg-route 135.27.162.1
   ```
3. Enable SSH on the Appliance Virtualization Platform host and run the **`./serverInitialNetworkConfig`** command.

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

Related links

Preupgrade tasks on page 26

Shutting down the Appliance Virtualization Platform host

About this task

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

Procedure

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

2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Related links

Preupgrade tasks on page 26

Restarting the Appliance Virtualization Platform host

Procedure

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

   The system restarts the Appliance Virtualization Platform host and virtual machines.

Related links

Preupgrade tasks on page 26

Deleting an ESXi host

Procedure

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

Related links

Preupgrade tasks on page 26

Mapping the ESXi host to an unknown location

About this task

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

Procedure

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

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

   The system displays the ESXi host in the selected location.

Related links

Preupgrade tasks on page 26

New and Edit host field descriptions

Name	Description
Location	The location where the host is availabe. The field is read only.
Host Name	The hostname of Appliance Virtualization Platform or the ESXi host. For example, smgrdev.
Host FQDN or IP	The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.
User Name	The user name to log in to Appliance Virtualization Platform or the ESXi host. **Note:** For Appliance Virtualization Platform, provide the root login and password that you configured in the spreadsheet.
Password	The password to log in to Appliance Virtualization Platform or the ESXi host.

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

Related links

Preupgrade tasks on page 26

Change Network Parameters field descriptions

Network Parameters

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

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

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

Related links

Preupgrade tasks on page 26

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.

Related links

Preupgrade tasks on page 26

Change Password field descriptions

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

Button	Description
Change Password	Saves the new password.

Related links

Preupgrade tasks on page 26

Update 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.
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.

Related links

Preupgrade tasks on page 26

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.

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

Related links

Preupgrade tasks on page 26

Managing the virtual machine

Deploying the Utility Services OVA file

About this task

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

To deploy Utility Services, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable. Deploy Utility Services first, install the Release 7.0.1 feature pack, and then deploy all other applications one at a time.

Before you begin

- Complete the deployment checklist.

  For information about the deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.
- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file to System Manager.

Procedure

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

2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   1. In **Select Location**, select a location.
   2. In **Select Host**, select a host.
   3. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

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

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

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

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

    For more information about Configuration Parameters, see Network Parameters and Configuration Parameters field descriptions.
11. Click **Deploy**.

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

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

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

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

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

14. Install the Release 7.0.1 feature pack.

15. Reboot the Utility Services virtual machine.

Next steps

1. Deploy System Manager and install the Release 7.0.1 feature pack.
2. To activate the serviceability agent registration, reset the Utility Services virtual machine.
3. Deploy all other Avaya Aura® applications one at a time.

Related links

Preupgrade tasks on page 26

VM Deployment field descriptions on page 69

Network Parameters and Configuration Parameters field descriptions

Deploying an OVA file for an Avaya Aura® application

About this task

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

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

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

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.

3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.

4. In the Select Location and Host section, do the following:

   a. In **Select Location**, select a location.

   b. In **Select Host**, select a host.

   c. In **Host FQDN**, type the virtual machine name.

5. In **Data Store**, select a data store.

   The page displays the capacity details.

6. Click **Next**.

7. In the Deploy OVA section, do the following:

   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      To deploy the OVA by using the Solution Deployment Manager client, you can use the default software library that is set during the client installation.

   b. In **Select OVAs**, select the OVA file that you want to deploy.

   c. In **Flexi Footprint**, select the footprint size that the application supports.

8. Click **Next**.

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

9. In the Network Parameters section, ensure that the following fields are preconfigured:

   - **Public**
   - **Services**: Only for Utility Services
   - **Duplicate Link**: Only for duplex Communication Manager
   - **Out of Band Management**: Only if Out of Band Management is enabled

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

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

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

11. Click **Deploy**.

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

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

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

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

Next steps

Install the Release 7.0.1 patch file for the Avaya Aura® application.

