Upgrading Avaya Aura® System Manager

Release 10.2.x
Issue 1
December 2023

© 2019-2023, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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.

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, 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

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

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 to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x on:

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

  Amazon Web Services (AWS), Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS) in Software-only environment.

This document:

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

The primary audience for this document is anyone who upgrades, configures, and verifies System 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

Chapter 2: Upgrade overview and considerations

Upgrade overview

The document provides the procedures for upgrading Avaya Aura® System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to System Manager Release 10.2.x.

Note:

- Before upgrading System Manager to Release 10.2, Avaya recommends that the older System Manager Release version must be on the latest version of its releases. The latest version for Release 7.1.x, 8.0.x, and 8.1.x are Release 7.1.3.8, 8.0.1.2, and 8.1.3.8 respectively.
- For upgrading System Manager from Release 7.0.x to Release 10.2 and later, first upgrade System Manager Release 7.0.x to 10.1.x, and then upgrade to Release 10.2 and later. You cannot directly upgrade the Release 7.0.x system to Release 10.2 and later. If you upgrade the application directly from Release 7.0.x to Release 10.2 and later, the upgrade might fail.
- For upgrading System Manager from Release 6.x to Release 10.1 and later, first upgrade System Manager Release 6.x to 8.1.x, and then upgrade to Release 10.1 and later. You cannot directly upgrade the Release 6.x system to Release 10.1 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1 and later, the upgrade fails.
- If you upgrade System Manager from an older release like 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x, and the goal is to apply the latest Feature Pack or Service pack of 10.2.x, then you can install the latest service pack or feature pack of System Manager Release 10.2.x as part of the migration process. You do not have to install the 10.2 GA patch as an intermediate step.

  For example, if you upgrade System Manager from Release 10.1.x to Release 10.2.x, then you can directly apply the Release 10.2.x patch as part of data migration. You do not need to apply the 10.2 GA patch (`System_Manager_10.2.0.0_GA_Patch_rxxxxxxxxx.bin`) in the intermediate step.

When upgrading to System Manager Release 10.2.x on VMware, the VMware ESXi version must be 7.0 or 8.0.

Note:

- From Release 10.1 and later, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0) Release 5.1.
- From Release 10.1 and later, Avaya Aura® applications will no longer have the Amazon Web Services (AWS) and Kernel-based Virtual Machine (KVM) OVAs. Alternately, you can continue to deploy the application by using the software-only offer. For more information, see the product-specific Software-only and Infrastructure As a Service Environments deployment guide.

Use the Solution Deployment Manager client Release 10.2.x to upgrade System Manager to Release 10.2.x from the following:

- - System Manager Release 7.1.3.x, 8.0.x, or 8.1.x running on Appliance Virtualization Platform on Avaya-provided server to latest version of System Manager on Avaya Solutions Platform 130 (Avaya supplied ESXi 7.0) or on VMware in customer-provided Virtualized Environment.
  - System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x running on VMware in customer-provided Virtualized Environment to latest version of System Manager on Avaya Solutions Platform 130 (Avaya supplied ESXi 7.0) or on VMware in customer-provided Virtualized Environment.
  - System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x running on VMware in customer-provided Virtualized Environment or System Manager Release 7.1.3.x, 8.0.x, or 8.1.x running on Appliance Virtualization Platform to latest version of System Manager in Software-only environment.

Data migration utility

Use the data migration utility to migrate the backup data of System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to the latest release of System Manager.

Use the data migration utility process to upgrade across multiple releases or major versions within release. For example, upgrades from:

- Release 7.1.3.x to Release 10.2.x
- Release 8.0.x to Release 10.2.x
- Release 8.1.x to Release 10.2.x
- Release 10.1.x to Release 10.2.x

In the data migration utility method, the system does not support the rollback operation.

To revert to the previous release:

- If you have the old virtual machine, power off and delete the new virtual machine, and then power on the old virtual machine.
- If you deleted the old virtual machine, power off and delete the new virtual machine, and then perform the cold standby procedure.

  For information about the cold standby procedure, see “Changing over to Cold Standby server”.

Supported upgrade paths for System Manager

Important:

- Before starting the application upgrade, upgrade the platform and hypervisor.
- To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.
- Upgrade or migration using Solution Deployment Manager is only supported with the same IP Address of the application in a Software-only environment.

  Software-only upgrade is supported for VMware, KVM, RHVH, Hyper-V, AWS, GoogleCloud, and Azure.
- If the application supports the upgrade using Solution Deployment Manager, you can also use the CLI for upgrading that application.
- To upgrade the application from Release 6.x to Release 10.x, upgrade the application from 6.x to 8.1.x, and then upgrade to Release 10.x. You cannot directly upgrade the Release 6.x system to Release 10.1 and later.
- To upgrade the application from Release 7.0.x to Release 10.2.x, upgrade the application from 7.0.x to 10.1.x, and then upgrade to Release 10.2. You cannot directly upgrade the Release 7.0.x system to Release 10.2 and later.

For information about terms used in this table, see “Glossary”.

The following table displays all the upgrade paths from earlier releases to Release 10.2.

From offer	From Release	To Software-only (VMware, KVM, RHVH, OpenStack, Hyper-V, AWS, GoogleCloud, or Azure) 10.2 (ISO)	To ASP 130 (OVA)/VMware 10.2 (OVA)
AVP	7.1.3.x	Migration using CLI	Migration using CLI
	8.0.x	Migration using CLI	Migration using CLI
	8.1.x	Migration using SDM	Fully automated upgrade using SDM

Table continues…

From offer	From Release	To Software-only (VMware, KVM, RHVH, OpenStack, Hyper-V, AWS, GoogleCloud, or Azure) 10.2 (ISO)	To ASP 130 (OVA)/VMware 10.2 (OVA)
VMware	7.1.3.x	Migration using CLI	Migration using CLI
	8.0.x	Migration using CLI	Migration using CLI
	8.1.x	Migration using SDM	Fully automated upgrade using SDM
	10.1.x	Migration using SDM	Fully automated upgrade using SDM
Software-only	8.0.x	Migration using CLI	NA
	8.1.x	Migration using SDM	NA
	10.1.x	Migration using SDM	NA
KVM/OpenStack/RHVH (OVA)	7.1.3.x	Migration using CLI	Migration using CLI
	8.0.x	Migration using CLI	Migration using CLI
	8.1.x	Migration using CLI	Migration using CLI
AWS (OVA)	7.1.3.x	Migration using CLI	Migration using CLI
	8.0.x	Migration using CLI	Migration using CLI
	8.1.x	Migration using CLI	Migration using CLI

The following upgrade paths are currently supported:

System Manager running this version	Upgrade to this version
7.1.3.x	10.2
8.0.x	10.2
8.1.x	10.2
10.1.x	10.2 and later

Chapter 3: Planning and preconfiguration

Prerequisites for upgrading System Manager

General prerequisites

- Download the required System Manager OVA, patch files, and data migration utility from the Avaya Support website at http://support.avaya.com/.

  For information about software details, see “Software details of System Manager”.
- Calculate the MD5sum of the downloaded files and ensure that it has the same value as given on the Avaya PLDS website.
- Keep the following information handy to create a backup on the remote server:
  - IP address
  - Directory
  - User Name
  - Password
- Record the number of users and custom roles in the current release of System Manager.

  After the upgrade, you require this data to verify if System Manager has successfully imported the users and custom roles from the earlier release to the latest release of System Manager.

  For more information about managing users and custom roles, see *Administering Avaya Aura® System Manager*.
- During the System Manager upgrade, Session Manager performance data (perfdata) is not preserved. If performance data is required after the System Manager upgrade, backup the performance data on the NFS remote server.

  For information about the performance data storage using NFS remote server, see *Administering Avaya Aura® Session Manager*.

System prerequisites

- Verify that the existing server is compatible with System Manager Release 10.2.x. If the existing server is incompatible, change the server.

  For information, see Supported servers on page 16.
- Verify that the ESXi version is compatible with System Manager Release 10.2.x. If the existing ESXi version is incompatible, upgrade to the supported ESXi version.

  For information, see Supported ESXi version on page 18.

Geographically redundant System Manager prerequisites

- You can update the primary and secondary System Manager servers in any order. However, you should not simultaneously update the primary and secondary System Manager servers.

  At a time, install the patch on one server.

- Activate the secondary System Manager server only after installing the patch.

  To activate the secondary System Manager server, the primary and secondary System Manager servers must be on the same release and patch version.

- Take the snapshot only after disabling the Geographic Redundancy replication.

License preservation and license regeneration

- If you perform VMware OVA to VMware OVA upgrade of System Manager by using Solution Deployment Manager Client, the system retains the licenses. However, you must backup or export the licenses from the older System Manager server.

  If you are upgrading other applications by using System Manager Solution Deployment Manager, then Solution Deployment Manager retains the license file. However, if you are upgrading the application to a major release, install the new license file for those applications after the upgrade.

  For example, if you are upgrading System Manager and other applications to Release 10.1, Solution Deployment Manager retains the license file, but these license will not be valid. Therefore, install the new license file.

- If you use the CLI procedure to upgrade System Manager to Release 10.2.x, the system does not retain the System Manager WebLM licenses that are installed on the old System Manager server. This will impact each product that is using the licenses from System Manager WebLM. During or after the upgrade, those product might go in the license grace period mode or license error mode. To remediate this, after the upgrade, regenerate the licenses by using the new host ID. Ensure that all your Avaya License Activation Codes (LACs) for your system are available that is under contract with ‘Upgrade Advantage’ entitlement. Also, check that your account at Avaya PLDS website https://plds.avaya.com/ is functional to regenerate the license keys.

  Ensure to backup or export the System Manager license keys from the older System Manager server.

Upgrade worksheet

Use the following worksheet to record the data that you will need during the upgrade.

#	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of System Manager Web Console, enter the IP address of the remote server on which you saved the backup file.
2	**User Name and Password of the remote server**		To gain access to the backup file that is located on a remote server, enter the user name and the password for the account on the System Manager web console.
3	**System Manager command line interface credential**		Open an SSH session and login with the user who has administrator privileges.
4	**Path and the file name of the backup file on the remote server**		Enter the path and the file name of the backup file.
5	Check the server time and time zone before running the Data Migration utility tool to upgrade System Manager.		This step ensures that the time is properly synced with kernel and OS RPMs and prevents upgrade failure.

Supported servers

The following servers are supported for deployments and upgrades to Release 10.2.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	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y

Table continues…

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.x	Y Avaya Solutions Platform 130 Release 5.1
Avaya Solutions Platform S8300 Release 5.1 [4]	N	N	N	Y	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:

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. Avaya Solutions Platform future release

(Release 6.x) will support ESXi 8.0. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. Updating directly from Dell or VMware's website results in an unsupported configuration.

- 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 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 5.1.
- 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.

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 7.0 or 8.0
  - VMware® vCenter Server 7.0 or 8.0

  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 10.2 and later does not support vSphere ESXi 6.7.
- 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				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

Note:

- Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2.

  Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-801-release-notes/index.html.

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

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. Avaya Solutions Platform future release (Release 6.x) will support ESXi 8.0. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. Updating directly from Dell or VMware's website results in an unsupported configuration.
- 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 7.0 can be VMware ESXi 7.0 Update 3.
- Presence Services is deployed on the Avaya Breeze® platform, which supports VMware 7.0 and 8.0.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

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

Note:

If you are using ASP130/S8300 5.0 or earlier, then you *must* first upgrade to ASP130/S8300 5.1 before upgrading to Avaya Aura® Release 10.2.x

If the ESXi upgrade is required for upgrading the Avaya Aura® application to Release 10.2.x, you *must* upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 18.

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)

   Avaya recommends that you first upgrade the Endpoints. However, the older versions of Endpoints are supported with the latest versions of Avaya components in this list of upgrade sequence.

   Make sure that you visit the product compatibility matrix before you skip upgrading Endpoints.

   For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

2. Standalone Avaya WebLM.

   Note:

   With Release 10.2, there is no WebLM Release 10.2. To upgrade, use the latest WebLM Release 10.1.3.x. If you are upgrading Communication Manager or Application Enablement Services to 10.2 and have a standalone WebLM in the setup, upgrade the standalone WebLM to Release 10.1.3.1 or later otherwise the licensing for Communication Manager and Application Enablement Services might break.

3. SAL Gateway

Avaya recommends that you upgrade SAL in the same sequence. However, the older versions of SAL is also supported with the latest versions of Avaya components in this list of upgrade sequence.

Make sure that you visit the product compatibility matrix before you skip upgrading SAL.

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

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.

5. Avaya Aura® Session Manager (Core Session Managers only)
6. Avaya Breeze® platform and other Snap-ins
7. Avaya Call Management System
8. Avaya Experience Portal
9. Avaya Oceana®
10. Avaya Aura® Device Services
11. G4XX Media gateways or Avaya Aura® Media Server

    Note:

    The gateways require load 38.21.2 or newer to successfully upgrade to 43.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).

12. Avaya Aura® Branch Session Manager
13. Avaya Aura® Communication Manager Survivable Remote Servers (formerly known as Local Survivable Processors)
14. Avaya Aura® Application Enablement Services

    Avaya recommends that you upgrade AES in the same sequence. However, the older versions of AES is also supported with the latest versions of Avaya components in this list of upgrade sequence.

    Make sure that you visit the product compatibility matrix before you skip upgrading AES.

    For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

15. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
16. Avaya Aura® Communication Manager Survivable Core Servers (formerly known as Enterprise Survivable Processors)
17. Avaya Aura® Communication Manager feature servers and evolution servers

In duplex configuration, update the:

- Standby Communication Manager server
- Active Communication Manager server

18. Avaya IP Office™ platform
19. Avaya Aura® Messaging or IX Messaging (formerly known as Avaya Messaging)
20. Avaya Aura® Web Gateway
21. Workplace Clients

    Avaya recommends that you upgrade Workplace Clients in the same sequence. However, the older versions of Workplace Clients is also supported with the latest versions of Avaya components in this list of upgrade sequence.

