Upgrading Avaya Aura® Communication Manager

Release 10.1.x
Issue 14
July 2025

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License type(s)

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

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

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order, Documentation, or as authorized by Avaya in writing with a default of one (1) Cluster if not stated.

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, Documentation, or as authorized by Avaya in writing.

Named User License (NU). End User 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 as indicated in the order, Documentation, or as authorized by Avaya in writing. “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). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Transaction License (TR). End User may use the Software up to the number of Transactions as specified during a specified time period and as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Transaction” means the unit by which Avaya, at its sole discretion, bases the pricing of its licensing and can be, without limitation, measured by the usage, access, interaction (between client/server or customer/organization), or operation of the Software within a specified time period (e.g. per hour, per day, per month). Some examples of Transactions include but are not limited to each greeting played/message waiting enabled, each personalized promotion (in any channel), each callback operation, each live agent or web chat session, each call routed or redirected (in any channel). End User may not exceed the number of Transactions without Avaya’s prior consent and payment of an additional fee.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Communication Manager from Release 6.x, 7.x, or Release 8.x to Release 10.1.x on:

- Avaya Solutions Platform 130 (Avaya supplied ESXi 7.0) environment.
- VMware in customer-provided Virtualized Environment.
- Customer provided Software-only environment.

Note:

Amazon Web Services (AWS), Google Cloud, Microsoft Azure and Kernel-based Virtual Machine (KVM) use the Software-only ISO deployments.

This document:

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

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

Prerequisites

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

Knowledge

- Avaya Solutions Platform
- **For VMware:** VMware® vSphere™ virtualized environment
- KVM hypervisor
- **For Amazon Web Services (AWS):** AWS environment
- **For Google Cloud:** Google Cloud environment
- **For Azure:** Microsoft Azure environment

- **For IBM Cloud:** IBM Cloud for VMware Solutions environment
- Linux® Operating System
- System Manager

Skills

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

Change History

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

Issue	Date	Summary of changes
14	July 2025	Updated the following section: • Taking a snapshot of the virtual machine from the vCenter managed host or standalone host on page 130
13	June 2025	Updated the following section: • Taking a snapshot of the virtual machine from the vCenter managed host or standalone host on page 130

Table continues…

Issue	Date	Summary of changes
12	December 2024	Added the following sections: • Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) on page 22 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 24 • Supported footprints of Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10) on page 29 • Migrating Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 36 • Obtaining existing VMware details on page 37 • Performing prerequisite tasks to migrate Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 37 • Obtaining Communication Manager input configuration details for migration on page 38 • Virtual Machine Backups (clone) as an alternative to snapshots on page 159 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 159 • Validating a Virtual Machine Backup (clone) on page 164 • Rolling back using the Virtual Machine Backup (clone) on page 166
11	July 2024	Added the following sections: • Upgrading Communication Manager using customized backup • Creating a customized backup Removed the following section: • Upgrading Communication Manager using full backup •
10	April 2024	Updated the following sections: • Supported footprints of Communication Manager OVA on VMware • Supported footprints of Communication Manager ISO on Infrastructure as a Service • Supported footprints of Communication Manager Software-only ISO image for on-premise
9	January 2024	Updated the following sections: • Supported ESXi version • Creating a backup • Restoring backup

Table continues…

Issue	Date	Summary of changes
8	May 2023	Created new “Appendix C: Security Service Pack” chapter, and added the following sections: • Adding a user to the avcommonos group • Communication Manager SSP installation • Installing Communication Manager SSP using SDM • Installing Communication Manager SSP using SMI • Installing Communication Manager SSP using CLI Updated the following section: • Patch Installation or Patch Updates
7	January 2023	Updated the “Supported footprints of Communication Manager OVA on VMware” section.
6	November 2022	Updated the following sections: • Supported footprints of Communication Manager OVA on VMware • Supported footprints of Communication Manager Software-only ISO image for on-premise • Supported footprints of Communication Manager ISO on Infrastructure as a Service • Upgrading Communication Manager to Release 10.1 on Software-only environment using SMI
5	September 2022	In Release 10.1.0.2, updated the "Edit Upgrade Configuration field descriptions" section
4	May 2022	Updated the following sections: • Prerequisites • Upgrade path for Software-only environment
3	April 2022	Updated the following sections: • Upgrading Simplex Communication Manager Release 7.x or 8.x to Simplex Communication Manager Release 10.1 using System Manager Solution Deployment Manager • Upgrading Communication Manager Release 8.1.x to Communication Manager Release 10.1.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager

Table continues…

Issue	Date	Summary of changes
2	March 2022	Added the following sections: • Migrating Appliance Virtualization Platform deployed on S8300E with Communication Manager to Avaya Solutions Platform S8300 Release 5.1 • Upgrading Communication Manager Release 8.1.x to Communication Manager Release 10.1.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager • Migrating Appliance Virtualization Platform deployed on S8300D with Communication Manager to Avaya Solutions Platform S8300 Release 5.1 Updated the following sections: • Supported footprints of Communication Manager Software-only ISO image for on-premise • Supported footprints of Communication Manager ISO on Infrastructure as a Service • Key tasks for upgrading Communication Manager to Release 10.1 using SDM • Key tasks for upgrading Communication Manager to Release 10.1 using SMI
1	December 2021	Release 10.1 document

Chapter 2: Upgrade overview and considerations

Communication Manager upgrades

You can use System Manager Solution Deployment Manager, the centralized upgrade solution, to upgrade Communication Manager.

You can upgrade Communication Manager from:

- Release 8.x to Release 10.1.x
- Release 7.x to Release 10.1.x
- Release 6.x to Release 10.1.x

Note:

- A manual upgrade is a full backup and restore using the Communication Manager SMI pages. This process is supported on all deployment options. Best practice prior to an upgrade is to copy the IP address, naming information, your certificates, your logins, scheduled backup, syslog settings, and SNMP configuration. You must be prepared to install these manually after the restore.
- Fully automated upgrade using Solution Deployment Manager is not available for Avaya Solutions Platform 130 Release 5.x.
- For upgrading Communication Manager from Release 6.x to Release 10.1, *first upgrade the entire Aura Solution from 6.x to 8.1.x, and then upgrade the Aura Solution to Release 10.1*. You cannot directly upgrade the Release 6.x system to Release 10.1 and later.
- The full automated upgrade using Solution Deployment Manager can be used when migrating from Communication Manager 7.x or 8.x to 10.x in a customer-provided VMware environment.
- To upgrade Communication Manager using Solution Deployment Manager, you must have System Manager.
- In case if the offer does not support Communication Manager upgrade using System Manager Solution Deployment Manager, you must upgrade the application manually.

For more information about Solution Deployment Manager capabilities, see *Avaya Aura® System Manager Overview and Specification*.

Note:

- From Avaya Aura® Release 10.1, HP ProLiant DL360p G8 (CSR2), HP ProLiant DL360 G9 (CSR3), Dell™ PowerEdge™ R620 (CSR2), Dell™ PowerEdge™ R630 (CSR3), and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x, and S8300E can be upgraded to Avaya Solutions Platform S8300 R5.1.x.
- From Avaya Aura® Release 10.1, Appliance Virtualization Platform is not available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate the Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.x.
- From Release 10.1, Avaya Aura® applications *will not have* the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. Alternately, to continue to deploy the application, you can use the software-only offer. For more information, see the product-specific Software-only and Infrastructure As a Service Environments guide.

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 a 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 the same centralized license file.

Installing Communication Manager license file

About this task

You can install a license file on the WebLM server. Use the Uninstall functionality to remove the license file from the WebLM server.

Licenses installed for WebLM Release 7.1 and later, must support SHA256 digital signature and 14–character host ID.

Before you begin

- Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
- Log on to the WebLM web console with administrator privilege credentials.
- For standard license file, remove the older license file before you install the new file.

  Note:

  The system displays an error message if an older license file is still available.

  For centralized license file, the system automatically overwrites the older license file during installation.

For information about the license file installation errors while installing the license file, see *Administering standalone Avaya WebLM*.

Procedure

1. In the navigation pane, click **Install license**.
2. On the Install license page, click **Browse**, and select the license file.
3. Read the terms and conditions, and click **Accept the License Terms & Conditions**.
4. Click **Install**.

   WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as:

   - The digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Enabling centralized licensing

About this task

Use the following procedure to configure the Communication Manager license file in the Communication Manager duplex configuration for active and standby servers.

By default, centralized licensing is disabled. You must enable centralized licensing to use this feature.

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. Install the license file on the WebLM server for the licensed product.
3. In the navigation pane, click **Configure Centralized Licensing**.
4. Click **Enable Centralized Licensing** to enable centralized licensing for the Communication Manager.
5. In the Elements and License File Assignments section, click **New**.
6. On the Add Element Instance page, do the following:
    a. In **Element Display Name**, type the element display name.
    b. In **Centralized Licensing ID**, type the element IP address.

       Ensure that the IP address format must be in the following format: “CM @ element IP address”

       Note:

       Keep a blank space before and after the @ symbol.

       For example, CM @ 192.0.2.0

    a. In the **Select License File** section, select the license file to map to the element instance.
    b. Click **Save**.

Configuring WebLM server for Communication Manager license

Procedure

1. Log on to the active Communication Manager System Management Interface and do the following:
2. Click **Administration** > **Licensing**.
3. Click **WebLM Configuration**.
4. In **WebLM Server Address**, type the IP address of the WebLM server.
5. Click **Submit**.

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.

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 10.1.x 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:

Ensure that upgrade or update of host should not be simultaneously run with upgrade and updates of application. You can check the Job status on the **Home** > **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status** page. Any scheduled, pending, or running jobs for host must be completed before performing upgrade or update operations on host.

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.

   Note:

   In Geographic Redundancy configured System Manager, if Communication Manager or LSP has the **Unknown** status in the **Managed By** column on the **Inventory** > **Manage Elements** page, then you cannot perform the analyze operation. To change the **Unknown** status in the **Managed By** column to either **Primary** or **Secondary** depending upon from which system this action is performed, select the entry on the **Inventory** > **Manage Elements** page, and click **More Actions** > **Manage**.
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 10.1.x.
6. Install patches: To install the software patches, service packs, and feature pack, if applicable.

Upgrade automation level

- The upgrade of Communication Manager, Session Manager, and Branch Session Manager to Release 10.1.x 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.

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.

Chapter 3: Planning

Prerequisites

Serial Number	Prerequisites	Tasks/ Notes
1	Download the Avaya Aura® application software from the Avaya Support website at http://support.avaya.com. Copy the applications on the computer that you later use to perform the upgrade. If you placed an order for the hardware, ensure that the hardware is available onsite.	Download the following files: • OVA files of Avaya Aura® applications from PLDS • DVDs for the Solution Deployment Manager client and Avaya Solutions Platform from PLDS • The license file from PLDS • Preupgrade and postupgrade service packs from the Avaya Support website at http://support.avaya.com.
2	Verify that the existing server is compatible with Release 10.1.x version of the application. If the existing server is incompatible, change the server accordingly.	See, Supported servers on page 21.
3	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	-
4	Ensure that Avaya Solutions Platform host and all virtual machines running on the host are on the same subnet mask. For more information, see *Out of Band Management* guide, and *Installing the Avaya Solutions Platform 130 Series* document.	-

Supported servers

The following servers are supported for deployments and upgrades to Release 10.1.x and later:

- Avaya Solutions Platform S8300 for Communication Manager and Branch Session Manager
- Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640

For fresh installations, use Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

Supported servers for Avaya Aura® applications

The following table lists the supported servers of Avaya Aura® applications:

Supported servers	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
S8300D	Y	Y	N	N	N
S8300E[1]	Y	Y	Y	Y	N
HP ProLiant DL360 G7 (CSR1)	Y	Y	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	Y	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	Y	N
Dell™ PowerEdge™ R610 (CSR1)	Y	Y	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	Y	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	Y	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	N	Y	Y	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 [3]	N	N	Y	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.x
Avaya Solutions Platform S8300 Release 5.1 [4]	N	N	N	N	Y

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 5.1. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 5.1.x.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

[4] Avaya Solutions Platform 130 Appliance uses VMware vSphere ESXi Standard License to support virtualization.

[5] Avaya Solutions Platform S8300 supports virtualization using VMware vSphere ESXi Foundation License for Communication Manager and Branch Session Manager.

Note:

- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.1.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.x.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

Supported hardware for VMware

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

Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x and Avaya Solutions Platform S8300 Release 6.0.x.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0): Dell PowerEdge R640
- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 6.7 or 7.0
  - VMware® vCenter Server 6.7 or 7.0

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

✱ **Note:**

Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.0.x	7.1.x	8.0.x	8.1.x	10.1.x
ESXi 5.0	Y	N	N	N	N
ESXi 5.1	Y	N	N	N	N
ESXi 5.5	Y	Y	N	N	N
ESXi 6.0	N	Y	Y	Y	N
ESXi 6.5	N	Y	Y	Y	N
ESXi 6.7	N	N	Y	Y	Y
ESXi 7.0	N	N	N	Starting from Release 8.1.3: Y	Y

✱ **Note:**

- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

  For Avaya-provided environments (Avaya Solutions Platform 120 and 130 Release 4.0.x) only use Avaya-provided updates. Updating directly from the Dell or VMware's website will result in an unsupported configuration.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.

- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 6.7 can be VMware ESXi 6.7 Update 3.
- Device Adapter and Presence Services are deployed on the Avaya Breeze® platform, which supports VMware 6.7 and 7.0.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

Supported ASP R6.0.x (KVM on RHEL 8.10) version

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Y	Y

Note:

- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell R660 or Dell R640. The Dell R660 only ships with and supports KVM on RHEL 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-supplied ESXi 7.0.
- Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660 server only supports KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130 Dell R640 Release 4.0 supported ESXi 6.5
- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660) is a single host server with preinstalled KVM on RHEL R8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication Manager and Branch Session Manager.
- Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660, S8300E) is a single host server with preinstalled KVM on RHEL R8.10 software.
- With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific license key needed as was present with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in

PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Latest software updates and patch information

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

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

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

Upgrade sequence for Avaya components

You must upgrade Avaya components and solution in the following sequence. If any of the components are not part of your solution, you can skip that particular component and move to the next component.

1. Hard Endpoints (H.323 and SIP)

   You can upgrade endpoints after all Avaya Aura® Platform components are upgraded.

2. Standalone Avaya WebLM.

   Note:

   Upgrade to WebLM Release 10.1.2.

3. SAL Gateway

   You can choose to upgrade SAL Gateway after all components are upgraded.

4. Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager.

   In the:

   - Non-Geography Redundancy setup, update standalone System Manager.
   - Geography Redundancy setup, update the primary System Manager.

   Avaya recommends that you use System Manager to update Avaya Aura® applications.

5. Avaya Device Adapter Snap-in on Avaya Breeze® platform
6. Avaya Aura® Session Manager (Core Session Managers only)

7. Avaya Breeze® platform and other Snap-ins
8. Avaya Call Management System
9. Avaya Experience Portal
10. Avaya Oceana®
11. Avaya Aura® Device Services
12. G4XX Media gateways or Avaya Aura® Media Server

    Note:

    The gateways require load 38.21.2 or newer to successfully upgrade to 42.x. If the gateway runs older loads, the download fails with a failure message of `Incompatible software image`. To remove the error, you must first upgrade to 38.21.2 (G430) / 38.21.3 (G450).
13. Avaya Aura® Branch Session Manager
14. Avaya Aura® Application Enablement Services
15. Avaya Aura® Communication Manager Survivable Remote Servers (formerly known as Local Survivable Processors)
16. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
17. Avaya Aura® Communication Manager Survivable Core Servers (formerly known as Enterprise Survivable Processors)
18. Avaya Aura® Communication Manager feature servers and evolution servers

    In duplex configuration, update the:

    - Standby Communication Manager server
    - Active Communication Manager server
19. Avaya IP Office™ platform
20. Avaya Aura® Messaging or IX Messaging (formerly known as Avaya Messaging)
21. Avaya Aura® Web Gateway
22. Equinox Clients

    Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
23. Avaya Equinox® Conferencing
24. Avaya Session Border Controller

Note:

- System Manager is an integral part of the Avaya Aura® solution.
- System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 10.1 before you upgrade Communication Manager to 10.1.

  All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

- Remove the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.

  Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.1 OVA, Solution Deployment Manager Client version must be on Release 10.1. Solution Deployment Manager Client cannot be on Release 8.1.

For information about upgrading the application, see the application-specific upgrade guide on the Avaya Support website.

Software details of Communication Manager

For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at https://support.avaya.com/.

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Supported footprints

Supported footprints of Communication Manager OVA on VMware

Note:

- Avaya Aura® Communication Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware*.

  Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

The following table describes the resource requirements to support different profiles for Communication Manager on Customer-provided VMware and Avaya-supplied Avaya Solutions Platform 130:

Footprint (Max users)	vCPU	CPU Reservation (MHz)	Memory (MiB)	Hard disk (GiB)	Minimum CPU Speed (MHz)	Extra NICs
CM Main Max users 1000	2	3900	3584	64	1950	0
CM Survivable Max users 1000	1	1950	4096	64	1950	0
CM Simplex1 Max users 2400	2	4340	4096	64	2170	0
CM Simplex2 Max users 41000 (Can be used as Main or Survivable)	2	4340	4608	64	2170	0
CM Duplex Max users 30000 (CM Duplex–Main or Survivable–up to 30,000 users)	3	6510	5120	64	2170	1
CM High Duplex Max users 41000 (For Hi-Duplex Servers for Main or survivable)	3	7650	5120	64	2550	1

Note:

The following deployment options are for future use:

- CM Standard Duplex Array Max Users 300000
- CM High Duplex Array Max Users 300000
- CM Simplex Array Max users 300000

If you select any of these options during deployment, it results in an unsupported configuration, and you must redeploy Communication Manager with a supported profile.

A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not describe the same output of capacity technically. However, they are close in size. A gibibyte = 1024^3 and gigabyte = 1000^3.

The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size, One mebibyte equals 1.048576 megabytes.

Supported footprints of Communication Manager OVA on ASP R6.0.x (KVM on RHEL 8.10)

Note:

- Avaya Aura® Communication Manager supports ASP R6.0.x (KVM on RHEL 8.10) hosts with Hyperthreading enabled at the BIOS level.
- Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300.