Perform the following:

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

   Note:

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

Related links

Preupgrade tasks on page 26
Installing software patches on page 62
VM Deployment field descriptions on page 69

Installing software patches

About this task

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

Before you begin

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

Procedure

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

Note:

If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.

9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

    If the field displays ✗, review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

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

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

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

    The page displays all software patches that you can commit.

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

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

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

Related links

Preupgrade tasks on page 26
Preupgrade Configuration field descriptions

Upgrade Configuration field descriptions on page 104
Edit Upgrade Configuration field descriptions on page 105
Installed Patches field descriptions on page 101

Editing a virtual machine

Before you begin

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

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon (SDM CLIENT) on the desktop.
2. In VM Management Tree, select a location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.

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

   Important:

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

      Note:

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

Note:

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

c. Click **Update IP/FQDN in Local Inventory**.

d. Click **Update VM IP/FQDN**.

e. Provide the IP address and FQDN of the virtual machine.

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

6. Click **Save**.

Related links

Preupgrade tasks on page 26

Deleting a virtual machine

Procedure

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

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

Related links

Preupgrade tasks on page 26

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

About this task

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

Before you begin

- Connect the system on which Solution Deployment Manager is running to the new network for changing network parameters.

- When many Avaya Aura® applications are running on an Appliance Virtualization Platform host, ensure that you change the network parameter in the following order:
    1. Appliance Virtualization Platform
    2. Avaya Aura® applications that are running on the host except Utility Services.
    3. Utility Services

    ✱ **Note:**

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Network Parameters section, change the following as appropriate, and click **Save**:
    - IP address, subnetmask, and other parameters
    - Gateway IP address

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

    For more information, see *Administering Avaya Aura® application* available for each application. Also, see “Network Parameters for Avaya Aura® applications”.
6. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services:
    a. In the Edit VMs section, select a virtual machine and click **Edit**.

    b. Click **Update IP/FQDN in Local Inventory**.

    c. Click **Update VM IP/FQDN**.

    d. Provide the IP address and FQDN of the virtual machine.

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

    a. Click **More Actions** > **Re-establish connection**.

✱ **Note:**

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

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

✱ **Note:**

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

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

Related links

Preupgrade tasks on page 26
Change Network Parameters field descriptions on page 55
Changing the network parameters for an Appliance Virtualization Platform host on page 46
Network parameter update for Avaya Aura applications on page 77

Updating Services Port Static Routing on an Avaya Aura® application

About this task

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

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

Before you begin

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

Procedure

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

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

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

Related links

Preupgrade tasks on page 26
Update Static Routing field descriptions on page 75

Starting a virtual machine from Solution Deployment Manager

Procedure

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

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

Related links

Preupgrade tasks on page 26

Stopping a virtual machine from Solution Deployment Manager

About this task

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

Procedure

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

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

Related links

Preupgrade tasks on page 26

Restarting a virtual machine from Solution Deployment Manager

Before you begin

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

Procedure

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

2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to restart.
4. Click **Restart**.

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

Related links

Preupgrade tasks on page 26

VM Deployment field descriptions

Select Location and Host

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

Capacity Details

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

Note:

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

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

Deploy OVA on System Manager Solution Deployment Manager

Name	Description
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy.

Table continues…

Name	Description
Flexi Footprint	The footprint size supported for the selected host. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA on the Solution Deployment Manager client

Name	Description
Provide OVA path	The option to select a `.ova` file of the virtual machine that is available 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 **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of System Manager that you want to deploy.
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.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Configuration Parameters

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

Note:

For configuration parameter fields, for Communication Manager Messaging and Utility Services, see VM Deployment Configuration and Network Parameters field descriptions on page 72.

Name	Description
VM Name	The name of the virtual machine.