    Make sure that you visit the product compatibility matrix before you skip upgrading Workplace Clients.

    For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

    Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.

22. Avaya Session Border Controller for Enterprise (ASBCE)

    Avaya recommends that you upgrade ASBCE in the same sequence. However, the latest versions of ASBCE are also supported with the older versions of Avaya components in this list of upgrade sequence.

    Make sure that you visit the product compatibility matrix before you upgrade ASBCE.

    For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

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 10.2 before you upgrade Communication Manager to 10.2.

  All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.
- 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 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2. Solution Deployment Manager Client cannot be on Release 10.1 or Release 8.1.

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

Software details of System Manager

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

Customer configuration data for System Manager

The following table identifies the key customer configuration information that you must provide throughout the deployment and configuration process:

Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation.

Important:

Password must be 8 to 256 alphanumeric characters and without white spaces.

Required data	Description	Example Value for the system	✔
IP address	Management (Out of Band Management) and Public network configuration Configure Public network details only when Out of Band Management is enabled. If Out of Band Management is not enabled, Public network configuration is optional.	172.16.1.10	
Netmask		255.255.0.0	
Gateway		172.16.1.1	
DNS Server IP address		172.16.1.2	
Short hostname		myhost. The host name must be a valid short name. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.	
Domain name		mydomain.com	
Default search list		mydomain.com	
NTP server		172.16.1.100	
Time zone		America/Denver	
VFQDN short hostname	VFQDN	grsmgr	
VFQDN domain name		dev.com	
User Name Prefix	SNMP Parameters	org	
Authentication Protocol Password		orgpassword	

Table continues…

Required data	Description	Example Value for the system	✔
Privacy Protocol Password		orgpassword	
Backup Definition parameters	See Backup Definition Parameters	-	
EASG status	EASG	Enable or Disable	
Data Encryption	Data Encryption	Enable or Disable	

Supported footprints of System Manager on VMware

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

Note:

- Avaya Aura® System Manager supports VMware hosts with Hyper-threading 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.

Resource	Profile 2	Profile 3	Profile 4
vCPU Reserved	6	8	18
Minimum vCPU Speed	2185 MHz	2185 MHz	2185 MHz
CPU reservation	13110 MHz	17480 MHz	39330 MHz
Virtual RAM	12 GB	18 GB	36 GB
Memory reservation	12288 MB	18432 MB	36864 MB
Virtual Hard Disk	170 GB	270 GB	850 GB
Shared NICs	1	1	1
IOPS	44	44	44

Note:

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Supported footprints of System Manager *Software-Only ISO image* for on-premise

These footprint values are applicable for Software-Only deployments on VMware, Hyper-V, and KVM.

Note:

Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.

Footprint	CPUs (GHz)	Number of vCPUs	CPU reservation	RAM (GB)	Memory reservation	HDD (GB)	NICs
Profile 2	2.29	6	13740	12	12288	170	1
Profile 3	2.29	8	18320	18	18432	270	1
Profile 4	2.29	18	39600	36	39600	850	1

Supported footprints of System Manager on AWS

Note:

Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.

Footprint	Profile 2	Profile 3	Profile 4
Instance type	m4.2xlarge or higher, m5.2xlarge, m5a.2xlarge, c5a.2xlarge, or c5.2xlarge	m4.2xlarge or higher, m5.2xlarge, m5a.2xlarge, c5a.4xlarge, or c5.2xlarge	m4.10xlarge or higher, m5.8xlarge, m5a.8xlarge, c5.9xlarge, or c5a.8xlarge
HDD (GB)	170	270	850
NICs	1	1	1

Supported footprints of System Manager ISO on Google Cloud Platform

Note:

Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.

Footprint	Profile 2	Profile 3	Profile 4
vCPU	6	8	18
RAM (GB)	12	18	36
HDD (GB)	170	270	850
NICs	1	1	1

Supported footprints of System Manager ISO on Microsoft Azure

Note:

Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.

Footprint	Profile 2	Profile 3	Profile 4
Instance type	Standard_D8s_v3	Standard_D8s_v3	Standard_D32s_v3
HDD (GB)	170	270	850
NICs	1	1	1

Supported number of users on System Manager

The following System Manager resource requirements are based on the profile and are applicable for System Manager deployed on Customer-provided VMware, Avaya-supplied Avaya Solutions Platform 130, or Software-only environment.

Footprint	Max number of users	Max number of Branch Session Managers	Max number of Session Managers	Max number of Breeze	Max number of IP Office Branches
Profile 2	35,000 to 250,000	250	12	12	500
Profile 3	250,000	500	28	28	2000
Profile 4	300,000	5000	28	28	3500

System capacities for applications

For information about the system capacities, such as, number of users, gateways, and endpoints, see the product specific documentation on the Avaya Support website at http://support.avaya.com.

Chapter 4: Preupgrade tasks

Installing the Solution Deployment Manager client on your computer

About this task

When the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

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

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

Solution Deployment Manager must be used to deploy or upgrade Avaya Aura® applications on Avaya Aura® Appliance Virtualization Platform.

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at https://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Product Support** > **Downloads**, and type the product name as **System Manager**, and Release as **10.2.x**.
3. Click the **Avaya Aura® System Manager Release 10.2.x SDM Client Downloads,10.2.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.

7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

     If the `C:\Program Files\Avaya\AvayaSDMClient` directory is not empty, the installer displays the following message: `To install the SDM client, select an empty directory or manually delete the files from the installation directory.`

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

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

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

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

      You can save the artifacts in the specified directory.
   c. In **Data Port No**, select the appropriate data port.

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

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

      Note:

      After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
   e. **(Optional)** Click **Reset All to Default** to reset all values to default.
10. Click **Next**.
11. On the Summary and Validation page, verify the product information and the system requirements.

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

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

    After the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.
14. To start the client, click the Solution Deployment Manager client icon, .

Next steps

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

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

Accessing the Solution Deployment Manager client dashboard

About this task

Note:

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

Procedure

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

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

Accessing Solution Deployment Manager

About this task

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

Procedure

Perform one of the following:

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

  Note:

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

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

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

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.

Verifying the current software version

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the settings icon (), and then click **About**.

   The system displays the pop up window with the build details.
3. Verify the version number of System Manager with the highest build number for the release.

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. On the System Manager Web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. Click **Now**.

If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Creating the System Manager virtual machine snapshot

About this task

You can create the snapshot of the System Manager virtual machine by using vSphere Web Client.

Important:

- Do not perform any activity on System Manager until the snapshot is created.
- When you are upgrading VMware-based System Manager, remove all the snapshots from the older system before the upgrade. Otherwise, the rollback operation will fail.

Before you begin

In the Geographic Redundancy setup, do the following:

1. Disable the Geographic Redundancy replication on the primary System Manager server.
2. Shut down the System Manager server.

Procedure

1. From the list of virtual machines, right-click the required System Manager virtual machine, and click **Snapshot**.
2. On the **Take Virtual Machine Snapshot** dialog box, do the following:
   a. In the **Name** and **Description** fields, type a name and the description for the snapshot.
   b. Ensure that the following check boxes are cleared:
      - **Snapshot the virtual machine's memory**
      - **Quiesce guest file system (Needs VMware Tools installed)**
3. Click **OK**.
4. In the Recent Tasks window, do the following:
   a. Verify **Status** of the **Create virtual machine snapshot** task.
   b. Wait until the system displays `Completed`.

Creating a prestaging job

Creating a prestaging job for upgrade

About this task

Use this procedure to create the prestaging job to upload and store the service or feature pack and datamigration bin file on the datastore of the host that you can use while upgrading System Manager.

Note:

For upgrade, the files are also stored on the old System Manager system.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Click **New**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click **Upgrade**.
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.
8. In the Location and Platform Details section, do the following:
   a. In **Select Location**, click the location of the host.
   b. In **Select Platform**, click the platform name.

      When you select the platform name, Solution Deployment Manager fetches the host details and populates the data store configured on the host in **Datastore**.
   c. In **Virtual Machine**, click the System Manager virtual machine.

      The **Virtual Machine** field is applicable only when you select the **Upgrade** prestage operation type.

      Ensure that you selected the platform on which the System Manager virtual machine is residing.
   d. In **Select Prestage Folder**, click **Browse**.

      Solution Deployment Manager displays the DataStore Explorer window.

9. In the DataStore Explorer window, do one of the following:
   - To select the prestage folder location, navigate to the required folder, and click **Submit**.

     While selecting a folder on the VMware datastore ensure that the folder is empty.
   - To create a new prestaging folder location, click **New**.

     While creating a new folder, do not select any folder that has virtual machine files in it.

     a. In Folder Select, in **Enter Folder Name**, type the folder name, click **OK**.

     b. Click **Submit**.

        Solution Deployment Manager displays the Status pop-up message with the path of the prestage folder.

     c. Click **OK**.
10. Click **Next**.
11. To upload and store the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack file.
    - **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

      To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
12. To upload and store the data migration bin file, click the **Datamigration bin** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager data migration bin file.
    - **SW Library**, in the **File Name** field, select the System Manager data migration bin file.

      To use the **SW Library** option, the System Manager data migration bin file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
13. Click **Submit**.

    Solution Deployment Manager creates the prestaging job on the Pre-Staging page.

Related links

Upgrading System Manager from Release 8.1.x or 10.1.x to Release 10.2.x by using the Pre-staging feature of Solution Deployment Manager Client on page 73

Creating a prestaging job for update

About this task

Use this procedure to create the prestaging job to upload and store the OVA, service or feature pack and datamigration bin files on the datastore of the host that you can use while updating System Manager.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Pre-staging**.

   System Manager displays the Pre-Staging page.
4. Click **New**.

   Solution Deployment Manager displays the Application Pre-Stage window.
5. In Select Pre-Stage Operation Type, click **Update**.
6. Click **Next**.
7. In the Job Details section, do the following:
   a. In **Name**, type the name of the prestaging job.
   b. In **Description**, type the description of the prestaging job.
8. In the Location and Platform Details section, do the following:
   a. In **Select Location**, click the location of the host.
   b. In **Select Platform**, click the platform name.

      When you select the platform name, Solution Deployment Manager fetches the host details and populates the data store configured on the host in **Datastore**.
   c. In **Select Prestage Folder**, click **Browse**.

      Solution Deployment Manager displays the DataStore Explorer window.
9. In the DataStore Explorer window, do one of the following:
   - To select the prestage folder location, navigate to the required folder, and click **Submit**.

     While selecting a folder on the VMware datastore ensure that the folder is empty.
   - To create a new prestaging folder location, click **New**.

     While creating a new folder, do not select any folder that has virtual machine files in it.
     a. In Folder Select, in **Enter Folder Name**, type the folder name, click **OK**.
     b. Click **Submit**.

Solution Deployment Manager displays the Status pop-up message with the path of the prestage folder.

c. Click **OK**.

10. Click **Next**.
11. On the **OVA** tab, click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager OVA file.
    - **SW Library**, in the **File Name** field, select the System Manager OVA file.

      To use the **SW Library** option, the System Manager OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
12. To upload and store the latest service or feature pack, select the **Service or Feature Pack** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager service or feature pack file.
    - **SW Library**, in the **File Name** field, select the System Manager service or feature pack file.

      To use the **SW Library** option, the System Manager service or feature pack file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
13. To upload and store the data migration bin file, click the **Datamigration bin** tab, and click one of the following:
    - **Local Path**, in the **URL** field, type the absolute path of the System Manager data migration bin file.
    - **SW Library**, in the **File Name** field, select the System Manager data migration bin file.

      To use the **SW Library** option, the System Manager data migration bin file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation.
14. Click **Submit**.

    Solution Deployment Manager creates the prestaging job on the Pre-Staging page.

Related links

Installing service packs and software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client on page 87

Application Pre-Stage field descriptions

Select Pre-Stage Operation Type

Name	Description
Select Pre-Stage Operation	You can create the pre-staging job for deploying, upgrading, or updating System Manager. The options are: • **Deployment** • **Upgrade** • **Update**

Prestage Details: Job Details

Name	Description
Name	The pre-staging job name.
Description	The pre-staging job description.

Prestage Details: Parent Folder Details

When you select the **Advanced** > **Local Pre-staging** option, Solution Deployment Manager displays this section.

Name	Description
Local Pre-stage Parent Folder	The path of the local prestage parent folder. The default path for the local pre-stage folder is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

Prestage Details: Location and Platform Details

When you select the **Advanced** > **Local Pre-staging** option, Solution Deployment Manager does not display this section.

Name	Description
Select Location	The location name.
Select Platform	The platform name that you must select.
Virtual Machine	The virtual machine name. **Note:** The **Virtual Machine** field is available only when you select the **Upgrade** prestage operation type.
Datastore	The data store of the platform. The page populates the capacity details in the Capacity Details section.

Table continues…

Name	Description
Select Prestage Folder	You can click the **Browse** button to display the DataStore Explorer window and to select the pre-staging folder. When you click **New**, you can create a new prestaging folder.
New	Displays the Folder Select dialog box.
Enter Folder Name	Specifies the prestaging folder name.
Submit	Saves the prestaging folder path and displays next to the **Select Prestage Folder** field.

Select Artifacts

Based on the selected Select Pre-Stage Operation Type option, Solution Deployment Manager displays one or more of the following tabs. You can specify either the local path or the Software library path for the System Manager OVA, service pack, or data migration file.

- **OVA**

  Solution Deployment Manager enables the **OVA** tab when you select the **Deployment** or **Upgrade** prestage operation type.

- **Service or Feature Pack**

  Solution Deployment Manager enables the **Service or Feature Pack** tab when you select the **Deployment**, **Upgrade**, or **Update** prestage operation type.

- **Datamigration bin**

  Solution Deployment Manager enables the **Datamigration bin** tab when you select the **Upgrade** prestage operation type.