The following table describes the resource requirements to support different profiles for Communication Manager on Avaya-supplied Avaya Solutions Platform 130 Release 6.0:

Footprint (Max users)	vCPU	CPU Reservation (MHz)	Memory (MiB)	Hard disk (GiB)	Minimum CPU Speed (MHz)	Extra NICs
CM Main Max users 1000	2	3900	3584	64	1950	0
CM Survivable Max users 1000	1	1950	4096	64	1950	0
CM Simplex1 Max users 2400	2	4340	4096	64	2170	0
CM Simplex2 Max users 41000 (Can be used as Main or Survivable)	2	4340	4608	64	2170	0
CM Duplex Max users 30000 (CM Duplex–Main or Survivable–up to 30,000 users)	3	6510	5120	64	2170	1
CM High Duplex Max users 41000 (For Hi-Duplex Servers for Main or survivable)	3	7650	5120	64	2550	1

Note:

The following deployment options are for future use:

- CM Standard Duplex Array Max Users 300000
- CM High Duplex Array Max Users 300000
- CM Simplex Array Max users 300000

A gibibyte = 1024^3 and gigabyte = 1000^3

If you select any of these options during deployment, it results in an unsupported configuration, and you must redeploy Communication Manager with a supported profile.

Supported footprints of Communication Manager Software-only ISO image for on-premise

These footprint values are applicable for Software-Only deployments on:

- VMware
- KVM
- Hyper-v

Avaya Aura® Communication Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

Configuration	Profile (max users)	CPUs	CPU Reservation (MHz)	Minimum CPU Speed (MHz)	Memory (MB)	Number of Ethernet NICs (OOB optional)	Minimum Disk size (GB)
Communication Manager Simplex	Large (41000)	2	4340	2170	4608	2 - procr (eth0), OOB (eth1)	64
	Medium (2400)	2	4340	2170	4096	2 - procr (eth0), OOB (eth1)	64
	Small Main (1000)	2	3900	1950	3585	2 - procr (eth0), OOB (eth1)	64
	Small Survivable (1000)	1	1950	1950	4096	2 - procr (eth0), OOB (eth1)	64
Communication Manager Duplex	Duplex High (41000)	3	7650	2550	5120	3 - procr (eth0), dup link (eth1), OOB (eth2)	64

Table continues…

Configuration	Profile (max users)	CPUs	CPU Reservation (MHz)	Minimum CPU Speed (MHz)	Memory (MB)	Number of Ethernet NICs (OOB optional)	Minimum Disk size (GB)
	Duplex Standard (30000)	3	6510	2170	5120	3 - procr (eth0), dup link (eth1), OOB (eth2)	64

Supported footprints of Communication Manager ISO on Infrastructure as a Service

Here are supported footprints of Communication Manager ISO on:

- Amazon Web Services (AWS)
- Microsoft Azure (Azure)
- Google Cloud Platform (GCP)

Note:

Specifications for Avaya Aura® applications on IBM Cloud for VMware Solutions is same as that of the Virtualized Environment offer.

For IBM Cloud for VMware Solutions, instance type is not applicable.

Avaya Aura® Communication Manager supports VMware hosts with Hyperthreading enabled at the BIOS level.

Footprints		Configuration					
		Communication Manager Simplex				Communication Manager Duplex	
		Large	Medium	Small Main	Small Survivable	Duplex High	Duplex Standard
Profile (max users)		41000	2400	1000	1000	41000	30000
CPUs		2	2	2	1	3	3
Min CPU Speed (MHz)		2170	2170	1950	1950	2550	2170
Memory (MB)		4608	4096	3585	4096	5120	
Number of Ethernet NICs		1 - procr (eth0)				2 - procr (eth0), dup link (eth1)	
Min Disk	AWS / GCP	64				64	

Table continues…

Footprints		**Configuration**					
		Communication Manager Simplex				**Communication Manager Duplex**	
		Large	**Medium**	**Small Main**	**Small Survivable**	**Duplex High**	**Duplex Standard**
size (GB)	Azure	80				80	
Azure ISO instance type		• Standard D4as v4 (4 vCPUs, 16-GB memory) • Standard B2ms (2 vCPUs, 8-GB memory)			Standard DS1 v2 (1 vCPU, 3.5-GB memory)	Standard D4as v4 (4 vCPUs, 16-GB memory)	
AWS ISO instance type		• m4.large • m5.large • m5a.large • C5.large • C5a.large				• m4.xlarge • m5.xlarge • m5a.xlarge • C5.xlarge • C5a.xlarge	
GCP ISO instance type		• E2-custom-2- 5120 (2 vCPUs, 5-GB memory) • E2-standard-4 (4 vCPUs, 16-GB memory)				• E2-custom-4 (4 vCPUs, 16-GB memory) • N2-custom-4 (4 vCPUs, 16-GB memory)	

Note:

In Microsoft Azure, you must provide an additional 16 GB of disk space as the Communication Manager does not fully utilize the existing `/usr` partition, and the installer also ignores the `/usr` partition.

Chapter 4: Pre-upgrade tasks

Communication Manager upgrade methods

You can upgrade Communication Manager by using any of the following:

- Solution Deployment Manager
- Communication Manager SMI

Key tasks for upgrading Communication Manager to Release 10.1.x using SDM

The table contains the key tasks that are required to upgrade Communication Manager to Release 10.1.x.

For Duplex deployment, all the steps must be performed on both active and standby server. You must first start the upgrade process with the standby server.

Performing the pre-upgrade steps

Sl. no.	Task	Reference
1	Take a snapshot of the existing Communication Manager virtual machine.	For more information about taking a snapshot see Taking a snapshot of the virtual machine from the vCenter managed host or standalone host on page 130.
2	Take a full backup of the existing Communication Manager	For more information about creating a backup, see Creating a full backup on page 144.
3	Identify the host on which Communication Manager is running. Identify whether the ESXi host is a vCenter managed or a standalone host. Identify the host to which Communication Manager will be upgraded. Identify whether the ESXi host is a vCenter managed or a standalone host.	Go to **Services** > **Solution Deployment Manager** > **Application Management**. Under the **Application Management Tree**, you can see if the ESXi host is a vCenter managed or a standalone host.

Table continues…

Sl. no.	Task	Reference

4	When using System Manager Solution Deployment Manager, ensure that sufficient memory and space is available for the server that you have attached with the software library.	Login to SMGR CLI as a *root* user, and enter the following:
		`cd /`
		`df`
		List of available directories and the disk space usage details appear. Ensure that the `/swlibrary` directory has enough space.

5	Create a user in vCenter with administrator credentials to gain access for the applications using HTTP, FTP, SCP or SFTP services.	-
6	For the existing Communication Manager application instance, ensure that the user credentials specified while adding Communication Manager instance in System Manager can login to the Communication Manager SMI. Additionally, ensure that the same admin user must belong to the Profile 18 (prof18) user profile group.	For more information on creating an administrator user, see Creating a Privileged Administrator login on page 126. For more information on viewing the profile 18 user, see Viewing the admin account for profile 18 on page 127.
7	Configure SNMP access for the Communication Manager user. You *must* configure SNMP access for: • SNMP Version 1 for read-only • SNMP Version 1 for write-only For the Communication Manager application instance, make sure that the Read Community and Write Community used in the System Manager's **Inventory** > **Manage Elements** > **Select CM** > **Edit** > **SNMP attributes** tab, is same in Communication Manager SMI.	For more information on configuring SNMP access, see Configuring SNMP access for the Communication Manager user on page 127. For more information about the SNMP configuration details on the Communication Manager SMI, see Viewing the SNMP configuration on page 128.
8	Add the Communication Manager application license file.	For more information about licensing, see License file for Communication Manager on page 15.
9	Configure user settings	For more information about user settings, see User settings on page 88
10	Ensure that you have the PLDS access credentials and Company ID.	

Key tasks for upgrading Communication Manager to Release 10.1.x using SMI

The table contains the key tasks that are required to upgrade Communication Manager to Release 10.1.x.

For Duplex deployment, all the steps must be performed on both active and standby server. You must first start the upgrade process with the standby server.

Performing the pre-upgrade steps

Sr no.	Task	Note
1	Take a snapshot of the Communication Manager virtual machine.	For more information on taking a snapshot see, Taking a snapshot of the virtual machine from the vCenter managed host or standalone host on page 130.
2	Take a full backup of the Communication Manager	For more information on creating a backup see Creating a full backup on page 144.
3	Create a user in vCenter with administrator credentials to gain access for the applications using HTTP, FTP, SCP or SFTP services.	
4	For the Communication Manager application instance that you have created, create a user with Profile 18 user profile.	For more information on creating a user with Profile 18 user profile, see Creating a Privileged Administrator login on page 126.
5	Add the Communication Manager application license file.	For more information about licensing see License file for Communication Manager on page 15.
6	Ensure that you have the PLDS access credentials and Company ID.	

Chapter 5: Migrating from VMware to ASP R6.0.x (KVM on RHEL 8.10)

Migrating Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to migrate Communication Manager R10.1.x on ASP R5.x VMware to Communication Manager R10.1.x on ASP R6.0.x (KVM on RHEL 8.10).

When migrating, ensure that you match the Communication Manager version. That is to say, the restore has to be performed on the exact same Communication Manager version as the backup.

Procedure

1. Note down the existing VMware details.

   For more information, see Obtaining existing VMware details on page 37.

2. Perform prerequisite tasks to migrate Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10).

   For more information, see Performing prerequisite tasks to migrate Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 37.

3. Install ASP R6.0.x (KVM on RHEL 8.10).

   For more information, see *Installing the Avaya Solutions Platform 130 Appliance* at https://support.avaya.com/css/public/documents/101091802.

4. Deploy Communication Manager on ASP R6.0.x (KVM on RHEL 8.10) host.

   For more information, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

5. Restore Communication Manager Backup on the same software version when backup was taken on Step 2.

   For more information, see Restoring backup on page 145.

Obtaining existing VMware details

About this task

Obtain the configuration details of VMware and use them for ASP R6.0.x (KVM on RHEL 8.10).

For module-specific details, see Obtaining Communication Manager input configuration details for migration on page 38.

Use this procedure to obtain the network IP interface details.

Procedure

1. Log in to ESXi CLI, run the following commands:
    - `# esxcli network ip interface ipv4 get`: note down IPv4 network IP interface details.
    - `# esxcli network ip interface ipv6 get`: note down IPv6 network IP interface details.
2. Login to ESXi vSphere or vCenter and note down the VMware License serial number.

Performing prerequisite tasks to migrate Communication Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to perform the prerequisite tasks before you migrate Communication Manager from R10.1.x on ASP R5.x (VMware) to Communication Manager R10.1.x on ASP R6.0.x (KVM on RHEL 8.10).

Procedure

1. Note down all the available input configuration details of Communication Manager.

    For more information, see Obtaining Communication Manager input configuration details for migration on page 38.
2. Perform full backup from Communication Manager SMI to a remote server.

    For more information, see Creating a full backup on page 144.
3. Validate the backup taken in the previous step.
4. Perform XLN back from Communication Manager CLI to a remote server.

    For more information, see Performing XLN backup from Communication Manager CLI on page 38.
5. Log in to VMware host and power off the virtual machine.

Obtaining Communication Manager input configuration details for migration

About this task

Use this procedure to note down all the available input configuration details of Communication Manager so that you can use these configuration details for restoring Communication Manager on the ASP R6.0.x (KVM on RHEL 8.10) host.

Procedure

1. Log in to Communication Manager SMI.
2. In **Administration** > **Server (Maintenance)** > **Server Configuration** > **Server Role** screen, note down the value of **This Server's Memory Setting**.
3. In **Administration** > **Server (Maintenance)** > **Server Configuration** > **Network Configuration** screen, note down the values of **Host Name**, **DNS Domain**, **DNS IP Addresses**, **Server ID**, **IPv6 Details**, **Default Gateway**, **IP Configuration of all the networks (Public, OOBM, and Duplex)**, and **Subnet mask**.
4. In **Administration** > **Server (Maintenance)** > **Security** > **Server Access** screen, note down whether **Avaya Service Access via EASG** is enabled or disabled.
5. In **Administration** > **Server (Maintenance)** > **Server Configuration** > **NTP Configuration** screen, note down values of **NTP Servers**.
6. In **Administration** > **Server (Maintenance)** > **Server Upgrades** > **Manage Updates** screen, note down (SP/FP/Patch and SSP) details.
7. In **Administration** > **Licensing** > **WebLM Configuration** screen, note down WebLM Server address.
8. Log in to Communication Manager CLI and run the following command `# encryptionStatus` and note down the encryption status.

Performing XLN backup from Communication Manager CLI

About this task

Perform this procedure, *only* if the full backup does not work.

Procedure

1. Log in to Communication Manager CLI.

   Go to SAT and run the command `save translation all` and on successful execution of command, exit from the SAT (logoff).

For a duplex Communication Manager, run the following commands:

- `server -u` to lock the current data on active Communication Manager. The command also sends the data to standby Communication Manager.
- `server -U` to unlock the data on active Communication Manager.

2. Go to sroot or root, run the following scripts:
    - `cd /etc/opt/defty` to identify xln1 and xln2 files in the folder.
    - `cp xln1 CM_10_1_xln1` and `cp xln2 CM_10_1_xln2` to take XLN backup.
    - `cd /etc/opt/defty` to identify xln1 and xln2 backup files in the folder.
    - `ls -lrt` to verify the backup files.
3. Use SCP command to copy `CM_10_1_xln1` and `CM_10_1_xln2` to a remote server. scp `CM_10_1_xln1 CM_10_1_xln2 user@<remoter server IP>:<destination path>`.

Restoring XLN backup

Procedure

1. Use SCP command to copy `CM_10_1_xln1` and `CM_10_1_xln2` files from remote server to `CM(/var/home/ftp/pub)`.
2. Log in to Communication Manager CLI.
3. Switch to sroot or root, run the following scripts:
    - `cd /var/home/ftp/pub` to change the current working folder.
    - `cp CM_10_1_xln1 CM_10_1_xln2 /etc/opt/defty/` to copy the backup files to the folder.
    - `cd /etc/opt/defty` to identify xln1 and xln2 files in the folder.
    - `cp CM_10_1_xln1 xln1` and `cp CM_10_1_xln2 xln2` to restore XLN backup.
    - `drestart 1 4` to restart the Communication Manager service.
4. Go to Communication Manager SAT and verify the restored data.

Chapter 6: Upgrading Communication Manager to R10.1

Upgrading Communication Manager from Release 7.x or 8.x to 10.1 on ASP 130 or VMware

Communication Manager upgrade methods

You can upgrade Communication Manager by using any of the following:

- Solution Deployment Manager
- Communication Manager SMI

Upgrading Communication Manager by using System Manager Solution Deployment Manager

Upgrading Simplex Communication Manager Release 7.x or 8.x to Simplex Communication Manager Release 10.1.x using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade simplex Communication Manager to Release 10.1.x from:

- Release 7.x running on Appliance Virtualization Platform or on VMware.
- Release 8.x running on Appliance Virtualization Platform or on VMware.

Note:

- From Release 10.1, Appliance Virtualization Platform is no longer available. Therefore, if Communication Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x before upgrading Communication Manager to Release 10.1. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

The procedure covers upgrades on the same server and migration to a new server.

Before you begin

1. Ensure that System Manager is running on Release 10.1.
2. Add a location in the System Manager Solution Deployment Manager, if it is already not available.

   For information, see Adding a location on page 94.
3. If Communication Manager is running on:
   - ESXi host, Avaya Solutions Platform 130, then:
     1. First verify if the ESXi host is already added in the System Manager Solution Deployment Manager.
        - To verify go to **Solution Deployment Manager** > **Application Management**.
        - Under Application Managmet Tree, click **Application Management** > **<Location>** > **Platform**. Check if the ESXi host is available. If the ESXi host is available, then go to point 6 on page 42.
     2. If the ESXi host is not added, then add the ESXi host.

     For information about adding the ESXi host, Avaya Solutions Platform 130 host, see Adding an ESXi, or Avaya Solutions Platform 130 host on page 102.
   - vCenter managed host, then:
     1. First verify if the ESXi host is already added in the System Manager Solution Deployment Manager.
        - To verify go to **Solution Deployment Manager** > **Application Management** > **Map vCenter**. In the Map vCenter screen, check if the vCenter is already added. If the vCenter is available, then go to point 6 on page 42.
     2. If the vCentre is not added, add vCenter.

     For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 97

   Important:

   - If the application is running on the ESXi version that is not supported with Release 10.1, then first upgrade the ESXi to a supported ESXi version.

     For information about the supported ESXi version, see Supported ESXi version on page 23.

     For information about upgrading ESXi, see the VMware product documentation.
   - If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
   - If the application is running on the server that is not supported with Release 10.1.x, then deploy Avaya Solutions Platform 130.

     For information about supported servers, see Supported servers for Avaya Aura applications on page 21
4. On the Select the Communication Manager virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

For information, see Re-establishing trust for Solution Deployment Manager elements on page 121.

5. Manage elements

   To upgrade Communication Manager by using Solution Deployment Manager, you must add Communication Manager in the inventory.

   For information about adding a Communication Manager instance to System Manager, see “Adding or editing a standalone Communication Manager instance to System Manager”.

   For information about managing elements, see *Administering Avaya Aura® System Manager*.

6. Obtain the Communication Manager software.

   For information about downloading the software from Avaya PLDS, or from an alternate source to System Manager, see “Downloading the software”

   For information about the software details, see “Software details of Communication Manager”.

7. Ensure that elements that you want to upgrade are in sync with the elements displayed on the Upgrade Management page.

   To ensure that the elements are in sync, on the Communication Manager CLI, enter the following command: `swversion -s`. Communication Manager CLI displays the Communication Manager application details. The application details on the Communication Manager CLI must be same as the software details on the Upgrade Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select Communication Manager and associated elements, and then click **Pre-Upgrade Actions** > **Refresh Element(s)**.
4. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
5. To verify the status of Communication Manager that you refreshed, click the icon on the **Last Action Status** column.
6. After refresh is done, click **Pre-Upgrade Actions** > **Analyze**.
7. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
8. To verify the status of Communication Manager that you refreshed, click the icon on the **Last Action Status** column.
9. After analyze is done, click **Pre-upgrade Actions** > **Pre-upgrade Check**.

10. On the Pre-upgrade Configuration page, do the following:
    1. Do one of the following:
        - For same server, provide the mandatory parameters along with the same target host information.

          Following are the mandatory parameters:
            - **Target platform**: Select the platform on which Communication Manager is hosted
            - **Data store**: Select the existing host's data store
            - **New Target platform**: N/A
            - **Data store**: N/A
            - **Upgrade Source**: Select the upgrade source
            - **Upgrade/update to**: Select the target Communication Manager release (OVA/ISO)
            - **Flexi Footprint**: Select the appropriate footprint
        - For new target server, provide the mandatory parameters along with new target host information.