Product	The name of the Avaya Aura® application that is being deployed. The field is read-only.
Version	Release number of the Avaya Aura® application that is being deployed. The field is read-only.
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Table 2: Configuration Parameters for Communication Manager simplex OVA deployment

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

Network Parameters

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

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

Related links

Preupgrade tasks on page 26
VM Deployment Configuration and Network Parameters field descriptions on page 72

VM Deployment 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.

Table continues…

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

Configuration and Network Parameters for Utility Services deployment

Name	Description
Configuration Parameters	
Communication Manager IP	IP address of Communication Manager. **Note:** A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine.
TImezone setting	The selected timezone setting for the Utility Services virtual machine.
NTP Server IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management.

Table continues…

Name	Description
	Note: **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.
Utility Services Mode	The mode in which you want to deploy Utility Services. The options are: • **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services. With the services port feature, through a laptop connected to the services port of Appliance Virtualization Platform, you can gain access to Avaya virtual machines and the hypervisor that are deployed. • **Utility Servers Only**: Use to disable routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the services port becomes non-operational. • **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform. You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed. **Note:** For the Solution Deployment Manager client to connect to the services port features of Utility Services, change the IP address to 192.11.13.5 on the computer of the technician Utility Services can gain access to the hypervisor and all virtual machines. Utility Services provides application routing between the physical port and virtual applications.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirmation password	The confirmation password.
Network Parameters	
Default Gateway	The IP address of the default gateway. Required field unless you use DHCP.
DNS	The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP.
Public IP address	The IP address for this interface.

Table continues…

Name	Description
	Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.

Related links

Preupgrade tasks on page 26

Update Static Routing field descriptions

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

Button	Description
Update	Updates the static IP address for routing.

Related links

Preupgrade tasks on page 26

Installed Patches field descriptions

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

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

Related links

Preupgrade tasks on page 26

Update VM field descriptions

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

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

Related links

Preupgrade tasks on page 26

Reestablish Connection field descriptions

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

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

Related links

Preupgrade tasks on page 26

Network parameter update for Avaya Aura® applications

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

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

Tip:

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

Avaya Aura® application	Command	Interface where you perform the task
Appliance Virtualization Platform	`serverInitialNetworkConfig`	CLI
System Manager	`changeIPFQDN -IP <IP address> -FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names>`	CLI or vSphere client
Communication Manager	-	The Network Configuration page from **Administration** > **server(Maintenance)** >

Table continues…

Avaya Aura® application	Command	Interface where you perform the task
		ServerConfiguration on Communication Manager SMI.
Session Manager	`SMnetSetup`	vSphere client
Avaya Breeze™ and all installed snap-ins	-	vSphere client
Utility Services	`VMware_conf.sh`	CLI
Avaya Aura® Media Server	-	See the Avaya support website.
SAL Gateway	-	Currently, you cannot change Network Parameters for SAL Gateway

Related links

Preupgrade tasks on page 26

Certificate validation

Certification validation

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

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 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
- Does not validate certificates for hosts that vCenter manages

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 directly log on to the host and confirm that the details in the `/etc/vmware/ssl/rui.crt` file match the details displayed on the screen.

Related links

Preupgrade tasks on page 26

Generating and accepting certificates

About this task

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

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

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

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

Before you begin

Require permissions to add a host to generate certificates.

Procedure

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

5. On the Certificate window, do the following:
   a. Click **Generate Certificate**.

      Note:

      You can generate certificate only for the Appliance Virtualization Platform host.
   b. Click **Accept Certificate**.

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

Next steps

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

Related links

Preupgrade tasks on page 26
Adding an ESXi host on page 43
Generating new self-signed certificates for the ESXi host on page 82

Updating the certificate on the ESXi host from VMware

About this task

Use the procedure to update the ESXi host certificate.

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

Before you begin

Start an SSH session on the ESXi host.

