Upgrading Avaya Aura® Communication Manager
© 2019-2020, Avaya Inc. All Rights Reserved.

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

Warranty 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/getGenerictDetails?detailId=220951269112456651010 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 ACCESES 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 OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License type(s)

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

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

Cluster License (CL), End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.
Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

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

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at [https://support.avaya.com/Licenseinfo](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 the Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux 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](https://support.avaya.com/Copyright) or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms and referenced 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](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 EMBEDED 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](WWW.SIPRO.COM/CONTACT.HTML). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. See [HTTP://WWW.MPEGLA.COM](HTTP://WWW.MPEGLA.COM).

Compliance with Laws

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](https://support.avaya.com) or such successor site as designated by Avaya.
Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

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

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

**Chapter 1: Introduction**
- Purpose ............................................................................................................ 8
- Change history .................................................................................................. 8

**Chapter 2: Upgrade overview and considerations**
- Communication Manager upgrades ................................................................ 11
- Communication Manager upgrades from System Manager ......................... 12
- Communication Manager deployment options ............................................. 14
  - Communication Manager installation on Appliance Virtualization Platform .... 14
  - Communication Manager installation in VMware environment .................. 14
- Supported servers .......................................................................................... 15
- License file for Communication Manager ...................................................... 15
- Use of third-party certificates ....................................................................... 16
- Latest software updates and patch information ............................................ 16

**Chapter 3: Planning for upgrade**
- Upgrade paths .................................................................................................. 17
- Support for SIP Enablement Services ............................................................. 18
- Special circumstances ...................................................................................... 18
- Preupgrade requirements ............................................................................. 19
- Profile mapping for Communication Manager 6.x upgrades ........................ 20
- Upgrade order ................................................................................................. 20
- Upgrade process ............................................................................................. 21
- Installing the Solution Deployment Manager client on your computer .......... 24
- Accessing Solution Deployment Manager ..................................................... 26

**Chapter 4: Preupgrade tasks**
- Preupgrade checklist for Linux® Operating System upgrades .......................... 27
- Pre-upgrade checklist for System Platform upgrades ...................................... 28
- Preupgrade tasks ............................................................................................ 29
  - Preupgrade tasks overview ....................................................................... 29
  - Key tasks for upgrading Avaya Aura® applications to Release 7.1.3 .......... 29
  - Installing the Solution Deployment Manager client on your computer ...... 32
  - Upgrade target release selection ................................................................. 34
  - Preupgrade checklist for Linux® Operating System upgrades ................. 34
  - Pre-upgrade checklist for System Platform upgrades ............................ 35
  - Virtual machine management ................................................................. 36
- Backup and restore ....................................................................................... 109
  - Creating a backup .................................................................................. 109
  - Changing the hostname ........................................................................... 110
  - Restoring backup ..................................................................................... 110

**Chapter 5: Upgrade process** ........................................................................ 112
Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from the earlier releases to Release 7.1.3 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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>July 2020</td>
<td>Updated the “License file for Communication Manager” section.</td>
</tr>
<tr>
<td>7</td>
<td>June 2020</td>
<td>Added “Changing the hostname” section.</td>
</tr>
<tr>
<td>6</td>
<td>December 2018</td>
<td>Added the &quot;Entering initial system translations&quot; section under the Post-upgrade procedures chapter.</td>
</tr>
<tr>
<td>5</td>
<td>November 2018</td>
<td>Added the following section under Appendix:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “OS-level logins for Communication Manager”</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>May 2018</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Communication Manager installation in VMware environment” to support VMware vSphere ESXi 6.7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrade paths” to support VMware vSphere 6.7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Installing the Solution Deployment Manager client on your computer” to include new SDM client version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated the following sections to include Release 7.1.3 updates:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Communication Manager upgrades”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Communication Manager upgrades from System Manager”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrade paths”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Special circumstances”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Preupgrade requirements”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Profile mapping for Communication Manager 6.x upgrades”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrade process”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Key tasks for upgrading Avaya Aura® applications to Release 7.1.3”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrading Appliance Virtualization Platform from Solution Deployment Manager”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Virtual machine report”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrading Communication Manager from pre–5.2.1 to Release 7.1.3”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Checklist for upgrading Avaya Aura® applications to Release 7.1.3”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “Upgrading Avaya Aura® applications to Release 7.1.3”</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
</table>
| 3     | December 2017 | Added the following section:  
  • Upgrading Communication Manager from pre–5.2.1 to 7.1.2  
  Updated the following sections to include Release 7.1.2 updates:  
  • “Communication Manager upgrades”  
  • “Communication Manager upgrades from System Manager”  
  • “Upgrade paths”  
  • “Support for SIP Enablement Services”  
  • “Special Circumstances”  
  • “Profile mapping for Communication Manager 6.x upgrades”  
  • “Installing the Solution Deployment Manager client on your computer”  
  • “Preupgrade tasks overview”  
  • “Key tasks for upgrading Avaya Aura® applications to Release 7.1.2”  
  • “Upgrading Appliance Virtualization Platform from Solution Deployment Manager”  
  • “Checklist for upgrading Avaya Aura® applications to Release 7.1.2”  
  • “Upgrading Avaya Aura® applications to Release 7.1.2” |
| 2     | August 2017  | Updated the following sections to include Release 7.1.1 updates:  
  • “Communication Manager upgrades”  
  • “Communication Manager upgrades from System Manager”  
  • “Upgrade paths”  
  • “Preupgrade requirements”  
  • “Upgrade process”  
  • “Key tasks for upgrading Avaya Aura® applications to Release 7.1.1”  
  • “Checklist for upgrading Avaya Aura® applications to Release 7.1.1”  
  • “Upgrading Avaya Aura® applications to Release 7.1.1” |
| 1     | May 2017    | Initial release.                                                                                                                                                                                                     |
Chapter 2: Upgrade overview and considerations

Communication Manager upgrades

The guide provides the process and procedures for upgrading Avaya Aura® Communication Manager to Release 7.1.3.

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 7.0.x and later to Release 7.1.3
• Release 6.x to Release 7.1.3
• Release 5.2.1 to Release 7.1.3

 importante:

To upgrade from Release 5.2.1 to Release 7.1.3, you must install Communication Manager Release 7.1.3 by using the Solution Deployment Manager, and then you can manually restore the backup.

To upgrade Communication Manager by using Solution Deployment Manager, you must have System Manager.

Supported platforms

Communication Manager 7.1.3 supports the following platforms:

• Appliance Virtualization Platform
• VMware
• IBM Bluemix
• Kernel Based Virtual Machine (KVM)
• Amazon Web Services (AWS)

 importante:

ESXi 6.5 is not supported with HP ProLiant DL360 G7.

Supported upgrade paths

Avaya supports upgrade of Communication Manager from Release 6.0 or later to Release 7.1.3.
Supported migration paths
Avaya supports the following platform, and hardware and software upgrades:

- For systems on release earlier than 7.1, upgrade from Release 6.3.x to Release 7.1.3.
- For systems on Release 5.2.x, upgrade from Release 5.2.1 to Release 7.1.3.
- For systems on a release earlier than 5.2.1, upgrade from pre-5.1.2 to Release 7.1.3.

You can replace the existing server with the server that Communication Manager Release 7.1.3 supports and migrate to Communication Manager Release 7.1.3 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 7.1.3 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:
ESXi 6.5 is not supported with HP ProLiant DL360 G7.

Note the following upgrade considerations:

- Upgrade the servers on Communication Manager Release 5.2.1 to the supported servers of Release 7.1.3.
- Upgrade the servers on Communication Manager release earlier than 5.2.1 to Release 5.2.1 before you upgrade the servers to Release 7.1.3, 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 7.1.3 from a single view. Communication Manager includes associated devices, such as Gateways, TN boards, and media modules. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.
Important:

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

With Upgrade Management, you can perform the following:

1. Refresh elements: To get the current state or data such as current version of the Avaya Aura® application. For example, for Communication Manager, gateways, media modules, and TN boards.

2. Analyze software: To analyze whether the elements and components are on the latest release and to identify whether a new software is available for the inventory that you collected.

3. Download files: To download files that are required for upgrading applications.

   You can download a new release from Avaya PLDS to the software file library and use the release to upgrade the device software.

4. Preupgrade check: To ensure that conditions for successful upgrade are met. For example, checks whether:
   - The new release supports the hardware
   - The RAID battery is sufficient
   - The bandwidth is sufficient

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

   - The files are downloaded

5. Upgrade applications: To upgrade Avaya Aura® applications to Release 7.1.3.

6. Install patches: To install the software patches, service packs, and feature pack.

**Upgrade automation level**

- The upgrade of Communication Manager, Session Manager, Branch Session Manager, and Utility Services to Release 7.1.3 is automated. The upgrade process includes creating a backup, deploying OVA, upgrading, installing software patches, feature packs, or service packs, and restoring the backup.

- Upgrade of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVA files.

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

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

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

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

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

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 as an Open Virtualization Application (OVA) on VMware vSphere ESXi, 5.5, 6.0, 6.5, or 6.7. The Communication Manager VMware virtualization environment is packaged as a virtual appliance ready for deployment on VMware-certified hardware.

Note:

ESXi 6.5 is not supported with HP ProLiant DL360 G7.
## Supported servers

You can deploy Communication Manager using the following OVA types:

- **Simplex**: If you want to have only one Communication Manager server in your environment, then you can use simplex OVA.

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

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

<table>
<thead>
<tr>
<th>OVA type</th>
<th>Server configuration</th>
<th>Supported server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplex</td>
<td>• Main</td>
<td>• S8300D</td>
</tr>
<tr>
<td></td>
<td>• Survivable Core</td>
<td>• S8300E</td>
</tr>
<tr>
<td></td>
<td>• Survivable Remote</td>
<td>• Dell™ PowerEdge™ R610</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell™ PowerEdge™ R620</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell™ PowerEdge™ R630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360 G7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360p G8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360 G9</td>
</tr>
<tr>
<td>Duplex</td>
<td>• Main</td>
<td>• Dell™ PowerEdge™ R610</td>
</tr>
<tr>
<td></td>
<td>• Survivable Core</td>
<td>• Dell™ PowerEdge™ R620</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell™ PowerEdge™ R630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360 G7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360p G8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP ProLiant DL360 G9</td>
</tr>
</tbody>
</table>

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

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

## License file for Communication Manager

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

PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.
After you obtain the license file, use System Manager WebLM to install the license file. System Manager WebLM is a Web-based application for managing licenses and is installed as part of System Manager.

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

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

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

**Duplicated server licensing**

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

*Note:*

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

---

**Use of third-party certificates**

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

---

**Latest software updates and patch information**

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

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

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.
Chapter 3: Planning for upgrade

Upgrade paths

The table provides the supported upgrade paths from various releases of Communication Manager to Release 7.1.3.

**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 7.1.3.
- You can also upgrade Communication Manager from earlier releases to Release 7.1.3 on VMware vSphere™ 5.5, 6.0, 6.5, or 6.7 Virtualized Environment.

<table>
<thead>
<tr>
<th>Release</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.x and 5.1.x</td>
<td>Back up translations and restore to the Release 7.1.3 supported server. For more information, see Upgrading Communication Manager from pre–5.2.1 to 7.1.2 and later on page 116</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Migrate to Release 6.x by using the migration patch installed on Release 5.2.1 then migrate from Release 6.x to Release 7.1.3 by using System Manager Solution Deployment Manager. For more information, see Upgrading Communication Manager from pre–5.2.1 to 7.1.2 and later on page 116</td>
</tr>
<tr>
<td>6.0.x, 6.2</td>
<td>Upgrade or migrate to Release 7.1.3 supported server by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.</td>
</tr>
<tr>
<td>6.3.x</td>
<td>Upgrade the supported hardware remotely to Release 7.1.3 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.</td>
</tr>
<tr>
<td>7.0.x</td>
<td>Upgrade the supported hardware remotely to Release 7.1.3 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.</td>
</tr>
<tr>
<td>7.1</td>
<td>Upgrade the supported hardware remotely to Release 7.1.3 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.</td>
</tr>
</tbody>
</table>
Support for SIP Enablement Services

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

Special circumstances

Consider the following special situations when upgrading to Communication Manager Release 7.1.3.

- If you have Communication Manager Messaging or Intuity Audix 770 enabled on the existing system, backup and restore that dataset separately on the upgraded system.

- If you have Communication Manager and SIP Enablement Services (SES) co-resident on the S8300 Server, you cannot restore SES on the new server because Communication Manager Release 7.1.3 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.
• You download all the software and service packs.
• You copy the applications on the computer that you later use to perform the upgrade.
• You identify a server with adequate disk space to store the datasets.
• An Appliance Virtualization Platform host and all virtual machines running on the host is on the same subnet mask.

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

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

Hardware requirements

• HP ProLiant DL360 G7, HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, or Dell™ PowerEdge™ R630 Server to replace an existing standalone server that does not support Release 7.1.1 and later.
• S8300D and S8300E embedded servers are supported with Communication Manager Release 7.1.1 and later. If you are using other version of embedded servers, you must replace them with S8300D or S8300E embedded server.
• Required Ethernet CAT5 cables

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
• 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 browser version 11.
• Mozilla Firefox browser version 45 and later.
• 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 7.1.3 ensure the correct footprints are available.

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

Table 1: Summary of profile mapping

<table>
<thead>
<tr>
<th>Communication Manager 6.x template</th>
<th>Communication Manager Release 7.1.3 deployment option</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM_onlyEmbed on S8300D and S8300E</td>
<td>CM Main Max users 1000 Small Main supporting up to 1000 users</td>
<td>2vCPUs, 3900 MHz, 3.5 Gb RAM</td>
</tr>
<tr>
<td>CM_SurvRemoteEmbed on S8300D and S8300E</td>
<td>CM Survivable Max users 1000 Small Survivable supporting up to 1000 users</td>
<td>1vCPU, 1950 MHz, 3.5 Gb RAM</td>
</tr>
<tr>
<td>CM as part of Midsize_Ent</td>
<td>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.</td>
<td>2 vCPUs, 4400 MHz, 4.0 Gb RAM</td>
</tr>
<tr>
<td>CM_Simplex</td>
<td>CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users</td>
<td>2 vCPUs, 4400 MHz, 4.5 Gb RAM</td>
</tr>
<tr>
<td>CM_SurvRemote</td>
<td>CM Main/Survivable Max users 36000 Large Main/Survivable supporting up to 36,000 users</td>
<td>2 vCPUs, 4400 MHz, 4.5 Gb RAM</td>
</tr>
<tr>
<td>CM_Duplex</td>
<td>CM Duplex Max users 30000 Standard Duplex 30,000 users</td>
<td>3 vCPUs, 6600 MHz, 5.0 Gb RAM</td>
</tr>
<tr>
<td>CM_Duplex high capacity</td>
<td>CM High Duplex Max users 36000 High Duplex 36,000 users</td>
<td>3 vCPUs, 7800 MHz, 5.0 Gb RAM</td>
</tr>
</tbody>
</table>

Upgrade order

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

1. Endpoints
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the site has the server and other hardware.</td>
<td>√</td>
</tr>
<tr>
<td>Get the required software and preupgrade and postupgrade service packs.</td>
<td></td>
</tr>
<tr>
<td>Ensure that you have the server and disk space available to back up the upgrade data set.</td>
<td></td>
</tr>
<tr>
<td>Keep the required documentation and release notes handy.</td>
<td></td>
</tr>
<tr>
<td>Record the IP addresses and other data of the existing System Platform and Communication Manager that you later configure on the Release 7.1.3 system.</td>
<td>Use the worksheets provided in appendices to make sure that you capture all the required information.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convert private control networks to the corporate LAN.</td>
<td>Release 6.x does not support private networks (CNA and CNB).</td>
</tr>
<tr>
<td></td>
<td>For instructions, see Converting private control networks to corporate LAN.</td>
</tr>
<tr>
<td>Complete the routine preupgrade tasks on the existing server.</td>
<td></td>
</tr>
<tr>
<td>If Communication Manager Messaging is running on the system, if you use the traffic report, generate the traffic reports before you upgrade the system.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>The upgrade fails if you do not disable or configure Messaging or Communication Manager Messaging.</td>
<td></td>
</tr>
<tr>
<td>Back up all files on the existing server if you need to roll back to the original release.</td>
<td>• For release earlier than 5.2.1, obtain TMT from the STS team.</td>
</tr>
<tr>
<td></td>
<td>• For Release 5.2.1 or later, back up the migration data set</td>
</tr>
<tr>
<td>Install the preupgrade service pack on the existing server.</td>
<td>▼ Important:</td>
</tr>
<tr>
<td></td>
<td>To roll back the upgrade, you must deactivate the preupgrade patch.</td>
</tr>
<tr>
<td>Create the backup of the Communication Manager data set to be restored on the new server.</td>
<td></td>
</tr>
<tr>
<td>Create the backup of the Communication Manager Messaging data set that you will restore on the new server if messaging is enabled.</td>
<td></td>
</tr>
<tr>
<td>For a standalone server, shut down the existing server and remove all power cords and cables.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install one of the following servers in the rack and connect the power cord and cables:</td>
<td>You can install a new server before completing the tasks on the existing server.</td>
</tr>
<tr>
<td>• HP DL360 G7, HP DL360 G8, or HP DL360 G9 server</td>
<td></td>
</tr>
<tr>
<td>• Dell R610, Dell R620 or Dell R630 server</td>
<td></td>
</tr>
<tr>
<td>• S8300D or S8300E server. Install this embedded server in a branch gateway.</td>
<td></td>
</tr>
<tr>
<td>Get the System Manager and Communication Manager OVA files.</td>
<td>On the new server, you can install the ESXi host before completing the tasks on the existing server.</td>
</tr>
<tr>
<td>Get the license file from the PLDS website at <a href="https://plds.avaya.com">https://plds.avaya.com</a>. Install the file on the WebLM server.</td>
<td>On the new server, you can perform the step before completing the tasks on the existing server.</td>
</tr>
<tr>
<td>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 7.1.3 OVA files on the server.</td>
<td>On the new server, you can perform the step before completing the tasks on the existing server.</td>
</tr>
<tr>
<td>Deploy the Communication Manager Messaging OVA if the existing system contains Communication Manager Messaging.</td>
<td></td>
</tr>
<tr>
<td>Restore the Communication Manager dataset.</td>
<td></td>
</tr>
<tr>
<td>Using System Management Interface, configure Communication Manager</td>
<td></td>
</tr>
<tr>
<td>Restart the server by using System Management Interface.</td>
<td></td>
</tr>
</tbody>
</table>

**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.

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

Procedure

1. Download the Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.

2. On the Avaya Support website, click Support by Products > Downloads, and type the product name as System Manager, and Release as 7.1.x.