          Following are the mandatory parameters:
            - **Target platform**: Select the platform on which Communication Manager is hosted
            - **Data store**: Select the existing host's data store
            - **New Target platform**: Select the target platform on which Communication Manager should be hosted
            - **Data store**: Select the target host's data store
            - **Upgrade Source**: Select the upgrade source
            - **Upgrade/update to**: Select the target Communication Manager release (OVA/ISO)
            - **Flexi Footprint**: Select the appropriate footprint

       For information about parameters, see Preupgrade Configuration field descriptions on page 114.
    2. In the Job Schedule section, click **Schedule**.

       You can schedule the job now or for a later time.
11. On the Pre-upgrade Check Job Details page, ensure that the **Pre-upgrade Check Status** field displays ✅.
12. Click **Upgrade Actions** > **Upgrade/Update**.
13. 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.

14. To provide the upgrade configuration details, click **Edit**.
15. On the Edit Upgrade Configuration page, perform the following:
    a. Do one of the following:
        - For same server, provide the mandatory parameters along with same target host information, latest OVA/ISO file, and credentials
        - For new target server, provide the mandatory parameters along with new target host information, latest OVA/ISO file, and credentials

          Note:

          Auto-commit is supported for the same server migration only.

    b. Complete the parameters as mentioned in the Edit Upgrade Configuration field descriptions on page 57.

       Important:

       If you are upgrading from non-encrypted Communication Manager to encrypted Communication Manager, complete the details as mentioned in the Edit Upgrade Configuration field descriptions on page 57.

    c. Complete the details, and click **Save**.
16. 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.
17. Click **Save**.
18. To save the configuration, click **Save Configuration**.

    The update configuration is saved as a job in the Upgrade Jobs Status page.
19. On the Upgrade Configuration page, click **Upgrade**.
20. 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.
21. Click **Schedule**.
22. Click **Upgrade**.

Important:

If you are upgrading from non-encrypted system to encrypted system, then *do not* select the **Require Encryption Pass-Phrase at Boot-Time** check box. *Otherwise, your upgrade fails*.

23. On the Upgrade Management page, click 🔄.
    - After successful upgrade, the **Last Action** column displays **Upgrade**, and **Last Action Status** column displays ✓.
    - The **Last Action** field displays ⚠ with `COMMIT_ROLLBACK_PENDING` if **Auto Commit** is not selected. **Auto-commit** is supported for the same server migration only.
24. To Commit or Rollback, 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**.

    When you commit the changes, the system deletes the old virtual machine.

    When you rollback, the system deletes the newly created virtual machine and starts the old virtual machine automatically. If the old virtual machine does not start automatically, then manually start the old virtual machine.
25. 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.
26. Verify that the upgrade of the application is successful.

    At this step, the upgrade is complete from:
    - Release 7.x or 8.x to Release 10.1

Upgrading duplex Communication Manager servers

About this task

Use the following procedure to upgrade duplex Communication Manager servers.

Procedure

1. Prepare the Communication Manager servers.
2. Upgrade the standby Communication Manager servers.
3. Interchange the roles of Communication Manager servers.

   Now, the standby Communication Manager server becomes active, and the active Communication Manager server becomes standby.

4. Upgrade the new standby Communication Manager server.
5. Change the roles of two Communication Manager servers to the original state.

Preparing duplex Communication Manager servers for upgrade

About this task

The Communication Manager duplex system contains two Communication Managers that are linked together. Use the following procedure to prepare Communication Manager systems for upgrade.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. Select a duplex Communication Manager and click **Edit**.
   - In the **General attributes** tab, do the following:
     a. In the hostname or IP address provide the active Communication Manager IP address.
     b. In **Alternate IP address** enter standby Communication Manager IP address.
     c. Keep alias IP v4 address field blank.
     d. Ensure that the user login name is not same as the user account use to login into Communication Manager CLI.
     e. Select the **Add to Communication Manager** checkbox.

     In the **SNMP attributes** tab do the following:

     - Configure the SNMP settings.
   - In the **General attributes** tab, do the following:
     a. In the **hostname or IP address** field, provide the previously standby Communication Manager IP address.
     b. In **Alternate IP address** field, enter the previously active Communication Manager IP address.
     c. Keep alias IP v4 address field blank.
     d. Ensure that the user login name is not same as the user account use to login into Communication Manager CLI.
     e. Clear the **Add to Communication Manager** checkbox.

     In the **SNMP attributes** tab do the following:

     - Configure the SNMP settings.
3. To ensure that the changes made to the translation are saved, log in to the active Communication Manager server, and perform the following:
   a. Start a SAT session.
   b. Type `save translations all`.

4. Do one of the following:.

    a. On the active Communication Manager command line interface, type `server -u`.

    b. On the Communication Manager SMI, go to **Administration** > **Server (Maintenance)** > **Server Upgrades** > **Pre Update/Upgrade Step** click **Continue**.

       The translations are saved, locked, and the files are sent to the standby server.

5. Do a full backup using the Communication Manager SMI. For more information on creating a full backup, see Creating a full backup on page 144.

Upgrading duplex Communication Manager Release 7.x or 8.x to duplex Communication Manager Release 10.1.x on a same server by using System Manager Solution Deployment Manager

About this task

For upgrading duplex Communication Manager servers, you must use the following upgrade sequence:

1. Upgrade Standby Communication Manager

2. Upgrade Active Communication Manager

Use the procedure to upgrade duplex Communication Manager to Release 10.1.x from:

- Release 7.x running on Appliance Virtualization Platform or on VMware.
- Release 8.x running on Appliance Virtualization Platform or on VMware.

> **Note:**
>
> From Release 10.1, Appliance Virtualization Platform is no longer available. Therefore, if Communication Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x before upgrading Communication Manager to Release 10.1. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

The procedure covers upgrades on the same server.

Before you begin

- Ensure that the duplex Communication Manager is prepared for migration.

Procedure

1. To upgrade the standby Communication Manager, do the following:

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

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

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

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

d. Ensure that the existing server that you are going to upgrade is in the maintenance mode. Log in to the CLI of the standby and type the command server `-b`.

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

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

g. 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.

h. To provide the upgrade configuration details, click **Edit**.

i. On the Edit Upgrade Configuration page, perform the following:

a. Do one of the following:

- For same server, provide the mandatory parameters along with same target host information, latest OVA/ISO file, and credentials.
- For new target server, provide the mandatory parameters along with new target host information, latest OVA/ISO file, and credentials.

Note:

Auto-commit is supported for the same server migration only.

b. Complete the parameters as mentioned in the Edit Upgrade Configuration field descriptions on page 57

Important:

If you are upgrading from non-encrypted Communication Manager to encrypted Communication Manager, complete the details as mentioned in the Edit Upgrade Configuration field descriptions on page 57.

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

j. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

2. From the command line interface of the standby Communication Manager, perform the following:

a. To release the server from the busy out state, type `server -r`.

b. Type `server`, and ensure that the duplication link is active and the standby server refreshes.

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

4. To start the upgrade of the current standby Communication Manager server, do the following:

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

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

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

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

   d. Click **Upgrade Actions** > **Upgrade/Update**.

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

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

      Note:

      Auto-commit is supported for the same server migration only.

      Important:

      If you are upgrading from non-encrypted Communication Manager to encrypted Communication Manager, then *do not* select the **Require Encryption Pass-Phrase at Boot-Time** check box. *Otherwise, your upgrade fails*.

      For information about parameters, see Edit Upgrade Configuration field descriptions on page 57.

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

   h. Schedule the upgrade of Communication Manager.

   i. On the Upgrade Management page, in the **Release Status** column, verify that the status is **Paused**.

   j. For Avaya-provided server in Avaya Aura® Virtualized Appliance environment, install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from Application Management.

   k. To resume the upgrade process, click **Upgrade Actions** > **Resume** to resume the upgrade process.

   l. On the Resume Configuration, select the Appliance Virtualization Platform host and datastore.

   m. Check the job status for upgrade job.

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

5. Do the following:

   a. Type `server`, and ensure that the duplication link is active and the standby server refreshes.

b. **(Optional)** To interchange the roles of standby and active Communication Manager servers from the command line interface of the **active** or standby Communication Manager server, type `server -i`.

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

Upgrading duplex Communication Manager Release 7.x or 8.x to duplex Communication Manager Release 10.1.x and migrating to a new server by using System Manager Solution Deployment Manager

About this task

In duplex Communication Manager servers, you need to first upgrade the standby Communication Manager server, and then the active Communication Manager server.

Use the procedure to upgrade duplex Communication Manager to Release 10.1.x from:

- Release 7.x running on Appliance Virtualization Platform or on VMware.
- Release 8.x running on Appliance Virtualization Platform or on VMware.

  Note:

  From Release 10.1, Appliance Virtualization Platform is no longer available. Therefore, if Communication Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.x before upgrading Communication Manager to Release 10.1. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

The procedure covers upgrades and migration to a new server.

Before you begin

- Ensure that the duplex Communication Manager is prepared for migration.

  For more information, see Preparing duplex Communication Manager servers for upgrade on page 46.
- Ensure that the server that you are going to upgrade is in maintenance mode. For that, log in to the command line interface of the server, and then type the command `server —b`.
- Ensure that System Manager is running on Release 10.1.
- Add a location.

  For information, see Adding a location on page 94.
- Add the ESXi, vCenter, Appliance Virtualization Platform, or Avaya Solutions Platform 130 host.

  For information about adding the host, see Adding an ESXi, or Avaya Solutions Platform 130 host on page 102.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 97.

> **Important:**
>
> - If the application is running on the ESXi version that is not supported with Release 10.1, then first upgrade the ESXi to a supported ESXi version.
>
>   For information about the supported ESXi version, see Supported ESXi version on page 23.
>
>   For information about upgrading ESXi, see the VMware product documentation.
>
> - If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
>
> - If the application is running on the server that is not supported with Release 10.1.x, then deploy Avaya Solutions Platform 130.
>
>   For information about supported servers, see Supported servers for Avaya Aura applications on page 21

- Select the Communication Manager virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For information, see Re-establishing trust for Solution Deployment Manager elements on page 121.

- Ensure that elements that you want to upgrade are in sync with the elements displayed on the Upgrade Management page.

- Make a note of the Network configuration, Duplication Parameters, and Server role details. You may require these details during the upgrade.

Procedure

1. To start upgrading the standby Communication Manager server, do the following:

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

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

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

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

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

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

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

      > **Note:**
      >
      > **Auto-commit** is not supported if you are migrating to a new target server.

> **Important:**
>
> If you are upgrading from non-encrypted Communication Manager to encrypted Communication Manager, then *do not* select the **Require Encryption Pass-Phrase at Boot-Time** check box. *Otherwise, your upgrade fails*.

For information about parameters, see Edit Upgrade Configuration field descriptions on page 57.

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

h. Schedule the upgrade of the standby Communication Manager.

i. Check the job status for upgrade job.

The system upgrades the standby Communication Manager to the latest release, and restores the data on the same Communication Manager system.

2. **(Optional)** To configure the newly upgraded standby Communication Manager server, do the following:

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

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

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

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

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

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

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

5. To start upgrading the Communication Manager server that was active earlier, do the following:

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

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

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

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

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

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

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

   For information about parameters, see Edit Upgrade Configuration field descriptions on page 57.

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

h. Schedule the upgrade of the active Communication Manager.

i. Check the job status for upgrade job.

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

6. To configure the newly upgraded active Communication Manager server, do the following:

   a. Log on to the SMI of the active Communication Manager.

   b. Click **Administration** > **Server (Maintenance)** > **Server Configuration**

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

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

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

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

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

Upgrading survivable core and survivable remote servers

About this task

Use the following procedure to upgrade survivable core (formerly known as ESS) and survivable remote (formerly known as LSP) servers.

Procedure

1. Prepare the Communication Manager server.

> **Note:**
>
> For preparing the server, see Preparing duplex Communication Manager servers for upgrade on page 46.

2. Upgrade the standby Communication Manager server.

   For upgrading, see the following sections:

   - Upgrading Simplex Communication Manager Release 7.x or 8.x to Simplex Communication Manager Release 10.1.x using System Manager Solution Deployment Manager on page 40
   - Upgrading duplex Communication Manager Release 7.x or 8.x to duplex Communication Manager Release 10.1.x on a same server by using System Manager Solution Deployment Manager on page 47
   - Upgrading duplex Communication Manager Release 7.x or 8.x to duplex Communication Manager Release 10.1.x and migrating to a new server by using System Manager Solution Deployment Manager on page 50
3. Interchange the roles of Communication Manager systems.
4. Upgrade the active Communication Manager server.
5. Change the roles of two Communication Manager systems to the original state.

   For more information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300*.

Upgrade Management field descriptions

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

Name	Description
Name	The name of the device that you want to upgrade.
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board.
Sub-Type	The sub type of the device. For example, TN2302AP.
IP Address	The IP address of the device.

Table continues…

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

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade/ Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/ Rollback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download > **Download**	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Download > **Bulk Import Spreadsheet**	Downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

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

Table continues…

Name	Description
IP Address	The IP Address of the device.
Current Version	The release status of the device.
Override Preupgrade Check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system deletes the old virtual machine after the upgrade check.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. • ✗: Configuration incomplete. • ✓: Configuration complete.

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

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

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

Element Configuration: General Configuration Details

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

Table continues…

Name	Description
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/ Platform	The new target host on which you want to run the device.
Migrate With AVP Install	The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x 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 application and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

Name	Description
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.
Hostname	The IP address of the virtual machine.
DNS Search Path	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).

Table continues…

Name	Description
Password for cust	The password of the cust user.
Password for root	The password of the root user.
Timezone	The timezone of the virtual machine.
NTP server(s)	The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,). The application supports only the NTP server. It does not support the NTP pool.
EASG User Access	**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.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Public IP Address	The IP Address of AE Services virtual machine.
Public Netmask	The network mask of AE Services virtual machine.
Private IP Address	This field is optional and can be configured to be used for private network.
Private Netmask	This field is optional, and can be configured to be used for private network.
Out of Band Management Netmask	The subnet mask of the virtual machine for out of band management.

Table continues…

Name	Description
Out of Band Management IP Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: Data Encryption

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled. • In case the administrator forgets to add the passphrase at deployment time, then the boot will proceed with a blank passphrase. The administrator has to just press enter to proceed, because the passphrase is blank. The administrator will be prompted to set the passphrase, only after the Release 8.1.2 and later patch is installed and the system is rebooted. • **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase. • **On vCenter or ESXi:** When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields.
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.

Table continues…

Name	Description
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. ❗ **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the `encryptionRemoteKey` command after the deployment of the application.

Element Configuration: End User License Agreement

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

AVP Configuration: Existing Machine Details

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

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library

Table continues…

Name	Description
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. **Note:** IPv6 is only supported in a dual stack configuration.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.

Table continues…

Name	Description
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

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

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

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

Upgrading Communication Manager using SMI

Considerations for upgrading Communication Manager using full backup

Important:

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

1. When upgrading Communication Manager from 7.x or 8.x to 10.1, using the full backup, the system restores the configuration for the following:
    - **Accounts** (Logins, Profiles)
    - **Translations**
2. After a full backup upgrade of Communication Manager, the following must be manually configured using the Communication Manager System Management Interface:
    - **Schedule Backup**
3. Manually configure the **SID** and **MID** fields of the server after the restore process. This is needed for the file sync to work between the Survivable Remote server, Survivable Core server, and the Main server.

    Note:

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

Upgrading Communication Manager using customized backup

About this task

When upgrading Communication Manager from R7.x or R8.x to R10.1, take a backup of the Communication Manager R7.x or R8.x files and restore them on Communication Manager R10.1. You can take a backup and restore the following files:

- All Communication Manager configuration
- Certs
- Linux Users

After you upgrade and restore the Communication Manager files, you must manually configure the following:.

- **Schedule Backup** using the Communication Manager System Management Interface

- **SID** and **MID** fields of the server. This is needed for the file sync to work between the Survivable Remote server, Survivable Core server, and the Main server.

  Note:

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

Before you begin

- Make a note of the existing Communication Manager host name, DNS, SID, and MID information. You need to manually enter these details after restoring the backup files.

Procedure

1. Take backup of the existing Communication Manager virtual machine.

   For information about creating the backup, see Creating a customized backup on page 143.

2. Shut down the existing Communication Manager R7.x or R8.x virtual machine.

3. Deploy the new Communication Manager R10.1 virtual machine on a host server using the same network configuration.

   For information about deploying Communication Manager, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment* on the Avaya Support website.

   Note:

   Ensure that the host name and DNS information of the new Communication Manager is same as it was on the existing Communication Manager virtual machine. If the host name and DNS information of the new Communication Manager is not same as it was on the existing Communication Manager virtual machine, select the **Force restore if server name mismatch or server migration** field.

4. If the host name, IP address, and DNS information of the new Communication Manager is not same as it was on the existing Communication Manager virtual machine:

   a. To restore the backup on the new Communication Manager virtual machine, select **Force restore if server name mismatch or server migration** field. After restore is successful, IP address of the new Communication Manager virtual machine will change and the data is restored.

   b. To update Communication Manager IP address, go to new Communication Manager virtual machine console and enter the following command: **`serverInitialNetworkConfig`**. Optionally, you can also use **`serverNetworkConfig`** command to update the Communication Manager IPv4 address.

5. Power on the new Communication Manager virtual machine.

6. After all the services are up, restore the backup on the new Communication Manager virtual machine.

   For information about restoring the backup, see Restoring backup on page 145.

7. After restore is complete, reboot the new Communication Manager virtual machine.
8. Log in to Communication Manager System Management Interface and configure the following if applicable:
    - SNMP
    - Schedule Backup
    - WebLM Server
    - License Feature enablement
    - SID/MID configuration

    Note:

    Optionally, you can change the Communication Manager host name and DNS. This requires modification in WebLM if utilizing Centralized licensing.

Upgrading Communication Manager from Release 6.x to 8.1.x

About this task

For upgrading Communication Manager from Release 6.x to Release 10.1, *first upgrade the entire Aura Solution from 6.x to 8.1.x, and then upgrade the Aura Solution to Release 10.1*. You cannot directly upgrade the Release 6.x system to Release 10.1 and later.

For more information about upgrade sequence for Avaya components and solution, see Upgrade sequence for Avaya components on page 25.

For the supported server details, see “Supported servers” section.

For the supported footprint details, see “Supported footprints” section.