Procedure

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

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

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

Note:

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

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

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

The connection from Solution Deployment Manager 7.0.1 to a vCenter or ESXi host by using an IP address fails because the IP address is absent in the certificate and the connection is not sufficiently secure.

Related links

Preupgrade tasks on page 26

Generating new self-signed certificates for the ESXi host on page 82

Managing certificates for existing hosts

About this task

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

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

Before you begin

Require permissions to add a host to generate certificates.

Procedure

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

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

6. For vCenter, do the following:
    a. Click **Map vCenter**, select the vCenter server, and click **Edit**.
    b. In the Certificate dialog box, accept certificate, and click **Save**.

Related links

Preupgrade tasks on page 26
Generating new self-signed certificates for the ESXi host on page 82
Generating and accepting certificates on page 79

Generating new self-signed certificates for the ESXi host

About this task

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

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

Before you begin

Start an SSH session on the ESXi host.

Procedure

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

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

    Note:

    Do not perform the step if you are regenerating certificates because you deleted the certificates.

3. To generate new certificates, type `/sbin/generate-certificates`.
4. Restart the ESXi host.

    The generation process places the certificates places in the correct location.

5. **(Optional)** Do the following:
    a. Move the ESXi host to the maintenance mode.
    b. Install the new certificate.
    c. Restart management agents from Direct Console User Interface (DCUI).

6. Do the following to confirm that the host successfully generated new certificates:
    a. Type `ls -la`.
    b. Compare the time stamps of the new certificate files with `orig.rui.crt` and `orig.rui.key`.

Next steps

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

Related links

Preupgrade tasks on page 26

Managing vCenter

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 5.0, 5.1, 5.5, and 6.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

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

Before you begin

Ensure that you have the required permissions.

Procedure

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

      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.
    - **User Name**
    - **Password**
    - **Authentication Type**
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

Preupgrade tasks on page 26
Editing vCenter on page 84
Map vCenter field descriptions on page 85
New vCentre and Edit vCentre field descriptions on page 86

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

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

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

Related links

Preupgrade tasks on page 26

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

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

4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Related links

Preupgrade tasks on page 26

Map vCenter field descriptions

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

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

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

Related links

[Preupgrade tasks](#) on page 26

New vCentre and Edit vCentre 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

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

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	The version of the ESXi host. The options are: 5.0, 5.1, 5.5, and 6.0.

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

Related links

Preupgrade tasks on page 26

Monitoring a host and virtual machine

Monitoring a host

Procedure

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

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

Related links

Preupgrade tasks on page 26

Monitoring a virtual machine

Procedure

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

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

Related links

Preupgrade tasks on page 26

Backup and restore

Creating a backup

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
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, host name, 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`.

Related links

Preupgrade tasks on page 26

Restoring backup

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
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`.

Related links

Preupgrade tasks on page 26

Chapter 5: Upgrade process

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 the *craft* login.
6. Administer the new Communication Manager virtual machine:
    a. Administer the network parameters.
    b. Apply the Communication Manager patch.
    c. Set the time zone.
    d. Set up the network time protocol.
    e. Add an suser account.
7. On the new Communication Manager virtual machine, log in to Communication Manager System Management Interface and set the host name and DNS information of the new Communication Manager as it was on the existing Communication Manager virtual machine.
8. Restore the full backup on the new Communication Manager virtual machine.
9. Reboot the new Communication Manager virtual machine.
10. Log in to Communication Manager System Management Interface of the new Communication Manager virtual machine and configure the WebLM Server.

Upgrading Communication Manager 6.x to VMware

Before you begin

VMware is not supported on the S8300D server. 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 any the survivable remote server has the same version as the Communication Manager virtual application version. The survivable remote version must remain at 6.2. Use the 6.2 media if you must update the version.

Procedure

1. Download and save the *Migrating from Avaya Aura® Communication Manager 6.x to VMware® Workbook* from the Avaya support website at https://downloads.avaya.com/css/P8/documents/100167658. 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.