Name	Description
Local Path	The option to specify the absolute path from where you can get the System Manager OVA, service pack, or data migration bin file.
URL	Specify the absolute path from where you can get the System Manager OVA, service pack, or data migration bin file.
SW Library	The option to specify the absolute path of the software library from where you can get the System Manager OVA, service pack, or data migration bin file. You can save the files in the `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts` folder.
File Name	The option to select the System Manager OVA, service pack, or data migration bin file.

Button	Description
Submit	Saves the prestaging job.

Upgrading VMware ESXi version

About this task

If the ESXi upgrade is required for upgrading System Manager to Release 10.1, use the following procedure to upgrade ESXi to supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 18.

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 System Manager virtual machine and other virtual machines.
7. Install Solution Deployment Manager Client Release 10.1.
8. Launch Solution Deployment Manager Client and perform the following:
   a. Add the ESXi host.

      For information, see Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host on page 45.
   b. Establish trust with the System Manager virtual machine.

      For information, see Re-establishing trust for Solution Deployment Manager elements on page 54.
   c. Upgrade System Manager to Release 10.1.

      For information, see Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client on page 69.

Virtual machine management

Application management

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

- Defines the physical location of the **OS**, Appliance Virtualization Platform, Avaya Solutions Platform 130, or the ESXi platforms.
- Supports password change and patch installation of the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform Release 8.x or earlier and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

  Note:

  For the Avaya Aura® Messaging element, trust re-establishment is not required.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

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

Managing the location

Viewing a location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. Click the Locations tab.

   The Locations section lists all locations.

Adding a location

About this task

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

Procedure

1. On the desktop, click the SDM icon (), and then click **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

New and Edit location field descriptions on page 44

Editing the location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 44

Deleting a location

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. In the Delete confirmation dialog box, click **Yes**.

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

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

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

Managing the platform

Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

About this task

Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or Avaya Solutions Platform 130 Release 5.0 host. You can associate an ESXi host with an existing location.

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

Note:

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

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

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

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

You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to VMware ESXi host.

Note:

- To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA before you add the host to the SDM inventory.
- To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP Address of the ESXi host. Otherwise, Solution Deployment Manager does not support adding the ESXi host in Solution Deployment Manager.
- To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the IP address to add an Avaya Solutions Platform host.

Before you begin

Add a location.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a 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 such as the platform name, platform FQDN or IP address, username, and password.

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

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

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

   In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

Next steps

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

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**.

     On the desktop, click the SDM icon (), and then click **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.

Next steps

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.

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 10.2.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 desktop, click the SDM icon (), and then click **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.

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 desktop, click the SDM icon (), and then click **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.

Related links

Creating a data backup on a remote server on page 33
Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI on page 96
Restoring a backup from a remote server on page 133

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 desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.

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

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

Removing a platform

Procedure

1. On the desktop, click the SDM icon (), and then click **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**.

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. If you connect the Solution Deployment Manager client to Appliance Virtualization Platform through the services port, the platform IP address must be 192.168.13.6.
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.

Table continues…

Name	Description
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.

Downloading the OVA file to System Manager

About this task

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

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
   a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. Click **Download**.

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

8. Provide a valid file type.

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

   Note:

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

Managing the application

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 desktop, click the SDM icon (), and then click **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 ().
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.
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.

Managing vCenter

Creating a role for a user

About this task

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

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

Procedure

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

   The system displays the Create Role dialog box.

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

        Note:

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

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

        Note:

        You must select all the subprivileges under **Configuration**.
6. Click **OK** to save the privileges.

Next steps

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

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. 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 desktop, click the SDM icon (), and then click **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

Editing vCenter on page 59
Map vCenter field descriptions on page 59
New vCenter and Edit vCenter field descriptions on page 60

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

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

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

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the desktop, click the SDM icon (), and then click **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

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

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.

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.
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.

Table continues…

Name	Description
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.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 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.

Chapter 5: Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.0

Migrating Appliance Virtualization Platform deployed on Common Server 1, 2, or 3 with System 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 Common Server 1, 2, or 3 to Avaya Solutions Platform 130 Release 5.0 with System 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 System Manager and keep it on remote servers.

   For information about creating a backup on a remote server, see “Creating a data backup on a remote server”.

2. To do the graceful shutdown of the application, log in to the host UI by accessing the ESXi host, 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.

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 130 Release 5.0.

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

5. Deploy System Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.0.

   For information, see *Deploying Avaya Aura® System Manager in Virtualized Environment*

6. Run the **upgradeSMGR** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

   For information about running the data migration utility, see “Upgrading to System Manager Release 10.1 from CLI”.

7. After the upgrade and patch installation is successful, remove the patch bin file, backup file, data migration utility, log off from the system, and remove the snapshot.

Related links

Creating a data backup on a remote server on page 33
Shutting down Appliance Virtualization Platform host from CLI on page 49
Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI on page 96
Restoring a backup from a remote server on page 133

Migrating Appliance Virtualization Platform deployed on Avaya Solutions Platform 120 with System 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 System 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 System Manager and keep it on remote servers.

   For information about creating a backup on a remote server, see “Creating a data backup on a remote server”.

2. To do the graceful shutdown of the application, log in to the host UI by accessing the ESXi host, 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.

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 System Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.0.

   For information, see *Deploying Avaya Aura® System Manager in Virtualized Environment*

6. Run the **`upgradeSMGR`** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

   For information about running the data migration utility, see “Upgrading to System Manager Release 10.1 from CLI”.

7. After the upgrade and patch installation is successful, remove the patch bin file, backup file, data migration utility, log off from the system, and remove the snapshot.

Related links

Creating a data backup on a remote server on page 33
Shutting down Appliance Virtualization Platform host from CLI on page 49
Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI on page 96
Restoring a backup from a remote server on page 133

Chapter 6: Upgrading from System Manager Release 8.1.x or 10.1.x to Release 10.2.x on Avaya Solutions Platform 130 or VMware

Prerequisites

Following are the prerequisites for upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x.

- To upgrade a virtual machine, the host or the vCenter must have a valid certificate. The **SAN** field must contain the IP/FQDN of the host or the vCenter. If the **SAN** field is not available, then the **CN** field must contain the IP/FQDN of the host or the vCenter. You must ensure that the certificate is not expired.
- Ensure that ESXi is running on Release 7.0 and later.
- You must have additional 10 GB of space on the host to take snapshot of virtual machine.
- You must have additional 15 GB of space on the host where Solution Deployment Manager client is installed.
- System Manager must be in the `Running` state. Ensure that System Manager web console is accessible. You can confirm this by logging on to the System Manager web console.
- If System Manager is deployed from the same Solution Deployment Manager client, **Current Action Status** must be `Successful`.

Checklist for upgrading System Manager Release 8.1.x or 10.1.x in the Geographic Redundancy setup to Release 10.2.x

Use the following checklist for upgrading System Manager Release 8.1.x or 10.1.x in the Geographic Redundancy setup to System Manager Release 10.2.x.

No.	Task	Link/Notes	✔
1	Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at http://support.avaya.com.	
2	Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at http://support.avaya.com.	-	
3	Verify the software version of the current System Manager.	Verifying the current software version on page 32	
4	Disable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	
5	Create a backup of primary System Manager and copy to the remote server.	Creating a data backup on a remote server on page 33	
6	Install the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.	Installing the Solution Deployment Manager client on your computer on page 28	
7	If the existing server is not compatible with System Manager Release 10.2.x, change the server to supported server.	-	
8	Add a location.	Adding a location on page 43	
9	Add an Avaya Aura® Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host.	Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host on page 45	
10	Upgrade to System Manager Release 10.2.x.	Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client on page 69	
11	Verify that the new System Manager application is functional.	Verifying the functionality of System Manager on page 112	
12	Regenerate licenses from PLDS after migration.		
13	Convert the primary System Manager server that is upgraded to Release 10.2.x to the standalone server.	The system takes about 30 minutes to convert the primary System Manager server to the standalone server. See *Administering Avaya Aura® System Manager*.	
14	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 33	

Table continues…

No.	Task	Link/Notes	✔
15	Upgrade the secondary System Manager to Release 10.2.x.	-	
16	Configure CRL download on the secondary System Manager server.	See *Administering Avaya Aura® System Manager*.	
17	Configure Geographic Redundancy on the secondary System Manager server with the details of the primary System Manager server that you converted to standalone.	See *Administering Avaya Aura® System Manager*. Add the primary server CA certificate to the secondary System Manager trust store.	
18	On the primary System Manager server, enable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	

Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client

About this task

Use the procedure to upgrade System Manager to Release 10.2.x from:

- Release 8.1.x running on Appliance Virtualization Platform, VMware, or Avaya Solutions Platform 130.
- Release 10.1.x running on VMware or Avaya Solutions Platform 130.

Note:

- If you are upgrading System Manager Release 8.1.x or 10.1.x to Release 10.2.x by using the Solution Deployment Manager client then the license files are retained. However, you need to install the license file for System Manager Release 10.2.

  For more information, see “License preservation and license regeneration”.
- From Release 10.1 and later, Appliance Virtualization Platform is no longer available. Therefore, if System 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 5.1 before upgrading System Manager to Release 10.2. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).

Before you begin

- Install Solution Deployment Manager Client.

  For information, see Installing the Solution Deployment Manager client on your computer on page 28.

- Add a location.

  For information, see Adding a location on page 43.
- Add the required host.

  For information about adding the host, see “Managing the platform”.

  Important:

  - If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

    For information about the supported ESXi version, see Supported ESXi version on page 18.

    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 10.2.x, then deploy Avaya Solutions Platform 130.

    For information about supported servers, see Supported servers for Avaya Aura applications on page 16.
- Select the System Manager 8.1.x or 10.1.x virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For more information, see Re-establishing trust for Solution Deployment Manager elements on page 54.
- Obtain the System Manager software. See “Software details of System Manager”

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Upgrade Management**.
4. Select the System Manager 8.1.x or 10.1.x virtual machine.
5. Click **Upgrade**.
6. In **Platform FQDN**, select the required host.

   If the System Manager system prompts for the certificate, accept the certificate. When you accept the certificate, the system displays the following message: `Certificate added successfully in trust store.`
7. **(Optional)** Select the datastore on the host.

   If more than one datastore is available, select the datastore.

   If the host is part of a VMware cluster, the system displays the following message:

```
Host is in a cluster. Therefore, capacity details of CPU and memory
are unavailable! Ensure that the host resource requirements are met
before any action.
```

For information about resource details, see Supported footprints of System Manager on VMware on page 24.

8. Click **Next**.
9. On the **OVA** tab, click one of the following:
   - **URL**, in **OVA File**, type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the System Manager OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the System Manager OVA file from the drop-down list.

     To use the **S/W Library** option, the OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation. The system displays the directory name when the **S/W Library** option is selected.
   - **Browse**, select the required OVA file from your local computer, and click **Submit File**.
   - **Browse from Datastore**

     For information about upgrading System Manager using the Pre-staging feature, see “Upgrading System Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x by using the Pre-staging feature of Solution Deployment Manager Client”.

     For information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

     This option is applicable only for System Manager Release 10.1 and later.

   When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
10. To upload the data migration utility file, click the Data Migration tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest data migration utility file.
    - **S/W Library**, and select the latest data migration utility file from the drop-down list.

      The data migration utility file must be present in the local software library directory.
    - **Browse**, and select the latest data migration utility file from your local computer, and click **Submit File**.
11. To upload the latest service or feature pack, select the Service or Feature Pack tab, and click one of the following:
    - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.

- **S/W Library**, and select the latest service or feature pack from the drop-down list.
- **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

12. Click **Next**.
13. In the Config Parameters section, provide the required details.

    Note:

    Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.

    For information, see “Upgrade Management field descriptions”.
14. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
15. Click **Upgrade** and accept the license terms.

    The system takes the backup, shuts down the existing virtual machine (VM), deploys the OVA file, and restores the data on the new virtual machine.
16. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 100–150 minutes depending on the data on System Manager.

    Note:

    The upgrade process might involve multiple reboots during data migration. If you have selected the checkbox **Require Encryption Pass-Phrase at Boot-Time**, you must monitor the VM console for reboots and enter the **Encryption Pass-Phrase** promptly.

    If you fail to enter the **Encryption Pass-Phrase** timely, the upgrade process may timeout and fail. If this happens, restart the upgrade process.
17. Do one of the following:

    - If the upgrade is successfully completed, do the following:

      a. Verify that the new System Manager virtual machine is functional.

         For more information, see “Verifying the functionality of System Manager”.

      b. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

         The system deletes the old virtual machine.

      c. Click **Commit**.

         The system deletes the old virtual machine.

         If you already performed the **Commit** operation or manually deleted the older VM (For example, <vm_name>_old) after successful upgrade on host itself. In these cases, if you re-attempt the **Commit** operation then Solution Deployment

Manager displays the warning message `Unable to find <vm_name>_old` on the Commit status page.

- If the upgrade fails or you want to revert to the old system, then do the following:
  a. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.
  b. Click **Rollback**.

     The system deletes the newly created virtual machine and starts the old virtual machine.
  c. Again refresh both the host to get the latest virtual machine information.

Next steps

Install the valid license file for System Manager Release 10.2.x.

Upgrading System Manager from Release 8.1.x or 10.1.x to Release 10.2.x by using the Pre-staging feature of Solution Deployment Manager Client

About this task

The procedure describes the steps to upgrade System Manager by using the Pre-staging feature of Solution Deployment Manager Client.

For more information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

- Appliance Virtualization Platform-based System Manager Release 8.1.x to System Manager Release 10.2.x

  Note:

  From Release 10.1 and later, Appliance Virtualization Platform is no longer available. Therefore, if System 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 5.1 before upgrading System Manager to Release 10.2. Migration of Appliance Virtualization Platform is supported from Avaya Solutions Platform 120 (Dell PowerEdge R640).
- VMware-based System Manager Release 8.1.x or 10.1.x to System Manager Release 10.2.x

Before you begin

- Install Solution Deployment Manager Client.

  For information, see Installing the Solution Deployment Manager client on your computer on page 28.
- Add a location.