Procedure

1. Upgrade Communication Manager from 6.x to Release 8.1.x.

    To upgrade from Communication Manager 6.x to 8.1.x, see *Upgrading Avaya Aura® Communication Manager* Release 8.1.x on the Avaya Support website.
2. Upgrade from Communication Manager Release 8.1.x to 10.1.

    To upgrade from Communication Manager 8.1.x to 10.1, see the required section in this document.

Upgrading Communication Manager to Release 10.1 on Software-only environment

Upgrade path for Software-only environment

You can upgrade to Communication Manager Release 10.1 in a Software-only environment from:

- Release 8.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Communication Manager Release 7.x on AWS.
- Communication Manager Release 7.x on Appliance Virtualization Platform on Avaya provided server or on VMware in customer-provided Virtualized Environment.

Note:

For upgrading Communication Manager from Release 6.x to Release 10.1, *first upgrade the entire Aura Solution from 6.x to 8.1.x, and then upgrade the Aura Solution to Release 10.1*. You cannot directly upgrade the Release 6.x system to Release 10.1 and later.

Upgrading Communication Manager to Release 10.1.x on Software-only environment using System Manager Solution Deployment Manager

About this task

Use this procedure to upgrade the Communication Manager from any earlier releases to Release 10.1.x on Software-only environment using System Manager Solution Deployment Manager.

Before you begin

Ensure that you install the Red Hat Linux Version 8.4 on the target host. For more information, see the *Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments* document.

Procedure

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

Note:

If there are multiple elements available on the host, you must repeat this step to establish trust for each of these elements.

For more information, see Re-establishing trust for Solution Deployment Manager elements on page 121.

6. On the navigation bar, click **Upgrade Management**.
7. Select the element(s) that you want to upgrade and perform the following steps:
    a. Click **Pre-upgrade Actions** > **Refresh Element(s)** and click **Schedule**.
    b. Click **Pre-upgrade Actions** > **Analyze** and click **Schedule**.
    c. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
    d. On the **Pre-upgrade Configuration** page, select **Target Platform** as Software Only and select the **Upgrade Source** where the application source file is located.

    Note:

    If you upgrade to a different box, select the relevant option available under **New Target Platform**.
8. Select the elements to upgrade and click **Upgrade Actions** > **Upgrade/Update**.
9. On the **Upgrade Configuration** page, click **Edit** next to the element to upgrade.
10. On the **Edit Upgrade Configuration** page, configure the following options:
    - Select **ESXI/AVP host/Platform** as Software only.
    - Select **New Target ESXI/AVP host/Platform** if you upgrade to a different box.
    - Select **Upgrade Source**, which is the location where the application source file is located.
    - Select **Upgrade To**.
    - Select **Service/Feature Pack for auto-install after upgrade/migration** and provide the Release 10.1.x patch file.
    - Enter details of **Existing Administrative User** and **Existing Administrative Password** and click **Pre-populate Data**.
    - Configure **Enhanced Access Security Gateway (EASG)**.
    - Enter details of **CM Privileged Administrator User Login** and **CM Privileged Administrator User Password** and click **Pre-populate Data**.
    - Select the **Enable Customer Root Account for this Application** check box.
    - Select **Flexi Footprint**, **Datastore**, and **End User License Agreement**.
    - Click **Save**.
11. Click **Upgrade**.

    The **Upgrade Job Details** page appears.

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

Upgrading Communication Manager to Release 10.1.x on Software-only environment using SMI

About this task

Use the procedure to upgrade Communication Manager from any earlier releases to Release 10.1.x on Software-only environment by using the manual Backup-Restore process.

Note:

Use this procedure to upgrade Avaya Aura® application Release 8.x on Nutanix to Avaya Aura® application Release 10.1.x in the Software-only environment.

Before you begin

Ensure that you have,

- Installed the Red Hat Linux Version 8.4 on the target host. For more information, refer the *Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments* document.
- Run “Save Trans” utility using Communication Manager CLI before taking the backup.

Procedure

1. Log in to the old Communication Manager System Management Interface with admin credential.
2. Record the network parameters and system parameters, such as IP Address, and Netmask of the old system.
3. Create a backup of the system and copy to the remote server.
4. Deploy the Communication Manager Release 10.1 on the Software-only environment.

For information, see the *Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments* document.

Important:

You can use same network parameters and system parameters that you recorded on the older system or you can use different network parameters to configure the new system.

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

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

    Note:

    Configure the server if you want to verify or change the IP Address, and Netmask of the old system after the system reboots.
17. Verify the software version of the new system.

Chapter 7: Post-upgrade tasks

Accessing the Communication Manager server

After the sucessful upgrade, you can access Communication Manager server by using any of the following:

- Communication Manager SMI
- Communication Manager CLI

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.

7. Check the software version by doing the following:
   a. Click **Administration** > **Server (Maintenance)**.
   b. In the **Server** section, click **Software Version**.

   The Software Version page displays the software version of the active server.

8. Check the application service status by doing the following:
   a. Click **Administration** > **Server (Maintenance)**.
   b. In the **Server** section, click **Process Status**.

   The Process Status Results page displays the status of all the application services.

Related links

Saving translations on page 73
Resolving alarms on page 76
Logging off from all administration applications on page 77
Disconnecting from the server on page 77

Saving translations

Before you begin

Start a SAT session.

About this task

Perform the following procedure on the main server only.

Procedure

1. For simplex Communication Manager, enter `save translations all`.

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

2. For duplex Communication Manager, do the following:
    a. Enter `save translations all`
    b. At the command prompt, enter `filesync -Q all`.

       Verify that the system displays the filesync errors, if any.

Related links

Accessing the System Management Interface on page 72

Upgrade job status

Upgrade job status

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

You must complete the following jobs to complete the upgrade:

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

Related links

Accessing the System Management Interface on page 72

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.

Related links

Accessing the System Management Interface on page 72

Editing an upgrade job

Before you begin

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

Procedure

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

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

Related links

Accessing the System Management Interface on page 72

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.

Related links

Accessing the System Management Interface on page 72

Upgrade Job Status field descriptions

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

Button	Description
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Related links

Accessing the System Management Interface on page 72

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*
   - *Avaya Aura® Communication Manager Server Alarms*

Related links

Accessing the System Management Interface on page 72

Logging off from all administration applications

Procedure

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

Related links

Accessing the System Management Interface on page 72

Disconnecting from the server

Procedure

Unplug the portable computer from the services port.

Related links

Accessing the System Management Interface on page 72

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 Health check. 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 (http://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 or 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 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 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 currently installed on the system.

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.

Title	Description	Audience
Design		
Avaya Aura® Communication Manager Overview and Specification	Provides an overview of the features of Communication Manager	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Security Design	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager System Capacities Table	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
LED Descriptions for Avaya Aura® Communication Manager Hardware Components	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Communication Manager Survivability Options	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
Avaya Aura® Core Solution Description	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
Avaya Aura® Communication Manager Reports	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues…

Title	Description	Audience
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Alarms, Events, and Logs Reference	Provides procedures to monitor, test, and maintain Avaya servers, and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager SNMP Administration and Reference	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager Server Options	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Data Privacy Guidelines	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
Deploying Avaya Aura® Communication Manager in Virtualized Environment	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments	Describes the implementation instructions while deploying Communication Manager on a software-only environment and on Amazon Web Service, Microsoft Azure and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues…

Title	Description	Audience
Upgrading Avaya Aura® Communication Manager	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Screen Reference	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
Avaya Aura® Communication Manager Special Application Features	Describes the special features that are requested by specific customers for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.

4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).

Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura®
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager Release 10.1
61451V	Administering Avaya Aura® Communication Manager Release 10.1

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

  ✱ **Note:**

  Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to http://www.avaya.com/support.
2. Log in to the Avaya support 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: Appendix

Solution Deployment Manager configuration settings

Download Management

User settings

You require the PLDS connection to gain access to Avaya from where you can obtain all software and firmware files that are required for upgrade, migration, and updates. Ensure that you add the required ports and websites to the customer firewall. For example, you require access to the ftp.avaya.com website to get the `versions.xml` and http to grant access to plds.avaya.com. If the customer decides not to open PLDS in the organization firewall, an alternate source must be set to access the software. For example, if the customer wants to test the latest versions of software before using the software for production. By using the alternate source, the customers can get the software that is recommended by the analyze operation.

Establishing PLDS connection to Avaya

About this task

Use the procedure to configure the location from where System Manager displays information about the latest software and firmware releases during Analyze operation. The entitlements depend on the credentials that you provide on the **User Settings** page.

Before you begin

- Obtain a company ID to configure PLDS.
- Add the required ports and websites to a firewall of customer.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **User Settings**.
2. On the User Settings page, click **Edit**.
3. Select the **Use Avaya Support Site** check box, and provide the SSO username and SSO password for PLDS, and the company ID.
4. Configure the PLDS settings and proxy settings for the software download.
5. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.

Note:

If you are using a proxy server that uses certificates, add the full CA certificate chain of the identity certificate that is used to secure the proxy server into the System Manager trust store. Failure to do so will result in errors when System Manager tries to connect to the proxy server to reach out to Avaya PLDS.

For more information about how to add a CA certificate to the System Manager trust store, see Adding trusted certificates on page 89.

6. Click **Commit**.

Obtaining a company ID

Before you begin

Ensure that you have access and user credentials to log in to the PLDS website at https://plds.avaya.com.

Procedure

1. On the web browser, type the PLDS URL, `https://plds.avaya.com`.
2. In the **Email address** field, enter the user name, and in the **Password** field, enter the password.
3. Click **Submit**.
4. After successful log in, on the Home page, click **Administration** > **My Company**.

   The system displays the company ID followed by a company name.

Adding trusted certificates

About this task

Use the following procedure to import the certificates that you want to add as trusted certificate in the trust store of the element.

Note:

From Release 8.1, you can add trusted certificates for multiple elements. All the elements must be of same **Type** and **Version**. When you add trusted certificates for multiple elements, the system creates a scheduled job. To view the certificate management job status, select the element, and click **View Certificate Add Status** on the Manage Elements page.

If you select multiple elements, click **More Actions** > **Manage Trusted Certificates**, and the version of the elements is not up to date or empty then System Manager displays the following error message:

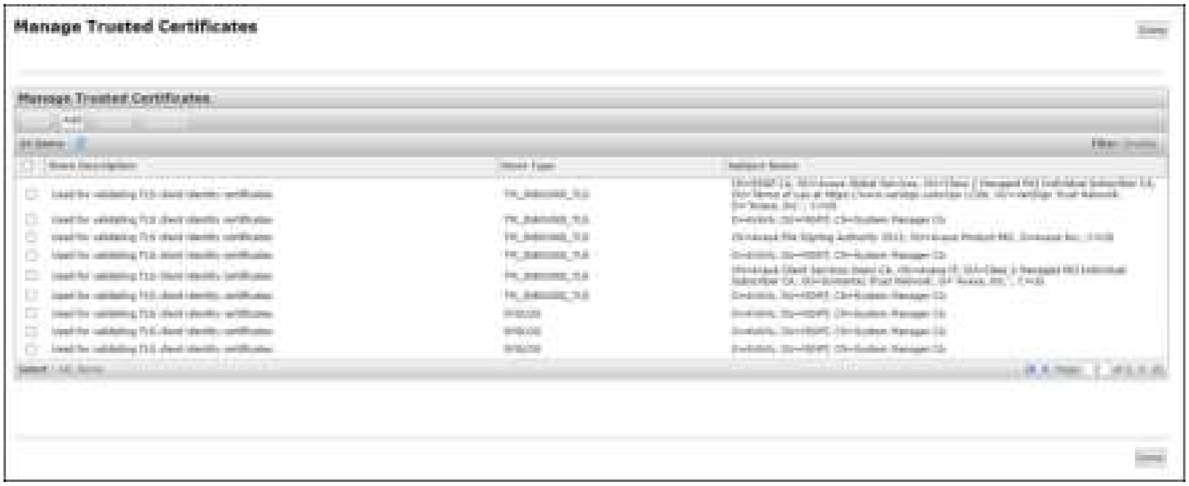
```
ElementType and Version of Selected Elements do not match.
```

Before you begin

Perform the **Refresh Element(s)** operation under **Pre-upgrade Actions** on the **Services** > **Solution Deployment Manager** > **Upgrade Management** page and ensure that the version in the **Current Version** column is up to date for all the elements on which you plan to add trusted certificates at once.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select one or more elements, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.



Manage Trusted Certificates

Manage Trusted Certificates

4. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select a store type or select **All** if you are unsure of the store type.
5. To import certificates from a file, do the following:
   a. Click **Import from file**.
   b. Type the file name or click **Browse** to select a file.

      Note:

      System Manager validates the file type. If you provide an invalid file type, the system displays an error message.
   c. Click **Retrieve Certificate**.
6. To import certificates in the PEM format, do the following:
   a. Locate the PEM certificate.
   b. Open the certificate in the Notepad application.
   c. Select and copy the contents in the file.
   d. On the Add Trusted Certificates page, click **Import as PEM certificate**.
   e. Paste the contents from the PEM file in the text box provided on the Add Trusted Certificates page.
7. To import certificates from existing certificates, do the following:
   a. Click **Import from existing certificates**.

   b. In the Global Trusted Certificate section, select a certificate.

8. To import certificates by using TLS, do the following:
   a. Click **Import using TLS**.
   b. In **IP Address**, type the IP address of the computer.
   c. In **Port**, type the port of the computer.
   d. Click **Retrieve Certificate**.
9. Click **Commit**.
10. Restart the System Manager Application server.

User Settings field descriptions

Source configuration

Name	Description
Use Avaya Support site	The option to find the information and download the software releases from the Avaya Support website. **Note:** • To download the firmware and analyze the software on System Manager, you must gain access to `plds.avaya.com` `pldsxml.avaya.com`, and `downloads.dlavaya.com`. • Select the **Use Avaya Support Site** check box, to use **Avaya Support Site**. Enter the SSO user name, SSO password, and Company ID details. The SSO authentication is required to get entitlements for **Analyze** and artifacts for download. • If you select the check box, the **Alternate Source** is unavailable.
Alternate Source	The website location from where you can get the latest software. The alternate source is an HTTP URL and an alternate to the Avaya Support website. You must set the alternate source. For more information, see *Setting up an alternate source*. **Note:** • The XML files compare the available software version and the latest available version in PLDS. • Clear the **Use Avaya Support Site** check box, to use alternate source repository. You must enter a http URL, for example: `http://10.10.10.10/SUMDATA/`. • The IP address of the alternate source can be the same as the IP address of the software library. However, ensure that the URL location and the server path for software library configuration are different.

PLDS configuration

Name	Description
SSO User Name	The user name used as a single sign on for PLDS.
SSO Password	The single sign on password for PLDS.
Confirm SSO Password	The SSO password that you retype in this field.
Company ID	The company ID for PLDS. For more information, see Obtaining a company ID. ✱ **Note:** After upgrading System Manager, if the system does not auto populate the **Company ID** field, then you must manually edit the field with appropriate value after the upgrade.

Proxy settings

You require proxy settings to use the Avaya PLDS and the Avaya Support site. If your network configuration requires a proxy, enter the details in the **Proxy Settings** section.

Name	Description
Use Proxy	The option to use the proxy server for PLDS.
Host	The host name of the proxy.
Port	The port of the proxy.
Password	The password of the proxy server for the Avaya Support website.
Confirm Password	The password of the proxy server that you retype for the Avaya Support website.

Button	Description
Edit	Displays the edit page to change the user settings.
Commit	To save the changes to the user settings.
Reset to Default	To reset the page and clear the values.
Cancel	To cancel the changes and return to the previous page.

Downloading the software

Before you begin

If you are downloading the software from PLDS or alternate source, configure the User Settings.

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

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

The system displays the File Download Manager page.

3. To change the display settings, click one of the following:
   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.
4. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
5. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

   The time to complete the refresh operation depends on the source configuration in **User Settings**.
6. Click **Show Files**.
7. In **Select Files Download Details**, do the following:
   a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.
   b. Select the files that you want to download.
   c. Click **Download**.

      In File Download Status, the system displays the file that you selected for download.

Application management

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

- Defines the physical location for ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change and patch installation, restart the shutdown, and certificate validation of 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.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

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

Managing the location

Viewing a location

Procedure

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

   The Locations section lists all locations.

Related links

Application management on page 93

Adding a location

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
4. Click **Save**.

   System Manager displays the new location in the **Application Management Tree** section.

Related links

Application management on page 93
New and Edit location field descriptions on page 95

Editing the location

Procedure

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

5. Click **Save**.

Related links

Application management on page 93
New and Edit location field descriptions on page 95

Deleting a location

Procedure

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

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

Related links

Application management on page 93

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

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

Table continues…

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

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

Related links

Application management on page 93

Managing vCenter

Creating a role for a user

About this task

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

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

Procedure

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

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

- **Network**
- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

Note:

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

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

Note:

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

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

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Related links

Application management on page 93

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, and 7.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

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

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.

4. In the New vCenter section, provide the following vCenter information:
    a. In **vCenter FQDN**, type FQDN of vCenter.
        - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
        - The FQDN value must match with the value of the **SAN** field of the vCenter certificate. The FQDN value is case sensitive.

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

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

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

        PSC must have a valid certificate.

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

    f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

    The system generates the certificate and adds vCenter.

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

Related links

Application management on page 93
Editing vCenter on page 98
Map vCenter field descriptions on page 99
New vCenter and Edit vCenter field descriptions on page 100

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.

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

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

Related links

Application management on page 93

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

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

    The system deletes the vCenter from the inventory.

Related links

Application management on page 93

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.

Table continues…

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

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

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

Related links

Application management on page 93

New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.

Table continues…

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

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

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.

Table continues…

Name	Description
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 8.1 and later, do not select the 5.0 and 5.1 versions. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Related links

Application management on page 93

Managing the platform

AVP/ESXi host platform

Adding an ESXi, or Avaya Solutions Platform 130 host

About this task

Use the procedure to add an ESXi, or Avaya Solutions Platform 130 Release 5.x host. You can associate an ESXi host with an existing location.

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

Note:

You can add a VMware ESXi host in Solution Deployment Manager only if Standard or Enterprise VMware license is applied on the VMware ESXi host.

If VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or VMware ESXi host is in evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

Solution Deployment Manager only supports the VMware ESXi hosts. If you try to add another host, the system displays an error message.

You can add Avaya Solutions Platform 130 Release 5.x (Avaya Supplied ESXi) in the same manner as VMware ESXi host.

Before you begin

Add a location.