Upgrading Avaya Aura® applications

Checklist for upgrading Avaya Aura® applications to Release 7.0.1

Note:

For Release 7.0 system, install the Release 7.0.1 feature pack to upgrade to Release 7.0.1.

No.	Task	References	✔
1	Install Solution Deployment Manager client on your computer.	Installing the Solution Deployment Manager client on your computer on page 23	
2	To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.		
3	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.0 OVA file, and install the Release 7.0.1 bin file by using the Solution Deployment Manager client. • Available: Upgrade System Manager to Release 7.0 and install the Release 7.0.1 bin file.		
4	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	"Discovering elements" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
5	Configure user settings.	"User settings" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
6	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for TN Boards and media gateway upgrades is not supported.	"User settings" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
7	Refresh the elements in the inventory.	"Refreshing elements" in *Administering Avaya Aura® System Manager for Release 7.0.1*	

Table continues…

No.	Task	References	✔
8	Analyze the software.	"Analyzing software" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
9	Download the required firmware for the Avaya Aura® application upgrade.	"Downloading the software" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
10	Analyze the software.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
11	Perform the preupgrade check.	"Performing the preupgrade check" in *Administering Avaya Aura® System Manager for Release 7.0.1*	
12	Perform the upgrade.	Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0.1 on page 95	
13	Verify that the upgrade is successful.	-	
14	For Release 7.0 system, install the Release 7.0.1 feature pack to upgrade to Release 7.0.1.	Installing software patches on page 62	

Upgrading Avaya Aura® applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0.1

About this task

Use the procedure to upgrade Communication Manager, Session Manager, Branch Session Manager, Utility Services from earlier releases to Release 7.0. The process automatically updates to Release 7.0.1 when you provide the Release 7.0.1 patch file. The procedure covers upgrades on the same server and on a different server.

Note:

For Release 7.0 system, install the Release 7.0.1 feature pack to upgrade to Release 7.0.1.

Before you begin

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

Procedure

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

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

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

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

6. To provide the upgrade configuration details, click **Edit**.
7. On the Edit Upgrade Configuration page, and perform the following:
    a. In **Service/Feature Pack for auto-install after migration**, provide the Release 7.0.1 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.

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.
14.
15. On the Upgrade Management page, click 🔄.

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

16. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
17. Verify that the upgrade of the application is successful.

    For upgrades on the same server, the system goes to the pause state.
18. For upgrades on the same server, perform the following:
    a. Install the Appliance Virtualization Platform host.
    b. From the VM Management page, add the Appliance Virtualization Platform host.
    c. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    d. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.
    e. Continue with the upgrade process.

Related links

Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 104
Edit Upgrade Configuration field descriptions on page 105

Installing software patches

About this task

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

Before you begin

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

Procedure

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

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

   Note:

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

    If the field displays ❌, review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

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

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

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

    The page displays all software patches that you can commit.

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

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

19. Click **Schedule**.

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

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

Related links

Preupgrade tasks on page 26
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 104
Edit Upgrade Configuration field descriptions on page 105
Installed Patches field descriptions on page 101

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

Procedure

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

10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

    If the field displays ✗, review the information on the Edit Upgrade Configuration page.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.

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

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

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

    The page displays all software patches that you can commit.

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

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

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

Related links

Uploading a custom patch on page 109

Uploading custom patch field descriptions on page 110

Installed Patches field descriptions

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

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

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.

Table continues…

Name	Description
Time	The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

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

Upgrade Management field descriptions

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

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

Table continues…

Name	Description
	• ❌: Operation failed
Update Status	The update status of the device. The upgrade status can be: • ✅: Upgraded successfully • ⚠: Ready for upgrade • 🕓: Pending execution • ?: Status unknown • ⏸: Upgrade process paused • ⊗: Nonupgradable • ❌: Operation failed
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • ✅: Mandatory checks and recommended checks passed • ⚠: Mandatory checks are successful, but recommended checks failed. • ❌: Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
Location	The location of the device.