  For information, see Adding a location on page 43.

- Add the ESXi, vCenter, Appliance Virtualization Platform, or Avaya Solutions Platform 130 host.

  For information about adding the host, see “Managing the platform”.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 57.

  Important:

  - If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

    For information about the supported ESXi version, see Supported ESXi version on page 18.

    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 10.2.x, then deploy Avaya Solutions Platform 130.

    For information about supported servers, see Supported servers for Avaya Aura applications on page 16.

- Create a prestaging job for upgrade.

  For more information, see “Creating a prestaging job for upgrade”.

- Select the System Manager 8.1.x or 10.1.x virtual machine and click **More Actions** > **Re-establish connection** to establish the trust.

  For more information, see Re-establishing trust for Solution Deployment Manager elements on page 54.

- Obtain the System Manager software. See “Software details of System Manager”

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Upgrade Management**.
4. On the Upgrade Management page, select the System Manager virtual machine.
5. Click **Upgrade**.
6. In **Platform FQDN**, select the required host.

   If the system prompts for the certificate, accept the certificate. When you accept the certificate, the system displays the following message: `Certificate added successfully in trust store.`

7. **(Optional)** Select the datastore on the host.

   If more than one datastore is available, select the datastore.

If the host is part of a VMware cluster, the system displays the following message:

```
Host is in a cluster. Therefore, capacity details of CPU and memory
are unavailable! Ensure that the host resource requirements are met
before any action.
```

For information about resource details, see Supported footprints of System Manager on VMware on page 24.

8. Click **Next**.
9. On the **OVA** tab, click **Browse from Datastore**, and do the following:
   a. In **Select Pre-stage Directory**, click **Browse**.
   b. In the DataStore Explorer dialog box, select the data store folder where the System Manager OVF file are stored, and click **Select**.

      For information about prestaging the System Manager files, see “Creating a prestaging job”.

   This option is enabled when you upgrade System Manager in the VMware virtualized environment. This option is applicable only for System Manager.

   When you select the OVA, the system:

   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
10. To upload the latest service or feature pack, click Data Migration, and do the following:
    a. Click **Browse from Datastore**.
    b. In **Select Pre-stage Directory**, click **Browse**.
    c. In the DataStore Explorer dialog box, select the data store folder where the System Manager bin file is stored, and click **Select**.

       For information about prestaging the System Manager files, see “Creating a prestaging job for upgrade”.
11. To upload the latest service or feature pack, click **Service or Feature Pack**, and do the following:
    a. Click **Browse from Datastore**.
    b. In **Select Pre-stage Directory**, click **Browse**.
    c. In the DataStore Explorer dialog box, select the data store folder where the latest System Manager data migration utility file is stored, and click **Select**.

       For information about prestaging the System Manager files, see “Creating a prestaging job for upgrade”.
12. Click **Next**.
13. In the Config Parameters section, provide the required details.

Note:

Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.

For information, see “Upgrade Management field descriptions”.

14. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
15. Click **Upgrade** and accept the license terms.

    The system takes the backup, shuts down the existing virtual machine (VM), deploys the OVA file, and restores the data on the new virtual machine.
16. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 100–150 minutes depending on the data on System Manager.

    Note:

    The upgrade process might involve multiple reboots during data migration. If you have selected the checkbox **Require Encryption Pass-Phrase at Boot-Time**, you must monitor the VM console for reboots and enter the **Encryption Pass-Phrase** promptly.

    If you fail to enter the **Encryption Pass-Phrase** timely, the upgrade process may timeout and fail. If this happens, restart the upgrade process.
17. Do one of the following:
    - If the upgrade is successfully completed, do the following:
      a. Verify that the new System Manager virtual machine is functional.

         For more information, see “Verifying the functionality of System Manager”.
      b. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.

         The system deletes the old virtual machine.
      c. Click **Commit**.

         The system deletes the old virtual machine.
    - If the upgrade fails or you want to revert to the old system, then do the following:
      a. If you upgraded System Manager on a different host, refresh both hosts in Solution Deployment Manager.
      b. Click **Rollback**.

         The system deletes the newly created virtual machine and starts the old virtual machine.
      c. Again refresh both the host to get the latest virtual machine information.

Next steps

Install the valid license file for System Manager Release 10.2.x.

Related links

Creating a prestaging job for upgrade on page 35

Upgrade Management field descriptions

Name	Description
Install on Same Host	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update. **Note:** When upgrading from System Platform-based System Manager to AVP or ESXi, the system displays this field.
Platform FQDN	The platform FQDN to which you want to upgrade. The system displays the CPU and memory details of the platform in the Capacity Details section.
Application Name	The application name displayed on the Add Element page.

OVA/ISO Details

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.

Table continues…

Name	Description
Browse from Datastore	The option to provide the prestaged folder. This option is enabled when you upgrade the application on the Appliance Virtualization Platform, VMware ESXi, and vCenter platforms. For upgrade, this option is applicable only for System Manager.
Select Pre-stage Directory	Displays the Datastore Explorer dialog box to select the prestage folder from the data store. The field is available when you select **Browse Pre-stage Location**
View Prestage Details	Displays the details of the prestage folder.
Validate checksum of OVA files	Validates the checksum of the OVA file.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is .
SMGR Data migration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest data migration bin that is available for the System Manager release.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.

Configuration Parameters

The system populates the values for most of the fields from the 7.x or 8.0.x system. You must provide information, such as password, FQDN, time zone, and EASG.

Management Network Settings

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application for Out of Band Management. This field is an optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager application.
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).

Table continues…

Name	Description
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. This field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. This field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. This field is optional.
Default Search List	The search list of domain names. This field is optional.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. This field is optional. Separate the IP addresses with commas (,). This field is not applicable for software-only deployment. The application supports only the NTP server. It does not support the NTP pool.
Time Zone	The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country. This field is not applicable for the software-only deployment.

Public Network Settings

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager application. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager application. The field is optional.
Public FQDN	The FQDN to assign to the System Manager application. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager application. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.

Table continues…

Name	Description
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

SMGR CLI USER

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.

Table continues…

Name	Description
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using vSphere Client (HTML5).
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

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

Data Encryption

Note:

Data Encryption is supported only for Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware Virtualized Environment.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

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. • **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.

Network Parameters

Name	Description
Out of Band Management IP Address	The IP Address that you must assign to the Out of Band Management port group. The field is mandatory.
Public	The port number that you must assign to public port group. The field is optional.

Button	Description
Upgrade	Displays the EULA acceptance screen. To accept EULA and start the upgrade process, click **Accept**.

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

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using Solution Deployment Manager Client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the Applications for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. Click **More Actions** > **Refresh App**.

   If **Refresh App** is disabled or fails, proceed to next step.
6. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **More Actions** > **Refresh App**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
7. Click **More Actions** > **Update App**.

   If Solution Deployment Manager detects a previous uncommitted patch, the system displays a dialog box with **Commit** and **Rollback**. You need to either commit previous uncommitted patch or rollback. Only after this, the system displays the System Manager Update dialog box to provide the patch file.
8. Click **Select bin file from Local SDM Client** and provide the absolute path to the software patch or service pack.

   Note:

   The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.
9. **(Optional)** Click the **Auto commit the patch** check box.
10. Click **Install**.

    In the Applications for Selected Location <location name> section, the system displays the status.
11. To view the details, in the **Current Action** column, click **Status Details**.

    SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.
12. On the Installed Patches page, perform the following:
    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.

b. Click **Get Info**.

c. Select the patch, service pack or feature pack, and click **Commit**.

Note:

To **Commit** or **Rollback** the System Manager patch, use this step.

Installing service packs and software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using the Pre-staging feature of Solution Deployment Manager Client.

For more information about the Pre-staging feature, see *Using the Solution Deployment Manager client*.

Before you begin

- Install the Solution Deployment Manager client.
- Create a prestaging job for update.

  For more information, see “Creating a prestaging job for update”.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the Applications for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. Click **More Actions** > **Refresh App**.

   If **Refresh App** is disabled or fails, proceed to next step.
6. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **More Actions** > **Refresh App**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.

7. Click **More Actions** > **Update App**.

   If Solution Deployment Manager detects a previous uncommitted patch, the system displays a dialog box with **Commit** and **Rollback**. You need to either commit previous uncommitted patch or rollback. Only after this, the system displays the System Manager Update dialog box to provide the patch file.

8. Click **Browse Pre-stage Location** and do the following:

   a. In **Select Pre-stage Directory**, click **Browse**.

   b. In the DataStore Explorer dialog box, select the data store folder where the System Manager patch file is stored, and click **Select**.

      For information about prestaging the System Manager files, see “Creating a prestaging job for update”.

9. **(Optional)** Click the **Auto commit the patch** check box.

10. Click **Install**.

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

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

    SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.

12. On the Installed Patches page, do the following:

    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.

    b. Click **Get Info**.

    c. Select the patch, service pack or feature pack, and click **Commit**.

Related links

Creating a prestaging job for update on page 37

Chapter 7: Upgrading from System Manager Release 7.0.x

Upgrading from System Manager Release 7.0.x

About this task

To upgrade System Manager from Release 7.0.x to 10.2, first upgrade System Manager 7.0.x to 10.1.x, and then upgrade to Release 10.2. You cannot directly upgrade the Release 7.0.x system to Release 10.2 and later.

Procedure

1. Upgrade System Manager from Release 7.0.x to 10.1.x.

   To upgrade from System Manager Release 7.0.x to 10.1.x, see *Upgrading Avaya Aura® System Manager* Release 10.1.x on the Avaya Support website.

2. Upgrade from System Manager Release 10.1.x to 10.2.

   To upgrade from System Manager 10.1.x to 10.2.x, see the required section in this document.

Chapter 8: Upgrading from System Manager Release 6.x

Upgrading from System Manager Release 6.x

About this task

For upgrading System Manager from Release 6.x to Release 10.2, first upgrade System Manager 6.x to 8.1.x, and then upgrade to Release 10.2. You cannot directly upgrade the Release 6.x system to Release 10.1 and later.

Procedure

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

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

2. Upgrade from System Manager Release 8.1.x to 10.2.

   To upgrade from System Manager 8.1.x to 10.2.x, see the required section in this document.

Upgrade Management field descriptions

Upgrade Elements

Name	Description
SMGR Name	System Manager name.
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
C-DOM IP/FQDN	The IP address or the FQDN of console domain.
Element Type	The type of the element.
Current Version	The current version of the element.
Upgrade To Version	The upgrade to version for the element.

Table continues…

Name	Description
Upgrade Status	The status of the upgrade process. The status can be **Upgrading**, **Completed**, or **Failed**. The **Status Details** link provides more information about the System Manager upgrade.
Last Action	The last upgrade action.
Related VM	The associated virtual machine.

Button	Description
Add Elements	Displays the Add Element page where you add System Manager.
Upgrade	Displays the Upgrade Management page where you upgrade the System Manager virtual machine.
Edit	Displays the Edit Element page where you can change the details of System Manager that you added.
Delete	Deletes the System Manager virtual machine.
Commit	Saves the changes and upgrades the System Manager virtual machine.
Rollback	Reverts the upgrade of the System Manager virtual machine.

Chapter 9: Upgrading to System Manager Release 10.2.x by using CLI

Checklist for upgrading to System Manager Release 10.2.x from CLI

Checklist for upgrading VMware-based System Manager to Release 10.2.x by using CLI

No.	Task	Link/Notes	✔
1	Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at http://support.avaya.com.	
2	Record the number of users and number of roles. You require this information later to verify that the upgrade is successful	For more information about managing users and custom roles, see *Administering Avaya Aura® System Manager*.	
3	Record the System Manager FQDN and Time Zone.	See Customer configuration data for System Manager on page 23.	
4	Before you turn off the system, copy the Avaya Breeze® platform snap-in svar files that you might need in the future to the `/var/avaya/svars` location on the local computer.	Do this, if you have the System Manager Release 6.3.8 or later system and Avaya Breeze® platform is configured.	
5	Ensure that the server is compatible with System Manager Release 10.2.x.	For Appliance Virtualization Platform, see Supported servers on page 16. For the Customer-provided Virtualized Environment offer, see: • Software requirements on page 18	
6	Create a backup of System Manager.	Creating a data backup on a remote server on page 33	

Table continues…

No.	Task	Link/Notes	✔
7	Turn off the old System Manager application.	**Note:** To migrate or upgrade from an earlier release (starting from Release 7.x and above) to Release 10.1 and later, shutdown System Manager immediately after taking the backup of your system. This will reduce the possibility of System Manager repairing all the configured elements after the upgrade.	
8	On the ESXi server, deploy the System Manager OVA file. If you are using the third-party certificates, use the same FQDN and vFQDN as that of the existing System Manager. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.	See “Deploying System Manager in Virtualized Environment”.	
9	Copy the Release Release 10.2.x data migration utility, the Release 10.2.x patch file, and the backup file to the `/swlibrary` location on System Manager Release 10.2.x.	To copy files, use the tools, such as SCP, WinSCP, and FileZilla.	
10	Create the snapshot of the System Manager application after the post-deployment steps are successful.	Creating the System Manager virtual machine snapshot on page 34	

Table continues…

No.	Task	Link/Notes	✔
11	After deploying the System Manager OVA, run **upgradeSMGR** with data migration utility, backup file, and the service pack or feature pack as inputs. The upgrade takes about 80 to 90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade. As part of running the data migration utility, the system performs the patch installation in the background that takes about 60–90 minutes.	Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI on page 96	
12	Verify that the new System Manager application is functional.	Verifying the functionality of System Manager on page 112	
13	After the upgrade and patch installation is successful, remove the patch bin file, backup file, data migration utility, log off from the system, and remove the snapshot.	-	
14	Reinstall the license files because after the data migration the existing license files become invalid.	-	
15	Copy the Avaya Breeze® platform snap-in svar files that you saved earlier to the Release 10.1 system.	-	

Checklist for upgrading VMware-based System Manager in the Geographic Redundancy setup to Release 10.2.x by using CLI

No.	Task	Link/Notes	✔
1	Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at http://support.avaya.com.	
2	Disable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	
3	Create a backup of primary System Manager and copy to the remote server.	Creating a data backup on a remote server on page 33	

Table continues…

No.	Task	Link/Notes	✔
4	Turn off or remove the primary System Manager application.	-	
5	Deploy the System Manager OVA file. **Note:** After deploying the Release 10.1 OVA file and before performing operations, such as configuring Geographic Redundancy and changing the IP or FQDN, you must run the data migration utility. Verify that the System Manager installation is successful and post-installation verification is complete.	See “Deploying System Manager in Virtualized Environment”.	
6	Copy the Release Release 10.2.x data migration utility, the Release 10.2.x patch file, and the backup file to the `/swlibrary` location on System Manager Release 10.2.x.	To copy files, use the tools, such as SCP, WinSCP, and FileZilla.	
7	Create the snapshot of the System Manager application after the post-deployment steps are successful.	Creating the System Manager virtual machine snapshot on page 34	
8	Run the data migration utility and provide the backup file and the Release 10.2.x bin file.	Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI on page 96	
9	Verify that the data is successfully migrated to Release 10.2.x.	-	
10	Convert the primary System Manager server that is upgraded to the latest release to the standalone server.	See *Administering Avaya Aura® System Manager*.	
11	Reinstall the license files because after the data migration, the existing license files become invalid.	-	
12	Turn off or remove the secondary System Manager application	-	
13	Deploy the System Manager OVA file. Verify that the System Manager installation is successful and post-installation verification is complete.	See “Deploying System Manager in Virtualized Environment”.	