3. Click the Avaya Aura® System Manager Release 7.1.x SDM Client Downloads, 7.1.x link. Save the zip file, and extract to a location on your computer by using the WinZip application.

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

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

   The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click Next.

6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click I accept the terms of the license agreement and click Next.

7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click Next.
   - To specify a different location for installing the Solution Deployment Manager client, click Choose, and browse to an empty folder. Click Next.

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

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

9. On the Pre-Installation Summary page, review the information, and click Next.

10. On the User Input page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.
      The default software library of the Solution Deployment Manager client is C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts.
      You can save the artifacts in the specified directory.
   c. In **Data Port No**, select the appropriate data port.
      The default data port is 1527. The data port range is from 1527 through 1627.
   d. In **Application Port No**, select the appropriate application port.
      The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.
      **Note:**
      After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
   e. (Optional) Click **Reset All to Default**.

11. Click Next.

12. On the Summary and Validation page, verify the product information and the system requirements.
    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.

13. Click **Install**.

14. To exit the installer, on the Install Complete page, click **Done**.
    The installer creates a shortcut on the desktop.

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

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

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

Related links
- [Preupgrade tasks](#) on page 27
Chapter 4: Preupgrade tasks

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

Related links
- Preupgrade checklist for Linux Operating System upgrades on page 27
- Pre-upgrade checklist for System Platform upgrades on page 28

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.

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

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

Preupgrade tasks overview

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

Related links
Preupgrade tasks on page 27

Key tasks for upgrading Avaya Aura® applications to Release 7.1.3

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

Performing the preconfiguration steps

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Note</th>
</tr>
</thead>
</table>
| 1. Install the physical or virtual servers that support the Avaya Aura® applications that you want to deploy. | 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. |
| 2. Deploy System Manager 7.1. | |
| 3. For Release 7.1.3 system, install the Release 7.1 OVA file to upgrade to Release 7.1.3. | |

### Managing elements inventory

<table>
<thead>
<tr>
<th>Task</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Avaya Aura® application for administration and SNMP access.</td>
<td>&quot;Managing inventory“ in <em>Administering Avaya Aura® System Manager</em></td>
</tr>
<tr>
<td>For Communication Manager, configure the access for the H.248 Gateway device.</td>
<td></td>
</tr>
</tbody>
</table>

### Performing the configuration settings required for upgrade

<table>
<thead>
<tr>
<th>Task</th>
<th>Note</th>
</tr>
</thead>
</table>
| 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](http://plds.avaya.com). Use your PLDS account to get your Company ID. On the System Manager web console, go to Services > Solution Deployment Manager > User Settings. Enter the following details to get entitlements for analyze and artifacts for download:  
1. SSO user name  
2. SSO password  
3. Company ID |
| Option 2: Set up the PLDS access through an alternate source. | |
| Set up the software library. | “Solution deployment and upgrades“ in *Administering Avaya Aura® System Manager* |
Performing the upgrade process

<table>
<thead>
<tr>
<th>Task</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the elements in inventory.</td>
<td>“Solution deployment and upgrades” in Administering Avaya Aura® System Manager</td>
</tr>
<tr>
<td>Perform the analyze software operation for the Avaya Aura® application that you selected.</td>
<td>“Solution deployment and upgrades” in Administering Avaya Aura® System Manager</td>
</tr>
<tr>
<td>Download the software.</td>
<td>“Solution deployment and upgrades” in Administering Avaya Aura® System Manager</td>
</tr>
<tr>
<td>Perform the preupgrade check.</td>
<td>“Solution deployment and upgrades” in Administering Avaya Aura® System Manager</td>
</tr>
</tbody>
</table>
| Run the upgrade operation.                                           | Upgrading Avaya Aura applications to Release 7.1.3 on page 119
                                                                  | Checklist for upgrading Avaya Aura applications to Release 7.1.3 on page 117 |
                                                                  | Note: The system takes about 2.5 hours to complete the upgrade process. |

Installing feature packs and service packs

<table>
<thead>
<tr>
<th>Task</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Release 7.1.3 feature pack and any required software patches on the Avaya Aura® application.</td>
<td>Installing software patches on page 77</td>
</tr>
</tbody>
</table>
| 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 27
Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

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

Procedure

1. Download the `Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip` file from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com) or from the Avaya PLDS website, at [https://plds.avaya.com/](https://plds.avaya.com/).

2. On the Avaya Support website, click **Support by Products > Downloads**, and type the product name as **System Manager**, and Release as **7.1.x**.

3. Click the **Avaya Aura® System Manager Release 7.1.x SDM Client Downloads, 7.1.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

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

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

   The system displays the Avaya Solution Deployment Manager screen.

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

6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.

7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

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

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

9. On the Pre-Installation Summary page, review the information, and click **Next**.

10. On the User Input page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

   The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`
   
   You can save the artifacts in the specified directory.
   c. In **Data Port No**, select the appropriate data port.

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

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

   **Note:**

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

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

11. Click **Next**.

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

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

13. Click **Install**.

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

   The installer creates a shortcut on the desktop.

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

**Next steps**

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

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

Related links

Preupgrade tasks on page 27

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 27
Selecting the target release for upgrade on page 34

Selecting the target release for upgrade

Procedure

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

⚠️ Important:

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

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

Related links

Upgrade target release selection on page 34

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.

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

Related links
[Preupgrade tasks](#) on page 27
[Preupgrade tasks](#) on page 27

### 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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that you assign a different IP address for the ESXi host.</td>
</tr>
<tr>
<td>2</td>
<td>Ensure that you have added all the elements on the System Platform and you have established a structural relationship among all those elements.</td>
</tr>
<tr>
<td>3</td>
<td>After you perform the Refresh Element(s) operation, ensure that your system contains the latest version of all the elements.</td>
</tr>
</tbody>
</table>

Table continues…
Preupgrade tasks

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>After you perform the <strong>Analyze</strong> operation, verify on the Upgrade Job Status page that the operation that you performed is successful.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Download the OVA file for the element that you want to upgrade.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>After you have performed the <strong>Analyze</strong> job, verify that the element that you want to upgrade displays the <strong>Ready for Upgrade</strong> status.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as <strong>Successful</strong>.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>In the <strong>Upgrade Job Status</strong> section, on the Pre-upgrade Configuration page, verify the configuration values are correct.</td>
<td></td>
</tr>
</tbody>
</table>

**Related links**
- Preupgrade tasks on page 27
- Preupgrade tasks on page 27

---

**Virtual machine management**

**Virtual machine management**

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

VM Management provides the following capabilities:

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

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

Preupgrade tasks on page 27
Certification validation on page 99

Managing the location

Viewing a location

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. Click the Locations tab.
   The Locations section lists all locations.

Adding a location

About this task

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

Procedure

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

Editing the location

Procedure

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

4. In the Edit Location section, make the required changes.

5. Click **Save**.

Related links

- Preupgrade tasks [on page 27](#)
- New and Edit location field descriptions [on page 44](#)

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 27](#)

**VM Management field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Reload VM Management Tree</td>
<td>The option to automatically reload the VM Management Tree after the completion of operations, such as, refreshing virtual machines.</td>
</tr>
</tbody>
</table>

**Locations**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Name</td>
<td>The location name.</td>
</tr>
<tr>
<td>City</td>
<td>The city where the host is located.</td>
</tr>
<tr>
<td>Country</td>
<td>The country where the host is located.</td>
</tr>
</tbody>
</table>

**Button**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
</tr>
<tr>
<td>Edit</td>
</tr>
<tr>
<td>Delete</td>
</tr>
</tbody>
</table>
## Hosts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The name of the host.</td>
</tr>
<tr>
<td>Host IP</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Host FQDN</td>
<td>FQDN of the host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the host.</td>
</tr>
<tr>
<td>vCenter FQDN</td>
<td>FQDN of vCentre.</td>
</tr>
<tr>
<td>Current Action</td>
<td>The operation that is currently being performed on the host.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last completed operation on the host.</td>
</tr>
<tr>
<td>License Status</td>
<td>The status of the license.</td>
</tr>
<tr>
<td>Host Version</td>
<td>The host version.</td>
</tr>
<tr>
<td>Offer Type</td>
<td>The host type. The options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>AVP</strong>: Appliance Virtualization Platform host</td>
</tr>
<tr>
<td></td>
<td>- <strong>Customer VE</strong>: customer-provided VMware ESXi host</td>
</tr>
<tr>
<td>SSH Status</td>
<td>The SSH service status. The values are enabled and disabled.</td>
</tr>
<tr>
<td>Host Certificate</td>
<td>The certificate status of the Appliance Virtualization Platform host. The</td>
</tr>
<tr>
<td></td>
<td>values are:</td>
</tr>
<tr>
<td></td>
<td>- ![Checkmark]: The certificate is added in Solution Deployment Manager</td>
</tr>
<tr>
<td></td>
<td>and correct.</td>
</tr>
<tr>
<td></td>
<td>- ![X]: The certificate is not accepted or invalid.</td>
</tr>
<tr>
<td></td>
<td>You can click <strong>View</strong> for details of the certificate status.</td>
</tr>
<tr>
<td>vCenter Certificate</td>
<td>The certificate status of the ESXi host. The values are:</td>
</tr>
<tr>
<td></td>
<td>- ![Checkmark]: The certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>The system enables all the options in <strong>More Actions</strong> that apply to</td>
</tr>
<tr>
<td></td>
<td>VMware ESXi host.</td>
</tr>
<tr>
<td></td>
<td>- ![X]: The certificate is not accepted or invalid.</td>
</tr>
<tr>
<td></td>
<td>You can click <strong>View</strong> for details of the certificate status.</td>
</tr>
</tbody>
</table>

**Note:**

Depending on the Appliance Virtualization Platform host and vCenter certificate status, the system enables the options in **More Actions**.
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Auto Refresh** | The option to automatically refresh the page with the latest changes. For example, the page updates:  
  • The VM state when a virtual machine changes  
  • The license status or certificate status of host when host changes  
  The system refreshes the data every minute. |
| **Add** | Displays the New Host section where you can provide the details of the host that you want to add. |
| **Edit** | Displays the Host Information section where you can change the details of an existing host. |
| **Remove** | Removes the hosts that you select only from the Solution Deployment Manager client.  
  The system moves the hosts associated with the deleted locations to unknown location. |
| **Change Network Params > Change Host IP Settings** | Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host. |
| **Change Network Params > Change Network Settings** | Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host. |
| **Refresh** | Refreshes the status of the hosts. |
| **More Actions > AVP Update/Upgrade Management** | Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host. |
| **More Actions > Change Password** | Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host. |
| **More Actions > SSH > Enable SSH** | Enables SSH for the Appliance Virtualization Platform host.  
  When SSH for the Appliance Virtualization Platform host is enabled, the system displays "SSH enabled successfully." |
| **More Actions > SSH > Disable SSH** | Disables SSH on the Appliance Virtualization Platform host.  
  When SSH for Appliance Virtualization Platform is disabled, the system displays "Disabling SSH for AVP host with <IP address> <FQDN>, <username>." |

*Table continues…*
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Actions &gt; Syslog config &gt; Push</td>
<td>Displays the Push Syslog Configuration section where you can push the syslog configuration on the virtual machine host. Also Syslog is only for Appliance Virtualization Platform. You can select multiple Hosts and Push syslog configuration on selected hosts.</td>
</tr>
<tr>
<td>More Actions &gt; Syslog config &gt; View</td>
<td>Displays the View Syslog Configuration section where you can view syslog profiles of selected the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>More Actions &gt; Syslog config &gt; Delete</td>
<td>Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.</td>
</tr>
<tr>
<td>More Actions &gt; Lifecycle Actions &gt; Host Restart</td>
<td>Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>More Actions &gt; Lifecycle Actions &gt; Host Shutdown</td>
<td>Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.</td>
</tr>
</tbody>
</table>
| More Actions > AVP Cert. Management > Generate/Accept Certificate | Displays the Certificate dialog box where you can manage certificates for the host. Depending on the host type, the options are:  
  • **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only.  
  • **Accept Certificate**: To accept a valid certificate for the host or vCenter.  
  • **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate. |
| More Actions > AVP Cert. Management > Manage Certificate | Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected host. |
| More Actions > AVP Cert. Management > Generic CSR | Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data. |
| More Actions > Snapshot Manager | Displays the Snapshot Manager dialog box from where you can view and delete the virtual machine snapshot. |

Table continues…
### More Actions > Set Login Banner

Displays the Message of the Day dialog box from where you can push the login banner text to the selected host.

⚠️ **Note:**
This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support Set Login Banner.

### Virtual Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>VM IP</td>
<td>The IP address of the virtual machine.</td>
</tr>
<tr>
<td>VM FQDN</td>
<td>FQDN of the virtual machine.</td>
</tr>
<tr>
<td>VM IPv6</td>
<td>The IPv6 address of the virtual machine, if any.</td>
</tr>
<tr>
<td>VM App Name</td>
<td>The name of the application virtual machine. For example, Session Manager.</td>
</tr>
<tr>
<td>VM App Version</td>
<td>The version of the application virtual machine. For example, 7.1.</td>
</tr>
<tr>
<td>VM State</td>
<td>The state of the virtual machine. The states are <strong>Started</strong> and <strong>Stopped</strong>.</td>
</tr>
<tr>
<td>Current Action Status</td>
<td>The status of the current operation. The statuses are:</td>
</tr>
<tr>
<td></td>
<td>• Deploying</td>
</tr>
<tr>
<td></td>
<td>• Starting</td>
</tr>
<tr>
<td></td>
<td>• Stopping</td>
</tr>
<tr>
<td></td>
<td>The <strong>Status Details</strong> link provides the details of the operation in progress.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last action performed on the virtual machine.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The hostname of the VMware host or Appliance Virtualization Platform host on which the virtual machine resides.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Name | Description
--- | ---
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.

### Button | Description
--- | ---
New | Displays the VM Deployment section where you can provide the host and deploy an application.
Edit | Displays the VM Deployment section where you can change the details of a virtual machine.
Delete | Turns off the virtual machines and deletes the selected virtual machine from host and Solution Deployment Manager Client.
Start | Starts the selected virtual machines.
Stop | Stops the selected virtual machines.
Show Selected | Displays only the selected virtual machines.
More Actions > Restart | Starts the selected virtual machines that were stopped earlier.
More Actions > Refresh VM | Updates the status of the virtual machines.
More Actions > Re-establish connection | Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the Trust Status changes to **Success**.
More Actions > Update Static Routing | Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.
More Actions > Syslog config > Push | Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected virtual machine.
More Actions > Syslog config > View | Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > Syslog config > Delete | Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
Related links

**Preupgrade tasks** on page 27

### New and Edit location field descriptions

#### Required Location Information

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

#### Optional Location Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>The IP address of the virtual machine gateway. For example, 172.16.1.1.</td>
</tr>
<tr>
<td>DNS Search List</td>
<td>The search list of domain names.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>The DNS IP address of the primary virtual machine. For example, 172.16.1.2.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.</td>
</tr>
<tr>
<td>NetMask</td>
<td>The subnetwork mask of the virtual machine.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
</tbody>
</table>

#### Button

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the location information and returns to the Locations section.</td>
</tr>
<tr>
<td>Edit</td>
<td>Updates the location information and returns to the Locations section.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the location information, and moves the host to the Unknown location section.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the add or edit operations, and returns to the Locations section.</td>
</tr>
</tbody>
</table>

Related links

**Preupgrade tasks** on page 27
Managing the host

Adding an Appliance Virtualization Platform or ESXi host

About this task

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

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

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

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

Before you begin

A location must be available.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> section, click Add.
4. In the New Host section, provide the Host name, IP address or FQDN, user name, and password.
5. Click Save.
   The system generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can only accept the certificate. If the certificate is invalid, to generate certificate, see the VMware documentation.
   In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select the required virtual machine.
   b. Click More Actions > Re-establish connection.
      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
c. Click **More Actions > Refresh VM**.

