Upgrading Avaya Aura® System Manager
Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter(evt=GenericDetails detailId=C2009112312456651010) under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

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

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

License types

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

Heritage Nortel Software

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

© 2019-2020, Avaya Inc. All Rights Reserved.
Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Hosted Service, or hardware provided by Avaya. All content on this site, the materials on this site, the Documentation, Software, Hosted Service, or otherwise, any license or right in and to the Marks without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. This PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

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

Chapter 1: Introduction .......................................................................................................................................................... 10
  Purpose.................................................................................................................................................................................. 10
  Prerequisites........................................................................................................................................................................... 10
  Change history....................................................................................................................................................................... 11

Chapter 2: Upgrade overview and considerations .................................................................................................................. 13
  Upgrade overview.................................................................................................................................................................... 13
  Data migration utility............................................................................................................................................................... 13
  Supported upgrade paths for System Manager ................................................................................................................. 14

Chapter 3: Planning and preconfiguration ........................................................................................................................................ 16
  Prerequisites for upgrading System Manager .................................................................................................................. 16
  Upgrade worksheet................................................................................................................................................................ 17
  Supported servers.................................................................................................................................................................... 17
  Supported servers for Avaya Aura® applications................................................................................................................ 18
  Supported hardware for VMware............................................................................................................................................ 18
  Software requirements.............................................................................................................................................................. 19
  Supported ESXi version........................................................................................................................................................... 19
  Latest software updates and patch information..................................................................................................................... 19
  Upgrade order for Avaya components.............................................................................................................................. 20
  Software details of System Manager..................................................................................................................................... 22
  Customer configuration data for System Manager............................................................................................................ 22
  Supported footprints for System Manager on Appliance Virtualization Platform........................................................ 23
  Supported footprints for System Manager on VMware..................................................................................................... 24
  Supported footprints for System Manager on KVM................................................................................................................ 25
  Supported footprints for the System Manager on AWS....................................................................................................... 25
  System capacities for applications.......................................................................................................................................... 26

Chapter 4: Preupgrade tasks ....................................................................................................................................................... 27
  Installing the Solution Deployment Manager client on your computer............................................................................... 27
  Accessing the Solution Deployment Manager client dashboard........................................................................................ 29
  Accessing Solution Deployment Manager........................................................................................................................ 30
  Refreshing elements................................................................................................................................................................. 30
  Analyzing software................................................................................................................................................................. 31
  Verifying the current software version.................................................................................................................................. 31
  Creating a data backup on a remote server.......................................................................................................................... 32
  Upgrading VMware ESXi version............................................................................................................................................ 33
  Creating the System Manager virtual machine snapshot.................................................................................................. 34
  Virtual machine management................................................................................................................................................... 35
    Application management........................................................................................................................................................ 35
    Managing the location............................................................................................................................................................ 35
    Managing the host................................................................................................................................................................. 38

August 2020

Upgrading Avaya Aura® System Manager

Comments on this document? infodev@avaya.com
Implementing the cold standby procedure on another computer................................. 148

Chapter 14: Post-upgrade Verification............................................................................. 149
Post-upgrade checklist.................................................................................................. 149
Verifying the functionality of System Manager.............................................................. 150
Installing software patches.......................................................................................... 151
Edit Upgrade Configuration field descriptions............................................................ 153
Creating a Snapshot restore......................................................................................... 160
Third-party certificate for upgrades............................................................................ 160
  Using third-party certificates while upgrading from System Manager Release 6.3.x, 7.0.x or 8.0.x.  160
  Using third-party certificates while upgrading from System Manager Release 6.2.x or earlier.  161
License management...................................................................................................... 162
  Finding LAC for System Manager in PLDS................................................................. 162
  Installing a license file............................................................................................... 162
  Install license field descriptions................................................................................ 163
Installing language pack on System Manager.............................................................. 163
Deleting the virtual machine snapshot........................................................................ 164
  Deleting the virtual machine snapshot from the Appliance Virtualization Platform host.  164
  Deleting the virtual machine snapshot from the vCenter managed host or standalone host..  165
Enhanced Access Security Gateway overview............................................................ 165
  Enhanced Access Security Gateway (EASG) overview............................................. 165

Chapter 15: Maintenance............................................................................................... 168
Backup and restore the System Manager data............................................................... 168
  Creating a data backup on a remote server.............................................................. 168
  Creating a data backup on a local server................................................................. 169
  Restoring a backup from a remote server............................................................... 170
  Restoring data backup from a local server............................................................. 171
Backup and Restore field descriptions........................................................................ 172
Common upgrade procedures...................................................................................... 173
  Methods of System Manager deployment.............................................................. 173
  Deploying System Manager in Virtualized Environment.......................................... 174
  Virtual machine migration from one host to another host.................................... 188
  changelPFQDN command....................................................................................... 188
  Installing the System Manager service pack or patch from CLI............................. 191
  System Manager command line interface operations............................................ 192

Chapter 16: Resources................................................................................................. 200
System Manager documentation.................................................................................. 200
  Finding documents on the Avaya Support website................................................ 201
  Accessing the port matrix document....................................................................... 201
  Avaya Documentation Portal navigation.............................................................. 202
Training....................................................................................................................... 203
Viewing Avaya Mentor videos.................................................................................... 203
Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® System Manager from Release 6.3.x, 7.x, and 8.0.x to Release 8.1.2 on:

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

This document:

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

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

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

Skills
To administer:
• Solution Deployment Manager
• VMware® vSphere™ virtualized environment
• KVM hypervisor
• AWS Management Console
• Google cloud
• Microsoft Azure

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

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>August 2020</td>
<td>Added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upgrading the data from non-file encryption System Manager to file system encryption System Manager in the Geographic Redundancy setup on page 59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updating the System Manager Release 8.1 or 8.1.1 to Release 8.1.2 in the Geographic Redundancy setup on page 124</td>
</tr>
<tr>
<td>7</td>
<td>May 2020</td>
<td>Added the section: Updating the System Manager Release 8.1 or 8.1.1 to Release 8.1.2 on page 123</td>
</tr>
<tr>
<td>6</td>
<td>March 2020</td>
<td>For Release 8.1.2, added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Encryption on page 57</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upgrading the data from non-file encryption System Manager Release 8.1 or 8.1.1 to file system encryption System Manager Release 8.1.2 on page 58</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>October 2019</td>
<td>For Release 8.1.1, added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Supported ESXi version</a> on page 19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Upgrading VMware ESXi version</a> on page 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Release 8.1.1, updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Data migration utility</a> on page 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Supported upgrade paths for System Manager</a> on page 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 7.x or 8.0.x to Release 8.1.2 by using the Solution Deployment Manager client</a> on page 63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Upgrading to System Manager Release 8.1.2 from CLI</a> on page 120</td>
</tr>
<tr>
<td>4</td>
<td>August 2019</td>
<td>Updated the <a href="#">Supported upgrade paths for System Manager</a> on page 14 section.</td>
</tr>
<tr>
<td>3</td>
<td>July 2019</td>
<td>Updated the <a href="#">Data migration utility</a> on page 13 section.</td>
</tr>
<tr>
<td>2</td>
<td>June 2019</td>
<td>Added the <a href="#">Accessing the port matrix document</a> on page 201 section.</td>
</tr>
<tr>
<td>1</td>
<td>June 2019</td>
<td>Release 8.1 document.</td>
</tr>
</tbody>
</table>
Chapter 2: Upgrade overview and considerations

Upgrade overview

The document provides the procedures for upgrading Avaya Aura® System Manager from Release 6.x, 7.x, or 8.0.x to System Manager Release 8.1.2.

🌟 Note:

When upgrading to System Manager Release 8.1.2 on VMware, the VMware ESXi version must be 6.0, 6.5, or 6.7.

- Use the Solution Deployment Manager client Release 8.1.2 to upgrade System Manager to Release 8.1.2 from the following:
  - System Manager Release 7.x or 8.0.x running on VMware in customer-provided Virtualized Environment to latest version of System Manager on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
  - System Manager Release 7.x or 8.0.x running on VMware in customer-provided Virtualized Environment or on Appliance Virtualization Platform to latest version of System Manager on Software-only environment.

Data migration utility

Use the data migration utility to migrate the backup data of System Manager Release 6.x, 7.x, and 8.0.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 6.3.x to Release 7.x
- Release 6.3.x to Release 8.x
- Release 7.0.x to Release 7.1.x
- Release 7.0.x to Release 8.x
• Release 7.1.x to Release 8.x
• Release 8.0.x to Release 8.1

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”.

• Import System Platform data and the Services VM data.

---

**Supported upgrade paths for System Manager**

The following table displays all the upgrade paths from earlier releases to Release 8.1.x.

**Note:**

• Before starting the application upgrade, upgrade the platform and hypervisor.

• For upgrading System Manager, use Solution Deployment Manager Client. For upgrading applications other than System Manager, use System Manager Solution Deployment Manager.