Procedure

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

3. In **Application Management Tree**, select a location.
4. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
5. In the New Platform section, do the following:
    a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

       For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root user name.

    b. In **Platform Type**, select **AVP/ESXi**.
    c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.
6. Click **Save**.
7. In the Certificate dialog box, click **Accept Certificate**.

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

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

       For more information, see Re-establishing trust for Solution Deployment Manager elements on page 121.

    c. Click **More Actions** > **Refresh App**.

   Important:

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

Next steps

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

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

Related links

Application management on page 93

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

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

Related links

Application management on page 93

Application management on page 93
Application management on page 93

Removing a platform

Procedure

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

Related links

Application management on page 93
Application management on page 93

Software only platform

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 10.1.x, the System Manager system supports the Red Hat Enterprise Linux Release 8.4 (64-bit) operating system.

Before you begin

Add a location.

Procedure

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

   For a software-only deployment, the username must have permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

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

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

The System Manager system displays the added base operating system on the **Platforms** tab.

Related links

Application management on page 93

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

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

Related links

Application management on page 93
Application management on page 93
Application management on page 93

Removing a platform

Procedure

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

Related links

Application management on page 93
Application management on page 93

Restarting a 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 Web Client or through the Solution Deployment Manager client.

Procedure

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

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

Related links

Application management on page 93

ASP 130

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
    1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
    2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

       For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface”.
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
    - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
    - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
    a. Provide details of Platform name, Platform FQDN, username, and password.

       For Avaya Solutions Platform 130 deployment, you can also provide the root username.

    b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

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

Next steps

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

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

Related links

Application management on page 93

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.

Table continues…

Name	Description
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

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

Related links

Application management on page 93
Application management on page 93
Application management on page 93

Removing a platform

Procedure

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

Related links

Application management on page 93
Application management on page 93

Applications pre-upgrade functions

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.
- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
    a. Select one or more devices.
    b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. 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.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

    The **Last Action Status** column displays ✓ and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

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.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

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

3. On the Upgrade Management page, do the following:

    a. Select a device that you want to analyze.

    b. Click **Pre-upgrade Actions** > **Analyze**.

4. 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.

5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

    The **Last Action Status** column displays a ✓, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

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

    The system displays the File Download Manager page.

3. To change the display settings, click one of the following:

    - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
    - **List View**: To view the list of elements in the list format. Every element is displayed individually.

4. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
5. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

    The time to complete the refresh operation depends on the source configuration in **User Settings**.

6. Click **Show Files**.
7. In **Select Files Download Details**, do the following:

    a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.

b. Select the files that you want to download.

c. Click **Download**.

In File Download Status, the system displays the file that you selected for download.

File Download Manager field descriptions

Select Software/Hardware Types

Name	Description
Family Name	The name of the device family.
Hardware/Software	The name of the associated software or hardware.

Select Files Download Details

Name	Description
Source	The source from where Download Manager gets the software or firmware files. The options are: • **Avaya PLDS/Alternate Source** • **My Computer**

Name	Description
File name	The file name.
Version	The file version.
Entitled	The file entitlements.
File Size (in bytes)	The file size in bytes.
Hardware/Software	The name of the hardware or the software.
Family Name	The name of the device family.
Content Type	The type of the content.
Software Library	The status of the file download.
File Description	A description of the file that you download.

Button	Description
Refresh Families	Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page. **Note:** When you add or update details in the `versions.xml` file, you must click **Refresh Families** to get the updated information.
Show Files	Displays the files associated with the element that you selected.

File Download Status

Name	Description
File Name	The file name of the software or firmware file.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.
Status	The status of the download activity.
Scheduled By	The user who scheduled the download job.

Button	Description
Delete	Deletes the files that you have selected.

Performing the preupgrade check

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   Note:

   To upgrade to different server, in **Target Host**, select the target server host.
5. 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.
6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a ✓.

Preupgrade Configuration field descriptions

Pre upgrade Configuration Parameters

Name	Description
Element name	The name of the application that you want to upgrade.
Parent name	The parent of the application that you want to upgrade.

Table continues…

Name	Description
IP Address	The IP address of the application that you want to upgrade.
Current Version	The current version of the application that you want to upgrade.
Target Platform	The Appliance Virtualization Platform or ESXi host of the virtual machine.
Data Store	The data store. When you set the **Target Host** as **Same Box**, the system enables the **Data Store** field.
New Target Platform	The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine. For upgrades on a different server, add Appliance Virtualization Platform or ESXi host from Application Management.
Upgrade Source	The location where OVA or the software patches are available in the local storage or remote server.
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

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.

Adding or editing a Communication Manager instance to System Manager

About this task

Use the following procedure for adding or editing the Simplex or Duplex Communication Manager instance to System Manager.

> ❗ **Important:**
>
> When you deploy the Communication Manager duplex pair through Solution Deployment Manager Application Management, Solution Deployment Manager creates the Active Communication Manager and Standby Communication Manager element entries by using the IP Address or FQDN of the respective Communication Manager on the System Manager **Services** > **Inventory** > **Manage Elements** page.
>
> - To perform the Communication Manager synchronization and other operations, you must select the current Active Communication Manager entry and edit the following fields:
>   - **Alternate IP Address**: Provide the current Standby Communication Manager server IP Address or FQDN.
>   - **Add to Communication Manager**: Select this to administer Communication Manager on System Manager.
>   - **Enable Notifications**: Select this to enable the Communication Manager Notify Sync feature.
>
>   For more information about Communication Manager notify synchronization, see *Administering Avaya Aura® System Manager*.
> - Do not edit the entry of the Standby Communication Manager element.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, do one of the following:
    - To add Communication Manager, click **New**.

      On the New Elements page, in the **Type** field, click **Communication Manager**.

      System Manager displays the Add Communication Manager page.
    - To edit Communication Manager, click **Edit**.

      System Manager displays the Edit Communication Manager <CMName> page.
4. On the **General Attributes** tab, provide the following information:
    a. In **Name**, type the Communication Manager server name.

       The Communication Manager name can be upto 256 characters.

    b. In **Hostname or IP Address**, type the host name or IP Address of the Communication Manager server.

The IP address can be in the IPv4 or IPv6 format.

Note:

- For the active Communication Manager server provide the host name or IP address in **Hostname or IP Address** and for the standby Communication Manager server provide the host name or IP address in **Alternate IP Address**.
- In a duplex configuration, while adding a Communication Manager instance to System Manager, virtual address of Communication Manager must not be used as it is not supported.

c. In **Login**, type the customer login name that is required to access Communication Manager.

d. In **Authentication Type**, select the required option.

e. Enter and reenter the password, or ASG key required to access Communication Manager.

f. In **Port**, type the port number of the Communication Manager server.

g. To administer Communication Manager on System Manager, select the **Add to Communication Manager** check box.

When you select **Add to Communication Manager** check box, Communication Manager instance appears in the **Synchronize CM Data and Configure Options** page, under **Services** > **Inventory** > **Synchronization** > **Communication instance**.

h. In **CM Type**, click **Standalone** to add a Communication Manager.

5. On the **SNMP Attributes** tab, perform the following:

   a. Under **Version**, select **V1**.

   b. Enter the required information.

   c. From **Device Type**, select the type of Communication Manager.

6. Click **Commit**.

   System Manager displays the Communication Manager instance that you added on the Manage Elements page.

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 Web Client or through the Solution Deployment Manager client.

Procedure

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

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

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

Shutting down the Appliance Virtualization Platform host

About this task

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

Procedure

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

   The Appliance Virtualization Platform host and virtual machines shut down.

Shutting down Appliance Virtualization Platform host from CLI

About this task

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh`.

   The system displays `Are you sure you want to stop all VMs and shutdown?`
3. To confirm the shutdown operation, type `Y`.

   The system shuts down Appliance Virtualization Platform host, and stops all virtual machines running on the Appliance Virtualization Platform host. The host does not restart automatically.

   You must manually turn on the Appliance Virtualization Platform server. All virtual machines running on Appliance Virtualization Platform automatically start.

Managing the application

Editing an application

Before you begin

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

Procedure

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

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

    ✱ **Note:**

    To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

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

    ✱ **Note:**

    To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

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

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

    e. Provide the IP address and FQDN of the application.

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

5. Click **Save**.

Starting an application from Solution Deployment Manager

Procedure

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

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

Stopping an application from Solution Deployment Manager

About this task

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

Procedure

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

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

Restarting an application from Solution Deployment Manager

Before you begin

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

Procedure

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

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

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application.

Before you begin

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

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 (SDM CLIENT).
2. Click **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the **Applications** tab, in the Applications for Selected Location <location name> area, select an application.
5. Click **More Actions** > **Re-establish connection**.
6. Select the release version of the product deployed on the application.

   The options are:

   - **6.3 and below**: When you select this, the system displays the following message:

     `Trust cannot be established for this version VM.`
   - **7.0**
   - **7.1 and above**
   - **others**

   Note:

   When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
7. When you select the version **7.0** or **others**, in **User Name**, type the user name of the application.
8. When you select the version **7.0** or **others**, in **Password**, type the password of the application.
9. Click **Reestablish Connection**.

Common causes for application deployment failure

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

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

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

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

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

Reestablish Connection field descriptions

Name	Description
Select Version	Select the required version. The options are: • **6.3 and below** • **7.0** • **7.1 and above** • **others** ✱ **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Application Name	The name of the application.
VM IP/FQDN	The IP address or FQDN of the application.
User Name	The user name of the application. ✱ **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

Table continues…

Name	Description
Password	The password of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

Button	Description
Reestablish Connection	Establishes connection between System Manager and the application.
Cancel	Cancels the changes and returns to the previous page.

Virtual machine report

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

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

Important:

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

generate_report.sh command

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

Syntax

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

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

Generating a virtual machine report

Before you begin

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

Procedure

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

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

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

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

   Note:

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

Viewing the status of the virtual machine report

Procedure

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

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

Aborting the virtual machine report generation

About this task

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

Procedure

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

3. Type the `./generate_report.sh –a` command.

   The system aborts the virtual machine report generation process.

Communication Manager configuration settings

OS-level logins for Communication Manager

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

- **root:** A default user login that cannot be removed . By default, a root user has complete access.
- **sroot:** A root-level user login that is used by Avaya Services. The init, inads, craft, and rasaccess users are also Avaya services logins that are equivalent to customer super-users in CM. These logins (including sroot) can be removed if desired, but that does make the system difficult for services to troubleshoot should the need the arise.

  Note:

  Sroot and root cannot login directly from either SSH or the web GUI.
- **acpsnmp:** acpsnmp user is used internally by Communication Manager to handle SNMP-related tasks. As you can see, it has a shell of /sbin/nologin and cannot login on the Web or via SSH. It has customer super-user access because it needs to perform administration operations. This user cannot be deleted, nor can the password be changed (it doesn't have a password anyway).
- **csadmin:** csadmin is used by the System Manager orchestration software in Solution Deployment Manager to perform upgrades and other maintenance that is required. This login is a customer super-user that should not be removed in order to allow Solution Deployment Manager to continue working.
- **init, inads, rasaccess, craft, and csadmin:** Users with these users logins cannot change their passwords. The csadmin login user will use keys, and the other users are protected by EASG challenge-response logins.

Warning:

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

- **`sroot`**
- **`init`**
- **`craft`**

License management

Following are the use cases for managing licenses when an application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 8.0 and later, Software-only Environment supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to Software-only Environment, but only the applications move to Software-only Environment, then you do not have to regenerate the license for those applications that move to Software-only Environment.
- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to Software-only Environment, then all the licenses need to migrate to the centralized System Manager Release 8.0 and later with integrated WebLM in AWS and the applications that move need to regenerate the license files.

Creating a Privileged Administrator login

About this task

Use the following procedure to create a Communication Manager privileged administrator login account.

Procedure

1. On the Communication Manager System Management Interface, go to **Administration** > **Server (Maintenance)**.
2. In the left navigation pane, under Security, click **Administrator Accounts.**
3. On the Administrator Accounts page, select **Add Login** > **Privileged Administrator**.
4. Click **Submit**.

   Communication Manager displays the Administrator Accounts -- Add Login: Privileged Administrator page.
5. In **Login name**, enter a login name for the administrator.
6. In **Additional groups (profile)**, keep the default value **prof18**.
7. Enter a password.

> **Important:**
>
> Note the administrator user credentials that you enter. You will require these credentials during the Communication Manager upgrade process.

8. Enter other details as required.
9. Click **Submit**.

Viewing the Privileged Administrator account for Profile 18

About this task

Follow the given steps to create a priviledged administrator login:

Procedure

1. On SMI page, under **Administration** tab, select **Server (Maintenance)**.
2. Under Security section, click **Administrator Accounts**.
3. On Administrator Accounts page, select **Change** > **<custom user>** from the drop-down.
4. Click **Submit**.
5. In the Additional groups (profile), the value must be **prof18**.

Configuring SNMP access for the Communication Manager user

Procedure

1. Log in to the Avaya Aura® Communication Manager web interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the SNMP section, click **Access**.
4. Click **Add/Change**.
5. On the Access page:
   - To create an SNMPv1 user, in the SNMP Version 1 section, enter the following details:
     - IP address
     - Access
     - Community Name
   - To create an SNMPv2 user, in the SNMP Version 2 section, enter the following details:
     - IP address
     - Access
     - Community Name
   - To create an SNMPv3 user, in the SNMP Version 3 section, enter the following details:
     - Access

  - User Name
  - Authentication Protocol
  - Authentication Password
  - Privacy Protocol
  - Privacy Password

6. Click **Submit**.

Viewing SNMP configuration details

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. Under the SNMP section, click **Access**.

   On the Access page, view the SNMP configuration details.

General configuration settings

Upgrading Avaya Solutions Platform 130 Release 4.0 to 5.x with Avaya Aura® Communication Manager

About this task

Use the following procedure to upgrade the Avaya Solutions Platform 130 from Release 4.0 (Avaya Supplied ESXi 6.5) to Release 5.x (Avaya Supplied ESXi 7.0) with Communication Manager Release 8.1.x installed on it.

Procedure

1. Take the backup of Communication Manager and keep it on remote servers.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:

   a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

      The system displays the following message:

      ```
      Are you sure you want to shut down <virtual_machine_name>.
      ```

   b. To proceed, click **Yes**.

Note:

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Upgrade Avaya Solutions Platform 130 from Release 4.0 to 5.x.

   For information about upgrading Avaya Solutions Platform 130 from Release 4.0 to 5.x, see Avaya Solutions Platform 130 Series: Upgrading to ESXi 7.0 u2 from ESXi 6.5.x

   - If the Avaya Solutions Platform 130 upgrade is successful, power on the Communication Manager application and ensure Communication Manager is up and running.

     If the Communication Manager application is not up and running, go to step 4.

   - If the Avaya Solutions Platform 130 upgrade fails:

     a. Do the fresh deployment of Avaya Solutions Platform 130 Release 5.x.

        For information about installing Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series.*

     b. Deploy Communication Manager at the same version that was before the Avaya Solutions Platform upgrade.

     c. Restore the backup that is taken at step1 and ensure everything is working fine.

        For information about restoring the backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

4. **(Optional)** If the Communication Manager application is not up and running:

   a. Do the fresh deployment of Communication Manager at the same version that was before the Avaya Solutions Platform 130 upgrade.

   b. Restore the backup taken at step1 and ensure everything is working fine.

      For information about restoring the backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

Note:

If multiple applications are on the same server, follow the upgrade order for restoring the backup.

Upgrading VMware ESXi version

About this task

If the ESXi upgrade is required for upgrading the application to Release 10.1.x, use the following procedure to upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 23.

Before you begin

Take the backup of the application and keep it on remote servers. For information about creating a data backup on a remote server, see the application-specific document.

Procedure

1. Shut down all the virtual machines that are hosted on the ESXi.
2. Put the ESXi into maintenance mode.

   For information about performing steps on ESXi, see VMware product documentation website.
3. Upgrade ESXi to supported ESXi version.

   For information about upgrading ESXi, see VMware product documentation website.
4. After upgrading the ESXi host, log in to the host UI, and exit from the ESXi maintenance mode.
5. Apply the license key for the upgraded ESXi.
6. Power on the virtual machines.

Taking a snapshot of the virtual machine from the vCenter managed host or standalone host

About this task

When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user.

Before you begin

Refer section *Best Practices for VMware features* in *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

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:
   - On the vCenter managed host, select the host, and then select the virtual machine.
   - On the Standalone host, select the virtual machine.
3. In the right pane, click **Actions** > **Take Snapshot**.
4. In the **Name** field, enter a name for the snapshot.
5. In the Description field, provide a suitable description.
6. Click **OK**.

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:

- On the vCenter managed host, select the host, and then select the virtual machine.
- On the Standalone host, select the virtual machine.

3. Right-click the selected virtual machine and click **Snapshot** > **Snapshot Manager**.

   The vSphere Client displays the Snapshot for the <Virtual machine name> dialog box.
4. Select the snapshot and click **Delete**.

   The vSphere Client deletes the selected snapshot.

Patch Installation or Patch Updates

You can apply the Communication Manager patch by using any of the following:

- Solution Deployment Manager
- Communication Manager SMI
- Communication Manager CLI

Related links

Applying the Communication Manager patch using SMI on page 138
Applying the Communication Manager patch using CLI on page 139
Avaya Aura Security Service Packs overview on page 169
Installing software patches by using Solution Deployment Manager on page 131

Software and custom patches using SDM

Installing software patches by using Solution Deployment Manager

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.

To apply patch on the duplex server, you must first apply the patch on the standby server, and then apply patch on the new standby server.

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.
- From Communication Manager Release 10.1.3, Solution Deployment Manager supports the installation of Communication Manager Release 10.1.x Security Service Packs. For Communication Manager Release 10.1.x version earlier than Release 10.1.3, use the command-line interface.

Before you begin

- Perform refresh and analyze operations.
- You must uninstall the previous feature pack or service pack, if available.

  For more information on uninstalling the feature pack or service pack by using the Solution Deployment Manager, see Uninstalling the feature pack or service pack by using Solution Deployment Manager on page 141.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
    1. Select the virtual machine.
    2. To establish trust, click **More Actions** > **Re-establish Connection**.
    3. Click **Refresh VM**.

Procedure

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

   Note:

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

10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

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

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

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

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

    The page displays all software patches that you can commit.

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

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

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

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.
21. To apply patch on the duplex server, do the following:
    a. On the active Communication Manager CLI, enter `server -u` to lock the translations.

b. On the standby Communication Manager server, repeat step 1 to step 20.

c. On the active or standby Communication Manager CLI, enter `server -i` to do interchange.

d. On the new standby Communication Manager server, repeat step 1 to step 20.