**Important:**

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

8. On the **Hosts** tab, select the required host and click **Refresh**.

**Next steps**

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

1. Under VM Management Tree, establish trust for all the virtual machines that are deployed on the host.
2. Ensure that the system populates the **Application Name** and **Application Version** for each virtual machine.
3. Once you have performed a trust establishment and refresh host operation on all virtual machines, you can perform refresh operation on the host.

**Related links**

- [Preupgrade tasks](#) on page 27
- [New and Edit host field descriptions](#) on page 68
- [Generating and accepting certificates](#) on page 100

**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 27
- [New and Edit host field descriptions](#) on page 68
Upgrading Appliance Virtualization Platform from Solution Deployment Manager

About this task

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

⚠️ Note:

- From System Manager Solution Deployment Manager, you cannot update Appliance Virtualization Platform that hosts this System Manager.
- When you update Appliance Virtualization Platform, the system shuts down all the associated virtual machines and restarts the Appliance Virtualization Platform host. During the update process, the virtual machines will be out of service. Once Appliance Virtualization Platform update is complete, the system restarts the virtual machines.
- If you are upgrading or updating the Appliance Virtualization Platform host, then you must not restart, shutdown, upgrade, or install the patch on the virtual machine that is hosted on the same Appliance Virtualization Platform host.
- If you are deploying or upgrading a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.
- If you are installing a patch on a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.
- If you are using services port to update or upgrade Appliance Virtualization Platform, connect the system directly with the Appliance Virtualization Platform services port (Gateway 192.168.13.1). If you connect the system using the Utility Services services port (Gateway 192.11.13.1), the Appliance Virtualization Platform update or upgrade fails.

Before you begin

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

⚠️ Note:

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

Procedure

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

5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.

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

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

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

   **Enable: (Recommended)**

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

   **Disable:**

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

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

      Avaya recommends to enable EASG.

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

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

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

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

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

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

   Host Create/Update Status window displays the details. The patch installation takes some time. When the patch installation is complete, the **Current Action** column displays the status.
Next steps
If the virtual machines that were running on the Appliance Virtualization Platform host do not automatically restart, manually restart the machines.

Related links
Preupgrade tasks on page 27
Update Host field descriptions on page 71

Changing the network parameters for an Appliance Virtualization Platform host

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

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click Change Network Params > Change Host IP Settings.
4. In the Host Network/ IP Settings section, change the IP address, subnetmask, and other parameters as appropriate.
   Note:
   An Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

   If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:
   - Public or signaling traffic, Appliance Virtualization Platform, and all virtual machines public traffic.
   - Management, Appliance Virtualization Platform, and all virtual machine management ports.

5. To change the gateway IP address, perform the following:
   a. Click Change Gateway.
      The Gateway field becomes available for providing the IP address.
   b. In Gateway, change the IP address.
Preupgrade tasks

c. Click **Save Gateway**.

6. Click **Save**.

The system updates the Appliance Virtualization Platform host information.

Related links

- [Preupgrade tasks](#) on page 27
- [Change Network Parameters field descriptions](#) on page 69

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

About this task

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

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

**Note:**

- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fails because public IP address cannot be reached with the service port. To avoid this error, edit the host with the service port IP address again.

- If FQDN of the Appliance Virtualization Platform host is updated by using Host Network/IP setting for domain name, refresh the host to get the FQDN changes reflect in Solution Deployment Manager.

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

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click Change Network params > Change Network Settings.

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

You can configure port groups for the following switches:

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

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

      The section displays the vSwitch details.

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

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

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

      For more information about the value, see NIC teaming.

   d. Click **OK**.

   The system displays the new VLAN ID.

**Note:**

You can change the services port VLAN ID for S8300D servers only through Solution Deployment Manager.
6. To change the NIC speed, perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.
      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.
      For more information, see VLAN ID assignment.
      The system displays the updated NIC speed in the **Speed** column.
      If the NIC is connected, the system displays ✓ in **Link Status**.
   
   ✤ **Note:**
   You can change the speed only for common servers. You cannot change the speed for S8300D and S8300E servers.

7. To change the NIC teaming, perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.
      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or unteamning, 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 27
[Host Network / IP Settings field descriptions](#) on page 70
Changing the password for an Appliance Virtualization Platform host

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click More Actions > Change Password.
4. In the Change Password section, type the current password and the new password.
   For more information about password rules, see “Password policy”.
5. Click Change Password.
   The system updates the password of the Appliance Virtualization Platform host.

Related links
Preupgrade tasks on page 27
Password policy on page 53
Change Password field descriptions on page 71

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: myPassword1ok
If the password does not meet the requirements, the system prompts you to enter a new password. Enter the existing password and the new password in the correct fields.

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

Related links
Changing the password for an Appliance Virtualization Platform host on page 53
Generating the Appliance Virtualization Platform kickstart file

**Procedure**

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

2. In the lower pane, click **Generate AVP Kickstart**.

3. On **Create AVP Kickstart**, enter the appropriate information, and click **Generate Kickstart File**.

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

**Related links**

- [Preupgrade tasks](#) on page 27
- [Create AVP Kickstart field descriptions](#) on page 54

**Create AVP Kickstart field descriptions**

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

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secondary IPv4 NTP Server</strong></td>
<td>Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.</td>
</tr>
<tr>
<td><strong>Main IPv4 DNS Server</strong></td>
<td>Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.</td>
</tr>
<tr>
<td><strong>Secondary IPv4 DNS server</strong></td>
<td>Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.</td>
</tr>
<tr>
<td><strong>AVP management IPv6 address</strong></td>
<td>IPv6 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>AVP IPv6 prefix length</strong></td>
<td>IPv6 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>AVP gateway IPv6 address</strong></td>
<td>IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.</td>
</tr>
<tr>
<td><strong>IPv6 NTP server</strong></td>
<td>IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td><strong>Secondary IPv6 NTP server</strong></td>
<td>Secondary IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td><strong>Main IPv6 DNS server</strong></td>
<td>Main IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td><strong>Secondary IPv6 DNS server</strong></td>
<td>Secondary IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
</tbody>
</table>
| **Public vLAN ID (Used on S8300D and E only)** | VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. 
Use **Public VLAN ID** only on S8300D and S8300E servers. |
| **Out of Band Management Setup**          | The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. 
The options are:
• **yes**: To enable Out of Band Management
  The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode.
• **no**: To disable Out of Band Management. The default option. |
| **OOBM vLAN ID (Used on S8300D and E only)** | Out of Band Management VLAN ID for S8300D. Use **OOBM VLAN ID** only on the S8300D server. 
• For S8300E, use the front plate port for Out of Band Management 
• For common server, use eth2 for Out of Band Management. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVP Super User Admin Password</td>
<td>Admin password for Appliance Virtualization Platform. The password must contain 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Admin password for Appliance Virtualization Platform.</td>
</tr>
<tr>
<td>Enable Stricter Password</td>
<td>The check box to enable or disable the stricter password. The password must contain 14 characters.</td>
</tr>
<tr>
<td>WebLM IP/FQDN</td>
<td>The IP Address or FQDN of WebLM Server.</td>
</tr>
<tr>
<td>WebLM Port Number</td>
<td>The port number of WebLM Server. The default port is 52233.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate Kickstart File</td>
<td>Generates the Appliance Virtualization Platform kickstart file and the system prompts you to save the file on your local computer.</td>
</tr>
</tbody>
</table>

Related links

[Generating the Appliance Virtualization Platform kickstart file](#) on page 54

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

About this task

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

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, click **More Actions > SSH > Enable SSH**.
5. On the Confirm dialog box, in the **Time (in minutes)** field, type the time after which the system times out the SSH connection.
   - The value range is from 10 minutes through 120 minutes.
6. Click **Ok**.
   - The system displays **enabled** in the **SSH status** column.
7. To disable SSH, click **More Actions > SSH > Disable SSH**.
The system displays disabled in the SSH status column.

Related links
Preupgrade tasks on page 27

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

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

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

Before you begin
Start an SSH session.

Procedure
1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Navigate to the $MGMT_HOME/infra/bin/avpSSHUtility location.
3. Type ./enableDisableSSHOnAVP.sh.
   The system displays the following options:
   • Enable SSH on the Appliance Virtualization Platform host.
   • Disable SSH on the Appliance Virtualization Platform host.
   • Check the SSH status on the Appliance Virtualization Platform host.
4. To enable SSH, perform the following:
   a. At the prompt, type 1 and press Enter.
   b. Type the IP address of the Appliance Virtualization Platform host.
   c. Type the time in minutes.
      The time is the duration after which the system blocks any new SSH connections. The valid range 10 to 120 minutes.
      The system displays the message and enables SSH on Appliance Virtualization Platform host.
      For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.
5. To disable SSH, perform the following:
   a. At the prompt, type 2 and press Enter.
b. Type the IP address of the Appliance Virtualization Platform host.

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

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

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

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

**Related links**

- [Preupgrade tasks](#) on page 27

**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 255.255.255.0 -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 27

Appliance Virtualization Platform license

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

<table>
<thead>
<tr>
<th>Server type</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
</table>
| • Avaya S8300D  
  • Avaya S8300E | Maximum AVP single CPU Embedded Servers |
| Common Server Release 1  
  • HP ProLiant DL360 G7  
  • Dell™ PowerEdge™ R610 | • Maximum AVP single CPU Common Servers  
  • VALUE_AVP_1CPU_CMN_SR VR  
  • VALUE_AVP_2CPU_CMN_SR VR |
| Common Server Release 3  
  • Dell™ PowerEdge™ R630  
  • HP ProLiant DL360 G9 | • Maximum AVP dual CPU Common Servers  
  • VALUE_AVP_XL_SRVR |
| Common Server Release 3  
  • Dell™ PowerEdge™ R630  
  • HP ProLiant DL360 G9 | Maximum AVP XL Server  
  • VALUE_AVP_XL_SRVR |

To configure the Appliance Virtualization Platform license file:

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

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

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

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

- **Normal**: If the Appliance Virtualization Platform host has acquired a license, the License Status column displays Normal.

- **Error**: If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The License Status column displays Error - Grace period expires: <DD/MM/YY> <HH:MM>.

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

Note:

Restricted administrative actions for:

- **AVP Host**: AVP Update/Upgrade Management, Change Password, Host Shutdown, and AVP Cert. Management.

- **Virtual Machine**: New, Delete, Start, Stop, and Update.

**Appliance Virtualization Platform licensing alarms**

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

**Configuring WebLM Server for an Appliance Virtualization Platform host**

**Before you begin**

1. Add an Appliance Virtualization Platform host. For information about adding a host, see “Adding an Appliance Virtualization Platform or ESXi host”.

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

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click More Actions > WebLM Configuration.
      The system displays the WebLM Configuration dialog box.
4. In WebLM IP Address/FQDN, type the IP address or FQDN of WebLM Server.
   For WebLM configuration, if you select:
   • Only one host then WebLM IP Address/FQDN displays the existing WebLM Server IP Address.
   • Multiple hosts then WebLM IP Address/FQDN will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.
5. In Port Number, type the port number of WebLM Server.
   Embedded System Manager WebLM Server supports both 443 and 52233 ports.
6. Click Submit.
   The system displays the status in the Current Action column.
   The system takes approximately 9 minutes to acquire the Appliance Virtualization Platform host license file from the configured WebLM Server. On the Hosts tab, you can click the Refresh icon.
   When the Appliance Virtualization Platform host acquires the license, on the Hosts tab, the License Status column displays Normal.

WebLM Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebLM IP Address/FQDN</td>
<td>The IP Address or FQDN of WebLM Server.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number of WebLM Server. The default port is 52233.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit</td>
<td>Saves the WebLM Server configuration.</td>
</tr>
</tbody>
</table>
**Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager**

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the License Status column.

**Shutting down the Appliance Virtualization Platform host**

**About this task**

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

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.

4. Click More Actions > Lifecycle Action > Host Shutdown.

   The Appliance Virtualization Platform host and virtual machines shut down.

**Related links**

[Preupgrade tasks](#) on page 27

**Restarting Appliance Virtualization Platform or an ESXi host**

**About this task**

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

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.

4. Click More Actions > Lifecycle Action > Host Restart.
5. On the confirmation dialog box, click **Yes**.

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

**Related links**

[Preupgrade tasks](#) on page 27

**Removing an ESXi host**

**Procedure**

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

2. On the Host tab, in the Hosts for Selected Location <location name> section, select one or more hosts that you want to delete.

3. Click **Remove**.

4. On the Delete page, click **Yes**.

**Related links**

[Preupgrade tasks](#) on page 27

**Configuring the login banner for the Appliance Virtualization Platform host**

**About this task**

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

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Host tab, in Hosts for Selected Location <location name>, select one or more Appliance Virtualization Platform hosts on which you want to configure the message.

4. Click **More Actions > Push Login Banner**.

   You can change the login banner text only on the Security Settings page from **Security > Policies** on System Manager.

5. On the Message of the Day window, click **Push Message**.

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

**Mapping the ESXi host to an unknown location**

**About this task**

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

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In the left navigation pane, click the Unknown location host mapping link.
3. In the Host Location Mapping section, select an ESXi host and click Edit.
   The system displays the Host Information page.
4. Select a location to which you want to map the ESXi host.
5. Click Submit.
   The system displays the ESXi host in the selected location.

Related links
Preupgrade tasks on page 27

Applying third-party AVP certificates

Applying third-party Appliance Virtualization Platform certificates

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

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

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. To generate CSR, do the following:
   b. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click View/Generate CSR.
      The system displays the View/Generate CSR dialog box.
   d. Add or edit the details of the generic CSR.
      For more information, see “Creating or editing generic CSR”.

Comments on this document? infodev@avaya.com
e. Click **Generate CSR**.

   The system generates CSR for the Appliance Virtualization Platform host.

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

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

5. To download CSR, do the following:

   a. Click **More Actions > AVP Cert. Management > Manage Certificate**.

   b. Click **Download CSR**.

   c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

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

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

   e. When the system displays a prompt, save the file.

6. Extract the downloaded certificates, and ensure that the third-party signs them.

7. To upload and push the signed certificate from third-party CA, do the following:

   a. Click **More Actions > AVP Cert. Management > Manage Certificate**.

   b. Click **Browse** and select the required certificates for one or more Appliance Virtualization Platform hosts.

   c. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

   d. Agree to add the same certificate on Solution Deployment Manager.

   e. Click **Push Certificate**.

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

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

Related links

- [Preupgrade tasks](#) on page 27

**Creating or editing generic CSR**

**About this task**

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

**Procedure**

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

3. Click More Actions > AVP Cert. Management > Generic CSR.

4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.

5. Click Create/Edit CSR and then click OK.

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

Related links
Preupgrade tasks on page 27

Load AVP host certificate field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>The IP address of the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>Host FQDN</td>
<td>The FQDN of the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>Certificate</td>
<td>The option to select the signed certificate for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>I agree to accept to add the same certificate in SDM.</td>
<td>The option to accept the certificate in Solution Deployment Manager.</td>
</tr>
</tbody>
</table>

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

Related links
Preupgrade tasks on page 27

Create or edit CSR field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>The organization name of the CSR.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>The organization unit of the CSR.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Locality</td>
<td>The locality of the organization associated with the CSR.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the organization associated with the CSR.</td>
</tr>
<tr>
<td>Country</td>
<td>The country of the organization associated with the CSR. In the Edit mode, you can specify only two letters for the country name.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address associated with the CSR.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Button</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Create/Edit CSR</td>
<td>Saves or edits the information entered associated to the CSR.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the add or edit operation of the CSR.</td>
</tr>
</tbody>
</table>

**Related links**

- [Preupgrade tasks](#) on page 27

**Deleting the virtual machine snapshot by using Solution Deployment Manager**

**About this task**

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

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host.