Table continues…

No.	Task	Link/Notes	✔
14	Install the System Manager Release 10.2.x patch file. The patch installation takes about 45 minutes to complete.	-	
15	Create the snapshot of the System Manager application after the post-deployment steps are successful.	Creating the System Manager virtual machine snapshot on page 34	
16	Configure CRL download on the secondary System Manager server.	See *Administering Avaya Aura® System Manager*.	
17	Add the primary server CA certificate to the secondary System Manager trust store.	See *Administering Avaya Aura® System Manager*.	
18	Configure Geographic Redundancy on the secondary System Manager server with the details of the primary System Manager server that you converted to standalone.	See *Administering Avaya Aura® System Manager*.	
19	On the primary System Manager server, enable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	
20	Once the system verification is successful, log off from the system, and remove the snapshot of the primary and secondary servers.	-	

Upgrading System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through CLI

About this task

Use the procedure to upgrade System Manager from Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x running on VMware by using command-line interface.

Note:

- For upgrading System Manager from Release 7.0.x to Release 10.2 and later, first upgrade System Manager Release 7.0.x to 10.1.x, and then upgrade to Release 10.2 and later. You cannot directly upgrade the Release 7.0.x system to Release 10.2 and later. If you upgrade the application directly from Release 7.0.x to Release 10.2 and later, the upgrade might fail.
- For upgrading System Manager from Release 6.x to Release 10.1 and later, first upgrade System Manager Release 6.x to 8.1.x, and then upgrade to Release 10.1 and later. You cannot directly upgrade the Release 6.x system to Release 10.1 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1 and later, the upgrade fails.

When you upgrade System Manager to Release 10.1.x and later by using the data migration utility from CLI, you need to provide the patch file along with backup to the data migration utility. Therefore, do not perform the patch installation separately.

Before you begin

Warning:

If you use the CLI procedure to upgrade System Manager to Release 10.2.x, the system does not retain the System Manager WebLM licenses that are installed on the old System Manager server. This will impact each product that is using the licenses from System Manager WebLM. During or after the upgrade, those product might go in the license grace period mode or license error mode. To remediate this, after the upgrade, regenerate the licenses by using the new host ID. Ensure that all your Avaya License Activation Codes (LACs) for your system are available that is under contract with 'Upgrade Advantage' entitlement. Also, check that your account at Avaya PLDS website https://plds.avaya.com/ is functional to regenerate the license keys.

Important:

- If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.

  For information about the supported ESXi version, see Supported ESXi version on page 18.

  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.

Download the System Manager OVA, data migration utility, and patch files from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the old System Manager web console.
2. Record the software version of old System Manager from the **About** link.

   For information, see "Verifying the current software version".
3. Create a System Manager remote backup by using System Manager web console.

   Note:

   Use the backup for restoring the data while using the data migration utility and also in case if the upgrade fails.
4. Export the System Manager license keys and ensure you have a LAC available to regenerate this key once the new System Manager 10.2 instance is deployed.

   Note:

   If you fail to do this step, then you will lose all the System Manager licenses including the other installed product licenses.
5. Shut down the old System Manager.

6. Deploy the System Manager OVA on the supported ESXi version.

   For information about the supported ESXi version, see Supported ESXi version on page 18.

   For information about deploying System Manager on VMware, see Deploying the System Manager OVA on vCenter by using vSphere Client (HTML5) on page 144 and Deploying the System Manager OVA by accessing the ESXi host directly on page 146.

   Important:

   It is recommended to use the same network parameters and system parameters that you recorded on the existing system. If you are not using any third-party certificates, then you can also use the different network parameters to configure the new system

   For information about parameters, see Customer configuration data for System Manager on page 23.

7. Copy the following files to the `/swlibrary` location on System Manager.
   - Data Migration Utility
   - Latest patch
   - System Manager backup file that you created in Step 3.

8. Do the following:
   a. Create a snapshot of the System Manager system.
   b. Ensure that the System Manager web console is accessible.
   c. Check the server time before you run the data migration utility to upgrade System Manager.
   d. To run the data migration utility, type the following command:

      ```
      upgradeSMGR /swlibrary/<DMUtility_bin file name>.bin -m -v
      ```

      You must provide the absolute path of the data migration utility.
   e. In **Enter the location of backup file (full path)**, type the absolute path of the backup file.

      ```
      /swlibrary/<backupfile name.*>
      ```

      The system validates the backup file and displays the parameters.

      Note:

      If you provide the System Manager Release 6.x backup file, the system displays a message. For example:

      ```
      System Manager 10.1 does not support direct migration from
      version <6.x>.
      ```

   f. In **Enter the patch file**, type the absolute path of the patch file:

      ```
      /swlibrary/<patch file name>.bin
      ```

      For example, `/swlibrary/System_Manager_R10.2.0.0.xxxxxxxxx.bin`.

The system validates the patch file and displays the following message:

```
You are about to run the System Manager Data Migration utility.
The System Manager will be inaccessible for approximately 60
minutes, depending on the resources available on the system.
```

g. To continue, type `Y`.

The system displays the following message:

```
WARNING:- The system is now going down for a halt and will be
inaccessible for some time.
Remote broadcast message (<Day Month DD HH:MM:SS Year>):
INFO:- System Manager Data Migration would now be executed
in background process. For details, see System Manager
Data Migration logs in the /var/log/Avaya/datamigration/
data_migration.log.
```

9. Log on to System Manager CLI to monitor the upgrade.

The upgrade takes about 80 to 90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.

As part of running the data migration utility, the system performs the patch installation in the background that takes about 60–90 minutes.

You can monitor the progress of System Manager:

- Data Migration Utility from the `/var/log/Avaya/datamigration/data_migration.log` file.
- Patch from the `/var/log/Avaya/SMGR_Patch.log` file.

After the upgrade is successful, the system displays the messages:

- For Data Migration Utility: `<Day Month Date HH:MM:SS IST Year #### Data Migration Utility Completed Successfully. ####`
- For Patch: `<Day Month Date HH:MM:SS IST Year #### ########Patch execution completed Successfully.`

10. Perform one of the following:

- If the upgrade and patch installation is successful, remove the patch bin file, backup file, data migration utility, log off from the system, and remove the snapshot.

Note:

Snapshots occupy the system memory and degrade the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

- If the upgrade or patch installation fails, use the snapshot to restore the system to the original state.

To collect logs, you can run the **`collectLogs`** command. System Manager creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file at `/swlibrary` directory. Copy the

`LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

Next steps

- Regenerate new licenses for all components from PLDS by using the associated LACs.
- Install all the regenerated license file on System Manager Release 10.2.x.

Related links

Creating a data backup on a remote server on page 33
Shutting down Appliance Virtualization Platform host from CLI on page 49
Restoring a backup from a remote server on page 133

Chapter 10: Upgrading System Manager to Release 10.2.x on Software-only environment

Upgrade path for Software-only environment

You can upgrade to System Manager Release 10.2.x on Software-only environment from:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 8.0.x or 8.1.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.
- System Manager Release 7.1.3.x on AWS
- System Manager Release 7.1.3.x on Appliance Virtualization Platform on Avaya provided server or on VMware in customer-provided Virtualized Environment.

Note:

- For upgrading System Manager from Release 7.0.x to Release 10.2 and later, first upgrade System Manager Release 7.0.x to 10.1.x, and then upgrade to Release 10.2 and later. You cannot directly upgrade the Release 7.0.x system to Release 10.2 and later. If you upgrade the application directly from Release 7.0.x to Release 10.2 and later, the upgrade might fail.
- For upgrading System Manager from Release 6.x to Release 10.1 and later, first upgrade System Manager Release 6.x to 8.1.x, and then upgrade to Release 10.1 and later. You cannot directly upgrade the Release 6.x system to Release 10.1 and later. If you upgrade the application directly from Release 6.3.x to Release 10.1 and later, the upgrade fails.

Upgrading to System Manager Release 10.2.x on Software-only through CLI

About this task

Use the procedure to:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Upgrade System Manager from Release 8.0.x or 8.1.x on VMware/ KVM OVA in customer-provided Virtualized Environment, AWS OVA to the System Manager Release 10.2.x on Software-only IaaS offer.
- Upgrade the System Manager Release 7.1.3.x AWS instance to the System Manager Release 10.2.x on Software-only offer.

Note:

Use this procedure to upgrade Avaya Aura® application Release 8.1.x on Nutanix to Avaya Aura® application Release 10.2.x in the Software-only environment.

Procedure

1. Log on to the old System Manager web console.
2. Record the software version of old System Manager from the **About** link.

   For information, see “Verifying the current software version”.
3. Create a System Manager remote backup by using System Manager web console.

   Note:

   Use the backup for restoring the data while using the data migration utility and also in case if the upgrade fails.
4. Shut down the old System Manager.
5. Deploy the System Manager Release 10.2 application.

   For information, see *Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments*.
6. Log in to the System Manager command-line interface of the new system.
7. Copy the following files to the `/swlibrary` location on System Manager.
   - Data Migration Utility
   - Latest patch
   - System Manager backup file that you created in Step 3.
8. Do the following:
   a. Create a snapshot of the System Manager system.
   b. Ensure that the System Manager web console is accessible.

c. Check the server time before you run the data migration utility to upgrade System Manager.

d. To run the data migration utility, type the following command:

```
upgradeSMGR /swlibrary/<DMUtility_bin file name>.bin -m -v
```

You must provide the absolute path of the data migration utility.

e. In **Enter the location of backup file (full path)**, type the absolute path of the backup file.

```
/swlibrary/<backupfile name.*>
```

The system validates the backup file and displays the parameters.

Note:

If you provide the System Manager Release 6.x backup file, the system displays a message. For example:

```
System Manager 10.1 does not support direct migration from
version <6.x>.
```

f. In **Enter the patch file**, type the absolute path of the patch file:

```
/swlibrary/<patch file name>.bin
```

For example, `/swlibrary/System_Manager_R10.2.0.0.xxxxxxxxx.bin`.

The system validates the patch file and displays the following message:

```
You are about to run the System Manager Data Migration utility.
The System Manager will be inaccessible for approximately 60
minutes, depending on the resources available on the system.
```

g. To continue, type `Y`.

The system displays the following message:

```
WARNING:- The system is now going down for a halt and will be
inaccessible for some time.
Remote broadcast message (<Day Month DD HH:MM:SS Year>):
INFO:- System Manager Data Migration would now be executed
in background process. For details, see System Manager
Data Migration logs in the /var/log/Avaya/datamigration/
data_migration.log.
```

9. Log on to System Manager CLI to monitor the upgrade.

The upgrade takes about 80 to 90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.

As part of running the data migration utility, the system performs the patch installation in the background that takes about 60–90 minutes.

You can monitor the progress of System Manager:

- Data Migration Utility from the `/var/log/Avaya/datamigration/data_migration.log` file.
- Patch from the `/var/log/Avaya/SMGR_Patch.log` file.

After the upgrade is successful, the system displays the messages:

- For Data Migration Utility: `<Day Month Date HH:MM:SS IST Year #### Data Migration Utility Completed Successfully. ####`
- For Patch: `<Day Month Date HH:MM:SS IST Year #### ########Patch execution completed Successfully.`

10. Verify the software version of the new System Manager.
11. Perform one of the following:
    - If the upgrade and patch installation is successful, remove the patch bin file, backup file, data migration utility, log off from the system, and remove the snapshot.

      Note:

      Snapshots occupy the system memory and degrade the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

    - If the upgrade or patch installation fails, use the snapshot to restore the system to the original state.

      To collect logs, you can run the **`collectLogs`** command. System Manager creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file at `/swlibrary` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

Next steps

- Regenerate new licenses for all components from PLDS by using the associated LACs.
- Install all the regenerated license file on System Manager Release 10.2.x.

Upgrading from AVP or VMware based System Manager to Software-only environment by using the Solution Deployment Manager client

About this task

The procedure describes the steps to upgrade Appliance Virtualization Platform or VMware based System Manager Release 8.1.x or 10.1.x to System Manager Release 10.2.x on Software-only environment.

Before you begin

- Install the Solution Deployment Manager client.
- Add a location.
- Add the ESXi, vCenter, or Appliance Virtualization Platform host from the Application Management page.
- Select the System Manager virtual machine and click **More Actions** > **Re-establish connection** to establish the trust. For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
- Obtain the System Manager application for Software-only environment, the data migration utility file and the latest service or feature pack file. See “Software details of System Manager”

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **Application Management**.
3. In the lower pane, click **Upgrade Management**.
4. On the Upgrade Management page, select the System Manager virtual machine.
5. Click **Upgrade**.
6. On **Select Platform**, select the **Software Only** check box.
7. Click **Continue**.