Note:

If the upgrade is not successful, and you want to unlock the translations, then on the active Communication Manager CLI, enter `server -U`.

Related links

Patch Installation or Patch Updates on page 131
Preupgrade Configuration field descriptions on page 114
Upgrade Configuration field descriptions on page 56
Edit Upgrade Configuration field descriptions on page 57
Installed Patches field descriptions on page 136
Installing software patches by using Solution Deployment Manager on page 131

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® Communication Manager. 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.

Procedure

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

12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

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

Related links

Patch Installation or Patch Updates on page 131
Installing software patches by using Solution Deployment Manager on page 131

Installed Patches field descriptions

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

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.
Patch Type	The type of the software patch. The options are: • service pack or feature pack or software patch • Security
Patch State	The state of the software patch. The options are: • Active (when patch is activated) • Installed (when patch is unpacked) • Pending (when patch is pending a commit)

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.

Related links

Patch Installation or Patch Updates on page 131

Installing software patches by using Solution Deployment Manager on page 131

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.

Related links

Patch Installation or Patch Updates on page 131

Installing software patches by using Solution Deployment Manager on page 131

Uploading custom patch field descriptions

Name	Description
Software Library	The remote software library where you want to upload the custom patch file.
Product Family	The product family to which the file belongs. In a product family, the number of devices are listed.

Table continues…

Name	Description
Device Type	The device type that you can upgrade using the software library file. For example, B5800 and IP Office are the device types for IP Office.
Software Type	The type of software file which includes firmware and images.
File Version	The software file version that you want to upload. For example, OVA, service pack, and feature pack. Version number is mandatory if you are uploading files, such as OVA, service pack, and feature pack because analyze operation works on version number and the system might have to install the version of the file. Custom patching does not require the analyze operation, and therefore, the file version number is optional.
Hardware Compatibility	The hardware compatibility for the file you upload. For IP Office, this field can be null.
File Size (in bytes)	The file size of the patch file you want to upload.
File	The patch file you want to upload to the remote software library. Click **Choose File** to browse to the file you want to upload.

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

Related links

Patch Installation or Patch Updates on page 131

Installing software patches by using Solution Deployment Manager on page 131

Applying the Communication Manager patch using SMI

About this task

Use the Communication Manager System Management Interface (SMI) to apply the Communication Manager patch.

To apply patch on the duplex server, you must first apply the patch on the standby server, and then apply patch on the new standby server.

Before you begin

Deploy the Communication Manager Release 10.1.

Procedure

1. Log in to Communication Manager System Management Interface using a service account.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous** > **Download Files**.

   The system displays the Download Files page.

4. Select the **File(s) to download from the machine I'm using to connect to the server** option, click **Choose File** to browse the file from your local machine, and click **Download**.
5. In the left navigation pane, click **Server Upgrades** > **Manage Updates**.

   The system displays the Manage Updates page.
6. Select the update ID and click **Unpack**.

   The status of the selected file changes to unpacked.
7. Select the update ID and click **Activate**.

   The status of the patch file changes to activated.

   Note:

   - Activating Communication Manager Service Pack impacts service. You can schedule this activity in a maintenance window.
8. To apply patch on the duplex server, do the following on the Communication Manager SMI:
   a. On the active Communication Manager server, go to **Server Upgrades** > **Pre Update/ Upgrade Step**, and click **Continue**.
   b. On the standby Communication Manager server, repeat step 1 on page 138 to step 7 on page 139.
   c. On the active Communication Manager server, go to **Server** > **Interchange Servers**, and click **Interchange**.
   d. On the new standby Communication Manager server, repeat step 1 on page 138 to step 7 on page 139.

   Note:

   If the upgrade is not successful, and you want to unlock the translations, then on the active Communication Manager server, go to **Server Upgrades** > **Pre Update/ Upgrade Step**, and click **Undo**.

Related links

Patch Installation or Patch Updates on page 131

Installing software patches by using Solution Deployment Manager on page 131

Applying the Communication Manager patch using CLI

About this task

You can apply the Communication Manager patch for simplex and duplex using the Communication Manager CLI.

To apply patch on the duplex server, you must first apply the patch on the standby server, interchange the server, and then apply patch on the new standby server.

Before you begin

Deploy the Communication Manager Release 10.1.

Procedure

1. To apply patch for simplex, do the following:
    a. Copy the patch to the following location: `/var/home/ftp/pub`.
    b. Enter `update_unpack /var/home/ftp/pub/<patch number>`,
    c. Enter `update_show` to view the details on whether any other patch is activated.

       If a patch is already activated, the status of the patch appears as **activated** under the **Status** column.
    d. Enter `save_trans`.
    e. If any old patch is activated, then enter `update_deactivate <patch number>` .

       Patch number apprears under the **Update ID** column.
    f. Enter `update_activate <patch number>` to activate the latest patch.
    g. Enter `statapp` command to check if the services are up.
2. To apply patch for duplex, do the following:
    a. Copy the patch to the following location in both active and stand by servers: `/var/home/ftp/pub`.
    b. Enter `update_unpack /var/home/ftp/pub/<patch number>`,
    c. On the active Communication Manager CLI, enter `save_trans` command and then enter `server -u` to lock the translations.
    d. On the standby Communication Manager, do the following:
        a. Enter `update_show` to view the details on whether any other patch is activated.

           If a patch is already activated, the status of the patch appears as **activated** under the **Status** column.
        b. If any old patch is activated, then enter `update_deactivate <patch number>`.

           Patch number apprears under the **Update ID** column.
        c. Enter `update_activate <patch number>` to activate the latest patch.
        d. Enter `statapp` command to check if the services are up.
    e. Enter `server -i` to do interchange.
    f. To apply patch on the duplex server, on the new standby Communication Manager, repeat substep 2c on page 140.

    Note:

    If the upgrade is not successful, and you want to unlock the translations, then on the new active Communication Manager CLI, enter `server -U`.

Related links

[Patch Installation or Patch Updates](#) on page 131
[Installing software patches by using Solution Deployment Manager](#) on page 131

Patch uninstallation or Rollback process

Patch uninstallation or Rollback

If you want to uninstall a patch and go to the previous state of your system, you can do so. You can uninstall the Communication Manager patch by using any of the following:

- Solution Deployment Manager
- Communication Manager SMI
- Communication Manager CLI

Related links

[Upgrade rollback](#) on page 141
[Uninstalling the feature pack or service pack by using Solution Deployment Manager](#) on page 141

Upgrade rollback

The upgrade rollback is initiated in two cases:

- Upgrade process of an element fails: Administrator need not rollback upgrade of all the elements. When the element upgrade fails, the system stops the entire upgrade process and displays the failure status on the Upgrade Management page. The entire upgrade process does not roll back. Only the failed element upgrade rolls back.
- Upgrade process of the entire system fails: Admin specifies rollback all when the system upgrade fails. The system stops the upgrade and rolls back the overall upgrade process.

Related links

[Patch uninstallation or Rollback](#) on page 141

Uninstalling the feature pack or service pack by using Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select Communication Manager application, and click **Upgrade Actions** > **Installed Patches**.

   The system displays the Installed Patches screen.

4. In the **Patch Operation** section, select **Uninstall**.
5. Select the patch that you want to uninstall.
6. In the **Job Schedule** section, set the **Schedule Job** options as required, and click **Schedule**.

   The selected patch is uninstalled.

Related links

[Patch uninstallation or Rollback](#) on page 141

Deactivating the Communication Manager patch using SMI

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Upgrades** > **Manage Updates**.

   The Manage Updates page displays the status of the files available on the server.

   If the Communication Manager patch is already activated, the status of the patch shows as **activated**.

   Patch number displays under the **Update ID** column.
4. Select the Communication Manager patch and click **Deactivate**.
5. On the confirmation page, click **Yes**.

   The status of the selected patch changes to **unpacked**.

Deactivating the Communication Manager patch using CLI

Procedure

1. To view the currently activated patch details, log in to Communication Manager CLI and enter `update_show`.

   Patch number apprears under the **Update ID** column.
2. Enter `update_deactivate <patch number>`.

   After the patch is deactivated, status of the selected patch changes to **unpacked**.
3. **(Optional)** To remove the patch from the server, enter `update_remove <patch number>`.

Backup and restore

Changing the hostname

Procedure

1. Log in to the Communication Manager System Management Interface (SMI) with administrator privilege user credentials.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   SMI displays the Network Configuration page.
4. Enter the hostname and click **Change**.

   Note:

   If a backup is created with a hostname containing an underscore (_) character, then the backup is not restored on any Communication Manager. Ensure you have a valid hostname before creating a backup.

Creating a customized backup

About this task

When upgrading Communication Manager from R7.x or R8.x to R10.1, you can take a backup from Communication Manager R7.x or R8.x and restore the following files on Communication Manager R10.1:

- All Communication Manager configuration
- Certs
- Linux Users

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 143.

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 **Specify Data Sets** and select the required .

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. Under the **Encryption** section, in the **Encrypt backup using pass phrase**, enter a password to backup the data.

   The pass phrase must be an arbitrary string of 15 to 256 characters, and it can contain the following characters: `a-z, A-Z, 0-9, period (.), underscore (_), dollar sign ($), pound sign (#), equal sign (=), plus sign (+).`
7. Click **Start Backup**.

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

Creating a full 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 143.

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`.

   After a successful backup, the Communication Manager generates the following file:

   `full_<elementname>_<time>_<date>.tar.gz`

   The full backup file consists of the following files:

   - `os_<elementname>_<time>_<date>.tar.gz`
   - `xln_<elementname>_<time>_<date>.tar.gz`
   - `security_<elementname>_<time>_<date>.tar.gz`

Restoring backup

Before you begin

Ensure that Communication Manager is on the latest target release before restoring the backup.

Procedure

1. Log in to 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** > **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 username.
   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. Do any of the following:
   a. To restore full backup file, click `full_<elementname>_<time>_<date>.tar.gz`.
   b. To restore any specific file from the full backup file, extract the full backup file and select the required files from the list.

   Full back up file consists of the following files:

   - `os_<elementname>_<time>_<date>.tar.gz`
   - `xln_<elementname>_<time>_<date>.tar.gz`
   - `security_<elementname>_<time>_<date>.tar.gz`
7. Select **Force restore if server name mismatch or server migration**.
8. Click **Restore**.

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

   9640380

Note:

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

Appendix B: Migration

Migrating Appliance Virtualization Platform deployed on Common Server 1, 2, or 3 with Communication Manager to Avaya Solutions Platform 130 Release 5.x

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on Avaya Common Server 1, 2, or 3 to Avaya Solutions Platform 130 Release 5.x with Communication Manager deployed on it.

Note:

Common Server R1, R2, and R3 (HP DL360 G7/G8/G9 and Dell R610/R620/R630) do not support Avaya Aura® Release 10.1. The last supported release for these servers is Avaya Aura® 8.1.3.x. You must place an order for the new Avaya Solutions Platform 130 R5.x. The Avaya Solutions Platform 130 R5.x installer needs the current Appliance Virtualization Platform and Communication Manager IP and naming information. The installer also needs the Communication Manager server backup details like the user name, password, and directory path.

Note:

If multiple applications are on the same server, follow the upgrade order.

Before you begin

Important:

This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform 130.

Procedure

1. Take the backup of Communication Manager and keep it on remote servers.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:
    1. Select the application, right-click, and then click **Guest OS** > **Shut down**.

        The system displays the following message:

        ```
        Are you sure you want to shut down <virtual_machine_name>.
        ```
    2. To proceed, click **Yes**.

    ✱ **Note:**

    - If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
    - Ensure that no calls are running on the system.
3. Shut down the Appliance Virtualization Platform host using the command line interface.

    For information, see “Shutting down Appliance Virtualization Platform host from CLI”.
4. The CSR1/R2/R3 is now offline. If there are issues with the Avaya Solutions Platform 130 R5.x deployment, you can bring back the CSR1/R2/R3 server on-line.
5. If a rollback is required, you can bring back the CSR1/R2/R3 server on-line.
6. Deploy Avaya Solutions Platform 130 Release 5.x.

    For information about deploying Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series*.
7. Deploy Communication Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.x.

    For information, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.
8. Restore the backup taken and ensure everything is working fine.

    For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

Migrating Appliance Virtualization Platform deployed on Avaya Solutions Platform 120 with Communication Manager to Avaya Solutions Platform 130 Release 5.0

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on Avaya Solutions Platform 120 to Avaya Solutions Platform 130 Release 5.0 with Communication Manager deployed on it.

Note:

If multiple applications are on the same server, follow the upgrade order.

Before you begin

Important:

This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform 130.

Procedure

1. Take the backup of Communication Manager and keep it on remote servers.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:

   a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

      The system displays the following message:

      ```
      Are you sure you want to shut down <virtual_machine_name>.
      ```

   b. To proceed, click **Yes**.

   Note:

   - If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
   - Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

   For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

4. Migrate Appliance Virtualization Platform (Dell PowerEdge R640) to Avaya Solutions Platform 130 Release 5.0.

   For information, see *Migrating Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.0*.

5. Deploy Communication Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.0.

   For information, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

6. Restore the backup taken and ensure everything is working fine.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

Migrate Appliance Virtualization Platform deployed on S8300E with Communication Manager to Avaya Solutions Platform S8300 Release 5.1

To migrate Appliance Virtualization Platform deployed on S8300E to Avaya Solutions Platform S8300 Release 5.1 with Communication Manager survivable core or main server deployed on it, you can have one of the following scenarios:

- **Appliance Virtualization Platform Release 8.1.x deployed on S8300E:** Migrate Appliance Virtualization Platform Release 8.1.x to Avaya Solutions Platform S8300 on the same S8300E card and then upgrade Communication Manager Release 8.1.x to Release 10.1.x with the same profile and footprint details.

  For information, see Migrating Appliance Virtualization Platform deployed on S8300E with Communication Manager to Avaya Solutions Platform S8300 Release 5.1 on page 150.

- **Appliance Virtualization Platform Release 7.x or 8.0.x deployed on S8300E:** You need to deploy Avaya Solutions Platform S8300 on the same S8300E card and then deploy Communication Manager with the same profile and footprint details.

  For information, see Migrating Appliance Virtualization Platform deployed on S8300E with Communication Manager to Avaya Solutions Platform S8300 Release 5.1 on page 150.

- **Appliance Virtualization Platform Release 7.x, 8.0.x, or 8.1.x deployed on S8300D:** You need to reinsert the S8300E card, deploy Avaya Solutions Platform S8300 on the it, and then deploy Communication Manager with the same profile and footprint details.

  For information, see Migrating Appliance Virtualization Platform deployed on S8300D with Communication Manager to Avaya Solutions Platform S8300 Release 5.1 on page 157.

Migrating Appliance Virtualization Platform deployed on S8300E with Communication Manager to Avaya Solutions Platform S8300 Release 5.1

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on S8300E to Avaya Solutions Platform S8300 Release 5.1 with Communication Manager survivable remote or main server deployed on it.

Note:

If multiple applications are on the same server, follow the upgrade order.

Before you begin

Important:

This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform S8300.

- Use the following steps to migrate Appliance Virtualization Platform (S8300E) Release 8.1.x to Avaya Solutions Platform S8300 Release 5.1.
    1. Take the backup of Communication Manager and keep it on remote servers.

       For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.
    2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:
        a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

           The system displays the following message:

           ```
           Are you sure you want to shut down <virtual_machine_name>.
           ```
        b. To proceed, click **Yes**

           Note:

           - If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
           - Ensure that no calls are running on the system.
    3. Migrate Appliance Virtualization Platform (S8300E) to Avaya Solutions Platform S8300 Release 5.1.

       For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300*.
    4. After successful migration, power on Communication Manager, if not already.
    5. Upgrade Communication Manager to Release 10.1.x on Avaya Solutions Platform S8300 Release 5.1.

       For information, see Upgrading Communication Manager Release 8.1.x to Communication Manager Release 10.1.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager on page 152.
- Use the following steps to migrate Appliance Virtualization Platform (S8300E) Release 7.x or 8.0.x to Avaya Solutions Platform S8300 Release 5.1.
    1. Take the backup of Communication Manager and keep it on remote servers.

       For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.
    2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:
        a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

           The system displays the following message:

```
Are you sure you want to shut down <virtual_machine_name>.
```

b. To proceed, click **Yes**

Note:

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

   For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

4. Deploy Avaya Solutions Platform S8300 Release 5.1 on the existing S8300E card.

   For information about deploying Avaya Solutions Platform S8300, see *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300*.

5. Remove the existing Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only.

   Do not add an Avaya Solutions Platform S8300 Release 5.1 host using the IP address.

6. Deploy Communication Manager Release 10.1.x with the same profile and footprint details on Avaya Solutions Platform S8300 Release 5.1 using System Manager Solution Deployment Manager.

   For information, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

7. Restore the backup taken and ensure everything is working fine.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

Upgrading Communication Manager Release 8.1.x to Communication Manager Release 10.1.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade Communication Manager main or survivable remote server (LSP) Release 8.1.x running on Appliance Virtualization Platform to Release 10.1.x on Avaya Solutions Platform S8300.

For migrating Communication Manager survivable remote server or main on Avaya Solutions Platform S8300 Release 5.1, only the **CM Main Max User 1000** and **CM Survivable Max User 1000** profiles are supported.

Note:

From Release 10.1, Appliance Virtualization Platform is no longer available. Therefore, if Communication Manager is deployed on Appliance Virtualization Platform Release 7.x or 8.0.x, then first upgrade Appliance Virtualization Platform to Release 8.1.x and then migrate Appliance Virtualization Platform 8.1.x to Avaya Solutions Platform S8300.

Before you begin

1. Ensure to migrate Appliance Virtualization Platform to Avaya Solutions Platform S8300.

   For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300*.

2. Ensure that System Manager is running on Release 10.1.
3. Add a location in the System Manager Solution Deployment Manager, if it is already not available.

   For information, see Adding a location on page 94.

4. If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) is available in Solution Deployment Manager on the **Platforms** tab, then first remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only. Do not add an ASP S8300 Release 5.1 host using the IP address.

   Add the Avaya Solutions Platform S8300 host in the System Manager Solution Deployment Manager.

5. Add Communication Manager in the inventory.

   For information about adding a Communication Manager instance to System Manager, see “Adding or editing a standalone Communication Manager instance to System Manager”

   For information about managing elements, see *Administering Avaya Aura® System Manager*.