4. Click **More Actions > Snapshot Manager**.
   - The system displays the Snapshot Manager dialog box.

5. Select one or more snapshots, and click **Delete**.
   - The system deletes the selected snapshots.

**Related links**

- [Preupgrade tasks](#) on page 27
- [Snapshot Manager field descriptions](#) on page 68
Snapshot Manager field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM ID</td>
<td>The ID of the virtual machine.</td>
</tr>
<tr>
<td>Snapshot Age</td>
<td>The duration of snapshot creation.</td>
</tr>
<tr>
<td></td>
<td>For example: 75 days 19 hours</td>
</tr>
<tr>
<td>VM Name</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>Snapshot Name</td>
<td>The name of the snapshot.</td>
</tr>
<tr>
<td>Snapshot Description</td>
<td>The description of the snapshot.</td>
</tr>
<tr>
<td>SDM Snapshot</td>
<td>The snapshot taken from Solution Deployment Manager.</td>
</tr>
<tr>
<td></td>
<td>The options are <strong>Yes</strong> and <strong>No</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel</td>
<td>Exits from the Snapshot Manager dialog box.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected snapshot.</td>
</tr>
</tbody>
</table>

Related links
Deleting the virtual machine snapshot by using Solution Deployment Manager on page 67

New and Edit host field descriptions

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the host information and returns to the Hosts for Selected Location &lt;location name&gt; section.</td>
</tr>
</tbody>
</table>
### Change Network Parameters field descriptions

#### Network Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Appliance Virtualization Platform host. The field is display-only.</td>
</tr>
<tr>
<td>IPv4</td>
<td>The IPv4 address of the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the Appliance Virtualization Platform host (if any).</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name the Appliance Virtualization Platform host</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name the Appliance Virtualization Platform host</td>
</tr>
<tr>
<td>Preferred DNS Server</td>
<td>The preferred DNS server</td>
</tr>
<tr>
<td>Alternate DNS Server</td>
<td>The alternate DNS server</td>
</tr>
<tr>
<td>NTP Server1 IP/FQDN</td>
<td>The NTP Server1 IP address of the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>NTP Server2 IP/FQDN</td>
<td>The NTP Server2 IP address of the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>IPv4 Gateway</td>
<td>The gateway IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you click <strong>Change IPv4 Gateway</strong>.</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>The default gateway IPv6 address (if any).</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you IPv6 has been configured for the system. The user, also needs to click <strong>Change IPv6 Gateway</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change IPv4 Gateway</td>
<td>Makes the IPv4 Gateway field available, and displays <strong>Save IPv4 Gateway</strong> and <strong>Cancel IPv4 Gateway Change</strong> buttons.</td>
</tr>
<tr>
<td>Change IPv6 Gateway</td>
<td>Makes the IPv6 Default Gateway field available, and displays <strong>Save IPv6 Default Gateway</strong> and <strong>Cancel IPv6 Default Gateway Change</strong> buttons.</td>
</tr>
<tr>
<td>Save IPv4 Gateway</td>
<td>Saves the gateway IPv4 address value that you provide.</td>
</tr>
</tbody>
</table>

*Table continues...*
Preupgrade tasks

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel IPv4 Gateway Change</td>
<td>Cancels the changes made to the IPv4 gateway.</td>
</tr>
<tr>
<td>Save IPv6 Default Gateway</td>
<td>Saves the default IPv6 gateway address value that you provide.</td>
</tr>
<tr>
<td>Cancel IPv6 Default Gateway Change</td>
<td>Cancels the changes made to the IPv6 default gateway.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the changes that you made to network parameters.</td>
</tr>
</tbody>
</table>

Related links

- Preupgrade tasks on page 27

Host Network / IP Settings field descriptions

Port Groups

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>or VLAN ID link</td>
<td>Displays the Port Group Properties page where you configure VLAN ID.</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change NIC speed</td>
<td>Displays the vmnic&lt;n&gt; dialog box.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC team/unteam</td>
<td>Displays the Out of Band Management Properties vSwitch&lt;n&gt; dialog box.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move Up</td>
<td>Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.</td>
</tr>
<tr>
<td>Move Down</td>
<td>Moves the VMNIC from active to standby adapter or from standby to unused adapter.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the page.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves the changes.</td>
</tr>
</tbody>
</table>

Related links
Preupgrade tasks on page 27

Change Password field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Password</td>
<td>The password for the user you input when adding the host.</td>
</tr>
<tr>
<td>New Password</td>
<td>The new password</td>
</tr>
<tr>
<td>Confirm New Password</td>
<td>The new password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</td>
<td>Saves the new password.</td>
</tr>
</tbody>
</table>

Related links
Preupgrade tasks on page 27

Update Host field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch location</td>
<td>The location where the Appliance Virtualization Platform patch is available. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Select Patch from Local SMGR: To use the Appliance Virtualization Platform patch that is available on the local System Manager.</td>
</tr>
<tr>
<td></td>
<td>• Select Patch from software library: To use the Appliance Virtualization Platform patch that is available in the software library.</td>
</tr>
</tbody>
</table>

Table continues…
Preupgrade tasks

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Signature Validation</td>
<td>Ignores the signature validation for the patch.</td>
</tr>
<tr>
<td></td>
<td>Note: If the Appliance Virtualization Platform patch is unsigned, you must select the Ignore signature validation check box.</td>
</tr>
<tr>
<td>Select patch file</td>
<td>The absolute path to the Appliance Virtualization Platform patch file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Host</td>
<td>Installs the patch on the Appliance Virtualization Platform host.</td>
</tr>
</tbody>
</table>

Related links
Related links
Preupgrade tasks on page 27

**Downloading the OVA file to System Manager**

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

**Before you begin**
Set the local software library.

**Procedure**

1. Download the OVA file on your computer.
2. On the System Manager web console, click Services > Solution Deployment Manager.
3. In the navigation pane, click Download Management.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click Show Files.
   b. In the Select Files Download Details section, in the Source field, select My Computer.
   c. Click Download.
   The system displays the Upload File page.
5. In the Software Library field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click Browse and select the OVA file from the location on the system.
8. Provide a valid file type.
This system uploads the OVA file from local computer to the designated software library on System Manager.

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

**Related links**
Preupgrade tasks on page 27
Managing the virtual machine

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

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

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

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

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.
   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.
      The system displays the host name in the **Host FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.
   The page displays the capacity details.
6. Click **Next**.

7. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.
      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Flexi Footprint**, select the footprint size that the application supports.
      
         • **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
         • **Default**: For all other server platforms.

8. Click **Next**.

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

9. In the Network Parameters section, ensure that the following fields are preconfigured:
   
      • **Public**
      • **Services**: Only for Utility Services
      • **Duplicate Link**: Only for duplex Communication Manager
      • **Out of Band Management**: Only if Out of Band Management is enabled

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

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

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

11. Click **Deploy**.

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

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

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

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

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

14. Reboot the Utility Services virtual machine.

**Next steps**

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

Related links
Preupgrade tasks on page 27
VM Deployment field descriptions on page 85
Network Parameters and Configuration Parameters field descriptions

Deploying an OVA file for an Avaya Aura® application

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

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

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

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click New.
   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In Select Location, select a location.
   b. In Select Host, select a host.
      The system displays the host name in the Host FQDN field.
5. In Data Store, select a data store, if not displayed upon host selection.
   The page displays the capacity details.
6. Click Next.
7. To get the OVA file, select the OVA tab, and do one of the following:
   • Click URL, in OVA File, type the absolute path to the OVA file, and click Submit.
   • Click S/W Library, in File Name, select the OVA file.
8. In **Flexi Footprint**, select the footprint size that the application supports.

9. **(Optional)** To install the patch file for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
   • Click **URL**, and provide the absolute path to the latest service or feature pack.
   • Click **S/W Library**, and select the latest service or feature pack.
   • Click **Browse**, and select the latest service or feature pack.

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

10. Click **Next**.

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

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

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

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

13. Click **Deploy**.

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

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

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

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

**Next steps**

Perform the following for Communication Manager:

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

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

### Related links
- [Pre_upgrade_tasks](#) on page 27
- [Installing software patches](#) on page 77
- [VM Deployment field descriptions](#) on page 85

### Re-establishing trust for Solution Deployment Manager elements

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

#### Before you begin
- Add a location.
- Add an Appliance Virtualization Platform host to the location.

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

### Related links
- [Pre_upgrade_tasks](#) on page 27

### Installing software patches

#### About this task
Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.
Note:
When you are installing an element patch and the patch installation fails or the patch information is unavailable in Upgrade Actions > Installed Patches on the Upgrade Management page, then perform the following:

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

Before you begin

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

Procedure

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

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

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

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

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

15. To view the update status, click ✔. The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.
   When the update is complete, the **Update status** and **Last Action Status** fields display ✔.

16. Click **Upgrade Actions > Installed Patches**.

17. On the Installed Patches page, in the Patch Operation section, click **Commit**.
   The page displays all software patches that you can commit.
   You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.
   You can schedule to commit the patch at a later time by using the **Schedule later** option.

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

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

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

**Related links**

- [Preupgrade tasks](#) on page 27
- [Deleting the virtual machine snapshot from the Appliance Virtualization Platform host](#) on page 150
- [Deleting the virtual machine snapshot from the vCenter managed host or standalone host](#) on page 151
- [Preupgrade Configuration field descriptions](#)
- [Upgrade Configuration field descriptions](#) on page 129
- [Edit Upgrade Configuration field descriptions](#) on page 130
- [Installed Patches field descriptions](#) on page 125
Editing a virtual machine

Before you begin

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

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.
   The system displays the Edit VMs section.
4. **(Optional)** Click **Change Flexi Footprint** and do the following:
   a. Click **Change flexi foot print value**.
   b. In **Flexi Footprint**, select a footprint 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 27

**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 27

**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 27
Change Network Parameters field descriptions on page 69
Changing the network parameters for an Appliance Virtualization Platform host on page 49
Network parameter update for Avaya Aura applications on page 96

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 27
Update Static Routing field descriptions on page 94
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 27

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 27

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 27

**Common causes for VM deployment failure**

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

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

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

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

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

**Related links**

[Preupgrade tasks](#) on page 27

**VM Deployment field descriptions**

**Select Location and Host**

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

**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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name</td>
</tr>
<tr>
<td>Full Capacity</td>
<td>The maximum capacity</td>
</tr>
<tr>
<td>Free Capacity</td>
<td>The available capacity</td>
</tr>
<tr>
<td>Reserved Capacity</td>
<td>The reserved capacity</td>
</tr>
<tr>
<td>Status</td>
<td>The configuration status</td>
</tr>
</tbody>
</table>

**Deploy OVA on System Manager Solution Deployment Manager**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ME Deployment</td>
<td>The option to perform the Midsize Enterprise deployment.</td>
</tr>
<tr>
<td>Enable enhanced security</td>
<td>The option to enable JITC mode deployment.</td>
</tr>
<tr>
<td>Select Software Library</td>
<td>The software library where the .ova file is available.</td>
</tr>
<tr>
<td>Select OVAs</td>
<td>The .ova file that you want to deploy.</td>
</tr>
<tr>
<td>Flexi Footprint</td>
<td>The footprint size supported for the selected host.</td>
</tr>
</tbody>
</table>

**Note:**
System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.

**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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ME Deployment</td>
<td>The option to perform the Midsize Enterprise deployment.</td>
</tr>
<tr>
<td>Enable enhanced security</td>
<td>The option to enable JITC mode deployment.</td>
</tr>
</tbody>
</table>

The system displays the following options for deployment by providing OVA path.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>The option to enter the full/absolute path of the .ova file to install it as a virtual machine on the system that hosts the Solution Deployment Manager client.</td>
</tr>
<tr>
<td>OVA File</td>
<td>The absolute path to the .ova file on the system that hosts the Solution Deployment Manager client.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you click <strong>Provide OVA Path</strong>.</td>
</tr>
<tr>
<td>Submit File</td>
<td>Selects the .ova file of System Manager that you want to deploy.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>The file name of the .ova file that is to be installed on the system that hosts the Solution Deployment Manager client.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you click <strong>S/W Library</strong>.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The URL of the .ova file that is to be installed on the system that hosts the Solution Deployment Manager client.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you click <strong>URL</strong>.</td>
</tr>
<tr>
<td>Submit</td>
<td>Selects the .ova file to be deployed that is extracted from the URL.</td>
</tr>
</tbody>
</table>

The system displays the following common fields.

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

**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 90.

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

Table 2: Configuration Parameters for Communication Manager simplex OVA deployment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM IPv4 Address</td>
<td>The IPv4 address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Netmask</td>
<td>The IPv4 network mask of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Gateway</td>
<td>The IPv4 default gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Address</td>
<td>The IPv6 address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Gateway</td>
<td>The IPv6 gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>Out of Band Management IPv4 Address</td>
<td>The IPv4 address of the Communication Manager virtual machine for out of band management. The field is optional.</td>
</tr>
<tr>
<td>Out of Band Management IPv4 Netmask</td>
<td>The IPv4 subnetwork mask of the Communication Manager virtual machine for out of band management.</td>
</tr>
</tbody>
</table>

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

### Network Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>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.</td>
</tr>
</tbody>
</table>
Name | Description
--- | ---
Services | The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.

Duplication Link | The connection for server duplication. The field is available only when you deploy duplex Communication Manager.

Out of Band Management | The port number that is mapped to the out of band management port group.

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

**Related links**

[VM Deployment Configuration and Network Parameters field descriptions](#) on page 90

**VM Deployment Configuration and Network Parameters field descriptions**

**Table 3: Configuration Parameters for Communication Manager Messaging deployment**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging IPv4 address</td>
<td>The IP address of the Communication Manager Messaging virtual machine.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging IPv4 Netmask</td>
<td>The network mask of the Communication Manager Messaging virtual machine.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging IPv4 Gateway</td>
<td>The default gateway of the Communication Manager Messaging virtual machine. For example, 172.16.1.1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of Band Management IPv4 Address</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of Band Management IPv4 Netmask</td>
<td>The subnetwork mask of the Communication Manager Messaging virtual machine for out of band management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging Hostname</td>
<td>The hostname of the Communication Manager Messaging virtual machine.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Servers</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). The field is optional.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Name Description

**DNS Server(s)** The DNS IP address of the Communication Manager Messaging virtual machine. Separate the IP addresses with commas (,). The field is optional.

**Search Domain List** The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).

**WebLM Server IPv4 Address** The IP address of WebLM. The field is mandatory.

**Messaging Privileged Administrator User Login** The login name for the privileged administrator. You can change the value at any point of time.

**Messaging Privileged Administrator User Password** The password for the privileged administrator. You can change the value at any point of time.

**Confirm Password** The password required to be confirmed.

---

### Configuration and Network Parameters for Utility Services deployment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Networking Properties</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>Linux hostname or fully qualified domain name for Utility Services virtual machine.</td>
</tr>
<tr>
<td></td>
<td>💡 <strong>Note:</strong> The host name is regardless of the interface that is used to access. The Public interface is the default interface.</td>
</tr>
<tr>
<td><strong>Public IP address</strong></td>
<td>The IP address for this interface. Required field unless you use DHCP.</td>
</tr>
<tr>
<td><strong>Public Netmask</strong></td>
<td>The netmask for this interface. Required field unless you use DHCP.</td>
</tr>
<tr>
<td><strong>Public Default Gateway</strong></td>
<td>The IP address of the default gateway. Required field unless you use DHCP.</td>
</tr>
<tr>
<td></td>
<td>💡 <strong>Note:</strong> The default gateway should be configured for the Public network. You can use the <code>ovf_set_static</code> command to allow a static route to be assigned to the OOBM network, enabling OOBM network to reach a second subnet.</td>
</tr>
<tr>
<td><strong>Public IPv6 address</strong></td>
<td>The IP address for this interface. Required field unless you use DHCP.</td>
</tr>
<tr>
<td><strong>Public IPv6 Prefix</strong></td>
<td>The netmask for this interface. Required field unless you use DHCP.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default IPv6 Gateway</td>
<td>The IP address of the default gateway. Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Out of Band Management IP Address</td>
<td>The IP address for this interface.</td>
</tr>
<tr>
<td>Out of Band Management Netmask</td>
<td>The netmask for this interface.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Address</td>
<td>The IPv6 address for this interface. This field is optional.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Prefix</td>
<td>The IPv6 prefix for this interface. This field is optional.</td>
</tr>
<tr>
<td>Network Time Protocol IP</td>
<td>IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.</td>
</tr>
<tr>
<td>Timezone setting</td>
<td>The selected timezone setting for the Utility Services virtual machine.</td>
</tr>
<tr>
<td>DNS</td>
<td>The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP. You can specify up to three DNS Servers.</td>
</tr>
<tr>
<td>Name</td>
<td>Primary WebLM IP address for Licensing. A valid Utility Services license is required for all deployment types and modes other than deployment on Appliance Virtualization Platform.</td>
</tr>
<tr>
<td>Primary System Manager IP address for application registration</td>
<td>The IP address of System Manager that is required for application registration.</td>
</tr>
<tr>
<td>Enrollment Password</td>
<td>The enrollment password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The confirmation password.</td>
</tr>
<tr>
<td>Application Properties</td>
<td></td>
</tr>
<tr>
<td>Communication Manager IP</td>
<td>IP address of Communication Manager.</td>
</tr>
</tbody>
</table>

**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.
Utility Services Mode

The mode in which you want to deploy Utility Services. The options are:

- **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform.
  
  You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed.

- **Utility Services Only**: Use to disable routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the services port becomes non-operational.

- **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services, or when Utility Services are not required.

  With the services port feature, through a laptop connected to the services port of Appliance Virtualization Platform, you can gain access to Avaya virtual machines and the hypervisor that are deployed.

- **Hardened Mode Services Port Only**: Sets up the system for military grade hardening.