   The Solution Deployment Manager client takes the backup and shuts down the virtual machine.

8. Click the Refresh  icon until the **Upgrade Status** changes to **Upgrading (PAUSED)...RESUME** state.
9. Manually install and configure the RHEL OS with the same IP address of the old System Manager virtual machine.
10. Once the RHEL system is configured and running, access the Solution Deployment Manager client GUI and go to **Add Platform** to add the newly added Software-only platform.
11. On the **Add Platform** dialog box, configure the following options:
    - **Platform Name**: Type the name of the platform.
    - **Platform FQDN or IP**: Type the FQDN or IP address of the platform, that is, the RHEL system created for software-only.
    - **User Name**: Type the user name to access the platform.
    - **Password**: Type the password to access the platform.

- **Platform Type**: Select platform type as **OS** for Software-only upgrade.

12. Click **Save**.
13. Click **Upgrade Management** > **Upgrade Elements** and, then click **RESUME** displayed under the **Upgrade Status** column.
14. In the Provide admin and root Credentials section, do the following:
    a. In **Admin User of OS**, type the admin user name.
    b. In **Admin Password of OS**, type the admin user password.
    c. In **Root User of OS**, type the root user name.
    d. In **Root Password of OS**, type the root user password.
    e. **(Optional)** Click **Test Connection**.

       The system logs in to the platform by using the credentials to test the platform connectivity. If connectivity is established, the system displays the message: `Test Connection Successful`.

    f. Click **OK**.
15. Click **Next**.
16. To select the required application, on the **ISO** tab, click one of the following:
    - **SW Library** / **Select from software library**: Select the local library where the *ISO image* is available.

      If you are deploying the *ISO image* from the Solution Deployment Manager client, you can use the default software library that is set during the Solution Deployment Manager Client installation.
    - **Browse**: Select the *ISO image* from your local computer, and click **Submit File**.
    - **URL**: Click URL and provide the path to the *ISO image*.

    Select the required application, click **Submit**.
17. Click the **Data Migration** tab and provide the data migration file depending on your setup.

    If the application *ISO image* supports the patch deployment, the system enables the **Service or Feature Pack** tab.
18. To apply the latest patch file for the application, click **Service or Feature Pack**, and enter the appropriate parameters.
    a. Click **URL**, and provide the absolute path to the latest service or feature pack.
    b. Click **SW Library** / **Select from software library**, and select the latest service or feature pack.
    c. Click **Browse**, and select the latest service or feature pack.
19. Click **Next**.
20. In **Flexi Footprint**, select the footprint size for the application.

21. In Test Your Operating System Compatibility Against Element Software Package, click **Test Environment Compatibility**.

    The installer checks if the platform has all the dependent RPMs, network, CPU, memory, and hard disk configuration as specified for the element. This process takes about 4-5 minutes. After the process starts, you cannot proceed further until the process is complete. If you get any error or warning, make the necessary changes before the next steps. After the check is completed successfully, the system displays a message “Environment check is successful”.

    Note:

    If the browser hangs, the system provides the option to end the script or wait. Always click **Wait**.

22. **(Optional)** To view the installer compatibility results in a separate window, click **View Output**.

    The system displays the Environment Check Output window.

23. Click **Next**.
24. On the Configuration Parameters page, provide all the information required.

    For a *Software-Only* application upgrade, the **Network Parameters** tab is disabled.

25. Click **Upgrade**.
26. On the EULA Acceptance window, click **Accept**.

    After accepting EULA, the system displays Software only Installation Warning for software-only application upgrade.

27. To continue with the upgrade, click **Accept**.

    The system displays the upgrade status in the **Current Action Status** column and the upgraded application on the **Applications** tab.

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

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.

Chapter 11: Installing the System Manager patch

Installing the System Manager patch, service pack, or feature pack from CLI

About this task

Note:

- If you upgrade System Manager from an older release like 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x, and the goal is to apply the latest Feature Pack or Service pack of 10.2.x, then you can install the latest service pack or feature pack of System Manager Release 10.2.x as part of the migration process. You do not have to install the 10.2 GA patch as an intermediate step.

  For example, if you upgrade System Manager from Release 10.1.x to Release 10.2.x, then you can directly apply the Release 10.2.x patch as part of data migration. You do not need to apply the 10.2 GA patch (`System_Manager_10.2.0.0_GA_Patch_rxxxxxxxxx.bin`) in the intermediate step.
- If you perform the fresh deployment of System Manager Release 10.2 and the goal is to be on the latest Feature Pack or Service Pack of 10.2.x that is available, then after deploying the Release 10.2 OVA you can directly install the latest feature pack or service pack of System Manager Release 10.2.x. You do not have to install the 10.2 GA patch first.
- After enabling data encryption and installing the System Manager 8.1.2 and later patch, if the local or remote key store is not enabled, the Data Encrypted server prompts for the encryption passphrase. After you enter the encryption passphrase, System Manager automatically reboots. This happens only after the first reboot and prompts you to add the encryption passphrase again.

Before you begin

- Ensure that System Manager is running on Release 10.2.
- Download the System Manager patch bin file from the Avaya Support website at https://support.avaya.com/ and copy the file to the `/swlibrary` location on System Manager.

Procedure

1. Log in to the System Manager command-line interface with administrator privilege credentials.

2. Create a snapshot of the System Manager application.

   This activity might impact the service.

3. Type the following: `SMGRPatchdeploy <absolute path to the patch, service pack, or feature pack for System Manager>`

   If you do not provide the name of the patch, service pack, or feature pack, the console displays menu items. Provide the absolute path to the System Manager patch, service pack, or feature pack.

   System Manager displays the license information.

4. Read the End User License Agreement carefully, and to accept the license terms, type `Y`.

   The patch installation takes about 45 minutes to complete.

   If the installation is successful, the system displays a warning message on the dashboard and on the command line interface to restart System Manager, if the kernel is updated.

5. Perform one of the following:

   - If the patch installation is successful, remove the patch bin file, log off from the system, and remove the snapshot.

     Note:

     Snapshots occupy the system memory and degrade the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

   - If the patch installation fails, first collect logs and then use the snapshot to restore the system to the original state.

     To collect logs, you can run the **`collectLogs`** command. The system creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file in the `/swlibrary` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to the remote server and share the file with Avaya Support Team.

Next steps

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Log on to the System Manager web console. At your first login, change the System Manager web console credentials.

Important:

This does not apply to System Manager Release 10.1.2 and later.

For Software-Only ISO Release 10.1 deployment, after installing the Release 10.1.0.2 patch and before rebooting, do the following to ensure System Manager does not boot into emergency mode:

1. Take a live (running) snapshot of the System Manager virtual machine.

   Note:

   This is a special case, so live (running) snapshot is required.

2. Apply the latest System Manager Release 10.1.0.2 hotfix.

   For more information, see PSN005574u.

3. Reboot System Manager.
4. After 10-15 minutes, verify the System Manager command-line interface and web console access.
5. After successful verification, delete the System Manager virtual machine snapshot taken at step#1.

Related links

System Manager command line interface operations on page 161

Chapter 12: Post-upgrade Verification

Post-upgrade checklist

Sr. No.	Task	Link/Notes	✔
1	Verify that System Manager is installed properly after the upgrade.	See Verifying the functionality of System Manager on page 112.	
2	Install the license file.	See Installing a license file on page 124.	
3	Verify that the number of user profiles remains same before and after the upgrade.	See *Administering Avaya Aura® System Manager*.	
4	Add or edit user from user profile, if required.	See *Administering Avaya Aura® System Manager*.	
5	Verify that Communication Manager and Session Manager are synchronized with the System Manager.	See *Administering Avaya Aura® System Manager*.	
6	Install the language pack to get localization support, if required.	See Installing language pack on System Manager on page 126.	
7	Delete the virtual machine snapshots, if required.	See Deleting the virtual machine snapshot from the Avaya Aura Appliance Virtualization Platform host on page 127 and Deleting the virtual machine snapshot from the vCenter managed host or standalone host on page 127.	
8	Configure the EASG settings, if required.	See Managing EASG from CLI on page 128.	

Verifying the functionality of System Manager

About this task

To ensure that System Manager is operational after the upgrade, verify that the installation of System Manager is successful.

After upgrading System Manager from Release 7.0.x to Release 7.1.x and later, System Manager applies the hashing on the password by using secure sha2-based algorithms. Therefore, administrative users must reset the password before accessing the System Manager web console.

When you promote an end user to an administrator, the system resets the password to the login name of the user.

Procedure

1. To log on to the System Manager web console, in the web browser, type `https://<fully qualified domain name of System Manager>/SMGR`.
2. Click the settings icon (), click **About**, and verify that the system displays the version number of System Manager with the highest build number for the release.
3. On the upgraded system, verify that the number of users and custom roles matches the number of users and custom roles that you recorded before the upgrade.

   For more information about managing users and custom roles, see *Administering Avaya Aura® System Manager*.
4. Verify that you can perform the following tasks correctly:
   - Creation and deletion of a user
   - Creation of a role
   - Creation of a job
   - Creation of the remote data backup
   - Replication of the data by using Data Replication Service (DRS)

   Note:

   Data Replication synchronization between System Manager, Session Manager and other elements is an automatic process after the upgrade where no manual intervention is required. Do not run any commands on the Session Manager or other elements for repairing the nodes. If you have large number of nodes (more than 50 nodes), the system repairs the nodes one by one, and takes longer time to repair the nodes.

   For instructions to complete each verification task, see *Administering Avaya Aura® System Manager*.

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.

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.
- 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”.

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- **Element Configuration**

- **AVP Configuration**

Element Configuration: General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/ Platform	The new target host on which you want to run the device.
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.

Table continues…

Name	Description
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 (,).
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.

Table continues…

Name	Description
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.
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. • **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.

Creating a Snapshot restore

About this task

Important:

Do not perform any activity on the System Manager virtual machine until the Snapshot restoration is complete.

You can restore the Snapshot backup using the vCenter or vSphere Web Client.

Procedure

1. Select the deployed System Manager virtual machine from the list of VMs, right-click and select **Snapshot**.
2. Open **Snapshot Manager**.
3. Select the Snapshot version that you want to restore.
4. Click **Goto**.
5. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task and wait until the system displays `Completed`.

Third-party certificate for upgrades

When you upgrade System Manager to Release 7.1.3 and later, the system retains the third-party CA-issued identity certificates that was used before the upgrade.

Using third-party certificates while upgrading from System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x

About this task

If you are using third-party certificates on System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x and want to upgrade to System Manager Release 10.2, use the following procedure:

Procedure

1. Deploy the new System Manager Release 10.2 OVA using the same IP/FQDN and virtual FQDN values that are on System Manager Release 7.1.3.x, 8.0.x, 8.1.x, or 10.1.x.

   Identity certificates are acknowledged by certain parameters, such as FQDN, VFQDN, and IP Addresses. As third-party CA issued identity certificates are retained after upgrade, so upgrading System Manager with different FQDN or IP Address will cause failure.
2. Ensure that the identity certificate chain includes the third-party, CA-issued identity certificate and all the intermediate/Sub CA certificates, and the root CA certificate in the chain of trust. Otherwise, the upgrade might fail.

License management

Finding LAC for System Manager in PLDS

About this task

You can find License Activation Code (LAC) using a Group ID or a SAP order number. With LAC, you can activate the available associated entitlements.

Procedure

1. Log in to the PLDS at https://plds.avaya.com.
2. From the Assets menu, select **View Entitlements**.
3. In the **Application** field, select **System Manager**.
4. Do one of the following:
   - To search using group ID, in the **Group ID** field, enter the appropriate group ID.

     Note:

     All group IDs are numeric without any leading zeros.
   - To search using the SAP order number, click **Advanced Search**, and in the **Sales/ Contract #** field, enter the SAP order number.
5. Click **Search Entitlements**

   The system displays the LAC(s) in the search results.

Installing a 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.

Note:

If you have a mix of Communication Manager Release 6.3.x, 7.x, 8.x, and 10.1.x software with Communication Manager 6.3.x, 7.x, 8.x, and 10.1.x license files, then Avaya recommends to use the Communication Manager 10.1.x license file for all the Communication Manager Release software.

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.

Install license field descriptions

Name	Description
Enter license path	The complete path where the license file is saved.
Browse	The option to browse and select the license file.
Avaya Global License Terms & Conditions	Avaya license terms and conditions that the user must agree to continue the license file installation.

Button	Description
Install	Installs the product license file.

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

Note:

After installing the language pack, you cannot uninstall the language pack.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `locate LocalizationScript.sh`, and press `Enter`.

   System Manager displays the path of the localization script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/script/LocalizationScript.sh`
3. Type `locate FrenchResourceBundle.zip`, and press `Enter`.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path; the path might vary based on actual path that you get.
4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.
5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
6. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

   Note:

   During this activity, System Manager restarts the Application server. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode, then apply these steps on the secondary System Manager server also after secondary server is active.

7. Change the browser language setting to French.

Deleting the virtual machine snapshot

Deleting the virtual machine snapshot from the Avaya Aura® Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<vCenter or ESXi IP/FQDN address>/ui`
2. To log in to the Appliance Virtualization Platform host, provide the credentials.
3. In the left navigation pane, click **Virtual Machines**.
4. Select the virtual machine, click **Actions** > **Snapshots** > **Manage snapshots**.

   The system displays the Manage snapshots - <Virtual machine name> dialog box.
5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.

Deleting the virtual machine snapshot from the vCenter managed host or standalone host

Procedure

1. Log in to the vSphere Client for the vCenter managed host or the standalone host.
2. Depending on the host, perform one of the following:

- 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.