6. Ensure that elements that you want to upgrade are in sync with the elements displayed on the Upgrade Management page.

   To ensure that the elements are in sync, on the Communication Manager CLI, enter the following command: `swversion -s`. Communication Manager CLI displays the Communication Manager application details. The application details on the Communication Manager CLI must be same as the software details on the Upgrade Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select Communication Manager and associated elements, and then click **Pre-Upgrade Actions** > **Refresh Element(s)**.
4. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.

5. To verify the status of Communication Manager that you refreshed, click the icon on the **Last Action Status** column.
6. After refresh is done, click **Pre-Upgrade Actions** > **Analyze**.
7. On the next page, click **Schedule**.

   You can schedule the job now or for a later time.
8. To verify the status of Communication Manager that you refreshed, click the icon on the **Last Action Status** column.
9. After analyze is done, click **Pre-upgrade Actions** > **Pre-upgrade Check**.
10. On the Pre-upgrade Configuration page, do the following:
    1. Do one of the following:
       - For same server, provide the mandatory parameters along with the same target host information.

         Following are the mandatory parameters:
         - **Target platform**: Select the platform on which Communication Manager is hosted
         - **Data store**: Select the existing host's data store
         - **New Target platform**: N/A
         - **Data store**: N/A
         - **Upgrade Source**: Select the upgrade source
         - **Upgrade/update to**: Select the target Communication Manager release (OVA/ISO)
         - **Flexi Footprint**: Select the appropriate footprint
       - For new target server, provide the mandatory parameters along with new target host information.

         Following are the mandatory parameters:
         - **Target platform**: Select the platform on which Communication Manager is hosted
         - **Data store**: Select the existing host's data store
         - **New Target platform**: Select the target platform on which Communication Manager should be hosted
         - **Data store**: Select the target host's data store
         - **Upgrade Source**: Select the upgrade source
         - **Upgrade/update to**: Select the target Communication Manager release (OVA/ISO)
         - **Flexi Footprint**: Select the appropriate footprint

    For information about parameters, see Preupgrade Configuration field descriptions on page 114.

   b. In the Job Schedule section, click **Schedule**.

      You can schedule the job now or for a later time.

11. On the Pre-upgrade Check Job Details page, ensure that the **Pre-upgrade Check Status** field displays ✓.
12. Click **Upgrade Actions** > **Upgrade/Update**.
13. 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.

14. To provide the upgrade configuration details, click **Edit**.
15. On the Edit Upgrade Configuration page, perform the following:
    a. Do one of the following:
       - For same server, provide the mandatory parameters along with same target host information, latest OVA/ISO file, and credentials
       - For new target server, provide the mandatory parameters along with new target host information, latest OVA/ISO file, and credentials

       Note:

       Auto-commit is supported for the same server migration only.

    b. Complete the parameters as mentioned in the Edit Upgrade Configuration field descriptions on page 57.

       Important:

       If you are upgrading from non-encrypted Communication Manager to encrypted Communication Manager, complete the details as mentioned in the Edit Upgrade Configuration field descriptions on page 57.

    c. Complete the details, and click **Save**.
16. 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.

17. Click **Save**.
18. To save the configuration, click **Save Configuration**.

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

19. On the Upgrade Configuration page, click **Upgrade**.

20. 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.
21. Click **Schedule**.
22. Click **Upgrade**.

    Important:

    If you are upgrading from non-encrypted system to encrypted system, then *do not* select the **Require Encryption Pass-Phrase at Boot-Time** check box. *Otherwise, your upgrade fails*.

23. On the Upgrade Management page, click ⟳.
    - After successful upgrade, the **Last Action** column displays **Upgrade**, and **Last Action Status** column displays ✓.
    - The **Last Action** field displays ⚠ with `COMMIT_ROLLBACK_PENDING` if **Auto Commit** is not selected. **Auto-commit** is supported for the same server migration only.
24. To Commit or Rollback, do the following:
    1. On the Upgrade Management page, select the element.
    2. Click **Upgrade Actions** > **Commit/Rollback Upgrade**.

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

    When you commit the changes, the system deletes the old virtual machine.

    When you rollback, the system deletes the newly created virtual machine and starts the old virtual machine automatically. If the old virtual machine does not start automatically, then manually start the old virtual machine.
25. To view the upgrade status, perform the following:
    1. In the navigation pane, click **Upgrade Job Status**.
    2. In the **Job Type** field, click **Upgrade**.
    3. Click the upgrade job that you want to view.
26. Verify that the upgrade of the application is successful.

    At this step, the upgrade is complete from:
    - Release 7.x or 8.x to Release 10.1

Migrating Appliance Virtualization Platform deployed on S8300D with Communication Manager to Avaya Solutions Platform S8300 Release 5.1

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on S8300D to Avaya Solutions Platform S8300 Release 5.1 with Communication Manager survivable remote or main server deployed on it.

Note:

If multiple applications are on the same server, follow the upgrade order.

Before you begin

Important:

This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform S8300.

Procedure

1. Take the backup of Communication Manager and keep it on remote servers.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:

   a. Select the application, right-click, and then click **Guest OS** > **Shut down**.

      The system displays the following message:

      ```
      Are you sure you want to shut down <virtual_machine_name>.
      ```

   b. To proceed, click **Yes**.

   Note:

   - If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
   - Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

   For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

   The S8300D is now offline. If there are issues with the Avaya Solutions Platform S8300 Release 5.1 deployment, you can bring back the S8300D server on-line.

4. Insert the new S8300E card and deploy Avaya Solutions Platform S8300 Release 5.1.

For information about deploying Avaya Solutions Platform S8300, see *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300*.

5. Remove the existing Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only.

   Do not add an Avaya Solutions Platform S8300 Release 5.1 host using the IP address.

6. Deploy Communication Manager Release 10.1.x with the same profile and footprint details on Avaya Solutions Platform S8300 Release 5.1 using System Manager Solution Deployment Manager.

   For information, see *Deploying Avaya Aura® Communication Manager in Virtualized Environment*.

7. Restore the backup taken and ensure everything is working fine.

   For information about creating a data backup on a remote server, see Creating a full backup on page 144 and Restoring backup on page 145.

Appendix C: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10)

Virtual Machine Backups (clone) as an alternative to snapshots

Avaya Aura® documentation refers to snapshots at the application level for various procedures. Snapshots apply to a VMware environment.

With the introduction of the alternative hypervisor in Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), RHEL 8.10 does not support snapshots and Linux does not support issues relating to the use of snapshots.

Virtual machine backup is a similar feature to snapshots. Virtual machine backups use the cloning feature. Use virtual machine backups in place of snapshots for ASP R6.0.x (KVM on RHEL 8.10).

You should only keep backups for a maximum 48 hours in order to ensure sufficient storage is available. You may need to remove them earlier.

Note:

The images and screenshots in this document are for illustration purposes only. The actual user interface may slightly vary due to updates and design changes.

Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to create a clone for backup purposes.

Before you begin

- Ensure there is sufficient space to create the Virtual Machine Backup (clone). Clones are created as “thick provisioned” and require the same size as the virtual machine you are cloning.

- Refer to application documentation for guidelines on storage requirements for different application profiles.
- Shut down the virtual machine for which you are creating a backup (clone). This is a service impacting activity. Perform these steps within a customer-approved maintenance window.

Note:

You must be root or use `sudo` with `custadm` account for CLI commands, and you must enable Administrative access when using the Cockpit user interface.

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

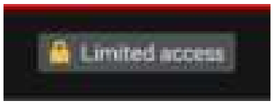
   

   Figure 1: Limited access button

   Note:

   You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.
3. In the Switch to administrative access window, enter the password for **`custadm`**.

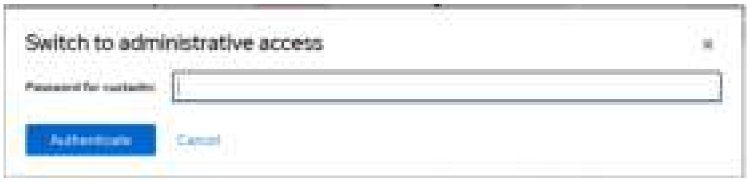
   

   Figure 2: Switch to administrative access

   The **Limited access** button on the top-right of the window changes to **Administrative access**.

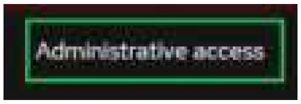
   

   Figure 3: Administrative access button
4. Navigate to **System** > **Virtual Machines** > **Storage Pools**.

   The Name guest_images is a label for `/var/lib/libvirt/images`. If you select guest_images, you can see additional information. If you select Storage Volumes, you can view all images in the `/var/lib/libvirt/images` directory.

5. Review the images and remove any of them that you no longer use.

   Images that do not have a ‘Used by’ value are typically safe to remove.

6. Confirm that you have the necessary space for your clone.
7. Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Run the following command to obtain a list of all virtual machines:

   ```
   sudo virsh list --all
   ```

   Example output:

   ```
   [custadm@asp130-r660xs-a31p ~]# sudo virsh list --all

   Id Name State9--------------------

   1 8HDD-RHEL-810-Fiotester2 running

   2 8HDD-RHEL810-Fiotester1 running

   3 8HDD-RHEL-810-Fiotester3 shut off

   3 8HDD-RHEL-810-Fiotester3-Clone shut off

   3 8HDD-RHEL-810-Fiotester3-clone shut off

   4 Agent_Testing shut off

   4 Agent_Testing-Clone shut off

   5 Agent_Testing2 shut off

   -Agent_Testing3 shut off
   ```

   In this example, the virtual machine Agent_Testing3 is shut off state, ready for backup (clone).

9. Run the following command to backup (clone) the virtual machine. You must use the nonsparse option to ensure the clone is created as thick provisioned.

   ```
   sudo virt-clone --original <Domain-to-be-cloned> --auto-clone-
   nonsparse
   ```

   Example output:

   ```
   sudo virt-clone --original Agent_Testing3 --auto-clone--nonsparse

   Allocating 'RHEL810-agenttestvm3-fat-clone.qcow2' | 50 GB 00:01:06

   Clone 'Agent_Testing3-clone1' created successfully.
   ```

   This command creates a backup (clone) with default values. You can create a clone with any name for the virtual machine and QCOW2 labels by specifying a full path and using the following command:

   ```
   virt-clone --original <VM Domain> --name <Clone VM Label> --
   file /var/lib/libvirt/images/<VM Domain QCOW2 file name>.qcow2--
   nonsparse
   ```

Example for single QCOW2 image:

```
virt-clone --original RHEL810-fiotester1 --name RHEL810-fiotester2
--file /var/lib/libvirt/images/RHEL810-fiotester2.qcow2--nonsparse
```

Example for multiple QCOW2 images:

```
sudo virt-clone --original Duplex_Active_974
--name Duplex_Active_974_CloneTest --file /var/lib/
libvirt/images/Duplex_Active_974_CloneTest_system.qcow2--
nonsparse --file /var/lib/libvirt/images/
Duplex_Active_974_CloneTest_Var_Disk.qcow2--nonsparse
```

Note:

Completion time varies depending on the size of original virtual machine disk.

Calculating space for the clone

About this task

Use this procedure to figure out if you have the necessary space for the clone. This example refers to System Manager but the same information applies to all Avaya Aura® components.

You can use the Cockpit user interface to calculate this information. You can also use the Command Line Interface (CLI). The units of measure may differ. The Cockpit user interface (UI) uses International Electrotechnical Commission (IEC) values, such as Gibibyte. The CLI uses International System of Units (SI) values, such as Gigabyte.

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

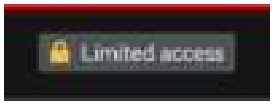
   

   Figure 4: Limited access button

   Note:

   You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.
3. In the Switch to administrative access window, enter the password for **`custadm`**.

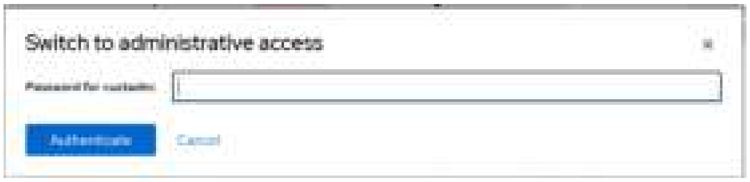


Figure 5: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

Figure 6: Administrative access button

4. Navigate to **System** > **Virtual Machines** > **Storage Pools**.
5. View the information on the **Storage Pools** screen.
6. Divide the amount of used and available space to get the percentage.

   In this example, approximately 18% of the available storage is used (579.51/3299 ~ 18%).

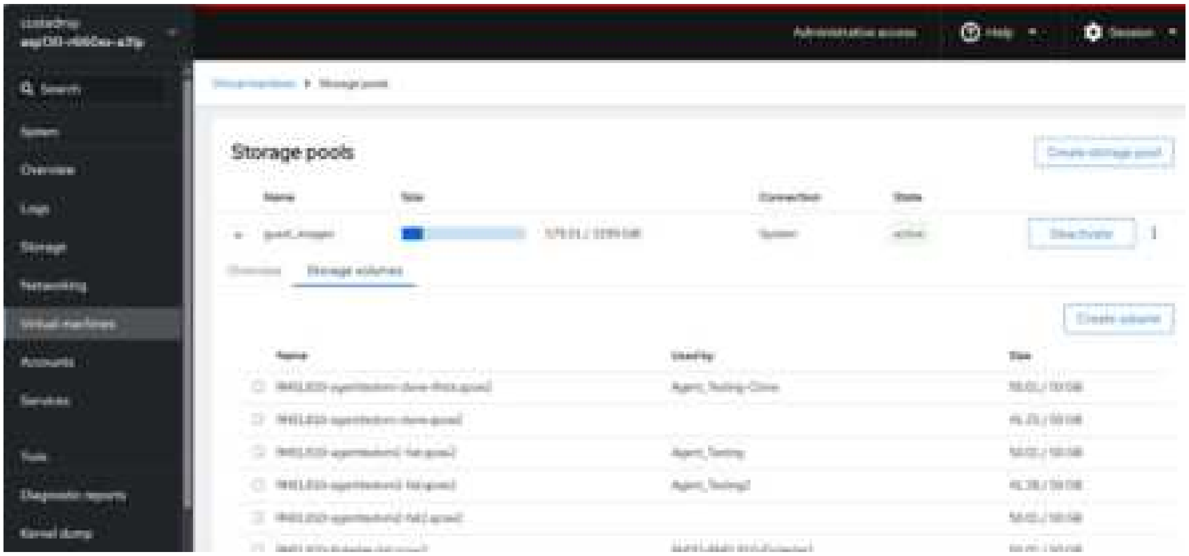


Figure 7: Example size

7. **(Optional)** Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Change the directory to `/var/lib/libvirt/images` and identify the available space.

   In the example below, 18% of available storage is being used on the host.

   Example output:

```
[custadm@asp130-r660xs-a31p ~]$ cd /var/lib/libvirt/images
```

```
[custadm@asp130-r660xs-a31p images]$ df -h .

Filesystem Size Used Avail Use% Mounted on

/dev/mapper/vg_system-lv_libvirt 3.3T 580G 2.7T 18% /var/lib/
libvirt
```

Validating a Virtual Machine Backup (clone)

Procedure

1. Login to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
2. Run the following command to validate the backup (clone):

   ```
   sudo virsh list --all
   ```

   Example output:

   ```
   [custadm@asp130-r660xs-a31p ~]# sudo virsh list --all

   Id Name State9--------------------

   1 8HDD-RHEL-810-Fiotester2 running

   2 8HDD-RHEL810-Fiotester1 running

   3 8HDD-RHEL-810-Fiotester3 shut off

   3 8HDD-RHEL-810-Fiotester3-Clone shut off

   3 8HDD-RHEL-810-Fiotester3-clone shut off

   4 Agent_Testing shut off

   4 Agent_Testing-Clone shut off

   5 Agent_Testing2 shut off

   -Agent_Testing3 shut off

   -Agent_Testing3-clone shut off
   ```

   In this example, the virtual machine Agent_Testing3-clone is the cloned virtual machine.
3. Confirm that the clone is thick provisioned by running the following command on the clone and ensuring that the virtual size is the same as the disk size:

   ```
   cd /var/lib/libvirt/images

   sudo qemu-img info <clone name>
   ```

   Example output:

   ```
   cd /var/lib/libvirt/images

   sudo qemu-img info Agent_Testing3-clone.qcow2
   ```

```
image: Agent_Testing3-clone.qcow2
file format: qcow2
virtual size: 50 GiB (53687091200 bytes)
disk size: 50 GiB
cluster_size: 65536
Format specific information:
compat: 1.1
compression type: zlib
lazy refcounts: true
refcount bits: 16
corrupt: false
extended l2: false
```

4. Run the following command to ensure that the virtual machine is cloned with the same disk name that is provided during the backup (clone):

   ```
   sudo virsh domblklist <cloned VM name>_8_1
   ```

   For example, the output of the command appears as follows:

   ```
   hda /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
   ```

5. Log in to the KVM Cockpit web console as **custadm** in the following format: https://<*IP address or FQDN of KVM host*>:9090.