• Upgrade or migration using Solution Deployment Manager is only supported with same IP Address of the application in Software-only environment.

  Software-only upgrade is supported for VMware, KVM, Nutanix, RHVH, OpenStack, Hyper-V, AWS, GoogleCloud, and Azure.

• If the application supports the upgrade by using Solution Deployment Manager, you can also use the CLI for upgrading that application.

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

<table>
<thead>
<tr>
<th>From offer</th>
<th>From Release</th>
<th>To Software-only 8.1.x (ISO)</th>
<th>To AVP 8.1.x (OVA)</th>
<th>To VMware 8.1.x (OVA)</th>
<th>To AWS 8.1.x (OVA)</th>
<th>To KVM/ OpenStack/ Nutanix/RHVH 8.1.x (OVA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVP</td>
<td>7.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
</tr>
</tbody>
</table>
## Supported upgrade paths for System Manager

<table>
<thead>
<tr>
<th>From offer</th>
<th>From Release</th>
<th>To Software-only 8.1.x (ISO)</th>
<th>To AVP 8.1.x (OVA)</th>
<th>To VMware 8.1.x (OVA)</th>
<th>To AWS 8.1.x (OVA)</th>
<th>To KVM/OpenStack/Nutanix/RHVH 8.1.x (OVA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>8.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td>6.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>7.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>7.1.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>8.0.x</td>
<td>Migration using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Fully automated upgrade using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>KVM</td>
<td>7.1.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>8.0.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>Software-only 8.0.x</td>
<td>Migration using SDM</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>AWS</td>
<td>7.1.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>8.0.x</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
<tr>
<td>System Platform 6.x</td>
<td>Migration using SDM</td>
<td>Migration using SDM</td>
<td>Migration using SDM</td>
<td>Migration using CLI</td>
<td>Migration using CLI</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3: Planning and preconfiguration

Prerequisites for upgrading System Manager

General prerequisites

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

System prerequisites

- Verify that the existing server is compatible with System Manager Release 8.1.2. If the existing server is incompatible, change the server.
  For information, see Supported servers on page 17.
- Verify that the ESXi version is compatible with System Manager Release 8.1.2. If the existing ESXi version is incompatible, upgrade to supported ESXi version.
  For information, see Supported ESXi version on page 19.

Geographically redundant System Manager prerequisites

- You can update the primary and secondary System Manager servers in any order. However, you should not update the primary and secondary System Manager servers simultaneously.
  At a time, install the patch on one server.
- Activate the secondary System Manager server only after installing the patch.
For activating the secondary System Manager server, the primary and secondary System Manager servers must be on the same release and patch version.

- You must take the snapshot only after disabling the Geographic Redundancy replication.

---

### Upgrade worksheet

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

<table>
<thead>
<tr>
<th>#</th>
<th>Field</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP address of external device for remote backup</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>User Name and Password of the remote server</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>System Manager command line interface credential</td>
<td></td>
<td>Open an SSH session and login with the user who has administrator privileges.</td>
</tr>
<tr>
<td>4</td>
<td>Path and the file name of the backup file on the remote server</td>
<td></td>
<td>Enter the path and the file name of the backup file.</td>
</tr>
<tr>
<td>5</td>
<td>Check the server time and time zone before running the Data Migration utility tool to upgrade System Manager.</td>
<td></td>
<td>This step ensures that the time is properly synced with kernel and OS RPMs and prevents upgrade failure.</td>
</tr>
</tbody>
</table>

---

### Supported servers

The following servers are supported for deployments and upgrades to Release 8.1 and later:

- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9
- S8300E, for Communication Manager and Branch Session Manager
• Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640
• Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640

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

For fresh installations, use Avaya Solutions Platform 120 Appliance or 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.

<table>
<thead>
<tr>
<th>Supported servers</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>S8300D</td>
<td>Y</td>
</tr>
<tr>
<td>S8300E</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360 G7</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360p G8</td>
<td>Y</td>
</tr>
<tr>
<td>HP ProLiant DL360 G9</td>
<td>Y</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R610</td>
<td>Y</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R620</td>
<td>Y</td>
</tr>
<tr>
<td>Dell™ PowerEdge™ R630</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640</td>
<td></td>
</tr>
</tbody>
</table>

Note:
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 [http://www.vmware.com/resources/guides.html](http://www.vmware.com/resources/guides.html).
Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 8.1.x
- Customer-provided Virtualized Environment offer supports the following software versions:
  - VMware® vSphere ESXi 6.0, 6.5, or 6.7
  - VMware® vCenter Server 6.0, 6.5, or 6.7


Note:

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

Supported ESXi version

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

<table>
<thead>
<tr>
<th>ESXi version</th>
<th>Avaya Aura® Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.0.x</td>
</tr>
<tr>
<td>ESXi 5.0</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 5.1</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 5.5</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 6.0</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 6.5</td>
<td>Y</td>
</tr>
<tr>
<td>ESXi 6.7</td>
<td></td>
</tr>
</tbody>
</table>

Note:

- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration.
- Avaya Aura® applications support the ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 6.7 can be VMware ESXi 6.7 Update 3.

Latest software updates and patch information

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

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

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

---

**Upgrade order for Avaya components**

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

1. **Hard Endpoints (H.323 and SIP)**
   
   You can upgrade endpoints after all Avaya Aura® Platform components are upgraded.

2. **Standalone Avaya WebLM**

3. **Avaya Aura® Appliance Virtualization Platform that hosts System Manager**
   
   Appliance Virtualization Platform of individual components must be upgraded first.
   
   **Note:**
   
   - If you are upgrading Avaya Aura® Appliance Virtualization Platform from Release 7.x to 8.x, Solution Deployment Manager also upgrades Utility Services to AVP Utilities during the Avaya Aura® Appliance Virtualization Platform upgrade.
   
   - If you are upgrading Avaya Aura® Appliance Virtualization Platform from Release 8.0.x to 8.1.x, you need to manually upgrade AVP Utilities after upgrading Avaya Aura® Appliance Virtualization Platform.

4. **AVP Utilities**

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

6. **Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager**
   
   In the:
   
   - Non-Geography Redundancy setup, update standalone System Manager.
   
   - Geography Redundancy setup, update the primary System Manager.
   
   Avaya recommends that you use System Manager to update Avaya Aura® applications.

7. **Avaya Device Adapter Snap-in on Avaya Breeze® platform**

8. **Avaya Aura® Session Manager (Core Session Managers only)**

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

⚠️ Note:
For S8300E, the Gateway must be on minimum version 33.x.

15. Avaya Aura® Branch Session Manager
16. Avaya Aura® Application Enablement Services
17. Avaya Aura® Communication Manager Survivable Remote Servers (formerly known as Local Survivable Processors)
18. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
19. Avaya Aura® Communication Manager Survivable Core Servers (formerly known as Enterprise Survivable Processors)
20. Avaya Aura® Communication Manager feature servers and evolution servers
   In duplex configuration, update the:
   • Standby Communication Manager server
   • Active Communication Manager server

21. Avaya IP Office™ platform
22. Avaya Aura® Messaging or IX Messaging (formerly known as Avaya IX™ Messaging)
23. Avaya Aura® Web Gateway
24. Equinox Clients
   Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
25. Avaya Equinox® Conferencing
26. Avaya Session Border Controller for Enterprise

⚠️ 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 8.1 before you upgrade Communication Manager to 8.1.

All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.
• Remove the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.
Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 8.1 OVA, Solution Deployment Manager Client version must be on Release 8.1. Solution Deployment Manager Client cannot be on Release 8.0.

• If an application is running on Release earlier than 8.0.x and if it has Utility Services, you must back up Utility Services files and install them on Avaya Aura® Device Services Release 8.0. For migrating data from the legacy Avaya Aura® Utility Services to the Utility Server embedded within Avaya Aura® Device Services Release 8.0, see Administering Avaya Aura® Device Services on the Avaya Support website.

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 of OVA, ISO, service patch, Data migration Utility, or Solution Deployment Manager Client, see Avaya Aura® Release Notes on the Avaya Support website at http://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.