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.

Table continues…

Button	Description
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
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	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, CommunicationManager_123.

Table continues…

Name	Description
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**.
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
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

General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade • Update

Table continues…

Name	Description
ESXI Host	The ESXi host on which you want to run the device. The options are: • Same host • List of hosts that you added from VM Management
VM Name	The name of the virtual machine.
Upgrade Source	The source where the installation files are available. The options are: • Local machine • Software library
Upgrade To	The Release 7.0.1 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 migration	The service pack or feature pack that you want to install on 7.0 system.

Upgrade Configuration Details

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

Name	Description
Auto Commit	The option to automatically commit the upgrade.
Existing Administrative User	The Communication Manager user name with appropriate privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. For Communication Manager Messaging, the button is unavailable and you must fill in all details. For Communication Manager Messaging you must provide a new IP address.
CM IPv4 Address	The IP address of the Communication Managervirtual machine.
CM IPv4 Netmask	The network mask of the Communication Managervirtual machine.

Table continues…

Name	Description
CM IPv4 Gateway	The default gateway of the Communication Managervirtual machine.
Out of Band Management IPv4 Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnetwork mask of the virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Services	The port number that is assigned to the services port. The system displays this field when Utility Services is available.

Table continues…

Name	Description
Duplication link	The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process. The field is available only for the Communication Manager duplex configuration and when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

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

Name	Description
Existing Administrative User	The user name of the administrator.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields.
IP Address	The IP address of the virtual machine.
Short Hostname	The hostname of the virtual machine. The hostname of the server and is often aligned with the DNS name of the server.
Network Domain	The domain name of the virtual machine.
Netmask	The network mask of the virtual machine.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Timezone	The timezone of the virtual machine.
Login Name	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Enter Customer Account Password	Password to log on to the system.
Primary System Manager IP	The IP address of System Manager.
Enrollment Password	The password that is required to establish trust between System Manager and Session Manager.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.

Table continues…

Name	Description
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

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

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

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

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

Upgrading Avaya Aura® Communication Manager

Upgrading Communication Manager 6.x to Release 7.0.1

About this task

Use the procedure to upgrade System Platform-based simplex Communication Manager, Branch Session Manager, and associated devices to Release 7.0. The process automatically updates to Release 7.0.1 when you provide the Release 7.0.1 patch file. The procedure covers upgrades on the same server and on a different server.

Before you begin

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

Procedure

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

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

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

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

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

c. Click **Done**.

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

   When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.
7. To provide the upgrade configuration details, click **Edit**.
8. On the Edit Upgrade Configuration page, and perform the following:
   1. In **Service/Feature Pack for auto-install after migration**, provide the Release 7.0.1 patch file.
   2. Complete the details, and click **Save**.
9. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

   If the field displays ✗, review the information on the Edit Upgrade Configuration page.
10. Click **Save**.
11. On the Upgrade Configuration page, click **Upgrade**.
12. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.
15. Click **Upgrade**.
16. On the Upgrade Management page, click 🔄.

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

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

19. For upgrades on the same server, perform the following:
    1. Install the Appliance Virtualization Platform host.
    2. From the VM Management page, add the Appliance Virtualization Platform host.
    3. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    4. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.
    5. Continue with the upgrade process.
20. On Communication Manager Release 7.0.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

Next steps

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

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

Preparing duplex Communication Manager for migration

About this task

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

Before you begin

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

Procedure

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

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

The system starts the second level discovery. The process adds System Platform in the system and creates the parent association with System Platform and Communication Manager.

3. To ensure that the changes made to the translation are saved, log in to the active Communication Manager server, and perform the following:
    a. Start a SAT session.
    b. Type `save translation`
4. In the command line interface of the active Communication Manager server, type `server -u`.

Migrating duplex Communication Manager on the same server

Before you begin

Prepare duplex Communication Manager for migration.

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

Procedure

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

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

       If the upgrade is successful, proceed with the next step.