6. For administration actions, on the top-right of the window, click on the **Limited access** button.

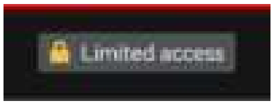
   

   Figure 8: Limited access button

   Note:

   You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

7. In the Switch to administrative access window, enter the password for **custadm**.

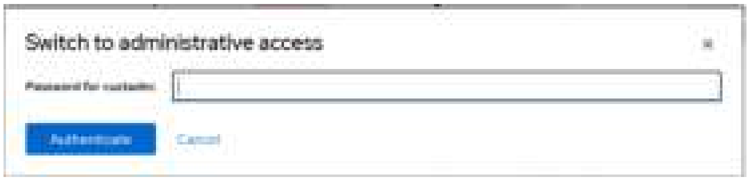
   

   Figure 9: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

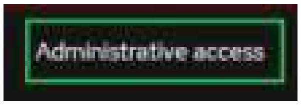
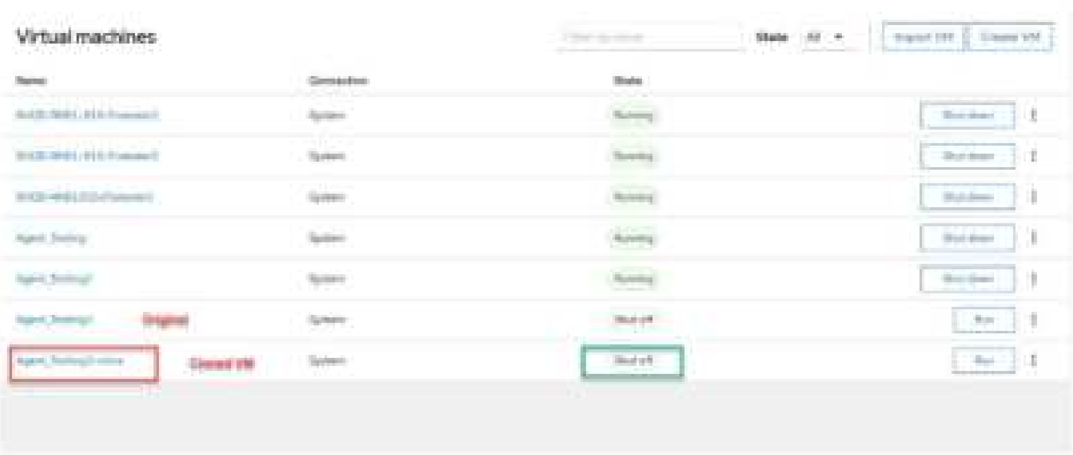


Figure 10: Administrative access button

8. Navigate to **System** > **Virtual Machines**.
9. View the cloned virtual machine in the virtual machines list.



Virtual machines

State All ▾ | Import VM | Create VM

Name	Connection	State		
[illegible]	System	Running	Shut down	⋮
[illegible]	System	Running	Shut down	⋮
[illegible]	System	Running	Shut down	⋮
Agent_Testing	System	Running	Shut down	⋮
[illegible]	System	Running	Shut down	⋮
[illegible] Original	System	Shut off	Run	⋮
[illegible] Cloned VM	System	Shut off	Run	⋮

Figure 11: Virtual machines list

Rolling back using the Virtual Machine Backup (clone)

About this task

If you experience a problem during an upgrade, you can roll back to a state using the cloned virtual machine.

Procedure

1. Log in to the KVM Cockpit web console as `custadm` in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

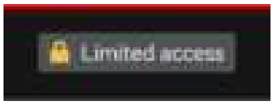
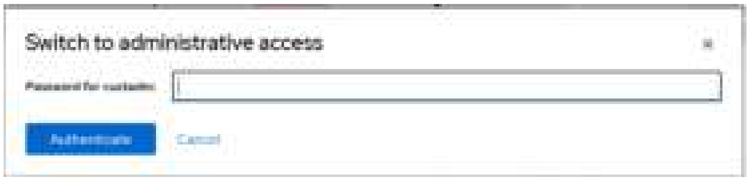


Figure 12: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.



Switch to administrative access

Password for custadm:

Figure 13: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

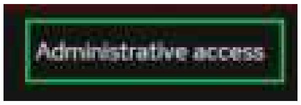


Figure 14: Administrative access button

4. Navigate to **System** > **Virtual Machines**.
5. Shut down the original virtual machine.
6. Rename the original virtual machine.

   For example: `Virtual_Machine_Broken`

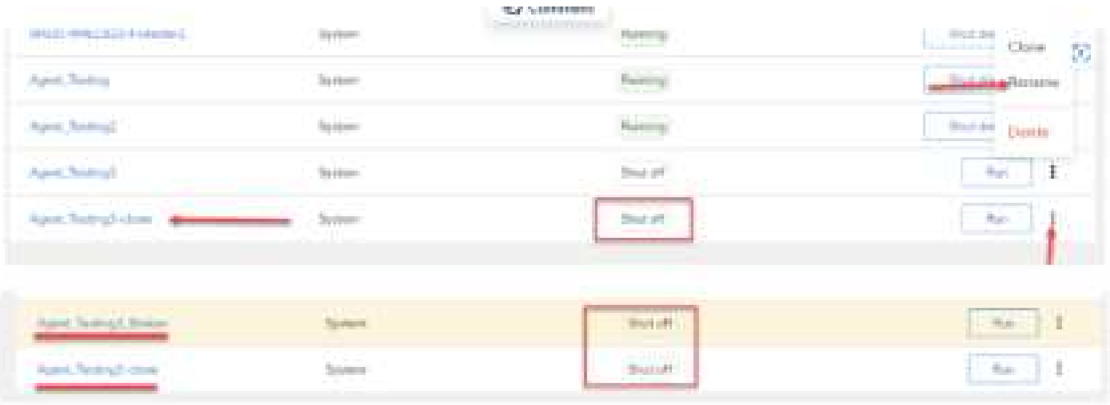


Figure 15: Roll back VM backup

7. While still in a power off state, edit the virtual machine clone Label to match the original virtual machine label. This ensures that the cloned virtual machine becomes the original virtual machine.

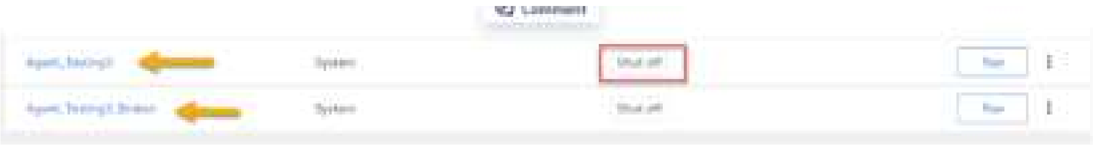


Figure 16: Edit Virtual Machine name

8. Configure the virtual machine that you renamed in step 5 to ensure the network interfaces and state match the broken virtual machine.

   For example: `bridge0 and state = up`

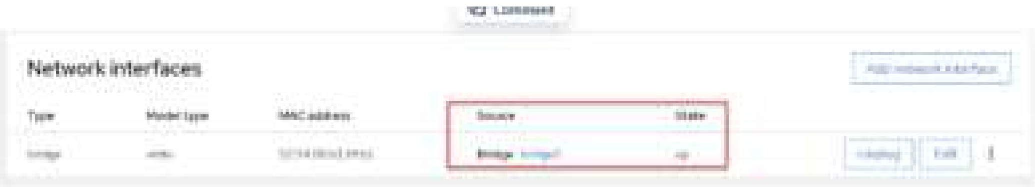


Figure 17: Network interfaces

9. Power on the virtual machine that you renamed in step 5.

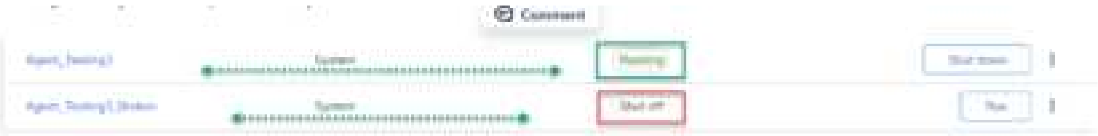


Figure 18: Power on

10. Delete any unused backups.

Appendix D: Security Service Pack

Avaya Aura® Security Service Packs overview

With Avaya Aura® Release 10.1.x, Avaya introduces a common version of Red Hat Enterprise Linux (RHEL) 8.4 to its Avaya Aura® platform. With the common versions of RHELs, Avaya has also changed how Security Service Packs (SSPs) are provided and installed. Currently, the following Avaya Aura® applications support this:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services

Note:

- From Release 10.1, Session Manager Release 10.1.0.1 Service Pack does not contain SSPs.
- Communication Manager Release 10.1 security updates (both Linux and Kernel) are now provided in an SSP. There is no longer a separate Kernel Service Pack (KSP).
- Application Enablement Services 10.1 Linux Security Updates (LSU) are now provided in an SSP. There is no longer an LSU.
- There is no separate System Manager SSP is released coincident with System Manager Release 10.1.0.1 (10.1.0.0 Service Pack 1). For System Manager 10.1, the SSP package is already embedded in 10.1.0.0 Service Pack 1 and is installed automatically along with Service Pack 1. For more information, see PCN2137S.

SSPs are cumulative for the release they apply to. The current SSP for a release includes the fixes from all previous SSPs for that release.

SSPs are applicable for Avaya Aura® Release 10.1.x running on:

- Avaya Solutions Platform 130 Release 5.0
- Avaya Solutions Platform S8300 Release 5.1 (For Communication Manager or Branch Session Manager)
- Customer-provided VMware® certified hardware

Note:

SSPs are not applicable for Software-Only deployments.

SSP file format and command

The format of the SSP file is the following:

```
AV-<product name><mainline release version>-RHEL<number>-SSP-<SSP #>-
<build #>.tar.bz2
```

Where:

- **<product name>:** This is the application name.

  For example:

Application	<product name>
Communication Manager	CM
System Manager	SMGR
Session Manager	SM
Application Enablement Services	AES

- **<Mainline release version>:** This is the mainline release version for the application. For example, 10.1
- **RHEL <number>:** RHEL version used in the Avaya Aura® application. For example, 8.4
- **SSP-<SSP #>:** This is a 3 digit number that defines the SSP version. For example, the first SSP # is 001.
- **<build #>:** The build number corresponds to the SSP version.

For example, `AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2`

You can use the **`av-update-os`** command to install SSP and **`av-version`** command to view the SSP version currently running on the application.

SSPs PCN Reference

- For more information about System Manager 10.1.x.x SSP, see PCN2138S.
- For more information about Session Manager 10.1.x.x SSP, see PCN2136S.
- For more information about Communication Manager 10.1.x.x SSP, see PCN2134S.
- For more information about Application Enablement Services 10.1.x.x SSP, see PCN2140S.

Adding a user to the avcommonos group

About this task

To install a Communication Manager SSP, the user must be a part of the **`avcommonos`** group. You can create one or more users to the **`avcommonos`** group.

Note:

You must add a comma to separate the groups.

Procedure

1. Log in to the Communication Manager System Management Interface (SMI) with the customer login.
2. Click **Server (Maintenance)** > **Security** > **Administrator Accounts.**
3. Select **Change Login** and select the user you want to modify.
4. Click **Submit**.
5. On the Administrator Accounts – Change Login page, select **Additional groups (profile)** and add the **`avcommonos`** group with a comma to separate it from the first group.
6. Click **Submit**.
7. After successful modification, click **Continue**.

Communication Manager SSP installation

You can install Communication Manager SSP using any one of the following:

- Solution Deployment Manager
- Communication Manager SMI
- Communication Manager CLI

Note:

To apply patch on the duplex server, first apply the patch on the standby server, interchange the server, and then apply patch on the new standby server.

Related links

Installing Communication Manager SSP using SDM on page 171
Installing Communication Manager SSP using SMI on page 173
Installing Communication Manager SSP using CLI on page 175

Installing Communication Manager SSP using SDM

About this task

From Communication Manager Release 10.1.3 onwards, you can install SSP using SDM.

Note:

Installation of SSP using SDM is only supported on Communication Manager Release 10.1.3.x and later.

Before you begin

- Deploy the Communication Manager Release 10.1.3.
- Take a full backup of the Communication Manager.
- Take a snapshot of the existing Communication Manager virtual machine.
- Add Communication Manager user service logins to the `avcommonos` group. For more information on how to add customer logins to the `avcommonos` group, see Adding a user to the avcommonos group on page 170.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select the Communication Manager application 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. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
9. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays ✓.

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

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

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

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

16. To see the installation status of the SSP, click **Upgrade Actions** > **Installed Patches**.
17. 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”.
18. To apply patch on the duplex server, do the following:
    a. On the active Communication Manager CLI, type `server -u` to lock the translations.
    b. On the standby Communication Manager server, repeat step 1 to step 17.
    c. On the active or standby Communication Manager CLI, type `server -i` to do interchange.
    d. On the new standby Communication Manager server, repeat step 1 to step 17.

    Note:

    If the upgrade is not successful and you want to unlock the translations, then on the active Communication Manager CLI, type `server -U`.

Related links

Communication Manager SSP installation on page 171

Installing Communication Manager SSP using SMI

About this task

From Communication Manager Release 10.1.3 onwards, you can install SSP using SMI.

Note:

Installation of SSP using SMI is only supported on Communication Manager Release 10.1.3.x and later.

Before you begin

- Deploy the Communication Manager Release 10.1.3.
- Take a full backup of the Communication Manager.
- Take a snapshot of the existing Communication Manager virtual machine.
- Add Communication Manager user service logins to the **avcommonos** group. For more information on how to add customer logins to the **avcommonos** group, see Adding a user to the avcommonos group on page 170.

Procedure

1. Log in to Communication Manager System Management Interface using a service account.
2. On the **Administration** menu, click **Server (Maintenance)**.

3. In the left navigation pane, click **Miscellaneous** > **Download Files**.

   The Communication Manager SMI displays the Download Files page.

4. Select the **File(s) to download from the machine I'm using to connect to the server** option, click **Choose File** to browse the file from your local machine, and click **Download**.
5. In the left navigation pane, click **Server Upgrades** > **Manage Updates**.
6. Select **Update ID** for SSP and click **Activate**.

   The Communication Manager SMI displays a warning that the active SSP will cause a server reboot.

7. In the `Do you want to continue?` prompt, click **Yes**.
8. Click continue and wait until the Communication Manager server reboots.

   ✱ **Note:**

   After you activate a higher version of the SSP patch, you cannot activate a lower version of the SSP patch.

   The SSP **Status** changes to **activated**. If you successfully activate a SSP, the SSP greys out and you cannot deactivate it. You can view the logs in the SSP Log History page.

9. To apply SSP on the duplex server, do the following on the Communication Manager SMI:
   a. On the active Communication Manager server, go to **Server Upgrades** > **Pre Update/ Upgrade Step**, and click **Continue**.
   b. On the standby Communication Manager server, repeat step 1 on page 173 to step 8 on page 174.
   c. On the standby Communication Manager server, go to **Server** > **Process Status** and ensure that all the services are up.
   d. On the active Communication Manager server, go to **Server** > **Interchange Servers**, and ensure that the **Standby Refreshed** status is **yes**.
   e. On the active Communication Manager server, go to **Server** > **Interchange Servers**, and click **Interchange**.
   f. On the new standby Communication Manager server, repeat step 1 on page 173 to step 8 on page 174.

   ✱ **Note:**

   If the upgrade is not successful, and you want to unlock the translations, then on the active Communication Manager server, go to **Server Upgrades** > **Pre Update/ Upgrade Step**, and click **Undo**.

Related links

Communication Manager SSP installation on page 171

Installing Communication Manager SSP using CLI

About this task

You can use the Communication Manager CLI to apply the Communication Manager SSP for simplex or duplex Communication Manager. The following users can install a Communication Manager SSP:

You can apply the Communication Manager SSP for simplex and duplex using the Communication Manager CLI. The following users can install a Communication Manager SSP:

- root
- services logins
- user, who is a part of the avcommonos group

Warning:

Ensure that you have a maintenance window, as SSP installation results in a reboot of the Communication Manager server.

Important:

After an SSP is activated, you cannot remove or deactivate it.

Before you begin

- Deploy the Communication Manager Release 10.1.3.
- Ensure that you have the PLDS access credentials and Company ID.
- Download the SSP from PLDS and copy it to `/var/home/ftp/pub` on Communication Manager.
- Take a full backup of Communication Manager.
- Take a snapshot of the existing Communication Manager virtual machine.
- Add the Communication Manager user service logins to the **`avcommonos`** group. For more information on how to add customer logins to the **`avcommonos`** group, see Adding a user to the avcommonos group on page 170.

Procedure

1. Log in to the Communication Manager CLI.
2. Go to the `/var/home/ftp/pub` directory.
3. Verify that the MD5sum matches with what is available in the PLDS Download ID description. For example,

   ```
   dadmin1@cm-cm101adupb> md5sum AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2
   023ea6ae26bea1e2017eb03df269e443  AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2
   ```

4. Run the following command:

   `av-update-os <SSP file name>`

5. To verify the SSP installation status or SSP installation is successful, do one of the following:
    - From the Communication Manager CLI, run the following command: **`av-version`**.

      Communication Manager displays the version number of the SSP installed.

      For example:

      ```
      OS_VERSION: Red Hat Enterprise Linux release 8.4
      AV_SSP_VERSION : 001
      AV_BUILD_NUMBER : 01
      ```
    - From the Communication Manager CLI, run the following command: **`swversion`**.
6. To apply a patch on the duplex server, do the following:
    a. Copy the SSP to the following location in active and standby servers: `/var/home/ftp/pub`.

    b. On the active Communication Manager CLI, enter the following commands to lock the translations.

    - **`save_trans`**
    - **`server -u`**

    c. On the standby Communication Manager, do the following:

    a. Enter **`update_show`** to view the details if any SSP is activated.

       If a previous SSP is already activated, the status of the previous SSP displays as activated under the **Status** column.

    b. To busy out the standby Communication Manager, type the following command: **`server -b`**

    c. To install the SSP, run the following command: **`av-update-os <SSP file name>`**

       SSP installation reboots the Communication Manager server.

    d. Enter **`statapp`** command to check if the services are up.

    e. To release the server from the busy out state, type the following command: **`server -r`**

    f. Type **`server`**, and ensure that the **Standby Refreshed** status is **yes**.

    g. Type **`server -i`** to interchange.

       The standby Communication Manager server becomes active, and the active Communication Manager server becomes standby.

    h. On the new active Communication Manager server, type **`server`**, and ensure that the **Standby Refreshed** status is **yes**.

d. On the new standby Communication Manager server, do the following:

   a. To busy out the standby Communication Manager, type the following command: **`server -b`**.

   b. To install the SSP, run the following command: **`av-update-os <SSP file name>`**

      SSP installation reboots the Communication Manager server.

   c. Enter **`statapp`** command to check if the services are up.

   d. To release the server from the busy out state, type the following command: **`server -r`**.

   e. Type **`server`**, and ensure that the **Standby Refreshed** status is **yes**.

   ✱ **Note:**

   If the upgrade is not successful and you want to unlock the translations, then on the active Communication Manager CLI, type `server -U`.

Related links

Communication Manager SSP installation on page 171

Glossary

Fully automated upgrade using Solution Deployment Manager

The fully automated upgrade process includes upgrading a product from earlier release to the latest release by using either Solution Deployment Manager Client or System Manager Solution Deployment Manager. In fully automated upgrade all subsequent steps are executed as a single process, including tasks such as backup, deploy, and post upgrade tasks such as applying patches or service packs.

For fully automated upgrade using Solution Deployment Manager, the system does not allow to change the IP Address of the application. Alternatively, you can use the Migration using CLI method.

To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.

Migration

The migration process includes changing the hypervisor or hardware while upgrading the application.

- **Migration using SDM:** Migration using Solution Deployment Manager is supported using same IP Address.

  For example, from AVP to VMware.

  To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.

  If you want to migrate using different IP Address for the application, use the CLI method.

- **Migration using SMI:** This is applicable only for Communication Manager. During migration, you need to perform backup and restore operations.

Update

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

Upgrade using CLI

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

Index