**Note:**
With Utility Services 7.1.2 onwards, you can apply extended security hardening by selecting one of the following modes only:

- **Services Port Only**
- **Hardened Mode services port only**

**Note:**
For the Solution Deployment Manager client to connect to the services port features of Utility Services, change the IP address to 192.11.13.5 on the computer of the technician

Utility Services can gain access to the hypervisor and all virtual machines through the IP address 192.11.13.6. Utility Services provides application routing between the physical port and virtual applications.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User Password</td>
<td>The admin user password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The confirmation password.</td>
</tr>
</tbody>
</table>
Out of Band Management Mode

The Out of Band Management mode in which you want to deploy. The options are as follows:

- **OOBM_Enabled**: To enable Out of Band Management.
- **OOBM_Disabled**: To disable Out of Band Management.

**Note:**

**OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.

---

### Update Static Routing field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The virtual machine name</td>
</tr>
<tr>
<td>VM IP/FQDN</td>
<td>The IP address or FQDN of the virtual machine</td>
</tr>
<tr>
<td>Utility Services IP</td>
<td>The IP address of Utility Services</td>
</tr>
</tbody>
</table>

**Button**

- **Update**: Updates the static IP address for routing.

---

### Related links

- [Preupgrade tasks on page 27](#)

---

### Installed Patches field descriptions

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<p>| 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.                                     |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The name of the System Manager virtual machine on which you want to install the patch.</td>
</tr>
<tr>
<td>VM IP</td>
<td>The IP address of System Manager on which you want to install the patch.</td>
</tr>
<tr>
<td>Patch Name</td>
<td>The software patch name that you want to install.</td>
</tr>
<tr>
<td>Patch Type</td>
<td>The patch type. The options are service pack and software patch.</td>
</tr>
<tr>
<td>Patch Version</td>
<td>The software patch version.</td>
</tr>
<tr>
<td>Patch State</td>
<td>The software patch state. The states are:</td>
</tr>
<tr>
<td></td>
<td>• Activated</td>
</tr>
<tr>
<td></td>
<td>• Deactivated</td>
</tr>
<tr>
<td></td>
<td>• Removed</td>
</tr>
<tr>
<td></td>
<td>• Installed</td>
</tr>
<tr>
<td>Patch Status</td>
<td>The software patch status.</td>
</tr>
</tbody>
</table>

**Related links**

[Preupgrade tasks](#) on page 27

**Update VM field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The System Manager virtual machine name</td>
</tr>
<tr>
<td>VM IP</td>
<td>The IP address of System Manager</td>
</tr>
<tr>
<td>VM FQDN</td>
<td>FQDN of System Manager</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name</td>
</tr>
<tr>
<td>Select bin file from Local SMGR</td>
<td>The option to select the software patch or service pack for System Manager.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This option is available only on the Solution Deployment Manager client.</td>
</tr>
<tr>
<td>Auto commit the patch</td>
<td>The option to commit the software patch or service pack automatically.</td>
</tr>
<tr>
<td></td>
<td>If the check box is clear, you must commit the patch from More Actions &gt; Installed Patches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Installs the software patch or service pack on System Manager.</td>
</tr>
</tbody>
</table>
Reestablish Connection field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The virtual machine name</td>
</tr>
<tr>
<td>VM IP/FQDN</td>
<td>The IP address or FQDN of the virtual machine</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name</td>
</tr>
<tr>
<td>Password</td>
<td>The password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reestablish Connection</td>
<td>Establishes connection between System Manager and the virtual machine.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Avaya Aura® application</th>
<th>Command</th>
<th>Interface where you perform the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Virtualization Platform</td>
<td>serverInitialNetworkConfig</td>
<td>CLI</td>
</tr>
<tr>
<td>System Manager</td>
<td>changeIPFQDN -IP &lt;IPv4 address&gt; -FQDN &lt;FQDN&gt; -GATEWAY &lt;IPv4 Gateway address&gt; -NETMASK &lt;Netmask address&gt; -DNS &lt;DNS address&gt; -SEARCH &lt;search list of domain names&gt; -IPV6 &lt;IPv6 address&gt; -IPV6GW &lt;IPv6 Gateway address&gt; -IPV6PREFIX &lt;IPv6 prefix&gt;</td>
<td>CLI</td>
</tr>
<tr>
<td>Avaya Aura® application</td>
<td>Command</td>
<td>Interface where you perform the task</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Communication Manager</td>
<td>-</td>
<td>The Network Configuration page from Administration &gt; server(Maintenance) &gt; ServerConfiguration on Communication Manager SMI.</td>
</tr>
<tr>
<td>Session Manager</td>
<td>SMnetSetup</td>
<td>CLI</td>
</tr>
<tr>
<td>Avaya Breeze™ and all installed snap-ins</td>
<td>CEnetSetup</td>
<td>CLI</td>
</tr>
<tr>
<td>Utility Services</td>
<td>VMware_conf.sh</td>
<td>CLI</td>
</tr>
<tr>
<td>Avaya Aura® Messaging</td>
<td>-</td>
<td>See the Avaya support website.</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>-</td>
<td>See the Avaya support website.</td>
</tr>
<tr>
<td>SAL Gateway</td>
<td>-</td>
<td>Currently, you cannot change Network Parameters for SAL Gateway</td>
</tr>
</tbody>
</table>

### Related links

[Preupgrade tasks](#) on page 27

### Virtual machine report

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

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

⚠️ **Important:**

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

#### generate_report.sh command

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

**Syntax**

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

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

Generating a virtual machine report

Before you begin

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

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password> command:
   For example: ./generate_report.sh -g -u admin -p password
   The system displays the following message: Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].
4. To proceed with report generation, type Y, and press Enter.
   The system generates the report in the .csv format in the /swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv folder.
   Note: If you re-run the report generation script when the report generation process is in progress, the system displays the following message: Report Generation Process is Already Running, Kindly try after some time.
5. (Optional) To view the logs, go to /swlibrary/reports/generate_report-YYYYMMDDxxxx.log.

Viewing the status of the virtual machine report

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh –s command.
   If the virtual machine report generation is in progress, the system displays the following message: Report Generation Process is Running.
**Aborting the virtual machine report generation**

**About this task**

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

**Procedure**

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

   The system aborts the virtual machine report generation process.

**Certificate validation**

**Certification validation**

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

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

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

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

**Note:**

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

- Log Certificate Validation Events

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

For the correct certificate:

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

• For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.

• For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

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

**Note:**

Solution Deployment Manager:

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

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

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

**Related links**

Generating and accepting certificates

**About this task**

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

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

• Get a correct certificate for the host and add the certificate.

• Regenerate a self-signed certificate on the host.

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

**Before you begin**

Require permissions to add a host to generate certificates.

**Procedure**

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

2. In VM Management Tree, select a location.

3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.

4. Click **More Actions > AVP Cert. Management > Generate/Accept Certificate**.
5. On the Certificate window, do the following:
   a. Click **Generate Certificate**.

   🌟 **Note:**
   You can generate certificate only for the Appliance Virtualization Platform host.

   b. Click **Accept Certificate**.

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

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

**Related links**
- Preupgrade tasks on page 27
- Adding an Appliance Virtualization Platform or ESXi host on page 45
- Generating new self-signed certificates for the ESXi host on page 103

**Updating the certificate on the ESXi host from VMware**

**About this task**
Use the procedure to update the ESXi host certificate.

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

**Before you begin**
Start an SSH session on the ESXi host.

**Procedure**
1. Start vSphere Web Client, and log in to the ESXi host as admin or root user.

2. Ensure that the domain name and the hostname of the ESXi host is set correctly and matches the FQDN that is present on the DNS servers, correct the entries to match if required.
   For security reason, the common name in the certificate must match the hostname to which you connect.

3. To **generate new certificates**, type `/sbin/generate-certificates`.
   The system generates and installs the certificate.

4. Restart the ESXi host.

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

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

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

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

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

Related links
- Preupgrade tasks on page 27
- Generating new self-signed certificates for the ESXi host on page 103

Managing certificates for existing hosts

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

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

Before you begin
Require permissions to add a host to generate certificates.

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

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

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

Related links
   Preupgrade tasks on page 27
   Generating new self-signed certificates for the ESXi host on page 103
   Generating and accepting certificates on page 100

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:

   ```sh
   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 27

**Managing vCenter**

**Adding a vCenter to Solution Deployment Manager**

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

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

**Before you begin**
Ensure that you have the required permissions.

**Procedure**
1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
   b. In **User Name**, type user name to log in to vCenter.
   c. In **Password**, type password to log in to vCenter.
   d. In **Authentication Type**, select the authentication type.
      If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.
e. *(Optional)* If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC).**

PSC must have a valid certificate.

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

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

5. Click **Save**.

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

   The system generates the certificate and adds vCenter.

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

**Related links**
- [Preupgrade tasks](#) on page 27
- [Editing vCenter](#) on page 105
- [Map vCenter field descriptions](#) on page 106
- [New vCenter and Edit vCenter field descriptions](#) on page 107

**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 27
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 27

Map vCenter field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vCenter server.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the vCenter server.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The FQDN of the vCenter server.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>License</th>
<th>The license type of the vCenter server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The license status of the vCenter server.</td>
</tr>
<tr>
<td>Certificate Status</td>
<td>The certificate status of the vCenter server. The values are:</td>
</tr>
<tr>
<td></td>
<td>* ✓: The certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>* ✗: The certificate is not accepted or invalid.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Displays the certificate status details of the vCenter server.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate/Accept Certificate</td>
<td>Displays the certificate dialog box where you can generate and accept certificate for vCenter.</td>
</tr>
<tr>
<td></td>
<td>For vCenter, you can only accept certificate. You cannot generate certificate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Displays the New vCenter page, where you can add a new ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the Edit vCenter page, where you can update the details and location of ESXi hosts.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the ESXi host.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Updates the list of ESXi hosts in the Map vCenter section.</td>
</tr>
</tbody>
</table>

**Related links**

[Preupgrade tasks](#) on page 27

**New vCenter and Edit vCenter field descriptions**

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves any changes you make to FQDN, username, and authentication type of vCenter.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the vCenter details.</td>
</tr>
</tbody>
</table>
Managed Hosts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The IP address of the ESXi host.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the ESXi host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>The option to edit the location and host.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>ESXi Version</td>
<td>Displays the versions of the ESXi host linked to vCenter FQDN.</td>
</tr>
</tbody>
</table>

**Note:**
For Release 7.1, do not select the 5.0 and 5.1 versions.

| IPv6          | The IPv6 address of the ESXi host.                                         |

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit</td>
<td>Saves all changes that you made to vCenter on the Map vCenter page.</td>
</tr>
</tbody>
</table>

Related links

Preupgrade tasks on page 27

Monitoring a host and virtual machine

**Monitoring a host**

**Procedure**

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

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

**Related links**

[Preupgrade tasks](#) on page 27

### 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 27

---

### Backup and restore

#### Creating a backup

**Before you begin**

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

For more information about changing the hostname, see [Changing the hostname](#) on page 110.

**Procedure**

1. Log in to the Communication Manager System Management Interface with administrator privilege user credentials.
2. On the Administration menu, click Server (Maintenance).
3. In the left navigation pane, click Data Backup/Restore > Backup Now.
   The system displays the Backup Now page.
4. Click Full Backup.
5. In the Network Device section, select the backup method and type the user name, password, hostname, and path of the directory in which you stored the data.
6. Click Start Backup.
   On the Backup Now Results page, the system displays the message Backup Successfully Completed.

Related links
Preupgrade tasks on page 27

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

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

Related links
Preupgrade tasks on page 27

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 27
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
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 Communication Manager from pre–5.2.1 to 7.1.2 and later

About this task

This procedure is applicable if you are upgrading from Communication Manager 3.1.4 or 4.0.5 to Communication Manager Release 7.1.2 and later.

Procedure

1. Log in to the existing Communication Manager web console as a custom user.
2. In the Disk Backup/Restore section, click Backup Now.
3. Select Specify Data Sets, and choose Avaya Call Processing (ACP) Translations and Save ACP translations prior to backup.
4. Under Backup Method, enter the login credentials, and IP address of the server where you want to backup the data.
5. Click Start Backup, and wait until the backup successful message appears.
6. Deploy Communication Manager Release 7.1.2 and later.
   For instructions, see Deploying Avaya Aura® Communication Manager guide.
7. If you are using the same Hostname and IP address of the previous system, shut down the previous system and start the new system.
8. Log in to the new Communication Manager SMI as a custom user.
9. Click Administration > Server (Maintenance).
10. In the Data Backup/Restore section, click View/Restore Data.
11. Select the restore method and provide the server details where the backup is stored, as mentioned in step 4.
12. Click View and verify that the system displays the backup tar.gz file.
13. If the host name is different on the new system than that of the old system, select Force restore if there is a server name mismatch or the server migration.
14. Click Restore, and wait for the Restore Successful message.
15. Restart Communication Manager.
17. Verify that expected Communication Manager translations are present.

Comments on this document? infodev@avaya.com
Next steps

You must configure the following Operating System related data on the new Communication Manager system:

- All customer created Linux users can be noted or copied from the old system and must be recreated manually (the /etc/passed file lists all logins) on the new system. The user login details are available at /etc/passed file.
- Manually copy all cron jobs by using the `crontab -l` CLI command on the old system and reconfigure them on the new system using the `crontab -l` CLI command.
- Since 6.3.1xx and 7.x systems use Net-SNMP, you must re-configure SNMP.
- All other customizations.

**Note:**

- Ensure that a new license file is installed.
- Communication Manager 7.1 and above does not require an authentication file.
- If using a different IP Address, all of the Media Gateways need to be reconfigured with the new MGC IP. This applies to other integrating products as well.
- Communication Manager 7.1 and above includes EASG.

---

**Upgrading Avaya Aura® applications**

**Checklist for upgrading Avaya Aura® applications to Release 7.1.3**

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the OVA files and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:**

For information about the upgrade sequence and the required patches, see the latest Avaya Aura® Release Notes for the specific release on the Avaya Support website.
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Download the Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip file from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Install the Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe file.</td>
<td><a href="#">Installing the Solution Deployment Manager client on your computer</a> on page 24</td>
</tr>
<tr>
<td>4</td>
<td>To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.</td>
<td></td>
</tr>
</tbody>
</table>
| 5   | If System Manager is:  
• Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.1 OVA file, and install the Release 7.1.3 bin file by using the Solution Deployment Manager client.  
• Available: Upgrade System Manager to 7.1 and install the Release 7.1.3 bin file. | |
| 6   | Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from Manage Elements > Discovery. | [“Discovering elements” in Administering Avaya Aura® System Manager](#) |
| 7   | Configure user settings. | [“User settings” in Administering Avaya Aura® System Manager](#) |
| 8   | Use a local System Manager library or create a remote software library.  
**Note:**  
For local, the software local library for TN Boards and media gateway upgrades is not supported. | [“User settings” in Administering Avaya Aura® System Manager](#) |
| 9   | Refresh the elements in the inventory. | [“Refreshing elements” in Administering Avaya Aura® System Manager](#) |
| 10  | Analyze the software. | [“Analyzing software” in Administering Avaya Aura® System Manager](#) |
| 11  | Download the required firmware for the Avaya Aura® application upgrade. | [“Downloading the software” in Administering Avaya Aura® System Manager](#) |

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Analyze the software.</td>
<td>“Solution deployment and upgrades” in Administering Avaya Aura® System Manager</td>
</tr>
<tr>
<td>13</td>
<td>Perform the preupgrade check.</td>
<td>“Performing the preupgrade check” in Administering Avaya Aura® System Manager</td>
</tr>
<tr>
<td>14</td>
<td>Perform the upgrade.</td>
<td>Upgrading Avaya Aura applications to Release 7.1.3 on page 119</td>
</tr>
<tr>
<td>15</td>
<td>Verify that the upgrade is successful.</td>
<td>-</td>
</tr>
</tbody>
</table>

### Upgrading Avaya Aura® applications to Release 7.1.3

**About this task**

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

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

**Before you begin**

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

**Procedure**

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

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

4. Click Upgrade Actions > Upgrade/Update.

5. On the Upgrade Configuration page, select the Override preupgrade check check box. When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

6. To provide the upgrade configuration details, click Edit.

7. On the Edit Upgrade Configuration page, and perform the following:
   a. In Service/Feature Pack for auto-install after migration, provide the Release 7.1.3 patch file.
   b. Complete the details, and click Save.

8. On the Upgrade Configuration page, ensure that the Configuration Status field displays ✓. If the field displays ❌, review the information on the Edit Upgrade Configuration page.

9. Click Save.

10. To save the configuration, click Save Configuration.

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

11. On the Upgrade Configuration page, click Upgrade.

12. On the Job Schedule page, click one of the following:
    • Run Immediately: To perform the job.
    • Schedule later: To perform the job at a scheduled time.

13. Click Schedule.

14. Click Upgrade.

15. On the Upgrade Management page, click 🌊.

    Last Action column displays Upgrade, and Last Action Status column displays ✓. For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, the field displays ❌. This icon indicates that the upgrade is successful and awaiting commit or rollback.

16. For upgrades from Release 7.0.x running on a virtualized environment to Release 7.1.3, do the following:
    a. On the Upgrade Management page, select the element.
    b. Click Upgrade Actions > Commit/Rollback Upgrade.

     The system displays the Job Schedule page.
    c. Select the action to be performed under the Upgrade Action column.
d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.

e. Click **Schedule**.

17. To view the upgrade status, perform the following:

   a. In the navigation pane, click **Upgrade Job Status**.

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

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

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

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

19. For upgrades on the same server, perform the following:

   a. Install the Appliance Virtualization Platform host.

   b. From the VM Management page, add the Appliance Virtualization Platform host.

   c. To continue with the upgrade, click **Upgrade Actions > Resume**.

   d. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.

   e. Continue with the upgrade process.

**Related links**

- [Preupgrade Configuration field descriptions](#)
- [Upgrade Configuration field descriptions](#) on page 129
- [Edit Upgrade Configuration field descriptions](#) on page 130

---

### Installing software patches

**About this task**

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

**Note:**

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

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

2. Refresh the element.

**Before you begin**

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

Procedure

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

⚠️ Note:

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

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

   If the field displays ❌, review the information on the Edit Upgrade Configuration page.
12. Click Upgrade.
13. On the Job Schedule page, click one of the following:

   • Run Immediately: To perform the job.
   • Schedule later: To perform the job at a scheduled time.
14. Click Schedule.

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

   The Upgrade Job Details page displays the detailed update checks that are in progress. Click Done to close the window.
When the update is complete, the Update status and Last Action Status fields display ✔.

16. Click Upgrade Actions > Installed Patches.

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

The page displays all software patches that you can commit.

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

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

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

19. Click Schedule.

The Upgrade Management page displays the last action as Commit.

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

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

Related links
Preupgrade tasks on page 27
Deleting the virtual machine snapshot from the Appliance Virtualization Platform host on page 150
Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 151
Preupgrade Configuration field descriptions
Upgrade Configuration field descriptions on page 129
Edit Upgrade Configuration field descriptions on page 130
Installed Patches field descriptions on page 125

Installing custom software patches

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

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

• Communication Manager
• Session Manager
• Branch Session Manager
• Utility Services
• Communication Manager Messaging
• WebLM
• Application Enablement Services

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions > Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. *(Optional)* Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✔.
    
    If the field displays ☓, review the information on the Edit Upgrade Configuration page.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    
    • **Run Immediately**: To perform the job.
    
    • **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.
    
    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display ✔.
16. To view the update status, click ✔.
    
    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.
    
    When the update is complete, the **Update status** and **Last Action Status** fields displays ✔.
17. Click **Upgrade Actions > Installed Patches**.

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

   The page displays all software patches that you can commit.

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

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

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

20. Click **Schedule**.

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

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

   **Note:**

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

### Next steps

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

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

### Related links

- [Uploading a custom patch](#) on page 139
- [Uploading custom patch field descriptions](#) on page 139

### Installed Patches field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commit</strong></td>
<td>The option to select the patches that you can commit.</td>
</tr>
<tr>
<td><strong>Uninstall</strong></td>
<td>The option to select the patches that you can uninstall.</td>
</tr>
<tr>
<td><strong>Rollback</strong></td>
<td>The option to select the patches that you can rollback.</td>
</tr>
<tr>
<td><strong>Show All</strong></td>
<td>The option to display all the available options.</td>
</tr>
</tbody>
</table>
## Name Description

### Name
- The name of the software patch.

### Element Name
- The element on which the software patch is installed.

### Patch Version
- The version of the software patch.

### Patch Type
- The type of the software patch. The options are:
  - service pack or software patch
  - Kernel

### Patch State
- The state of the software patch. The options are:
  - Installed
  - Activated
  - Deactivated
  - Removed
  - Uninstall
  - Pending

## Name Description

### Schedule Job
- The option to schedule a job:
  - **Run immediately**: To run the upgrade job immediately.
  - **Schedule later**: To run the upgrade job at the specified date and time.

### Date
- The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date.
- This field is available when you select the **Schedule later** option for scheduling a job.

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

### Time Zone
- The time zone of your region.
- This field is available when you select the **Schedule later** option for scheduling a job.

## Name Description

### Schedule
- Runs the job or schedules to run at the time that you configured in Job Schedule.
# Upgrade Management field descriptions

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

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

Table continues...
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Action</td>
<td>The last action performed on the device.</td>
</tr>
<tr>
<td>Last Action Status</td>
<td>The status of the last action that was performed on the device.</td>
</tr>
</tbody>
</table>
| 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**  

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

*Table continues…*
### Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Actions &gt; Cleanup</td>
<td>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.</td>
</tr>
<tr>
<td>Upgrade Actions &gt; Commit</td>
<td>Commits the changes that you made.</td>
</tr>
<tr>
<td>Upgrade Actions &gt; Rollback</td>
<td>Resets the system to the previous state.</td>
</tr>
<tr>
<td>Upgrade Actions &gt; Resume</td>
<td>Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>Download</td>
<td>Displays the File Download Manager page with the list of downloaded software required for upgrade or update.</td>
</tr>
<tr>
<td>Show Selected Elements</td>
<td>Displays only the elements that you selected for preupgrade or update.</td>
</tr>
</tbody>
</table>

### Upgrade Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Parent Name</td>
<td>The parent of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>The device type.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP Address of the device.</td>
</tr>
<tr>
<td>Current Version</td>
<td>The release status of the device.</td>
</tr>
<tr>
<td>Override Preupgrade Check</td>
<td>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.</td>
</tr>
</tbody>
</table>
Override Delete VM on Upgrade Check

The option to override upgrade check recommendations.

When you select this option, the system ignores any recommendations during upgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as Partial_Failure.

Edit

Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.

Configuration Status

An icon that defines the configuration status.

- ![X](Image) Configuration incomplete.
- ![Check](Image) Configuration complete.

Button

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import AVP Configuration(s)</td>
<td>Imports the AVP_Bulk import spread sheet.xlsx spreadsheet. The system displays the Upload AVP Xlsx File Configuration dialog box to upload the AVP_Bulk import spread sheet.xlsx spreadsheet.</td>
</tr>
<tr>
<td>Save Configuration</td>
<td>Saves the upgrade configuration. <strong>Note:</strong> The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Commits the upgrade operation.</td>
</tr>
</tbody>
</table>

### Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- Element Configuration
- AVP Configuration

#### Element Configuration: General Configuration Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>The system name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
</tbody>
</table>

Table continues…
### Operation
The operation that you want to perform on the device. The options are:
- Upgrade/Migration
- Update

### ESXi/AVP host
The ESXi host on which you want to run the device. The options are:
- Same Box
- List of hosts that you added from VM Management

### Migrate With AVP Install
The option to migrate System Platform-based system and Communication Manager Release 5.2.1 bare metal system to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.

### Upgrade Source
The source where the installation files are available. The options are:
- SMGR_DEFAULT_LOCAL
- Remote Software Library

### Upgrade To
The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.

### Service/Feature Pack for auto-install after upgrade/migration
The service pack or feature pack that you want to install.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Commit</td>
<td>The option to automatically commit the upgrade.</td>
</tr>
<tr>
<td>Existing Administrative User</td>
<td>The user name with appropriate admin privileges.</td>
</tr>
<tr>
<td>Existing Administrative Password</td>
<td>The password of the administrator.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-populate Data</td>
<td>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.</td>
</tr>
<tr>
<td>CM IPv4 Address</td>
<td>The IP address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Netmask</td>
<td>The network mask of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Gateway</td>
<td>The default gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Address</td>
<td>The IPv6 address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Gateway</td>
<td>The IPv6 default gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>Out of Band Management IPv4 Address</td>
<td>The IP address of the virtual machine for out of band management.</td>
</tr>
<tr>
<td></td>
<td>The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management Netmask</td>
<td>The subnetwork mask of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Address</td>
<td>The IPv6 address of the virtual machine for out of band management.</td>
</tr>
<tr>
<td></td>
<td>The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>CM Hostname</td>
<td>The hostname of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>The DNS IP address of the virtual machine.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Search Domain List</strong></td>
<td>The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).</td>
</tr>
<tr>
<td><strong>WebLM Server IPv4 Address</strong></td>
<td>The IP address of WebLM. The field is mandatory.</td>
</tr>
<tr>
<td><strong>CM Privileged Administrator User Login</strong></td>
<td>The login name for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td><strong>CM Privileged Administrator User Password</strong></td>
<td>The password for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td><strong>Flexi Footprint</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>The port number that you must assign to public port group.</td>
</tr>
<tr>
<td><strong>Out of Band Management</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>The port number that is assigned to the services port. The system displays this field when Utility Services is available.</td>
</tr>
<tr>
<td><strong>Duplication link</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Datastore</strong></td>
<td>The datastore on the target ESXi host. The field is available only when you select a different host.</td>
</tr>
</tbody>
</table>

The page displays the following fields when you upgrade Session Manager.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing Administrative User</strong></td>
<td>The user name of the administrator.</td>
</tr>
<tr>
<td><strong>Existing Administrative Password</strong></td>
<td>The password of the administrator.</td>
</tr>
<tr>
<td><strong>Pre-populate Data</strong></td>
<td>The option to get the configuration data displayed in the fields.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>The IP address of the virtual machine.</td>
</tr>
<tr>
<td><strong>Short Hostname</strong></td>
<td>The hostname of the virtual machine.</td>
</tr>
<tr>
<td></td>
<td>The hostname of the server and is often aligned with the DNS name of the server.</td>
</tr>
<tr>
<td><strong>Network Domain</strong></td>
<td>The domain name of the virtual machine.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td>The network mask of the virtual machine.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>The default gateway of the virtual machine.</td>
</tr>
<tr>
<td><strong>DNS Servers</strong></td>
<td>The DNS IP address of the virtual machine.</td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td>The timezone of the virtual machine.</td>
</tr>
<tr>
<td><strong>Login Name</strong></td>
<td>The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).</td>
</tr>
<tr>
<td><strong>Enter Customer Account Password</strong></td>
<td>Password to log on to the system.</td>
</tr>
<tr>
<td><strong>Primary System Manager IP</strong></td>
<td>The IP address of System Manager.</td>
</tr>
<tr>
<td><strong>Enrollment Password</strong></td>
<td>The password that is required to establish trust between System Manager and Session Manager.</td>
</tr>
<tr>
<td><strong>Flexi Footprint</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>The port number that you must assign to public port group.</td>
</tr>
<tr>
<td><strong>Out of Band Management</strong></td>
<td>The port number that is assigned to the out of band management port group.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
<tr>
<td><strong>Datastore</strong></td>
<td>The datastore on the target ESXi host.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
</tbody>
</table>
## Element Configuration: End User License Agreement

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Agree to the above end user license agreement</td>
<td>The end user license agreement. You must select the check box to accept the license agreement.</td>
</tr>
</tbody>
</table>

## AVP Configuration: Existing Machine Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>The source IP address.</td>
</tr>