Enhanced Access Security Gateway

Enhanced Access Security Gateway (EASG) overview

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

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, remove, restore or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message:

      ```
      By enabling Avaya Services Logins you are granting Avaya access
      to your system. This 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, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the
      Avaya support site (https://support.avaya.com/ registration)
      for additional information for registering products and
      establishing remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled`.

3. To disable EASG, do the following:

   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message:

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

b. When the system prompts, type `yes`.

The system displays the message: `EASG Access is disabled`.

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **`EASGProductCert --certInfo`**.

   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

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. 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.

2. 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.
3. 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 13: Maintenance

Backup and restore the System Manager data

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. On the System Manager Web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Creating a data backup on a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In **File name**, type the backup file that you want to create.
5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Restoring a backup from a remote server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager Release 8.1 with Release 8.1.1 software patch installed, System Manager on which you restore the backup must run Release 8.1 that has Release 8.1.1 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

For more information, see “Backup and restore”.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the **Backup Encryption Password** field.

   b. In **Backup Encryption Password**, type the encryption password.
5. To specify the file name for the restore operation, perform one of the following:
   - Click the **Backup List** tab, and select a file name.

     Use this method if the path of the backup file on the remote server is valid, and the credentials used while creating the backup file is unaltered.
   - Click the **Parameterized Restore** tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

     Note:

     System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
   - Click the **Parameterized Restore** tab, select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR

Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

6. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

7. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Restoring data backup from a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you must restore.

   If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

   Note:

   System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

System Manager displays the **Backup Encryption Password** field.

b. In **Backup Encryption Password**, type the encryption password.

6. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

7. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Backup and Restore field descriptions

Name	Description
Operation	The type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, the name of the backup file. • For the restore operation, the name of the backup file that was used for the restore.
Path	• For the backup operation, the path of the backup file. • For the restore operation, the path of the backup file that was used for the restore.
Status	The status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	The error details of the backup or restore operation that has failed.
Operation Time	The time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	The user who performed the operation.

Button	Description
Backup	Displays the Backup page from where you can back up the System Manager data.
Restore	Displays the Restore page from where you can restore the data to System Manager.

Backup field descriptions

Name	Description
Type	The type of computer on which you can back up the application data. The options are: • **Local**: The system backs up the data on a local computer. • **Remote**: The system backs up the data on a remote computer.

The page displays the following fields when you choose to create a backup of System Manager data in a location that is local to the System Manager file system.

Name	Description
File Name	The file name that identifies the backup. System Manager creates a backup file in the home directory of the specified user.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**
Backup Encryption Password	The password for the encrypted backup. The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters ($@!%*?&). **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

The page displays the following fields when you choose to create a backup of the System Manager data on a remote server.

Name	Description
Use Default	The option to use the default configured values. To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
File transfer protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the remote server.
Remote Server Port	The SSH port of the remote server.
User Name	The user name for logging into the remote server.
Password	The password for logging on to the remote server.
Test Credentials	Validates the login credential. The validation gives the connection result with the remote backup server.
File Name	The absolute path to the backup file and the file name. For example, `home/admin/smgr_backup_filename`. You can specify a different path for the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**
Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

Button	Description
Now	Creates a backup of the data in the specified location immediately.
Schedule	Displays the Schedule Backup page where you can enter the details to schedule a backup.
Cancel	Closes the Backup page and returns to the Backup and Restore page.

Restore field descriptions

Use this page to restore the application data from a local or a remote location.

Name	Description
Type	The type of computer from where you restore the application data. The options are: • **Local**. The data is restored from a local machine. • **Remote**. The data is restored from a remote machine.

The page displays the following fields, when you select **Local** as **Type**.

Name	Description
Select File Name	The list of files from where you select the backup file that you must restore.
File Name	The name of the backup file that you must restore. If the system does not display the file that you must restore, specify the complete path of the backup file. **Note:** System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**

Table continues…

Name	Description
Backup Encryption Password	The password for the encrypted backup. The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters ($@!%*?&). **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

Backup List

The page displays the following fields when you select **Remote** as **Type**.

The **Backup List** tab displays the list of remote backup files that are created using the SFTP or SCP protocol. Select a backup and click the **Parameterized Restore** tab to change the restore details. For example, if the location of a backup file is modified, specify the correct location of the file in the **File Name** field.

Parameterized Restore

The page displays the following fields when you select **Remote** as **Type**.

Name	Description
File Name	The name and complete path of the backup file that you want to restore.
File transfer protocol	The protocol that you can use to restore the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the SFTP or SCP server.
Remote Server Port	The SSH port of the SFTP or SCP server.
User Name	The user name for logging in to the SFTP or SCP server.
Password	Password for logging in to the SFTP or SCP server.
Use Default	Select this check box to use the default configured values. To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Restore	Restores the data from the specified backup file.
Cancel	Cancels any operation in progress, closes the Restore page, and displays the Backup and Restore page.

Changing over to Cold Standby server

Cold standby server as failover server for System Manager

Note:

If cold and standby System Manager server is not available, then the same procedure can be used to recover from disaster by setting up the new System Manager setup using a backup file.

When the main System Manager server fails, a cold standby System Manager server acts as a failover server.

This section describes the Cold Standby failover process for System Manager deployed on VMware with an example. The example has two nodes: Node A as the main server that is active and Node B, the cold standby node. Use the cold standby procedure with Node A going down and System Manager changed to Node B.

Prerequisites for the cold standby procedure

1. Ensure that the main server, Node A, and cold standby, Node B, servers are identical (For example, on the same profile and same version) and have the same IP address, host name, and VFQDN. When the main server is running, you must turn off the cold standby server.
2. Deploy System Manager on the main and cold standby server.
3. Ensure that the system time is synchronized on both the servers.
4. Using the remote backup capability of System Manager Element Manager, schedule a regular backup of the System Manager server on an external server. You can use this backup for restoring the data on a cold standby server when the main server fails.

Setting up a Cold Standby server

Before you begin

Ensure that the main server, also called Node A, is powered off.

Procedure

1. Power on the cold standby server also called as Node B.
2. Install the System Manager patches on Node B that were installed on Node A before you took the last backup on Node A.

   For example, if you installed patch 1 and patch 2 on System Manager on Node A before the backup, then install patch 1 and patch 2 on Node B before you restore the backup. In case, patch 3 is available and not installed on Node A when the backup was taken, install only patch 1 and patch 2 on Node B. Do not install patch 3.
3. Restore the last backup that you took from the Node A on Node B by using the backup and restore pages on the System Manager web console.

   For information, see Restoring a backup from a remote server on page 133.

4. Generate a new license file for products that are licensed using WebLM and that were installed prior to performing cold standby.

   Ensure that this new license file is generated from PLDS with the same count and the new Host Id.

5. When System Manager becomes operational, run repair on all the replica nodes. To repair the nodes, do the following:

   a. Log on to the System Manager web console with administrator privilege credentials.

   b. Click **Services** > **Replications**.

   c. Select all the replica groups and click **Repair**.

      The repair time of all the nodes depends on the number of nodes and the amount of configuration data on the System Manager server.

   Ensure that all the replicas have data that is consistent with the data restore on System Manager.

Creating a data backup on a remote server for cold standby

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup.

System Manager requires password authentication to connect to the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-authentication.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:

   - Perform the following:

     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.

     b. Enter the remote server IP, remote server port, user name, password, name and the absolute path of the backup file.

   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR

Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`
7. **(Optional)** To schedule the backup at a later time, click **Schedule**.

Restoring a backup from a remote server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager Release 8.1 with Release 8.1.1 software patch installed, System Manager on which you restore the backup must run Release 8.1 that has Release 8.1.1 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the **Backup Encryption Password** field.

b. In **Backup Encryption Password**, type the encryption password.

5. To specify the file name for the restore operation, click the **Parameterized Restore** tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

   Note:

   System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

6. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

7. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Restoring backup from local server

Procedure

1. Copy the backup from remote server to System Manager through winscp to the `swlibrary` directory.
2. Log in to the System Manager CLI with account created during deployment and change the permission of the backup file as shown below:

   ```
   $cd /swlibrary
   $chmod 777 <backup file name>
   ```

3. On the System Manager web console, click **Settings** > **Backup and Restore**.
4. On the Backup and Restore page, click **Restore**.
5. On the Restore page, click **Local**.
6. In the **File Name** field, type the path of the backup file as `</swlibrary/backup file name>`.
7. Click **Restore**.

Common upgrade procedures

Methods of System Manager deployment

You can deploy System Manager by using one of the following:

- For Avaya Solutions Platform 130 (Avaya-Supplied ESXI 7.0) and customer Virtualized Environment, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.
- For Software-Only Environment and Infrastructure as a Service Environment deployments, see *Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments*.

Deploying System Manager in Virtualized Environment

Deploying the System Manager OVA on vCenter by using vSphere Client (HTML5)

Procedure

1. To access the vCenter Server, do the following:
   a. On the web browser, type the vCenter FQDN or IP Address.
   b. Select vSphere Client (HTML5) and type the vCenter Server credentials.
2. Select the Cluster or ESXi host, right-click, and then click **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.
3. On the Select an OVF template page, do one of the following:
   - To download the System Manager OVA from a web location, select **URL**, and provide the complete path of the OVA file.
   - To access the System Manager OVA from the local computer, select **Local file**, click **Choose Files**, and navigate to the OVA file.
4. Click **Next**.
5. On the Select a name and folder page, do the following:
   a. In **Virtual machine name**, type a name for the virtual machine.
   b. In **Select a location for the virtual machine**, select a location for the virtual machine.
6. Click **Next**.
7. On the Select a compute resource page, select a host, and click **Next**.
8. On the Review details page, verify the OVA details, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I accept all license agreements**.

10. Click **Next**.
11. On the Select configuration page, in **Configuration**, select the required profile.
12. Click **Next**.
13. On the Select storage page, in **Select virtual disk format**, click the required disk format.
14. Click **Next**.
15. On the Select networks page, select the destination network for each source network.
16. Click **Next**.
17. On the Customize template page, enter the configuration and network parameters.

    For more information about the configuration and network parameters, see Network and configuration field descriptions on page 148.

    Note:

    - If you do not provide the details in the mandatory fields, you cannot turn on the virtual machine even if the deployment is successful.
    - During the startup, the system validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the console of the virtual machine.
18. Click **Next**.
19. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
20. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Click VM radio button, and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.
21. Click the **Console** tab and verify that the system startup is successful.

Next steps

From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file. Once the configuration is complete, the log file displays the following message: `SMGR Post installation configuration is completed`

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

The system displays the message: Installation of latest System Manager patch is mandatory.

- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Deploying the System Manager OVA by accessing the ESXi host directly

Before you begin

This procedure is applicable for ESXi 6.5 u2 onwards.

Procedure

1. To access the ESXI host, do the following:
   a. On the web browser, type the ESXi host FQDN or IP Address.
   b. In **User name**, type the user name of the ESXi host.
   c. In **Password**, type the password of the ESXi host.
   d. Click **Log in**.
2. Right-click an ESXi host and click **Create/Register VM**.

   The system displays the New virtual machine dialog box.
3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK files page, do the following:
   a. Type a name for the virtual machine.
   b. Click to select files or drag and drop the OVA file from your local computer.
6. Click **Next**.
7. On the Select storage page, select a datastore, and click **Next**.
8. To accept the End User License Agreement, on the License agreements page, click **I Agree**.
9. Click **Next**.
10. On the Deployment options page, do the following:
    a. In **Network mappings**, click the required network.
    b. In **Disk provisioning**, select the required disk format.

c. From **Deployment type**, select profile.

d. Uncheck **Power on automatically**.

11. Click **Next**.
12. On the Additional settings page, click **Next**.
13. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
14. To edit the virtual machine settings, click the VM radio option and perform the following:
    - Click **Actions** > **Edit Settings** to edit the required parameters.

      Note:
    - Click **Save** to save the reservation changes.

    Note:

    Ensure that the virtual machine is powered down to edit the settings.
15. To ensure that the virtual machine automatically starts after a hypervisor reboot, click the VM radio option, and click **Actions** > **Autostart** > **Enable**.

    Note:

    If you do not enable autostart, manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.
16. To start the System Manager virtual machine, if System Manager is not already powered on do one of the following steps:
    - Click VM radio option, and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.

    When the system starts for the first time, configure the parameters for System Manager. For more information about the configuration and network parameters, see Network and configuration field descriptions on page 148.
17. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the System Manager configuration parameters.

Next steps

From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file. Once the configuration is complete, the log file displays the following message: `SMGR Post installation configuration is completed`

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.

- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Network and configuration field descriptions

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application for Out of Band Management. This field is an optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager application.
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. This field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. This field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. This field is optional.
Default Search List	The search list of domain names. This field is optional.

Table continues…

Name	Description
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. This field is optional. Separate the IP addresses with commas (,). This field is not applicable for software-only deployment. The application supports only the NTP server. It does not support the NTP pool.
Time Zone	The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country. This field is not applicable for the software-only deployment.

Note:

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager application. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager application. The field is optional.
Public FQDN	The FQDN to assign to the System Manager application. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager application. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.

Table continues…

Name	Description
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.

Table continues…

Name	Description
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Out of Band Management	The port number that you must assign to the Out of Band Management port group. The field is mandatory.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description

Table continues…

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

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using vSphere Client (HTML5).
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

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

Data Encryption

Note:

Data Encryption is supported only for Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware Virtualized Environment.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

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. • **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.

Configuring the network parameters from the vSphere console

Before you begin

- Deploy the System Manager virtual machine OVA.
- Start the System Manager virtual machine.

  If the **Power on after deployment** check box is clear during deployment, you must manually start the virtual machine.
- To reach the System Manager command-line interface, start vSphere Web Client and click the **Console** tab or the  icon.

About this task

When first started, System Manager virtual machine collects the network parameters. Enter the network parameters at the system prompt when first started.

Procedure

1. At the prompt, enter the management network parameters, public network parameters, virtual FQDN parameters, SMGR CLI User parameters, and SNMPv3 parameters of the System Manager virtual machine.