<table>
<thead>
<tr>
<th>Required data</th>
<th>Description</th>
<th>Example Value for the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Management (Out of Band Management) and Public network configuration</td>
<td>172.16.1.10</td>
</tr>
<tr>
<td>Netmask</td>
<td></td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>DNS Server IP address</td>
<td>Configure Public network details only when Out of Band Management is enabled.</td>
<td>172.16.1.2</td>
</tr>
</tbody>
</table>

Table continues…
**Required data** | **Description** | **Example Value for the system** |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Short hostname</td>
<td>If Out of Band Management is not enabled, Public network configuration is optional.</td>
<td>myhost. The host name must be a valid short name.</td>
</tr>
<tr>
<td>Domain name</td>
<td></td>
<td>mydomain.com</td>
</tr>
<tr>
<td>Default search list</td>
<td></td>
<td>mydomain.com</td>
</tr>
<tr>
<td>NTP server</td>
<td></td>
<td>172.16.1.100</td>
</tr>
<tr>
<td>Time zone</td>
<td></td>
<td>America/Denver</td>
</tr>
<tr>
<td>VFQDN short hostname</td>
<td>VFQDN</td>
<td>grsmgr</td>
</tr>
<tr>
<td>VFQDN domain name</td>
<td></td>
<td>dev.com</td>
</tr>
<tr>
<td>User Name Prefix</td>
<td>SNMP Parameters</td>
<td>org</td>
</tr>
<tr>
<td>Authentication Protocol Password</td>
<td></td>
<td>orgpassword</td>
</tr>
<tr>
<td>Privacy Protocol Password</td>
<td></td>
<td>orgpassword</td>
</tr>
<tr>
<td>Backup Definition parameters</td>
<td>See Backup Definition Parameters</td>
<td>-</td>
</tr>
<tr>
<td>EASG status</td>
<td>EASG</td>
<td>Enable or Disable</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>Data Encryption</td>
<td>Enable or Disable</td>
</tr>
</tbody>
</table>

**Note:**
System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.

---

**Supported footprints for System Manager on Appliance Virtualization Platform**

The following table describes the resource requirements to support different profiles for System Manager on Appliance Virtualization Platform Avaya-Appliance offer.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Reserved</td>
<td>6</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>Minimum vCPU Speed</td>
<td>2185 MHz</td>
<td>2185 MHz</td>
<td>2185 MHz</td>
</tr>
<tr>
<td>CPU reservation</td>
<td>13110 MHz</td>
<td>17480 MHz</td>
<td>39330 MHz</td>
</tr>
<tr>
<td>Virtual RAM</td>
<td>12 GB</td>
<td>18 GB</td>
<td>36 GB</td>
</tr>
</tbody>
</table>

*Table continues...*
### Supported footprints for System Manager on VMware

The following table describes the resource requirements to support different profiles for System Manager on VMware customer-provided Virtualized Environment.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Reserved</td>
<td>6</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>Minimum vCPU Speed</td>
<td>2185 MHz</td>
<td>2185 MHz</td>
<td>2185 MHz</td>
</tr>
<tr>
<td>CPU reservation</td>
<td>13110 MHz</td>
<td>17480 MHz</td>
<td>39330 MHz</td>
</tr>
<tr>
<td>Virtual RAM</td>
<td>12 GB</td>
<td>18 GB</td>
<td>36 GB</td>
</tr>
<tr>
<td>Memory reservation</td>
<td>12288 MB</td>
<td>18432 MB</td>
<td>36864 MB</td>
</tr>
<tr>
<td>Virtual Hard Disk</td>
<td>105 GB</td>
<td>250 GB</td>
<td>850 GB</td>
</tr>
<tr>
<td>Shared NICs</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IOPS</td>
<td>44</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>Number of users</td>
<td>&gt;35000 to 250000 users with up to 250 Branch Session Manager and 12 Session Manager</td>
<td>&gt;35000 to 250000 users with up to 500 Branch Session Manager and 28 Session Manager</td>
<td>&gt;35000 to 300000 users with up to 5000 Branch Session Manager and 28 Session Manager</td>
</tr>
</tbody>
</table>

### 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.

- System Manager Release 8.0 and later profile 2 does not support CSR2 Small Appliance Virtualization Platform Server. Therefore, if you are upgrading from System Manager Release 7.1 to Release 8.0 and later on Appliance Virtualization Platform, you must use CSR2 Medium Appliance Virtualization Platform Server. For more information about the Appliance Virtualization Platform CSR2 server types, see Avaya Aura® Communication Manager Hardware Description and Reference.
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 for System Manager on KVM

<table>
<thead>
<tr>
<th>Footprint</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of vCPUs</td>
<td>6</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>RAM (GB)</td>
<td>12</td>
<td>18</td>
<td>36</td>
</tr>
<tr>
<td>HDD (GB)</td>
<td>105</td>
<td>250</td>
<td>850</td>
</tr>
<tr>
<td>NICs</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Number of users</td>
<td>250000</td>
<td>250000</td>
<td>300000</td>
</tr>
</tbody>
</table>

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 for the System Manager on AWS

<table>
<thead>
<tr>
<th>Footprint</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS instance type</td>
<td>m4.2xlarge or higher</td>
<td>m4.2xlarge or higher</td>
<td>m4.4xlarge or higher</td>
</tr>
<tr>
<td>AWS vCPU</td>
<td>8</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>AWS RAM (GB)</td>
<td>32</td>
<td>32</td>
<td>36</td>
</tr>
<tr>
<td>HDD (GB)</td>
<td>Total: 105</td>
<td>Total: 250</td>
<td>Total: 850</td>
</tr>
<tr>
<td></td>
<td>• HDD1: 44</td>
<td>• HDD1: 150</td>
<td>• HDD1: 650</td>
</tr>
<tr>
<td></td>
<td>• HDD2: 25</td>
<td>• HDD2: 30</td>
<td>• HDD2: 30</td>
</tr>
<tr>
<td></td>
<td>• HDD3: 15</td>
<td>• HDD3: 20</td>
<td>• HDD3: 20</td>
</tr>
<tr>
<td></td>
<td>• HDD4: 21</td>
<td>• HDD4: 50</td>
<td>• HDD4: 150</td>
</tr>
<tr>
<td>NICs</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

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

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

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

Procedure


2. On the Avaya Support website, click Support by Products > Downloads, and type the product name as System Manager, and Release as 8.1.x.

3. Click the Avaya Aura® System Manager Release 8.1.x SDM Client Downloads, 8.1.x link. Save the zip file, and extract to a location on your computer by using the WinZip application.

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

4. Right click on the executable, and select Run as administrator to run the Avaya_SDMClient_win64_8.1.2.0.0734476_28.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**.

  **Note:** 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.

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

   You can save the artifacts in the specified directory.

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

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

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

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

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

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

10. Click **Next**.

11. On the Summary and Validation page, verify the product information and the system requirements.
The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the user must make the required disk space, memory, and the ports available to start the installation process again.

12. Click **Install**.

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

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

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

**Next steps**

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

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

---

### Accessing the Solution Deployment Manager client dashboard

**About this task**

⚠️ **Note:**

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

**Procedure**

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

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

- On your desktop, click **SDM Client**.
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 entitled 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, do one of the following:
   • For System Manager Release 6.x, in the upper-right corner of the web console, click the About link.
   • For System Manager Release 6.3.19 and later, in the upper-right corner of the web console, click the settings icon (⚙️), and then click About.
The system displays the About System Manager 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.
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. Deselect 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!!

---

Upgrading VMware ESXi version

About this task

If the ESXi upgrade is required for upgrading System Manager to Release 8.1, use the following procedure to upgrade ESXi to supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 19.

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. Reboot the ESXi host.
5. Exit from the ESXi maintenance mode.
6. Apply the license key for the upgraded ESXi.
7. Power on the System Manager virtual machine and other virtual machines.
9. Launch Solution Deployment Manager Client and perform the following:
   a. Add the ESXi host.
      For information, see Adding an Appliance Virtualization Platform or ESXi host on page 38.
   b. Establish trust with the System Manager virtual machine.
      For information, see Re-establishing trust for Solution Deployment Manager elements on page 47.
c. Upgrade System Manager to Release 8.1.

For information, see Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 7.x or 8.0.x to Release 8.1.2 by using the Solution Deployment Manager client on page 63.

Creating the System Manager virtual machine snapshot

About this task

You can create the snapshot of the System Manager virtual machine using vSphere 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.
Virtual machine management

Application management

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

• Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.

• Supports password change and patch installation of the Appliance Virtualization Platform host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform and ESXi hosts. Also, enables and disables SSH on the host.

• Manages lifecycle of the OVA applications that are deployed on the Appliance Virtualization Platform or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

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 System Manager web console, click Services > Solution Deployment Manager > Application Management.

2. Click the Locations tab.

   The Locations section lists all locations.
Adding a location

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

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

Related links
New and Edit location field descriptions on page 37

Editing the location

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

Related links
New and Edit location field descriptions on page 37

Deleting a location

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. On the Locations tab, in the Locations section, select one or more locations that you want to delete.
3. Click Delete.
4. In the Delete confirmation dialog box, click Yes.
The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

## New and Edit location field descriptions

### Required Location Information

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

### Optional Location Information

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

### Button Description

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

Adding an Appliance Virtualization Platform or ESXi host

About this task

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

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

Note:

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

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

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

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

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. Click Application Management.
3. In Application Management Tree, select a location.
4. On the Platforms tab, in the Platforms for Selected Location <location name> section, click Add.
5. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

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

   b. In Platform Type, select AVP/ESXi.
c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.

6. Click **Save**.

7. In the Certificate dialog box, click **Accept Certificate**.

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

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

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:

   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.

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

      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.