<tr>
<td>Source Administrative User</td>
<td>The source user name with appropriate admin privileges.</td>
</tr>
<tr>
<td>Source Administrative Password</td>
<td>The source password of the administrator.</td>
</tr>
<tr>
<td>Source Root User</td>
<td>The source user name with appropriate root privileges.</td>
</tr>
<tr>
<td>Source Root Password</td>
<td>The source password of the root.</td>
</tr>
</tbody>
</table>

## AVP Configuration: Configuration Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Source</td>
<td>The source where the installation files are available. The options are:</td>
</tr>
<tr>
<td></td>
<td>• SMGR_DEFAULT_LOCAL</td>
</tr>
<tr>
<td></td>
<td>• Remote Software Library</td>
</tr>
<tr>
<td>Upgrade To</td>
<td>The OVA file to which you want to upgrade.</td>
</tr>
<tr>
<td></td>
<td>When you select the local System Manager library, the system displays the</td>
</tr>
<tr>
<td></td>
<td>fields and populates most of the data in the Configuration Details section.</td>
</tr>
<tr>
<td>Dual Stack Setup (with IPv4 and IPv6)</td>
<td>Enables or disables the fields to provide the IPv6 addresses.</td>
</tr>
<tr>
<td>AVP Management IPv4 Address</td>
<td>IPv4 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP IPv4 Netmask</td>
<td>IPv4 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP Gateway IPv4 Address</td>
<td>IPv4 address of the customer default gateway on the network. Must be on the</td>
</tr>
<tr>
<td></td>
<td>same network as the Host IP address.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AVP Hostname</strong></td>
<td>Hostname for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td></td>
<td>The hostname:</td>
</tr>
<tr>
<td></td>
<td>• Can contain alphanumeric characters and hyphen</td>
</tr>
<tr>
<td></td>
<td>• Can start with an alphabetic or numeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1 alphabetic character</td>
</tr>
<tr>
<td></td>
<td>• Must end in an alphanumeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1 to 63 characters</td>
</tr>
<tr>
<td><strong>AVP Domain</strong></td>
<td>Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the</td>
</tr>
<tr>
<td></td>
<td>default value. Format is alphanumeric string dot separated. For example, mydomain.com.</td>
</tr>
<tr>
<td><strong>IPv4 NTP server</strong></td>
<td>IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.</td>
</tr>
<tr>
<td><strong>Secondary IPv4 NTP Server</strong></td>
<td>Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.</td>
</tr>
<tr>
<td><strong>Main IPv4 DNS Server</strong></td>
<td>Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.</td>
</tr>
<tr>
<td><strong>Secondary IPv4 DNS server</strong></td>
<td>Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.</td>
</tr>
<tr>
<td><strong>AVP management IPv6 address</strong></td>
<td>IPv6 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>AVP IPv6 prefix length</strong></td>
<td>IPv6 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>AVP gateway IPv6 address</strong></td>
<td>IPv6 address of the customer default gateway on the network. Must be on the same network as the Host</td>
</tr>
<tr>
<td></td>
<td>IP address.</td>
</tr>
<tr>
<td><strong>IPv6 NTP server</strong></td>
<td>IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td><strong>Secondary IPv6 NTP server</strong></td>
<td>Secondary IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td><strong>Main IPv6 DNS server</strong></td>
<td>Main IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td><strong>Secondary IPv6 DNS server</strong></td>
<td>Secondary IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public vLAN ID (Used on S8300D and E only)</td>
<td>VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use <strong>Public VLAN ID</strong> only on S8300D and S8300E servers.</td>
</tr>
<tr>
<td>Enable Stricter Password (14 char pass length)</td>
<td>The check box to enable or disable the stricter password. The password must contain 14 characters.</td>
</tr>
<tr>
<td>AVP Super User Admin Password</td>
<td>Admin password for Appliance Virtualization Platform. The password must contain 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.</td>
</tr>
</tbody>
</table>
**Enhanced Access Security Gateway (EASG)**

Enable: (Recommended)

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

Disable

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

Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG.

**WebLM IP/FQDN**

The IP Address or FQDN of WebLM Server.

**WebLM Port Number**

The port number of WebLM Server. The default port is 52233.

**Button**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
</tr>
<tr>
<td>Cancel</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Library</td>
<td>The remote software library where you want to upload the custom patch file.</td>
</tr>
<tr>
<td>Product Family</td>
<td>The product family to which the file belongs. In a product family, the number of devices are listed.</td>
</tr>
<tr>
<td>Device Type</td>
<td>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.</td>
</tr>
<tr>
<td>Software Type</td>
<td>The type of software file which includes firmware and images.</td>
</tr>
</tbody>
</table>
### Upgrade job status

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

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

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

Editing an upgrade job

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager.
2. In the left navigation pane, click Upgrade Job Status.
3. On the Upgrade Job Status page, in the Job Type field, click Upgrade.
4. Select a pending upgrade job that you want to edit.
5. Click Edit Configuration.
   The system displays the Upgrade Configuration page.
6. To edit the configuration, see Upgrading Avaya Aura applications.

Related links
Upgrading Avaya Aura applications to Release 7.1.3 on page 119

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Type</td>
<td>The upgrade job type. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Refresh Element(s)</strong>: To view refresh elements jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Analyze</strong>: To view analyze jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pre-Upgrade Check</strong>: To view preupgrade check jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Upgrade</strong>: To view upgrade jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Commit</strong>: To view commit jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rollback</strong>: To view rollback jobs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Uninstall</strong>: To view uninstall jobs.</td>
</tr>
<tr>
<td>Job Name</td>
<td>The upgrade job name.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time when the system started the job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time when the system ended the job.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.</td>
</tr>
<tr>
<td>% Complete</td>
<td>The percentage of completion of the upgrade job.</td>
</tr>
<tr>
<td>Element Records</td>
<td>The total number of elements in the upgrade job.</td>
</tr>
<tr>
<td>Successful Records</td>
<td>The total number of times that the upgrade job ran successfully.</td>
</tr>
<tr>
<td>Failed Records</td>
<td>The total number of times that the upgrade job failed.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the upgrade job.</td>
</tr>
<tr>
<td>Re-run Checks</td>
<td>Performs the upgrade job again.</td>
</tr>
<tr>
<td>Edit Configuration</td>
<td>Displays the Upgrade Configuration page where you can change the upgrade configuration details.</td>
</tr>
</tbody>
</table>

## Support for Enhanced Access Security Gateway

Communication Manager supports Enhanced Access Security Gateway (EASG). EASG is a certificate based challenge-response authentication and authorization solution. Avaya uses EASG to securely access customer systems and provides support and troubleshooting.

EASG provides a secure method for Avaya services personnel to access the Communication Manager remotely and onsite. Access is under the control of the customer and can be enabled or
disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck. EASG must be enabled for Avaya Services to perform the required maintenance tasks.

You can enable or disable EASG through Communication Manager.

EASG only supports Avaya services logins, such as init, inads, and craft.

**Discontinuance of ASG and ASG-enabled logins**

EASG in Communication Manager 7.1.1 and later replaces Avaya’s older ASG feature. In the older ASG, Communication Manager allowed the creation of ASG-enabled user logins through the SMI Administrator Accounts web page. Such logins are no longer supported in Communication Manager 7.1.1 and later. When upgrading to Communication Manager 7.1.1 or later from older releases, Communication Manager does not support ASG-enabled logins.

For more information about EASG, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

---

**Enabling or disabling EASG through the CLI interface**

**About this task**

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

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

**Procedure**

1. Log in to the Communication Manager CLI interface as an administrator.
2. To check the status of EASG, run the following command: `EASGStatus`.
3. To enable EASG (Recommended), run the following command: `EASGManage --enableEASG`.
4. To disable EASG, run the following command: `EASGManage --disableEASG`. 
Enabling or disabling EASG through the SMI interface

About this task

By enabling Avaya Services Logins you are granting Avaya access to your system. This setting is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com for Avaya remote connectivity. See the Avaya support site support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Services Logins you are denying Avaya access to your system. This setting is not recommended, as it can impact Avaya’s ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

Procedure

1. Log on to the Communication Manager SMI interface.
2. Click **Administration > Server (Maintenance)**.
3. In the **Security** section, click **Server Access**.
4. In the **Avaya Services Access via EASG** field, select:
   - **Enable** to enable EASG.
   - **Disable** to disable EASG.
5. Click **Submit**.

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Communication Manager CLI interface.
2. Run the following command: `EASGProductCert --certInfo`.

EASG product certificate expiration

Communication Manager raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.
If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

---

**EASG site certificate**

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

**Managing site certificates**

**Before you begin**

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to `/home/cust` directory, where `cust` is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of `installed_pkcs7_name` in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

**Procedure**

1. Log in to the CLI interface as an administrator.
2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
4. To delete the site certificate, run the following command:

- `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
- `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.
Chapter 6: Post-upgrade procedures

Connecting the services computer to the server

Procedure
Using a CAT5 cable, connect the portable computer to the services port.

Accessing the System Management Interface

About this task
You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

Procedure
1. Open a compatible web browser.
2. Depending on the server configuration, choose one of the following:
   • LAN access by IP address
     If you log on to the corporate local area network, type the unique IP address for Communication Manager in the standard dotted-decimal notation, such as http://192.152.254.201.
   • LAN access by host name
     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as http://media-server1.mycompany.com.
3. Press Enter.

Note:
If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other virtual servers again, click the main menu link to Install Avaya Root Certificate after you log in.

The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   ✠ **Note:**
   
   If you use an Avaya services login that is protected by the Enhanced Access Security Gateway (EASG), you must have an EASG tool to generate a response for the challenge that the Logon page generates.

5. Click **Continue**.

6. Type the password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

---

### Busying out previously busied out equipment

**Procedure**

If you recorded any equipment that was busied out before the upgrade on the main server, busy out the equipment after you complete the upgrade.

---

### Enabling the scheduled maintenance

**About this task**

Use the procedure to schedule daily maintenance.

**Procedure**

Reset the settings that you recorded earlier in Disabling scheduled maintenance.

---

### Entering initial system translations

**Before you begin**

- Prepare the initial translations offsite and save the translations in the translation file.
- Store the translation file in the `/etc/opt/defty` folder with `xln1` and `xln2` file names.

   Alternatively, you can save the full backup of a system in a translation file, and restore the files on another system.

**Procedure**

1. Log in to the Communication Manager CLI as a root user.
2. If the system translations are prepared offsite, install the prepared translations, and reset Communication Manager using the command `reset system 4` or `drestart 1 4`.

3. If translations are not prepared offsite:
   a. Type `save translation` and press Enter to save the translations to the hard disk drive.
   b. Type `reset system 4` or `drestart 1 4` and press Enter.

4. Enter minimal translations to verify connectivity to the port networks or media gateway.

5. After you enter the translations, type `save translation`, and press Enter to save the translations to the hard disk drive.

---

### Saving translations

**Before you begin**
Start a SAT session.

**About this task**
Perform the following procedure on the main server only.

**Procedure**

1. Enter `save translation all`.
   
   The system displays the Command successfully completed or the all error messages are logged message.

2. At the command prompt, enter `filesync -Q all`.
   
   Verify that the system displays the filesync errors, if any.

---

### Resolving alarms

**Before you begin**
Log on to System Management Interface.

**Procedure**

1. On the Administration menu, click Server (Maintenance).

2. Click Alarms > Current Alarms.
   
   The system displays the Current Alarms page.

3. In the Server Alarms section, select the alarms that you must clear.
4. Click **Clear**.

5. To resolve new alarms after the server upgrade, use a SAT session.

For more information, see:

- *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431
- *Avaya Aura® Communication Manager Server Alarms*, 03-602798

---

### Logging off from all administration applications

**Procedure**

When you complete all administration activities, log off from all applications that you used.

---

### Disconnecting from the server

**Procedure**

Unplug the portable computer from the services port.

---

### Deleting the virtual machine snapshot

### Deleting the virtual machine snapshot from the Appliance Virtualization Platform host

**Procedure**

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`

2. To log in to the Appliance Virtualization Platform host, provide the credentials.

3. In the left navigation pane, click **Virtual Machines**.

4. Select the virtual machine, click **Actions > Snapshots > Manage snapshots**.

   The system displays the Manage snapshots - `<Virtual machine name>` dialog box.

5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.
Deleting the virtual machine snapshot from the vCenter managed host or standalone host

Procedure

1. Log in to the vSphere client for the vCenter managed host or the standalone host.
2. Depending on the host, perform one of the following
   a. On the vCenter managed host, select the host, and then select the virtual machine.
   b. On the Standalone host, select the virtual machine.
3. Right-click the selected virtual machine, click Snapshot > Snapshot Manager.
   The system displays the Snapshot for the <Virtual machine name> dialog box.
4. Select the snapshot and click Delete.
   The system deletes the selected snapshot.
Chapter 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

## Communication Manager documentation

The following table lists the documents related to Communication Manager. Download the documents from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager Overview and Specification</td>
<td>Provides an overview of the features of Communication Manager</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager Security Design, 03-601973</td>
<td>Describes security-related issues and security features of Communication Manager.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td>Avaya Aura® Solution Design Considerations and Guidelines, 03-603978</td>
<td>Describes the Avaya Aura® solution, IP and SIP telephony product deployment, and network requirements for integrating IP and SIP telephony products with an IP network.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager System Capacities Table, 03-300511</td>
<td>Describes the system capacities for Avaya Aura® Communication Manager.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td><strong>LED Descriptions for Avaya Aura® Communication Manager Hardware Components, 03-602804</strong></td>
<td>Describes the LED for hardware components of Avaya Aura® Communication Manager.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td><strong>Avaya Aura® Communication Manager Hardware Description and Reference, 555-245-207</strong></td>
<td>Describes the hardware requirements for Avaya Aura® Communication Manager.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td><strong>Avaya Aura® Communication Manager Survivability Options</strong></td>
<td>Describes the system survivability options for Avaya Aura® Communication Manager.</td>
<td>Sales Engineers, Solution Architects</td>
</tr>
<tr>
<td><strong>Maintenance and Troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Avaya Aura® Communication Manager Reports, 555-233-505</strong></td>
<td>Describes the reports for Avaya Aura® Communication Manager.</td>
<td>Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel</td>
</tr>
</tbody>
</table>

*Table continues*
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Procedures for Avaya Aura Communication Manager, Branch Gateways and Servers</td>
<td>Provides procedures to maintain Avaya servers and gateways.</td>
<td>Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Maintenance Commands for Avaya Aura Communication Manager, Branch Gateways and Servers, 03-300431</td>
<td>Provides commands to monitor, test, and maintain Avaya servers and gateways.</td>
<td>Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td></td>
<td>Provides procedures to monitor, test, and maintain Avaya servers, and describes the denial events listed on the Events Report form.</td>
<td>Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administering Avaya Aura Communication Manager, 03-300509</td>
<td>Describes the procedures and screens for administering Communication Manager.</td>
<td>Sales Engineers, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Administering Network Connectivity on Avaya Aura Communication Manager, 555-233-504</td>
<td>Describes the network connectivity for Communication Manager.</td>
<td>Sales Engineers, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Avaya Aura Communication Manager SNMP Administration and Reference, 03-602013</td>
<td>Describes SNMP administration for Communication Manager.</td>
<td>Sales Engineers, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Administering Avaya Aura Communication Manager Server Options</td>
<td>Describes server options for Communication Manager.</td>
<td>Sales Engineers, Implementation Engineers, Support Personnel</td>
</tr>
<tr>
<td>Implementation and Upgrading</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploying Avaya Aura Communication Manager in Virtualized Environment</td>
<td>Describes the implementation instructions while deploying Communication Manager on VMware and Kernel-based Virtual Machine (KVM).</td>
<td>Implementation Engineers, Support Personnel; Solution Architects</td>
</tr>
<tr>
<td>Deploying Avaya Aura Communication Manager in Virtual Appliance</td>
<td>Describes the implementation instructions while deploying Communication Manager on Appliance Virtualization Platform.</td>
<td>Implementation Engineers, Support Personnel; Solution Architects</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Audience</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Communication Manager in Infrastructure as a Service Environment</td>
<td>Describes the implementation instructions while deploying Communication Manager on Amazon Web Services, Microsoft Azure, Google Cloud Network.</td>
<td>Implementation Engineers, Support Personnel, Solution Architects</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Communication Manager in Software-Only Environment</td>
<td>Describes the implementation instructions while deploying Communication Manager on a software-only environment.</td>
<td>Implementation Engineers, Support Personnel, Solution Architects</td>
</tr>
<tr>
<td>Upgrading to Avaya Aura® Communication Manager</td>
<td>Describes instructions while upgrading Communication Manager.</td>
<td>Implementation Engineers, Support Personnel, Solution Architects</td>
</tr>
<tr>
<td>Understanding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205</td>
<td>Describes the features that you can administer using Communication Manager.</td>
<td>Sales Engineers, Solution Architects, Support Personnel</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager Screen Reference, 03-602878</td>
<td>Describes the screens that you can administer using Communication Manager.</td>
<td>Sales Engineers, Solution Architects, Support Personnel</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager Special Application Features</td>
<td>Describes the special features that are requested by specific customers for their specific requirement.</td>
<td>Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel</td>
</tr>
</tbody>
</table>

Finding documents on the Avaya Support website

Procedure

2. At the top of the screen, type your username and password and click Login.
3. Click Support by Product > Documents.
4. In Enter your Product Here, type the product name and then select the product from the list.
5. In Choose Release, select an appropriate release number.
6. In the Content Type filter, click a document type, or click Select All to see a list of all available documents.
   For example, for user guides, click User Guides in the Content Type filter. The list displays the documents only from the selected category.
7. Click Enter.
Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In Search, type Avaya Mentor Videos to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select Video in the Content Type column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

⚠️ Note:

Videos are not available for all products.

Training

About this task

You can view various training courses of Avaya products on the Avaya Learning website: https://www.avaya-learning.com. You can view/search learning courses based on the following criteria:

- Administration
- Design
- Develop
- Implementation
- Sales
- Support

You can also view courses based on Curriculum Maps. A Curriculum map is a compilation of multiple courses related to a product or solution. There are also certification courses and test/assessments for various specialization.
**Procedure**

2. Click Login.
3. After logging into the Avaya Learning site, search for the available courses by typing the product name in the search option.

---

**Support**

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

---

**Using the Avaya InSite Knowledge Base**

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

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

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

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

2. Log on to the Avaya website with a valid Avaya user ID and password.
   - The system displays the Avaya Support page.
3. Click **Support by Product > Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press Enter.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.
Appendix A: OS-level logins for Communication Manager

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

• **root**: A default user login that cannot be removed. By default, a root user has complete access.

• **sroot**: A root-level user login that is used by Avaya Services. The init, inads, craft, and rasaccess users are also Avaya services logins that are equivalent to customer super-users in CM. These logins (including sroot) can be removed if desired, but that does make the system difficult for services to troubleshoot should the need arise.

  **Note:**
  Sroot and root cannot login directly from either SSH or the web GUI.

• **acpsnmp**: acpsnmp user is used internally by Communication Manager to handle SNMP-related tasks. As you can see, it has a shell of /sbin/nologin and cannot login on the Web or via SSH. It has customer super-user access because it needs to perform administration operations. This user cannot be deleted, nor can the password be changed (it doesn’t have a password anyway).

• **csadmin**: csadmin is used by the System Manager orchestration software in Solution Deployment Manager to perform upgrades and other maintenance that is required. This login is a customer super-user that should not be removed in order to allow Solution Deployment Manager to continue working.

• **init, inads, rasaccess, craft, and csadmin**: Users with these users logins cannot change their passwords. The csadmin login user will use keys, and the other users are protected by EASG challenge-response logins.

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

  • sroot
  • init
  • craft
**Glossary**

**Migration**

The migration process includes changing the server hardware, change the operating system, and reinstallation of software that includes hypervisor.

During migration, you might need to perform backup and restore operations outside the normal upgrade process. You cannot rollback the upgrade easily.

**Update**

The update process includes installing patches of an application. For example, kernel patches, security patches, hotfixes, service packs, and feature packs.

**Upgrade**

The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor.

The process is triggered through the normal process without requiring additional backup and restore operations. You can rollback an upgrade.
Index

Special Characters
/sbin/generate-certificates .................................................. 103

Numerics
7.0 .......................................................... 127, 129

A
aborting
  virtual machine report generation ................................ 99
access Solution Deployment Manager .................................. 26
add
  virtual machine .......................................................... 90
adding
  Appliance Virtualization Platform host ......................... 45
  AVP host .................................................................. 45
  ESXi host ................................................................. 45
  location .................................................................... 37
  vCenter to SDM .......................................................... 104
adding certificates
  available hosts .......................................................... 102
  existing hosts ........................................................ 102
  migrated hosts ......................................................... 102
adding ESXi host .......................................................... 45
adding location ............................................................. 37
adding location to host .................................................. 105
adding vCenter to SDM .................................................. 104