   For information about the configuration and network parameters, see “VM Deployment field descriptions”.
2. To schedule the remote backup during the System Manager installation, in **Schedule SMGR Backup**, type the backup definition parameters for the System Manager virtual machine.

   For information, see “Backup Definition parameters”.

If you do not schedule a System Manager backup every 7 days, System Manager generates an alarm.

3. At the Data Encryption prompt, perform one of the following:
   - To enable data encryption, type `1`.
   - To disable data encryption, type `2`.
4. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

   Enable: (Recommended)

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

   Disable:

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

   a. 1: To enable EASG.

      Avaya recommends to enable EASG.

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

   b. 2: To disable EASG.
5. To confirm the network parameters, type `Y`.

   System Manager starts the configuration of the network parameters.

   From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file. Once the configuration is complete, the log file displays the following message: `SMGR Post installation configuration is completed`

Next steps

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.

- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Backup Definition parameters

Use the backup definition to schedule remote backup during the System Manager installation.

Note:

You can skip the configuration of the backup definition parameters to schedule the backup jobs later.

The backup time must be 6 hours later than the System Manager installation time.

If you set the **Backup Start Month** field to 5, **Backup Start Day** field to 24, and **Repeat Type** field to Weekly, the system executes the backup job every Friday if May 24th is a Friday.

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.

Table continues…

Name	Description
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • Hourly • Daily • Weekly • Monthly
Backup Frequency	The frequency of the backup taken for the selected backup type. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Virtual machine migration from one host to another host

When a user moves a virtual machine from one host to another host, the system displays the entry of the virtual machine on both the hosts until the user explicitly refreshes the old host. Also, if the user refreshes the new host before refreshing the old host, the system displays the entry of the virtual machine on both the hosts. This results in displaying duplicate entries of virtual machines. If trust is already established, you can also view the duplicate entries of virtual machines under the System Manager inventory.

To remove the duplicate entry of virtual machine, refresh the old host.

changeIPFQDN command

Use the **changeIPFQDN** command to change the Management IP address when Out of Band Management is enabled. With this command, you can change the IP address, FQDN, DNS address, Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address. You can also use this command to enable or configure to IPv4 or IPv6 network details.

Note:

On the System Manager Release 7.1 and later, if you change the IP Address of System Manager using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidates the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.

To change the Public IP address when Out of Band Management is enabled, use the **changePublicIPFQDN** command.

Syntax

```
changeIPFQDN -IP < >  -FQDN < > -GATEWAY < >-NETMASK < > -DNS < > -SEARCH < >-IPV6 < >
-IPV6GW < >-IPV6PREFIX < >
```

#	Option	Description	Usage
1	IP	The new Management IPv4 address of System Manager.	**changeIPFQDN -IP 10.11.12.13**
2	FQDN	The new Management FQDN of System Manager.	**changeIPFQDN -FQDN a.mydomain.smgr.com**
3	GATEWAY	The new Management Gateway IPv4 address of System Manager.	**changeIPFQDN -GATEWAY 10.11.1.1**
4	NETMASK	The new Management netmask address of System Manager.	**changeIPFQDN -NETMASK 255.255.203.0**
5	DNS	The new Management DNS address of System Manager. You can provide multiple DNS addresses. Separate each address by a comma.	**changeIPFQDN -DNS 10.11.1.2** **changeIPFQDN -DNS 10.11.12.5,10.11.12.3**
6	SEARCH	The new search list of domain names.	**changeIPFQDN -SEARCH smgr.com**
7	IPV6	The new Management IPv6 address of System Manager.	**changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080**
8	IPV6GW	The new Management Gateway IPv6 address of System Manager.	**changeIPFQDN -IPV6GW 2001:b00d::1**
9	IPV6PREFIX	The new Management netmask prefix of System Manager. The default value is 64.	**changeIPFQDN -IPV6PREFIX 64**

Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK
255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

```
changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080 -IPV6GW 2001:b00d::1
-IPV6PREFIX 64
```

Rebooting the System Manager virtual machine through command-line interface

About this task

When you start the reboot process, you cannot access the System Manager web console.

Important:

If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.

Procedure

1. Log in to the System Manager command-line interface.
2. Type **`rebootVM`** and press **Enter**.
3. At the **Do you want to continue ? .. (Yes/No)** prompt, type **Yes** and press **Enter**.

   System Manager starts the reboot process.

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	**changeIPFQDN**	• **-IP <new Management interface or Out of Band Management IP address for System Manager>** • **-FQDN <new Management or Out of Band Management fully qualified domain name for System Manager>** • **-GATEWAY <new Management interface or Out of Band Management Gateway address for System Manager>** • **-NETMASK <new Management interface or Out of Band Management netmask address for System Manager>** • **-DNS <new DNS address for System Manager>** • **-SEARCH <new search list for DNS address>**	Updates the existing Management interface or Out of Band Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value. **Note:** On the System Manager Release 7.1 and later, if you change the IP Address of System Manager using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidates the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.	• **changeIPFQDN -IP <new IP address>** • **changeIPFQDN -FQDN <new fully qualified domain name>** • **changeIPFQDN -IP <new IP address> -GATEWAY <new Gateway address for System Manager> -SEARCH <new search list for DNS address>**

Table continues…

#	Command	Parameters	Description	Usage
2	**changePublicIPFQDN**	• **-publicIP <new IP address for System Manager>** • **-publicFQDN <new fully qualified domain name for System Manager>** • **-publicGATEWAY <new Gateway address for System Manager>** • **-publicNETMASK <new netmask address for System Manage>**	Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.	• **changePublicIPFQDN -publicIP <new Public IP address>** • **changePublicIPFQDN -publicFQDN <new fully qualified domain name for public interface>** • **changePublicIPFQDN -publicIP <new Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>**
3	**upgradeSMGR**	**<absolute path to the dmutility.bin> -m –v**	Upgrades System Manager using the data migration utility.	**upgradeSMGR dmutility *.bin -m –v**
4	**SMGRPatchdeploy**	**<absolute path to the System Manager service pack or the software patch>**	Installs the software patch or the service pack for System Manager.	**SMGRPatchdeploy <absolute path to SMGRservicepackName>** **Note:** Copy the System Manager service pack or patches that you must install to `/swlibrary`.
5	**configureTimeZone**	**Time zone that you select**	Configures the time zone with the value that you select.	**configureTimeZone** **Select a time zone. For example, America/Denver**

Table continues…

#	Command	Parameters	Description	Usage
6	**configureNTP**	**<IP address of NTP server>**	Configures the NTP server details.	**configureNTP <IP address of NTP server>** Separate IP addresses or hostnames of NTP servers with commas (,).
7	**createCA**		Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size. For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	**createCA** You must provide the desired Common Name (CN)
8	**configureOOBM**		Enables or disables the Out of Band Management configuration.	• To enable Out of Band Management: **configureOOBM –EnableOOBM** • To disable Out of Band Management: **configureOOBM -DisableOOBM**
9	**enableOOBMMultiTenancy**		If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.	
10	**setSecurityProfile**		Enabling the commercial and military grade hardening.	• Enabling commercial grade hardening: **setSecurityProfile --enable-commercial-grade** • Enabling military grade hardening: **setSecurityProfile --enable-military-grade**

Table continues…

#	Command	Parameters	Description	Usage
11	**EASGManage**		Enables or disables EASG.	• **EASGManage --enableEASG** • **EASGManage --disableEASG**
12	**EASGStatus**		Displays the status of EASG.	
13	**EASGProductCert**		Displays the EASG certificate details.	**EASGProductCert --certInfo**
14	**EASGSiteCertManage**		To manage EASG Certificates.	
15	**editHosts**		To add, replace, and delete the IP Address, FQDN, or hostname entries in the `/etc/hosts` file.	
16	• **swversion** • **swversion -s**		• swversion: Displays the System Manager software information. • swversion -s: Displays the System Manager software version and also displays information about the application name, profile, and deployment type. • **Note:** The output varies based on the application deployment and the virtualization environment.	

Table continues…

#	Command	Parameters	Description	Usage
17	**changeVFQDN**		To change the System Manager Virtual FQDN.	**changeVFQDN** Type the System Manager Virtual FQDN. **Note:** When you run the **changeVFQDN** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.

Table continues…

#	Command	Parameters	Description	Usage
18	**pairIPFQDN**		Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode.	• If you changed both the IP address and FQDN of primary server, type the following on the secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server> -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>` • If you changed the IP address of primary server, type the following on secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server>` • If you changed FQDN of primary server, type the following on secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of`

Table continues…

#	Command	Parameters	Description	Usage
				the primary server> -NEWFQDN <New FQDN of the primary server>
19	**smgr**		Starts, stops, and checks the status of the Application server.	**smgr** start/stop/status
20	**smgr-db**		Starts, stops, and checks the status of postgresql.service.	**smgr-db** start/stop/status
21	**getUserAuthCert**		Generates a user specific certificate for System Manager to facilitate certificate-based authentication.	
22	**changeCipherSuiteList**		Configures cipher suite mode for System Manager	• To configure strict cipher suite list, type the following command. This would disable CBC ciphers: **changeCipherSuiteList LIST2** • To configure relax cipher suite list, type the following command. This would enable CBC ciphers: **changeCipherSuiteList LIST1**
23	**collectLogs**		Collects the required logs.	• To collect all the logs: **collectLogs** • To collect all the logs along with backup: **collectLogs -Db** • To collect all the logs along with CND data: **collectLogs -CND**

Table continues…

#	Command	Parameters	Description	Usage
24	**rebootVM**		Reboots the System Manager virtual machine. **Important:** If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.	Type `y` or `n` to reboot the System Manager virtual machine.
25	**powerOffVM**		Power off the System Manager virtual machine.	Type `y` or `n` to power off the System Manager virtual machine.
26	sudo /bin/ systemctl (parameter) snmpd	start/stop/restart/status	To start or stop, and to check status of the SNMP service.	
27	sudo /bin/ systemctl (parameter) spiritAgent	start/stop/restart/status	To start or stop, and to check status of the Spirit Agent service.	

Table continues…

#	Command	Parameters	Description	Usage
28	sudo /bin/ systemctl (parameter) cnd	start/stop/restart/status	To start or stop, and to check status of the CND service.	
29	encryptionPassphrase	[add | change | remove | list]	To add, change, remove, and display the encryption passphrase.	• **encryptionPassphrase add**: To add encryption passphrase. • **encryptionPassphrase change**: To change existing encryption passphrase. • **encryptionPassphrase remove**: To remove encryption passphrase. • **encryptionPassphrase list**: To display the encryption passphrase and slot assignment.
30	encryptionRemoteKey	[add | remove | list]	To add, remove, and display the remote key server.	• **encryptionRemoteKey add**: To add remote key server. • **encryptionRemoteKey remove**: To remove remote key server. • **encryptionRemoteKey list**: To display the remote key server and slot assignment.
31	encryptionLocalKey	[enable | disable]	To enable and disable the local key store.	• **encryptionLocalKey enable**: To enable local key store. • **encryptionLocalKey disable**: To disable local key store.

Table continues…

#	Command	Parameters	Description	Usage
32	encryptionStatus		Displays information about encryption on the system.	**encryptionStatus** displays information about encryption on the system.
33	**updateLogRetention.sh**	[-p] [-v] [maxRetentionTime]	Manages the log retention time.	
34	**pruneAllLogs.sh**	[-b] [-t] [-v] [-h] [maxRetentionTime]	Manages the deletion of log files.	
35	**manageEntityClassWhitelist**	[-h] [addAll *-e* <ENTITY_CLASS_NAME> *-f* <INPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [add *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [list *-e* <ENTITY_CLASS_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD> *-pn* <PAGENUMBER> *-ps* <PAGESIZE>] [view *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [subjectCheck *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [deleteAll *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [delete *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>]	You can add, list, view, and delete the subject names for the provided entity class. You can add and delete the bulk entries of subject names and check the status of the subject name validation for the entity class.	
36	**outboundConnectionLogging**	[enable] [disable]	If you enable this, you can capture the logs in the `/var/log/Avaya/connections` file for every new outgoing connections initiated from System Manager.	

Table continues…

#	Command	Parameters	Description	Usage
37	**configureOutboundFirewall**	[add {*-s*} {*-f*}] [list] [status] [remove {*-e*} {*-f*}] [disable] [overwrite {*-s*} {*-f*}] [enable-logging] [disable-logging] [logging-status]	If you enable this, you can configure System Manager outbound firewall.	
38	**setSecurityPolicy**	[--status] [--display-only] [--restore-standard] [--refresh-custom]	You can modify the default password policy settings of System Manager by using the **setSecurityPolicy** command. This command is only applicable for changing or setting up the password for the CLI user or root user that gets created at the time of deployment.	
39	**configureSyslog**	-h [-e] [-s <*syslog server destination*> ""]	You can configure, list, and delete the remote syslog server by using the **configureSyslog** command.	
40	**ASP_SSH**	[enable] [status]	If System Manager is deployed on the Avaya Solutions Platform 130 Release 5.1 host, you can enable SSH and check the SSH status of the Avaya Solutions Platform 130 host.	

Chapter 14: Resources

System Manager documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Select Release**, select the appropriate release number.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
9. Press **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list

8. In **Choose Release**, select the required release number.
9. 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.
10. Press **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 you login to the website, enter the course code or the title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
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 keyword or keywords 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 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.

Related links

Using the Avaya InSite Knowledge Base on page 176

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 https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.

4. Enter your **PASSWORD** and click **Sign On**.

   The system displays the Avaya Support page.
5. Click **Support by Product** > **Product-specific Support**.
6. In **Enter Product Name**, enter the product, and press `Enter`.
7. Select the product from the list, and select a release.
8. Click the **Technical Solutions** tab to see articles.
9. Select **Related Information**.

Related links

Support on page 176

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 CLI:** During migration, you need use the data migration utility. • **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.
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

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W