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

   **Important:**

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

9. On the **Platforms** tab, select the required platform and click **Refresh**.

**Next steps**

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

1. In Application Management Tree, establish trust for all the virtual machines that are deployed on the host.

2. Ensure that the system populates the **Application Name** and **Application Version** for each virtual machine.

**Appliance Virtualization Platform license**

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

To configure the Appliance Virtualization Platform license file:

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

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

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

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

- **Normal**: If the Appliance Virtualization Platform host has acquired a license, the License Status column displays Normal.
- **Error**: If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The License Status column displays Error - Grace period expires: <DD/MM/YY> <HH:MM>.
- **Restricted**: If the 30-day grace period of the Appliance Virtualization Platform license expires, the Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The License Status column displays Restricted. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

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

Appliance Virtualization Platform licensing alarms

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

The following table describes the applicable Appliance Virtualization Platform license type for S8300E and Common Server Release 2 and 3:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Avaya S8300E</td>
<td>VALUE_AVP_1CPU_EMBD_SRV</td>
<td>Maximum AVP single CPU Embedded Servers</td>
</tr>
<tr>
<td>Common Server Release 2</td>
<td>• VALUE_AVP_1CPU_CMN_SRV</td>
<td>• Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>• HP ProLiant DL360p G8</td>
<td>• VALUE_AVP_2CPU_CMN_SRV</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td>• Dell™ PowerEdge™ R620</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Server Release 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Dell™ PowerEdge™ R630</td>
<td>VALUE_AVP_XL_SRVR</td>
<td>Maximum AVP XL Server</td>
</tr>
<tr>
<td>• HP ProLiant DL360 G9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Server Release 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Dell™ PowerEdge™ R630</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HP ProLiant DL360 G9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table describes the applicable Appliance Virtualization Platform license type for Avaya Solutions Platform 120 Server:

<table>
<thead>
<tr>
<th>Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 2</td>
<td>VALUE_AVP_1CPU_CMN_SRV</td>
<td>Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>Profile 3</td>
<td>• VALUE_AVP_2CPU_CMN_SRV</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td></td>
<td>• VALUE_AVP_XL_SRVR</td>
<td>• Maximum AVP XL Server</td>
</tr>
<tr>
<td>Profile 4</td>
<td>VALUE_AVP_1CPU_CMN_SRV</td>
<td>Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>Profile 5</td>
<td>• VALUE_AVP_2CPU_CMN_SRV</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td></td>
<td>• VALUE_AVP_XL_SRVR</td>
<td>• Maximum AVP XL Server</td>
</tr>
</tbody>
</table>

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

Before you begin

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

**Procedure**

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

**WebLM Configuration field descriptions**

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

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

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

Shutting down the Appliance Virtualization Platform host

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

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

Restarting Appliance Virtualization Platform or an ESXi host

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. In Application Management Tree, select a location.
3. On the Platforms tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click More Actions > Lifecycle Action > Host Restart.
5. On the confirmation dialog box, click Yes.
   The system restarts the host and virtual machines running on the host.
Removing an Appliance Virtualization Platform or ESXi host

Procedure

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

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

3. Click Remove.

4. On the Delete page, click Yes.

Add and Edit platform field descriptions

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

Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the host information and returns to the Platforms for Selected Location &lt;location name&gt; section.</td>
</tr>
</tbody>
</table>

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

3. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

   The system displays the Edit App section.

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

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

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

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

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

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

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

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

5. Click **Save**.

### Starting an application from Solution Deployment Manager

**Procedure**

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

2. From the **Application Management Tree**, select a platform to which you added applications.

3. On the **Applications** tab, select one or more applications that you want to start.

4. Click **Start**.

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

### Stopping an application from Solution Deployment Manager

**About this task**

System Manager is operational and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. From the Application Management Tree, select a ESXi or vCenter host to which you added applications.
3. On the Applications tab, select one or more applications that you want to stop.
4. Click Stop.
   In Application State, the system displays Stopped.

Restarting an application from Solution Deployment Manager

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

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

Re-establishing trust for Solution Deployment Manager elements

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

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.

7. Enter the user name and password for applications with the following versions:
   - 7.0
   - others

8. 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.

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.

Update Static Routing field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The application name.</td>
</tr>
<tr>
<td>VM IP/FQDN</td>
<td>The IP address or FQDN of the application.</td>
</tr>
<tr>
<td>Utility Services IP</td>
<td>The IP address of AVP Utilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Updates the static IP address for routing.</td>
</tr>
</tbody>
</table>
Reestablish Connection field descriptions

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

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

Virtual machine report

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

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

⚠️ Important:

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

**generate_report.sh command**

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

**Syntax**

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

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

Generating a virtual machine report

**Before you begin**

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

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

   The system displays the following message: Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].

4. To proceed with report generation, type Y, and press Enter.

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

   Note:
   If you re-run the report generation script when the report generation process is in progress, the system displays the following message: Report Generation Process is Already Running, Kindly try after some time.

5. (Optional) To view the logs, go to `/swlibrary/reports/generate_report-YYYYMMDDxxxx.log`.

Viewing the status of the virtual machine report

Procedure

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

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

Abort the virtual machine report generation

About this task

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

Procedure

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

The system aborts the virtual machine report generation process.

---

Managing vCenter

Creating a role for a user

About this task

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

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

Procedure

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

   The system displays the Create Role dialog box.
3. In Role name, type a role name for the user.
4. To provide complete administrative-level privileges, select the All Privileges check box.
5. (Optional) To provide minimum mandatory privileges, do the following.

   a. In All Privileges, select the following check boxes:
      • Datastore
      • Datastore cluster
      • Distributed switch
      • Folder
      • Host profile
      • Network
      • Resource
      • Tasks
      • Virtual machine
      • vApp

   ✳ Note:

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

   Note:
   You must select all the subprivileges under Configuration.

6. Click OK to save the privileges.

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

Adding a vCenter to Solution Deployment Manager

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

Before you begin
Ensure that you have the required permissions.

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager > Application Management.
2. In the lower pane, click Map vCenter.
3. On the Map vCenter page, click Add.
4. In the New vCenter section, provide the following vCenter information:
   a. In vCenter FQDN, type FQDN of vCenter.
      • For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
      • 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 53
- **Map vCenter field descriptions** on page 54
- **New vCenter and Edit vCenter field descriptions** on page 55

**Editing vCenter**

**Before you begin**

Ensure that you have the required permissions.

**Procedure**

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

2. In the lower pane, click **Map vCenter**.

3. On the Map vCenter page, select a vCenter server and click **Edit**.

4. In the Edit vCenter section, change the vCenter information as appropriate.

5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.

6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   
   - Select an ESXi host and click the edit icon (✏).
   - Select one or more ESXi hosts, select the location, click **Bulk Update > Update**.

7. Click **Commit** to get an updated list of managed and unmanaged hosts.

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

Before you begin
Ensure that you have the required permissions.

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

Map vCenter field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vCenter server.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the vCenter server.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The FQDN of the vCenter server.</td>
</tr>
<tr>
<td>License</td>
<td>The license type of the vCenter server.</td>
</tr>
<tr>
<td>Status</td>
<td>The license status of the vCenter server.</td>
</tr>
<tr>
<td>Certificate Status</td>
<td>The certificate status of the vCenter server. The options are:</td>
</tr>
<tr>
<td></td>
<td>• ✔️: The certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>• ❌: The certificate is not accepted or invalid.</td>
</tr>
</tbody>
</table>

Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Displays the certificate status details of the vCenter server.</td>
</tr>
<tr>
<td>Generate/Accept Certificate</td>
<td>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.</td>
</tr>
</tbody>
</table>
### New vCenter and Edit vCenter field descriptions

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

### Managed Hosts

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

Table continues...
Preupgrade tasks

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>The option to edit the location and host.</td>
</tr>
<tr>
<td>Bulk Update</td>
<td>Provides an option to change the location of more than one ESXi hosts.</td>
</tr>
<tr>
<td>Note:</td>
<td>You must select a location before you click Bulk Update.</td>
</tr>
<tr>
<td>Update</td>
<td>Saves the changes that you make to the location or hostname of the ESXi host.</td>
</tr>
<tr>
<td>Commit</td>
<td>Commits the changes that you make to the ESXi host with location that is managed by vCenter.</td>
</tr>
</tbody>
</table>

Unmanaged Hosts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>ESXi Version</td>
<td>Displays the versions of the ESXi host linked to vCenter FQDN.</td>
</tr>
<tr>
<td>Note:</td>
<td>For Release 8.1, do not select the 5.0 and 5.1 versions.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the ESXi host.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>Commit</td>
<td>Saves all changes that you made to vCenter on the Map vCenter page.</td>
</tr>
</tbody>
</table>
Chapter 5: Upgrading from non-encrypted System Manager Release 8.1 or 8.1.1 to encrypted System Manager Release 8.1.2

Data Encryption

Note:

From Release 8.1.2, System Manager supports the file system data encryption feature. This requires a new encryption capable variant of Release 8.1E OVA as prerequisite. The encryption can be enabled only at the time of deploying System Manager 8.1E OVA. Updating from System Manager 8.1 or 8.1.1 to System Manager 8.1.2 with files system encryption requires cold and standby process.