add virtual machine ....................................................... 90
analyze job status ....................................................... 140
Appliance Virtualization Host
  configure login banner .................................................. 63
  push login banner ....................................................... 63
Appliance Virtualization Platform
  change password ....................................................... 53
  generating kickstart file ............................................ 54
  license file ............................................................. 59
  restarting .................................................................. 62
  shutting down ........................................................... 62
  update ...................................................................... 47, 71
WebLM Configuration ..................................................... 59
Appliance Virtualization Platform host Gateway
  change ...................................................................... 49
  edit ......................................................................... 49
Appliance Virtualization Platform host IP address
  change ...................................................................... 49
  edit ......................................................................... 49
Appliance Virtualization Platform host password
  changing ..................................................................... 53
Appliance Virtualization Platform network parameters
  applications ................................................................. 49
  log off ...................................................................... 150
  applying .................................................................. 64
  third-party AVP certificates ...........................................
Avaya Aura application
  Services Port static routing update ................................ 83
Avaya Aura applications
  Network Parameters change ........................................ 96
Avaya Aura application upgrade ....................................... 127
AVP license status ........................................................ 62

B
backup
  restore ..................................................................... 110
Branch Session Manager upgrade ....................................... 119
busying out
  busied-out equipment .................................................. 148
  busied-out previously busied-out equipment .................. 148

C
certificates
  accepting ................................................................. 100
  generating ............................................................... 100
  certificate update
    ESXi host ............................................................... 101
    vCenter ................................................................ 101
  VMware documentation ............................................... 101
  Certification
    validation ............................................................... 99
  Certification validation ............................................... 99
  change
    Appliance Virtualization Platform host IP address .......... 49
    Host/ IP Settings .................................................. 50
    hostname .............................................................. 110
    network settings .................................................. 70
    Network Settings ................................................... 50
  Change Gateway ......................................................... 69
  change IP address for AVP host .................................... 49
  Change IP FQDN ........................................................ 80
  change Netmask for Appliance Virtualization Platform host 49
  Change Network Params ............................................. 49
  changing
    IP address and default gateway .................................. 58
    changing Appliance Virtualization Platform host password . 53
    changing Network Parameters for Avaya Aura .......... 96
    checklist
      Branch Session Manager upgrade .......................... 117
      Communication Manager 7.x upgrade .................. 117
      Session Manager upgrade .................................. 117
    common causes
      VM deployment failure .......................................... 85
    Communication Manager
      installation on System Platform .............................. 14
Communication Manager (continued)

installation on VMware platform ........................................ 14
license file ...................................................................... 15
migrate to Virtualized Environment ................................... 113
upgrade ......................................................................... 29
upgrades ........................................................................ 11
Communication Manager update .................................... 77, 121, 123
Communication Manager upgrade ................................ 119
Communication Manager upgrade from Software Management ........................................ 12
Communication Manager upgrade from System Manager 12
Communication Manager upgrade paths ............................ 17
Communication Manager upgrades
footprints ........................................................................ 20
profile map ...................................................................... 20
Configuration Parameters ............................................... 85, 90
configure
login banner on host ...................................................... 63
configuring
WebLM Server on Appliance Virtualization Platform .......... 60
connect service computer to server ................................. 147
correcting ESXi host certificate ........................................ 101
courses ........................................................................... 156
create virtual machine .................................................... 75
creating backup ............................................................. 109
generic CSR .................................................................... 65
CSR
create field description .................................................. 66
edit field description ...................................................... 66
custom patch upload ......................................................... 139

disconnecting from the server .......................................... 150
documentation
Communication Manager ................................................. 153
document changes ......................................................... 8
download manager
uploading custom patch .................................................. 139
download software .......................................................... 72

E

EASG

disabling ......................................................................... 142
enabling ........................................................................ 143
SMI ................................................................................. 144
EASG certificate information ........................................... 144
EASG product certificate expiration .................................. 144
EASG site certificate edit................................................ 145
eSXi host virtual machine .................................................. 80, 81
Edit Host

editing
ESXi host ........................................................................ 46
generic CSR .................................................................... 65
location ........................................................................... 37
vCenter ........................................................................... 105
editing ESXi host ............................................................ 46
editing location ............................................................... 37
editing upgrade configuration ......................................... 141
editing vCenter ............................................................... 105
Edit Location .................................................................... 44
Edit Upgrade Configuration
AVP Configuration ......................................................... 130
Element Configuration .................................................. 130
Edit vCenter .................................................................... 107
eEdit virtual machine elements upgrade

target release ................................................................... 34
element upgrade ............................................................ 127
eenable scheduled maintenance ....................................... 148
enabling
SSH on Appliance Virtualization Platform ....................... 56
enabling SSH ................................................................. 57
Enhanced Access Security Gateway ................................. 142
esxconfig-route ............................................................. 58
esxcli network ip interface ipv4 set -i vmk0 -l ................... 58
ESXi host
adding ............................................................................ 45
editing ............................................................................ 46
removing ......................................................................... 63
restarting .......................................................................... 62
ESXi host certificate addition .......................................... 102
ESXi host certificate update ............................................. 101
ESXi host map to unknown location ............................... 63
existing hosts managing certificates ................................ 102
Index

existing vCenter managing certificates .................................................. 102

F
field descriptions change password ......................................................... 71
Create AVP Kickstart ............................................................................ 54
create CSR ............................................................................................. 66
edit CSR ................................................................................................. 66
Edit Host ................................................................................................. 68
Edit Location ......................................................................................... 44
Hosts ......................................................................................................... 38
load AVP host certificate ...................................................................... 66
Locations ................................................................................................. 38
Map vCenter ........................................................................................... 106
New Host ................................................................................................. 68
New Location ......................................................................................... 44
Upgrade Configuration ........................................................................... 129
upgrade management ............................................................................. 127
Virtual Machines ..................................................................................... 38
VM Deployment ........................................................................................ 90
WebLM Configuration ............................................................................. 61
field descriptions, Snapshot Manager .................................................. 68
footprint flexibility .................................................................................. 20

G
General Configuration Details ............................................................ 130
generate_report.sh ............................................................................... 97
generating certificates ........................................................................... 100
new self-signed certificates for ESXi host ............................................ 103
virtual machine report ........................................................................... 98
generic CSR creating ............................................................................ 65
editing ..................................................................................................... 65

H
host .......................................................................................................... 50, 70
generating kickstart file ......................................................................... 54
monitoring ............................................................................................... 108
Host update ............................................................................................. 71
Hosts ......................................................................................................... 38

I
inputting translations ............................................................................ 148
lnSite Knowledge Base .......................................................................... 157
install Application Enablement Services ............................................. 24, 32
Avaya Aura applications ........................................................................ 24, 32
Avaya Aura Media Server ...................................................................... 24, 32
Avaya Breeze ......................................................................................... 24, 32
install (continued) Branch Session Manager ........................................ 24, 32
Communication Manager ...................................................................... 24, 32
SAL .......................................................................................................... 24, 32
SDM .......................................................................................................... 24, 32
Session Manager .................................................................................... 24, 32
Solution Deployment Manager client .................................................. 24, 32
System Manager ..................................................................................... 24, 32
WebLM ................................................................................................... 24, 32
install AVP host patch Solution Deployment Manager ........................................ 47
install custom patches ........................................................................... 123
install custom software patches ........................................................... 123
installed logins ....................................................................................... 158
Installed Patches ..................................................................................... 125
Installed Patches field descriptions ...................................................... 94
install patches ......................................................................................... 77, 121
install services packs ............................................................................. 77, 121, 123
install software patches ......................................................................... 77, 121
Install System Manager patch ............................................................. 95
IP address and default gateway changing ............................................. 58

L
latest software patches ........................................................................... 16
learning ..................................................................................................... 156
legal notice ..............................................................................................
licensing
Communication Manager ........................................................................ 15
Life cycle management .......................................................................... 36
Linux Operating System upgrades ......................................................... 27, 34
preupgrade check ................................................................................... 27, 34
load AVP host certificate ........................................................................
field descriptions ...................................................................................
location adding ....................................................................................... 37
deleting .................................................................................................... 38
editing ..................................................................................................... 37
view .......................................................................................................... 37
Locations .................................................................................................. 38
logins installed ........................................................................................ 158
Log off applications .................................................................................. 150

M
Manage Software .................................................................................... 12
managing certificates migrated hosts .................................................... 102
map ESXi host to unknown location ...................................................... 63
Map vCenter ............................................................................................ 104–107
migrated hosts managing certificates ..................................................... 102
migrating
Communication Manager to VMware .................................................. 113
monitoring
Index

monitoring (continued)
host .......................................................... 108
virtual machine ........................................ 109
VM ......................................................... 109

N
network parameters
change .................................................... 69
Network Parameters change .................... 96
network parameters for AVP and virtual machines
change .................................................... 81
New Host ................................................. 68
New Location ........................................... 44
New vCenter ............................................ 107

P
password
change .................................................... 71
password change
Appliance Virtualization Platform host ........ 53
password policy ....................................... 53
password rules ....................................... 53
patch information .................................... 16
Preupgrade ............................................. 27
preupgrade check .................................... 27, 34
pre upgrade checks
System Platform upgrades ......................... 28, 35
preupgrade job status .............................. 140
preupgrade requirements ......................... 19
Preupgrade tasks .................................... 29
profile mapping for Communication Manager upgrades, push
login banner on host .............................. 63

R
reestablish
connection ............................................ 96
Reestablish Connection .......................... 38
re-establishing trust
SDM elements ........................................ 77
Solution Deployment Manager elements ...... 77
virtual machine ..................................... 77
re-establishing trust virtual machine .......... 77
refresh elements job status ...................... 140
release notes for latest software patches ........ 16
removing
ESXi host ................................................ 63
removing ESXi host .................................. 63
removing location from host .................... 105
removing vCenter .................................... 106
Resolving
alarms ................................................... 149
restart
virtual machine ..................................... 84
restoring
Appliance Virtualization Platform .......... 62
ESXi host ............................................... 62
restart virtual machine from SDM .......... 84
restoring
backup .................................................. 110
rollback
upgrade ................................................. 152
rollback upgrade .................................... 152
saving translations ................................. 148, 149
schedule daily maintenance .................... 148
SDM
installation ............................................. 24, 32
SDM elements
re-establishing trust ............................... 77
Select Flexi Footprint ................................ 80
select upgrade target release .................. 34
self-signed certificates for ESXi host
generate ................................................ 103
servers
accessing System Management Interface ... 147
Services Port static route update ............... 83
SES ....................................................... 18
Session Manager update ......................... 77, 121, 123
Session Manager upgrade ....................... 119
shutting down
AVP ...................................................... 62
SIP Enablement Services ......................... 18
site certificate
add ....................................................... 145
delete .................................................... 145
manage .................................................. 145
view ...................................................... 145
snapshot from Appliance Virtualization Platform
deleting ................................................. 150
snapshot from vCenter managed host
deleting ................................................. 151
Snapshot Manager
virtual machine snapshot ......................... 67
Snapshot Manager field descriptions .......... 68
software
download .............................................. 72
Software Management ........................... 12
software patches ................................... 16
Solution Deployment Manager ................ 12, 53, 56
access .................................................... 26
restart virtual machine ......................... 84
start ....................................................... 26
start virtual machine ............................. 84
stop virtual machine ............................... 84
update Appliance Virtualization Platform host . 47
Solution Deployment Manager elements
(continued)
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Deployment Manager elements (continued)</td>
<td>77</td>
</tr>
<tr>
<td>re-establishing trust</td>
<td>77</td>
</tr>
<tr>
<td>Special</td>
<td>18</td>
</tr>
<tr>
<td>circumstances</td>
<td>18</td>
</tr>
<tr>
<td>start</td>
<td>84</td>
</tr>
<tr>
<td>virtual machine</td>
<td>84</td>
</tr>
<tr>
<td>start Solution Deployment Manager</td>
<td>26</td>
</tr>
<tr>
<td>start virtual machine from SDM</td>
<td>84</td>
</tr>
<tr>
<td>static routing</td>
<td>83</td>
</tr>
<tr>
<td>changing</td>
<td>83</td>
</tr>
<tr>
<td>updating</td>
<td>83</td>
</tr>
<tr>
<td>status</td>
<td></td>
</tr>
<tr>
<td>Analyze</td>
<td>142</td>
</tr>
<tr>
<td>analyze job</td>
<td>140</td>
</tr>
<tr>
<td>Preupgrade check</td>
<td>142</td>
</tr>
<tr>
<td>preupgrade check job</td>
<td>140</td>
</tr>
<tr>
<td>Refresh elements job</td>
<td>140</td>
</tr>
<tr>
<td>upgrade job</td>
<td>140</td>
</tr>
<tr>
<td>upgrade jobs</td>
<td>142</td>
</tr>
<tr>
<td>stop</td>
<td></td>
</tr>
<tr>
<td>virtual machine</td>
<td>84</td>
</tr>
<tr>
<td>stop virtual machine from SDM</td>
<td>84</td>
</tr>
<tr>
<td>support</td>
<td>157</td>
</tr>
<tr>
<td>supported</td>
<td></td>
</tr>
<tr>
<td>servers</td>
<td>15</td>
</tr>
<tr>
<td>supported Communication Manager upgrade paths</td>
<td>17</td>
</tr>
<tr>
<td>System Manager</td>
<td></td>
</tr>
<tr>
<td>7.0</td>
<td>141</td>
</tr>
<tr>
<td>upgrade</td>
<td>141</td>
</tr>
<tr>
<td>System Manager VM management</td>
<td>94</td>
</tr>
<tr>
<td>System Manager VM update</td>
<td>95</td>
</tr>
<tr>
<td>System Platform upgrades</td>
<td></td>
</tr>
<tr>
<td>preupgrade checks</td>
<td>28, 35</td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>target release</td>
<td>34</td>
</tr>
<tr>
<td>select</td>
<td>34</td>
</tr>
<tr>
<td>third-party AVP certificates</td>
<td>64</td>
</tr>
<tr>
<td>applying</td>
<td>65</td>
</tr>
<tr>
<td>creating generic CSR</td>
<td>65</td>
</tr>
<tr>
<td>editing generic CSR</td>
<td>16</td>
</tr>
<tr>
<td>third-party certificates</td>
<td>156</td>
</tr>
<tr>
<td>training</td>
<td></td>
</tr>
<tr>
<td>inputting</td>
<td>148</td>
</tr>
<tr>
<td>saving</td>
<td>148</td>
</tr>
<tr>
<td>translations; save</td>
<td>149</td>
</tr>
<tr>
<td>U</td>
<td></td>
</tr>
<tr>
<td>Unknown location host mapping</td>
<td>63</td>
</tr>
<tr>
<td>update</td>
<td></td>
</tr>
<tr>
<td>Appliance Virtualization Platform</td>
<td>71</td>
</tr>
<tr>
<td>Appliance Virtualization Platform host</td>
<td>47</td>
</tr>
<tr>
<td>Branch Session Manager</td>
<td>123</td>
</tr>
<tr>
<td>update (continued)</td>
<td></td>
</tr>
<tr>
<td>Communication Manager</td>
<td>77, 121, 123</td>
</tr>
<tr>
<td>Session Manager</td>
<td>77, 121, 123</td>
</tr>
<tr>
<td>Utility Services</td>
<td>123</td>
</tr>
<tr>
<td>WebLM</td>
<td>123</td>
</tr>
<tr>
<td>update software</td>
<td>77, 121, 123</td>
</tr>
<tr>
<td>update static routing</td>
<td>94</td>
</tr>
<tr>
<td>Update Static Routing</td>
<td>38</td>
</tr>
<tr>
<td>update System Manager VM</td>
<td>95</td>
</tr>
<tr>
<td>Upgrade VM IP/FQDN</td>
<td>81</td>
</tr>
<tr>
<td>updating ESXi host or vCenter certificate</td>
<td>101</td>
</tr>
<tr>
<td>updating Services Port static routing</td>
<td>83</td>
</tr>
<tr>
<td>upgrade</td>
<td></td>
</tr>
<tr>
<td>Avaya Aura application</td>
<td>29, 119</td>
</tr>
<tr>
<td>Branch Session Manager</td>
<td>117, 119, 130</td>
</tr>
<tr>
<td>checklist</td>
<td>117</td>
</tr>
<tr>
<td>Communication Manager</td>
<td>29, 117, 119, 130</td>
</tr>
<tr>
<td>Communication Manager Messaging</td>
<td>119</td>
</tr>
<tr>
<td>elements</td>
<td>125</td>
</tr>
<tr>
<td>order</td>
<td>20</td>
</tr>
<tr>
<td>rollback</td>
<td>152</td>
</tr>
<tr>
<td>sequence</td>
<td>20</td>
</tr>
<tr>
<td>Session Manager</td>
<td>29, 117, 119, 130</td>
</tr>
<tr>
<td>target release</td>
<td>34</td>
</tr>
<tr>
<td>WebLM</td>
<td>119</td>
</tr>
<tr>
<td>Upgrade</td>
<td>129</td>
</tr>
<tr>
<td>upgrade Communication Manager</td>
<td>11</td>
</tr>
<tr>
<td>Upgrade Configuration</td>
<td></td>
</tr>
<tr>
<td>field descriptions</td>
<td>129</td>
</tr>
<tr>
<td>Upgrade Configuration Details</td>
<td>130</td>
</tr>
<tr>
<td>upgrade jobs</td>
<td></td>
</tr>
<tr>
<td>deleting</td>
<td>141</td>
</tr>
<tr>
<td>editing</td>
<td>141</td>
</tr>
<tr>
<td>status</td>
<td>142</td>
</tr>
<tr>
<td>upgrade job status</td>
<td>140</td>
</tr>
<tr>
<td>Upgrade job status</td>
<td></td>
</tr>
<tr>
<td>Viewing</td>
<td>141</td>
</tr>
<tr>
<td>upgrade management</td>
<td></td>
</tr>
<tr>
<td>field descriptions</td>
<td>127</td>
</tr>
<tr>
<td>Upgrade Management</td>
<td>12</td>
</tr>
<tr>
<td>upgrade order</td>
<td>20</td>
</tr>
<tr>
<td>upgrade paths</td>
<td>17</td>
</tr>
<tr>
<td>upgrade process</td>
<td>21</td>
</tr>
<tr>
<td>Upgrade Release Selection</td>
<td>34</td>
</tr>
<tr>
<td>upgrade rollback</td>
<td>152</td>
</tr>
<tr>
<td>upgrade sequence</td>
<td>20</td>
</tr>
<tr>
<td>Upgrade to release</td>
<td>34</td>
</tr>
<tr>
<td>upgrading</td>
<td></td>
</tr>
<tr>
<td>Communication Manager from pre-5.2.1 to 7.1.3</td>
<td>116</td>
</tr>
<tr>
<td>Upgrading</td>
<td></td>
</tr>
<tr>
<td>full backup</td>
<td>112</td>
</tr>
<tr>
<td>virtual machine</td>
<td>112</td>
</tr>
<tr>
<td>upload</td>
<td></td>
</tr>
<tr>
<td>custom patch</td>
<td>139</td>
</tr>
<tr>
<td>uploading a custom patch</td>
<td>139</td>
</tr>
<tr>
<td>uploading custom patch</td>
<td>139</td>
</tr>
<tr>
<td>uploading custom patch field description</td>
<td>139</td>
</tr>
</tbody>
</table>

Copyright © 2020 by Avaya Inc. All rights reserved.
Validation

certificate ................................................................. 99

vCenter

text from page