2. Configure the newly upgraded standby Communication Manager server by performing the following:
    a. Log on to the software management interface of the standby Communication Manager.
    b. On Communication Manager Release 7.0.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
        - **Network Configuration**
        - **Duplication Parameters**
        - **Server role**
    c. From the command line interface of the standby Communication Manager, perform the following:
        a. To release the server from the busy out state, type `server -r`.
        b. Type `server`, and ensure that the duplication link is active and the standby server refreshes.
3. From the command line interface, on the active Communication Manager, interchange the standby and active Communication Manager, type `server -if`.

    Upgrade to Communication Manager Release 7.0 is not connection preserving.
4. Start the upgrade of the current standby Communication Manager server:
    a. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
    b. In the left navigation pane, click **Upgrade Management**.
    c. Perform refresh, analyze, download the entitled version, analyze, and run the preupgrade check for the standby Communication Manager server.

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

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

5. Configure the newly upgraded active Communication Manager server by performing the following:
    a. Log on to the software management interface of the active Communication Manager.
    b. On Communication Manager Release 7.0.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:
        - **Network Configuration**
        - **Duplication Parameters**
        - **Server role**
    c. Type `server`, and ensure that the duplication link is active and the standby server refreshes.
    d. **(Optional)** To interchange the roles of standby and active Communication Manager servers, from the command line interface of the active Communication Manager server, type `server -i`.

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

Migrating duplex Communication Manager on a different server

Before you begin

Prepare duplex Communication Manager for migration.

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

Procedure

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

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

        The system upgrades the standby Communication Manager to 7.0, and restores the data on the Communication Manager 7.0 system.

2. Configure the newly upgraded standby Communication Manager server by performing the following:

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

    b. On Communication Manager Release 7.0.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

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

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

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

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

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

5. Start the upgrade for the Communication Manager that was earlier active:

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

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

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

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

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

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

    f. Schedule the upgrade of the active Communication Manager.

    g. Check the job status for upgrade job.

        The system upgrades the active Communication Manager to 7.0, and restores the data on the Communication Manager 7.0 system, and installs the Release 7.0.1 feature pack.

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

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

b. On Communication Manager Release 7.0.1, click **Administration** > **Server (Maintenance)** > **Server Configuration**, and configure the following parameters:

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

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

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

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

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

Upgrading Communication Manager using System Management Interface

Migrating from Communication Manager Release 5.2.1 to Release 7.0 and later

About this task

Use this procedure to migrate from the standard Communication Manager Release 5.2.1 installation to Communication Manager 7.0 and later virtual open application deployment.

Procedure

1. Back up data from the Communication Manager 5.2.1 System Management Interface page.
2. Deploy the Communication Manager 7.0 OVA.
3. Restore the data on the Communication Manager 7.0 server.
4. Restart the Communication Manager 7.0 server.
5. Install the Communication Manager 7.0 authentication file.
6. Apply the Communication Manager patch for 7.0.1.

Migrating from Communication Manager Release 6.3 to Release 7.0 and later

About this task

Use this procedure to migrate from the standard Communication Manager Release 6.3 installation to Communication Manager 7.0 and later virtual open application deployment.

Procedure

1. Take a full backup of Communication Manager Release 6.3.
2. Deploy the Communication Manager 7.0 OVA.
3. Restore the backup on the Communication Manager Release 7.0 server.
4. Restart the Communication Manager Release 7.0 server.
5. Install the Communication Manager Release 7.0 authentication file.
6. Apply the Communication Manager patch for 7.0.1.

Upgrade job status

Upgrade job status

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

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

Viewing the Upgrade job status

Procedure

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

   The system displays the Upgrade Job Status page.

Editing an upgrade job

Before you begin

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

Procedure

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

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

Related links

Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0.1 on page 95

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.

Chapter 6: Postupgrade procedures

Postupgrade tasks

To perform the postupgrade tasks after the Communication Manager upgrade, see *UpgradingAvaya Aura® Communication Manager to Release 6.3 6*.