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the Require Encryption Pass-Phrase at Boot-Time check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.
Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the `encryptionRemoteKey` command after the deployment of the application.

**Encryption of System Manager partitions**

When you enable data encryption for System Manager, the system encrypts the following partitions that have personal data.

- `/var/log`
- `/var/log/audit`
- `/var/lib/pgsql/data`
- `/var/opt/nortel/cnd`

---

**Upgrading the data from non-file encryption System Manager Release 8.1 or 8.1.1 to file system encryption System Manager Release 8.1.2**

**About this task**

The procedure describes the steps to upgrade a non-file encryption System Manager Release 8.1 or 8.1.1 to file system encryption System Manager Release 8.1.2.

**Note:**

If you do not want to upgrade to the encrypted file system, you can directly apply the Release 8.1.2 patch on your existing 8.1 or 8.1.1 system.

**Procedure**

1. On the non-file encryption System Manager Release 8.1 or 8.1.1, perform the following:
   a. Apply the Release 8.1.2 patch.
   b. Take remote back up of System Manager.
   c. Shut down System Manager.
2. Deploy the Release 8.1 encryption OVA.
Ensure to enable the data encryption during the deployment.

3. On the encrypted System Manager, apply the System Manager Release 8.1.2 patch.

4. Restore backup using System Manager native restore.

**Next steps**
Install the valid license file for System Manager Release 8.1.x.

---

**Upgrading the data from non-file encryption System Manager to file system encryption System Manager in the Geographic Redundancy setup**

**About this task**
The procedure describes the steps to upgrading a non-file encryption System Manager in the Geographic Redundancy setup to file system encryption System Manager in the Geographic Redundancy setup.

⚠️ **Important:**
From Release 8.1.2 and later, you can upgrade from a non-file encryption System Manager system to file encryption System Manager system.

**Before you begin**
- Download the required OVA and patch files from the Avaya Support website at [http://support.avaya.com/](http://support.avaya.com/) and copy the files to the /swlibrary location on System Manager.
- Calculate the MD5sum of the downloaded files and ensure that it has the same value as given on the Avaya PLDS website.
- You can update the primary and secondary System Manager servers in any order. However, you should not update the primary and secondary System Manager servers simultaneously. At a time, install the patch on one server.
- Activate the secondary System Manager server only after installing the patch.

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

**Procedure**
1. Disable the Geographic Redundancy replication on the primary System Manager server.
   
   For information about disabling Geographic Redundancy replication, see *Administering Avaya Aura® System Manager*.

2. Create the snapshot of the primary and secondary System Manager servers.
   
   This activity might impact the service.

   You must take the snapshot only after disabling the Geographic Redundancy replication.
3. Log in to the System Manager command line interface with CLI user credentials that you created at the time of application deployment.

4. In the non-file encryption System Manager in the Geographic Redundancy setup, do the following:
   a. Apply the Release 8.1.2 patch on the primary System Manager server.
   b. Convert the primary System Manager server that has the patch to the standalone server.
   c. Create remote back up of the primary System Manager server.
      For information, see “Creating a data backup on a remote server”.
   d. Shut down the primary System Manager server.

5. Deploy the primary System Manager server with Release 8.1 encryption OVA.
   Ensure to enable the data encryption during the deployment.

   ! Important:
   Use the same network parameters and system parameters that you recorded on the existing system.

   For information about deploying System Manager, see [Methods of System Manager deployment](#) on page 173.
   Ensure that the System Manager web console is operational.

6. Apply the System Manager Release 8.1.2 patch on the primary System Manager server.
   The patch version installed in Step 4a must match with the patch version installed at this step.

7. Verify the software version of the System Manager application.
   For information, see “Verifying the current software version”.

8. Restore backup using System Manager native restore.
   For information, see “Restoring a backup from a remote server”.

9. Shut down the secondary System Manager server.

10. Deploy the secondary System Manager server with Release 8.1 encryption OVA.
    Ensure to enable the data encryption during the deployment.

11. Apply the System Manager Release 8.1.2 patch on the secondary System Manager server.

12. Configure Geographic Redundancy on the primary and secondary System Manager.
    For information about configuring Geographic Redundancy replication, see [Administering Avaya Aura® System Manager](#).

13. Verify the software version of the System Manager application.
    For information, see “Verifying the current software version”.

14. Perform one of the following:
   • If the patch installation is successful, log off from the system, and remove the snapshot.
     
     Note:
     Snapshots occupy the system memory and degrades 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, 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 at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

Next steps
Install the valid license file for System Manager Release 8.1.x.
Chapter 6: Upgrading from System Manager Release 7.x or 8.0.x to Release 8.1.x on Appliance Virtualization Platform or VMware

Prerequisites

Following are the prerequisites for upgrading System Manager from Release 7.x or 8.0.x to Release 8.1.2.

- 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 6.0 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 System Manager Web Console.
- If System Manager is deployed from the same Solution Deployment Manager client, Current Action Status must be Successful.
Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 7.x or 8.0.x to Release 8.1.2 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 7.x or 8.0.x to System Manager Release 8.1.2.

Note:

If you are upgrading System Manager Release 7.x or 8.0.x to Release 8.1.2 by using the Solution Deployment Manager client then the license files will be retained. However, you need to install the license file for System Manager Release 8.1.x.

Before you begin

• Install Solution Deployment Manager Client.
  For information, see Installing the Solution Deployment Manager client on your computer on page 27.
• Add a location.
  For information, see Adding a location on page 36.
• Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform or ESXi host on page 38.
  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 52.

Important:

- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.
  For information about the supported ESXi version, see Supported ESXi version on page 19.
  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 8.1.x, then deploy Avaya Aura® Appliance Virtualization Platform and AVP Utilities on a supported server on latest release.
  For information about supported servers, see Supported servers for Avaya Aura applications on page 18.
• Select the System Manager 7.x or 8.0.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 47.
• 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 (SDM) 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 7.x or 8.0.x 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 for System Manager on VMware on page 24.
8. Click **Next**.
9. On the **OVA** tab, click one of the following:
   - **URL**, in the **OVA File** field, 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 the **File Name** field, 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**.
   - 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.

   For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

15. Click **Upgrade** and accept the license terms.

   The system takes the backup, shuts down the existing virtual machine, 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.

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 8.1.x.

---

### Upgrade Management field descriptions

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the OVA</td>
<td>The option to select a .ova file of the virtual machine that is available on System Manager.</td>
</tr>
<tr>
<td>OVA file</td>
<td>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. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.</td>
</tr>
<tr>
<td>Submit File</td>
<td>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.</td>
</tr>
<tr>
<td>Flexi Footprint</td>
<td>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 ✔️.</td>
</tr>
<tr>
<td>SMGR Data migration Utility file</td>
<td>The absolute path to the System Manager data migration utility file.</td>
</tr>
<tr>
<td>Note:</td>
<td>Provide the latest data migration bin that is available for the System Manager release.</td>
</tr>
<tr>
<td>Service Pack or Feature Pack</td>
<td>The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see the latest System Manager release notes.</td>
</tr>
</tbody>
</table>

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, timezone, and EASG.

Management Network Settings

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

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. The field is optional.

**IPv6 Network prefix** | The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.

**IPv6 Gateway** | The gateway IPv6 address to assign to the System Manager application. The field is optional.

**Default Search List** | The search list of domain names. The field is optional.

**NTP Server IP/FQDN** | The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).

**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.

### 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Hostname</td>
<td>The virtual hostname of the System Manager application.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td>• The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.</td>
<td></td>
</tr>
<tr>
<td>• VFQDN is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>• By default, VFQDN entry gets added in the /etc/hosts file during installation. Do not remove VFQDN entry from the /etc/hosts file.</td>
<td></td>
</tr>
<tr>
<td>• VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.</td>
<td></td>
</tr>
<tr>
<td>• You must keep VFQDN domain value same as of FQDN domain value.</td>
<td></td>
</tr>
<tr>
<td>• If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.</td>
<td></td>
</tr>
<tr>
<td>• After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:</td>
<td></td>
</tr>
<tr>
<td>1. Log in to System Manager with administrator privilege credentials.</td>
<td></td>
</tr>
<tr>
<td>2. Run the changeVFQDN command.</td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Virtual Domain</td>
<td>The virtual domain name of the System Manager application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3 User Name Prefix</td>
<td>The prefix for SNMPv3 user.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMPv3 User Authentication Protocol Password</td>
<td>The password for SNMPv3 user authentication.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the SNMPv3 user authentication protocol.</td>
</tr>
<tr>
<td>SNMPv3 User Privacy Protocol Password</td>
<td>The password for SNMPv3 user privacy.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you must provide to confirm the SNMPv3 user privacy protocol.</td>
</tr>
</tbody>
</table>

### SMGR CLI USER

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGR command line user name</td>
<td>The user name of the System Manager CLI user.</td>
</tr>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
<tr>
<td>SMGR command line user password</td>
<td>The password for the System Manager CLI user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the System Manager CLI user authentication.</td>
</tr>
</tbody>
</table>

### Backup Definition

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Backup?</td>
<td>• Yes: To schedule the backup jobs during the System Manager installation.</td>
</tr>
<tr>
<td></td>
<td>• No: To schedule the backup jobs later.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you select No, the system does not display the remaining fields.</td>
</tr>
<tr>
<td>Backup Server IP</td>
<td>The IP address of the remote backup server.</td>
</tr>
<tr>
<td>Note:</td>
<td>The IP address of the backup server must be different from the System Manager IP address.</td>
</tr>
<tr>
<td>Backup Server Login Id</td>
<td>The login ID of the backup server to log in through the command line interface.</td>
</tr>
<tr>
<td>Backup Server Login Password</td>
<td>The SSH login password to log in to the backup server from System Manager through the command line interface.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you reenter to log in to the backup server through the command line interface.</td>
</tr>
<tr>
<td>Backup Directory Location</td>
<td>The location on the remote backup server.</td>
</tr>
<tr>
<td>File Transfer Protocol</td>
<td>The protocol that you can use to create the backup. The values are SCP and SFTP.</td>
</tr>
<tr>
<td>Repeat Type</td>
<td>The type of the backup. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Hourly</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
<tr>
<td>Backup Frequency</td>
<td>The frequency of the backup taken for the selected backup type.</td>
</tr>
<tr>
<td></td>
<td>The system generates an alarm if you do not schedule a System Manager backup every seven days.</td>
</tr>
<tr>
<td>Backup Start Year</td>
<td>The year in which the backup must start. The value must be greater than or equal to the current year.</td>
</tr>
<tr>
<td>Backup Start Month</td>
<td>The month in which the backup must start. The value must be greater than or equal to the current month.</td>
</tr>
<tr>
<td>Backup Start Day</td>
<td>The day on which the backup must start. The value must be greater than or equal to the current day.</td>
</tr>
<tr>
<td>Backup Start Hour</td>
<td>The hour in which the backup must start. The value must be six hours later than the current hour.</td>
</tr>
<tr>
<td>Backup Start Minutes</td>
<td>The minute when the backup must start. The value must be a valid minute.</td>
</tr>
<tr>
<td>Backup Start Seconds</td>
<td>The second when the backup must start. The value must be a valid second.</td>
</tr>
</tbody>
</table>

### Enhanced Access Security Gateway (EASG) - EASG User Access

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG</td>
<td>Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• 1: To enable EASG.</td>
</tr>
<tr>
<td></td>
<td>• 2: To disable EASG.</td>
</tr>
<tr>
<td></td>
<td>Avaya recommends to enable EASG.</td>
</tr>
<tr>
<td></td>
<td>You can also enable EASG after deploying or upgrading the application by using the command: EASGManage --enableEASG.</td>
</tr>
</tbody>
</table>
Customer Root Account

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Customer Root Account for this Application</td>
<td>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.</td>
</tr>
<tr>
<td>Customer Root Password</td>
<td>The root password for the application</td>
</tr>
<tr>
<td>Re-enter Customer Root Password</td>
<td>The root password for the application</td>
</tr>
</tbody>
</table>

Data Encryption

Note:

- From Release 8.1.2, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption</td>
<td>Enables or disables the data encryption.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• 1: To enable the data encryption.</td>
</tr>
<tr>
<td></td>
<td>• 2: To disable the data encryption.</td>
</tr>
<tr>
<td></td>
<td>⚠ Important:</td>
</tr>
<tr>
<td></td>
<td>• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• On vCenter or ESXi: When the Data Encryption field is set to 1, enter the encryption passphrase in the Password and Confirm Password fields.</td>
</tr>
<tr>
<td>Encryption Pass-Phrase</td>
<td>This field is applicable when data encryption is enabled.</td>
</tr>
<tr>
<td></td>
<td>The passphrase for data encryption.</td>
</tr>
<tr>
<td></td>
<td>When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.</td>
</tr>
<tr>
<td></td>
<td>When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.</td>
</tr>
<tr>
<td>Re-enter Encryption Pass-Phrase</td>
<td>The passphrase for data encryption.</td>
</tr>
</tbody>
</table>

*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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Out of Band Management IP Address</strong></td>
<td>The IP Address that you must assign to the Out of Band Management port group. The field is mandatory.</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>The port number that you must assign to public port group. The field is optional.</td>
</tr>
</tbody>
</table>

**Button** | **Description** |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upgrade</strong></td>
<td>Displays the EULA acceptance screen. To accept EULA and start the upgrade process, click <strong>Accept</strong>.</td>
</tr>
</tbody>
</table>

---

**Checklist for upgrading System Manager Release 7.x in the Geographic Redundancy setup to Release 8.1.2**

Use the following checklist for upgrading System Manager Release 7.x in the Geographic Redundancy setup to System Manager Release 8.1.2 on Appliance Virtualization Platform.
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>. For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Download the Avaya_SDMClient_win64_8.1.2.0.0734 476_28.zip file from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Verify the software version of the current System Manager.</td>
<td><a href="#">Verifying the current software version</a> on page 31</td>
</tr>
<tr>
<td>4</td>
<td>Disable the Geographic Redundancy replication.</td>
<td><a href="#">See Administering Avaya Aura® System Manager</a></td>
</tr>
<tr>
<td>5</td>
<td>Create a backup of primary System Manager and copy to the remote server.</td>
<td><a href="#">Creating a data backup on a remote server</a> on page 32</td>
</tr>
<tr>
<td>6</td>
<td>Install the Avaya_SDMClient_win64_8.1.2.0.0734 476_28.exe file.</td>
<td><a href="#">Installing the Solution Deployment Manager client on your computer</a> on page 27</td>
</tr>
<tr>
<td>7</td>
<td>If the existing server is not compatible with System Manager Release 8.1.2, change the server to one of the following: • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9 • S8300E, for Communication Manager and Branch Session Manager • Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 • Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640</td>
<td>For more information, see <a href="#">Installing the HP ProLiant DL360p G8 Server</a> or <a href="#">Installing the Dell™ PowerEdge™ R620 Server</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Avaya Aura® Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Avaya Aura® Release 7.0 and later does not support S8510 and S8800 servers.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Add a location.</td>
<td><a href="#">Adding a location</a> on page 36</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Add an Avaya Aura® Appliance Virtualization Platform or ESXi host.</td>
<td>Adding an Appliance Virtualization Platform or ESXi host on page 38</td>
</tr>
<tr>
<td>10</td>
<td>Upgrade to System Manager Release 8.1.2.</td>
<td>Upgrading Appliance Virtualization Platform or VMware-based System Manager Release 7.x or 8.0.x to Release 8.1.2 by using the Solution Deployment Manager client on page 63</td>
</tr>
<tr>
<td>11</td>
<td>Verify that the new System Manager application is functional.</td>
<td>Verifying the functionality of System Manager on page 150</td>
</tr>
<tr>
<td>12</td>
<td>Regenerate licenses from PLDS after migration.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Convert the primary System Manager server that is upgraded to Release 8.1.2 to the standalone server.</td>
<td>The system takes about 30 minutes to convert the primary System Manager server to the standalone server. See Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>14</td>
<td>Create a backup of System Manager and copy to the remote server.</td>
<td>Creating a data backup on a remote server on page 32</td>
</tr>
<tr>
<td>15</td>
<td>Upgrade the secondary System Manager to Release 8.1.2.</td>
<td>-</td>
</tr>
<tr>
<td>16</td>
<td>Configure CRL download on the secondary System Manager server.</td>
<td>See Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>17</td>
<td>Configure Geographic Redundancy on the secondary System Manager server with the details of the primary System Manager server that you converted to standalone.</td>
<td>See Administering Avaya Aura® System Manager. Add the primary System Manager server CA certificate to the secondary System Manager trust store.</td>
</tr>
<tr>
<td>18</td>
<td>On the primary System Manager server, enable the Geographic Redundancy replication.</td>
<td>See Administering Avaya Aura® System Manager.</td>
</tr>
</tbody>
</table>

**Installing service packs and software patches on System Manager by using the 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 (SDM) 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. In **Select bin file from Local SDM Client**, 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**.

---

**Installing the mandatory System Manager Release 8.1.2 patch**

**About this task**

* **Note:**
  After enabling data encryption and installing the System Manager 8.1.2 patch, if the local or remote key store is not enabled, the Data Encrypted server prompts for the encryption passphrase. Once you enter the encryption passphrase, the system automatically reboots. This happens only after first reboot and prompts you to add the encryption passphrase one more time.

**Before you begin**

- Ensure that System Manager is running on Release 8.1.
- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the ![icon](image)
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Download the **System_Manager_R8.1.x_xxxx_manadatoryPatch.bin** file from the Avaya Support website at [http://support.avaya.com/](http://support.avaya.com/) and copy the file to the `/swlibrary` location on System Manager.