Chapter 7: Rollback process

Upgrade rollback

If the upgrade process of an element fails:

- If the admin does not specify rollback all, when the element upgrade fails, the system stops the entire upgrade process and display the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- If the admin specifies rollback all, when the element upgrade fails, the system stops the upgrade and rolls back the overall upgrade process. The system rolls back only the successfully upgraded elements.

Rolling back an upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Click the Avaya Aura® application that you want to rollback.

   The system selects the parent of the application that you select and all child applications of the parent. For example, the page displays the message `Selected System Platform or child of System Platform, and System Platform and all child applications`.
4. Click **Upgrade Actions** > **Rollback**.

Chapter 8: Resources

Documentation

To complete the upgrade process, you require the following documents. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementing			
	Installing the Dell™ PowerEdge™ R620 Server	Describes the installation instructions for the Dell™ PowerEdge™ R620 Server in a rack.	Solution architects, Implementation engineers, Support personnel, Technical support representatives
	Installing the HP ProLiant DL360p G8 Server	Describes the installation instructions for the HP ProLiant DL360p G8 Server in a rack.	Solution architects, Implementation engineers, Support personnel, Technical support representatives
	Installing the Dell™ PowerEdge™ R630 Server	Describes the installation instructions for the Dell™ PowerEdge™ R630 Server in the rack.	Solution architects, Implementation engineers, Support personnel, Technical support representatives
	Installing the HP ProLiant DL360 G9 Server	Describes the installation instructions for the HP ProLiant DL360 G9 Server in the rack.	Solution architects, Implementation engineers, Support personnel,

Table continues…

Document number	Title	Description	Audience
			Technical support representatives
03-300433	*Quick Start for Hardware Installation: Avaya G250 Media Gateway*	Describes the installation instructions for the S8300D Server in the G250 Branch Gateway.	Solution architects, Implementation engineers, Support personnel, Technical support representatives
03-300148	*Quick Start for Hardware Installation: Avaya G350 Media Gateway*	Describes the installation instructions for the S8300D Server in the G350 Branch Gateway.	Solution architects, Implementation engineers, Support personnel, Technical support representatives
03-603236	*Quick Start for Hardware Installation: Avaya G430 Media Gateway*	Describes the installation instructions for the S8300D Server in the G430 Branch Gateway	Solution architects, Implementation engineers, Support personnel, Technical support representatives
03-602053	*Quick Start for Hardware Installation: Avaya G450 Media Gateway*	Describes the installation instructions for the S8300D Server in the G450Branch Gateway	Solution architects, Implementation engineers, Support personnel, Technical support representatives
555-233-150	*Quick Start for Hardware Installation: Avaya G700 Media Gateway*	Describes the installation instructions for the S8300D Server in the G700 Branch Gateway	Solution architects, Implementation engineers, Support personnel, Technical support representatives
	Deploying Avaya Aura® Communication Manager	Describes the implementation instructions for Communication Manager.	Solution architects, Implementation

Table continues…

Document number	Title	Description	Audience
			engineers, Support personnel, Technical support representatives
555-234-100	*Installing and Upgrading the Avaya S8300 Server*	Describes the upgrading instructions for Communication Manager to Release 5.2 on the S8300A, B, C, or D Server	Solution architects, Implementation engineers, Support personnel, Technical support representatives

Related links

Finding documents on the Avaya Support website on page 126

Finding documents on the Avaya Support website

About this task

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

Procedure

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

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 124

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
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
2007V	What is New in Avaya Aura® 7.0
2009V	What is New in Avaya Aura® Communication Manager 7.0
2011V	What is New in Avaya Aura® System Manager & Avaya Aura® Session Manager 7.0
2009T	What is New in Avaya Aura® Communication Manager 7.0 Online Test
2013V	Avaya Aura® 7.0 Solution Management
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
2012V	Migrating and Upgrading to Avaya Aura® 7.0
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

  Note:

  Videos are not available for all products.

Support

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

Glossary

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