**Procedure**

1. Create the snapshot of the System Manager application.
   This activity might impact the service.

2. At the CLI prompt, run the following command:
   ```bash
   SMGRPatchdeploy <absolute path to the bin file>
   ```
   The system displays the license information.

3. 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 kernel is updated.
4. Perform one of the following:
   • If the patch installation is successful, log off from the system, and remove the snapshot.
     ✅ Note:
     Snapshots occupy the system memory and degrades 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, 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 at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to 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 log in, change the System Manager web console credentials.
Chapter 7: Upgrading System Manager through services port using SDM Client

Upgrading Appliance Virtualization Platform through services port

Upgrading Appliance Virtualization Platform from Release 7.x, 8.0.x to Release 8.1.x through services port using Solution Deployment Manager Client

About this task

Use the following procedure to upgrade Appliance Virtualization Platform from Release 7.x to Release 8.0.x through services port by using Solution Deployment Manager Client.

Before you begin

To upgrade from Appliance Virtualization Platform Release 7.x or 8.0.x to 8.1.x, ensure that:

- Appliance Virtualization Platform 7.x or 8.0.x is deployed on the server that is supported with Appliance Virtualization Platform 8.1.x.
- Utility Services 7.x is deployed on Appliance Virtualization Platform Release 7.x and trust is established with the application.

Note:

- If you are upgrading Avaya Aura® Appliance Virtualization Platform from Release 7.x to 8.x, Solution Deployment Manager also upgrades Utility Services to AVP Utilities during the Avaya Aura® Appliance Virtualization Platform upgrade.

Procedure

1. To configure laptop with below configuration for Appliance Virtualization Platform, go to Network or Internet Settings > Ethernet > Local Area Connection > Internet Protocol version 4 (TCP/IPv4) Properties, do the following:
   a. Select the Use the following IP address option.
b. In the **IP address** field, type `192.168.13.5`.

c. In the **Subnet mask** field, type `255.255.255.248`.

d. In the **Default Gateway** field, type `192.168.13.1`

Following is an example for changing the configuration for the Appliance Virtualization Platform host upgrade.

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)

2. Connect the Service port (eth1) of the Appliance Virtualization Platform host with laptop.

   **Important:**

   While connecting through service port, WiFi or any other network must be disconnected. Only Services port connectivity is recommended.

3. Install the latest version of the Solution Deployment Manager client to which you want to upgrade Appliance Virtualization Platform.

4. Launch the Solution Deployment Manager client.

5. Click **Application Management**.

6. In **Application Management Tree**, select a location.

7. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.

8. Add the Appliance Virtualization Platform host with the 192.168.13.6 IP Address on Solution Deployment Manager Client.

   Following is an example of adding the Appliance Virtualization Platform host.
9. For Appliance Virtualization Platform Release 7.x to 8.x upgrade, re-establish trust with Utility Services that is already deployed on the added Appliance Virtualization Platform host 7.x, and do the following:

   a. On the **Applications** tab, in the Applications for Selected Location <location name> area, select Utility Services.

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

If you need to re-establish trust with Utility Services Release 7.0, select the version as 7.0.

Following is an example of re-establishing trust with Utility Services.

![Virtual Machines](image)

Wait for 3 to 5 minutes for trust establishment to complete without any error as shown in below screen shot.
10. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions > AVP Update/Upgrade Management**.

11. On the Update Host page, click **Select patch from local SDM client machine**.

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

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

   For example, the absolute path on your computer can be `C:\tmp\avp\upgrade-avaya-avp-8.x.0.0.0.xx.zip`.

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

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

   **Enable: (Recommended)**

   By enabling Avaya Logins you are granting Avaya access to your system.

   This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

   In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

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

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

   Avaya recommends to enable EASG.

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

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

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

   This step is applicable when you upgrade from Release 7.x to Release 8.x.

   The system displays the Utility Services Upgrade window.

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

   This step is applicable when you upgrade from Release 7.x to Release 8.x.

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

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

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

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

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

   This step is applicable when you upgrade from Release 7.x to Release 8.x.

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

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

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

Host Patching Status

Host Patching Completed ✓

- Host Patching ✓
- Pre update check ✓
- Uploading Patch ✓
- Retrieving Patch Installation Status ✓
- pre-upgrade backup ✓
- Stopping all guest VMs ✓
- Enter Maintenance Mode ✓
- AVP patch installation ✓
- Verifying AVP State ✓
- HOST_REFRESH ✓
- VM-UPGRADE ✓
- Extract OVA ✓

Host Patching Status

Host Patching Completed ✓

- Check resource before host upload
- Prepare OVA file task ✓
- Create Environment File ✓
- Create VM and upload VMDK files task ✓
- Create Environment ISO ✓
- Attach Environment ISO to VM ✓
- Shut Down old VM ✓
- Ready to reconfigure VM ✓
- Starting VM ✓
- Running Status Plugin ✓
- Detach Environment ISO from VM ✓
- Update Service Port Task ✓
- Commit ✓
- Delete Old VM ✓
17. To view the details, in the **Current Action** column, click **Status Details**.

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

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

---

**Upgrading Appliance Virtualization Platform through services port using Solution Deployment Manager Client**

**About this task**

Use the following procedure to update Appliance Virtualization Platform from Release 8.0.x to Release 8.1.x through services port by using Solution Deployment Manager Client.

**Note:**

You can also use this procedure to update Appliance Virtualization Platform from Release 7.0.x to Release 7.1.x through services port by using Solution Deployment Manager Client. However, instances of AVP Utilities must be replaced with Utility Services.

**Procedure**

1. To configure laptop with below configuration for Appliance Virtualization Platform, go to **Network or Internet Settings > Ethernet > Local Area Connection > Internet Protocol version 4 (TCP/IPv4) Properties**, do the following:
   
   a. Select the **Use the following IP address** option.
   
   b. In the **IP address** field, type 192.168.13.5.
   
   c. In the **Subnet mask** field, type 255.255.255.248.
   
   d. In the **Default Gateway** field, type 192.168.13.1

Following is an example for changing the configuration for the Appliance Virtualization Platform host upgrade.
2. Connect the Service port (eth1) of the Appliance Virtualization Platform host with laptop.

**Important:**
While connecting through service port, WiFi or any other network must be disconnected. Only Services port connectivity is recommended.

3. Install the latest version of the Solution Deployment Manager client to which you want to upgrade Appliance Virtualization Platform.

4. Launch the Solution Deployment Manager client.

5. Click **Application Management**.

6. In **Application Management Tree**, select a location.

7. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.

8. Add the Appliance Virtualization Platform host with the 192.168.13.6 IP Address on Solution Deployment Manager Client.

Following is an example of adding the Appliance Virtualization Platform host.
9. For Appliance Virtualization Platform Release 8.0.x to Release 8.1.x update, establish trust with AVP Utilities that is already deployed on the added Appliance Virtualization Platform host.


11. On the Update Host page, click Select patch from local SDM client machine.

12. In Select patch file, provide the absolute path to the upgrade zip file of the host, and click Update Host.

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

   For example, the absolute path on your computer can be C:\tmp\avp\upgrade-avaya-avp-8.x.0.0.0.xx.zip.
13. Check the Appliance Virtualization Platform host update status after 20-25 minutes.

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

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

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

---

**Upgrading System Manager from Release 7.x or 8.0.x to Release 8.1.2 through services port by using Solution Deployment Manager Client**

**About this task**

The procedure describes the steps to upgrade Appliance Virtualization Platform-based System Manager Release 7.x or 8.0.x to System Manager Release 8.1.2.
Note:
If you are upgrading System Manager Release 7.x or 8.0.x to Release 8.1.2 by using the Solution Deployment Manager client then the license files will be retained. However, you need to install the license file for System Manager Release 8.1.2.

Procedure
1. Upgrade Appliance Virtualization Platform and AVP Utilities.
2. Log in to the AVP Utilities CLI with administrative credentials.
3. To check the IP forward status, type the `IP_Forward status` command.
   
   If the IP forward status is disabled, type the `IP_Forward enable` command

   Following is an example of checking the IP forward status and enabling the IP forward status.

   
   ```
   [admin@ve7/vme4 ~]$ IP_Forward status
   Last login: Tue Aug  6 14:23:13 IST 2019 on pva/0
   Customer Root Account is active
   Status of IP Forwarding
   .Disabled
   [admin@ve7/vme4 ~]$ IP_Forward enable
   Last login: Tue Aug  6 14:24:13 IST 2019 on pva/0
   Customer Root Account is active
   Enabling IP Forwarding
   Looking for net.ipv4.ip_forward in /etc/sysctl.conf
   Status of IP Forwarding
   .Enabled
   [admin@ve7/vme4 ~]$]
   ```

4. To configure laptop with below configuration for System Manager, go to Network or Internet Settings > Ethernet > Local Area Connection > Internet Protocol version 4 (TCP/IPv4) Properties, do the following:
   
   a. Select the Use the following IP address option.
   b. In the IP address field, type 192.11.13.5.
   c. In the Subnet mask field, type 255.255.255.252.
   d. In the Default Gateway field, type 192.11.13.6

   Following is an example for changing the configuration for the System Manager upgrade.
5. To re-establish trust with System Manager that is already deployed on the added Appliance Virtualization Platform host, do the following:

   a. On the **Applications** tab, in the Applications for Selected Location <location name> area, select System Manager.

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

If you need to re-establish trust with System Manager Release 7.0, select the version as 7.0.

Following is an example of re-establishing trust with System Manager.
Wait for 3 to 5 minutes for trust establishment to complete without any error as shown in the below screen shot.

6. After re-establishing trust with System Manager, click **Upgrade Management**.
   
   On the Upgrade Management page, the system displays the System Manager virtual machine.

7. On the Upgrade Management page, select the System Manager virtual machine, and then click **Upgrade**.

   The system displays the SMGR Upgrade window.

8. In **Platform FQDN**, select the required host.

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

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

10. Click **Next**.

11. On the **OVA** tab, click one of the following:

    • **URL**, in the **OVA File** field, 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 the **File Name** field, 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**.

When you select the OVA, the system:

• Displays the CPU, memory, and other parameters in the Capacity Details section.
• Disables the **Flexi Footprint** field.

12. 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**.

13. 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**.

14. Click **Next**.

15. 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”.

16. In the Network Parameters section, select the required Public and Out of Band Management network interface details.

   For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

17. Click **Upgrade** and accept the license terms.

   The system takes the backup, shuts down the existing virtual machine, deploys the OVA file, and restores the data on the new virtual machine.
18. 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.

19. 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. Click Commit.

     The system deletes the old virtual machine.

• If the upgrade fails or you want to revert to the old system, click Rollback.

     The system deletes the newly created virtual machine and starts the old virtual machine.
Chapter 8: Upgrading from System Manager Release 6.x to Release 8.1.x on Appliance Virtualization Platform or VMware

Upgrading System Platform-based System Manager Release 6.x to Release 8.1.x on the Avaya-provided server

Prerequisites

If you are upgrading the System Manager system prior to Release 6.3.11 by using the Solution Deployment Manager client, you must take the System Manager native backup from the System Manager Web console before starting the upgrade operation.

⚠️ Note:

When you upgrade System Platform-based System Manager to VMware by using Solution Deployment Manager Client, the system does not retain the license files.

Checklist for upgrading System Platform-based System Manager from Release 6.x to Release 8.1.2

Use the following checklist for upgrading System Platform-based System Manager from Release 6.0.x, 6.1.x, 6.2.x, or 6.3.x to System Manager Release 8.1.2 on Appliance Virtualization Platform:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td></td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
</table>
| 2   | Download the Avaya_SDMClient_win64_8.1.2.0.073_4476_28.zip file from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com). | ![ ](image)
| 3   | Verify the software version of the current System Manager.          | [Verifying the current software version](#) on page 31                     |
| 4   | Create a backup of System Manager and copy to the remote server.   | [Creating a data backup on a remote server](#) on page 32                  |
| 5   | Record the System Platform configuration data such as SAL Gateway configuration. | Use the data to configure the SAL Gateway configuration after deploying the SAL application on Appliance Virtualization Platform. |
| 6   | Record the System Manager FQDN and Time Zone.                      | Use the data while upgrading System Manager.                               |
| 7   | 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. |

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>If the existing server is not compatible with System Manager Release 8.1.2, change the server to one of the following:</td>
<td>- Dell™ PowerEdge™ R620 &lt;br&gt;• HP ProLiant DL360p G8 &lt;br&gt;• Dell™ PowerEdge™ R630 &lt;br&gt;• HP ProLiant DL360 G9 &lt;br&gt;• S8300E, for Communication Manager and Branch Session Manager &lt;br&gt;• Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 &lt;br&gt;• Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640</td>
</tr>
<tr>
<td>9</td>
<td>Install the Avaya_SDMClient_win64_8.1.2.0.073_4476_28.exe file.</td>
<td>Installing the Solution Deployment Manager client on your computer on page 27</td>
</tr>
<tr>
<td>10</td>
<td>For upgrading System Platform to Avaya Aura® Appliance Virtualization Platform, deploy Avaya Aura® Appliance Virtualization Platform on the supported server.</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>Add a location.</td>
<td>Adding a location on page 36</td>
</tr>
<tr>
<td>12</td>
<td>For System Platform-based System Manager, add System Platform in Solution Deployment Manager Client along with System Manager details. For VMware-based System Manager, add ESXi in Solution Deployment Manager Client along with System Manager details.</td>
<td>See Add Element field descriptions on page 113</td>
</tr>
<tr>
<td>13</td>
<td>Add an Avaya Aura® Appliance Virtualization Platform or ESXi host.</td>
<td>Adding an Appliance Virtualization Platform or ESXi host on page 38</td>
</tr>
</tbody>
</table>
### Checklist for upgrading System Platform-based System Manager Release 6.3.x in the Geographic Redundancy setup to Release 8.1.2

Use the following checklist for upgrading System Platform-based System Manager Release 6.3.x in the Geographic Redundancy setup to System Manager Release 8.1.2 on Appliance Virtualization Platform:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Download the Avaya_SDMClient_win64_8.1.2.0.0734 476_28.zip file from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Verify the software version of the current System Manager.</td>
<td>Verifying the current software version on page 31</td>
</tr>
<tr>
<td>4</td>
<td>Disable the Geographic Redundancy replication.</td>
<td>See Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>5</td>
<td>Create a backup of primary System Manager and copy to the remote server.</td>
<td>Creating a data backup on a remote server on page 32</td>
</tr>
<tr>
<td>6</td>
<td>Install the Avaya_SDMClient_win64_8.1.2.0.0734 476_28.exe file.</td>
<td>Installing the Solution Deployment Manager client on your computer on page 27</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>If the existing server is not compatible with System Manager Release 8.1.2, change the server to one of the following:</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• Dell™ PowerEdge™ R620</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HP ProLiant DL360p G8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dell™ PowerEdge™ R630</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HP ProLiant DL360 G9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S8300E, for Communication Manager and Branch Session Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Avaya Aura® Release 8.0 and later does not support S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Avaya Aura® Release 7.0 and later does not support S8510 and S8800 servers.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Add a location.</td>
<td>Adding a location on page 36</td>
</tr>
<tr>
<td>9</td>
<td>For System Platform-based System Manager, add System Platform in Solution Deployment Manager Client along with System Manager details.</td>
<td>See <a href="#">Add Element field descriptions</a> on page 113</td>
</tr>
<tr>
<td></td>
<td>For VMware-based System Manager, add ESXi in Solution Deployment Manager Client along with System Manager details.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Add an Avaya Aura® Appliance Virtualization Platform or ESXi host.</td>
<td><a href="#">Adding an Appliance Virtualization Platform or ESXi host</a> on page 38</td>
</tr>
<tr>
<td>11</td>
<td>Upgrade to System Manager Release 8.1.2.</td>
<td>Upgrading System Platform-based System Manager by using the Solution Deployment Manager client.</td>
</tr>
<tr>
<td>12</td>
<td>Verify that the new System Manager application is functional.</td>
<td><a href="#">Verifying the functionality of System Manager</a> on page 150</td>
</tr>
<tr>
<td>13</td>
<td>Regenerate licenses from PLDS after migration.</td>
<td></td>
</tr>
</tbody>
</table>

*Table continues…*
### Upgrading System Platform-based System Manager to Release 8.1.2 on a different server by using Solution Deployment Manager Client

#### About this task

The procedure describes the steps to upgrade System Platform-based System Manager to Release 8.1.2 on Appliance Virtualization Platform or VMware virtualized environment.

The procedure covers upgrades on the different server.

#### Before you begin

- Install Solution Deployment Manager Client.
  
  For information, see [Installing the Solution Deployment Manager client on your computer](#) on page 27.

- Add a location.
  
  For information, see [Adding a location](#) on page 36.

- Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  
  For information about adding the Appliance Virtualization Platform or ESXi host, see [Adding an Appliance Virtualization Platform or ESXi host](#) on page 38.
For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 52.

**Important:**
- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 19.

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 8.1.x, then deploy Avaya Aura® Appliance Virtualization Platform and AVP Utilities on a supported server on latest release.

For information about supported servers, see Supported servers for Avaya Aura applications on page 18.

- 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 (Ψ) on the desktop.

2. Click **Application Management**.

3. In the lower pane, click **Upgrade Management**.

   The system displays the Upgrade Elements page.

4. On the Upgrade Elements page, perform the following:
   a. Click **Add Elements**.
   b. Select **System Platform**.
   c. In the Required Element Information section, add the System Manager element information.
   d. In the Required C-DOM Information section, add the console domain information.
   e. Click **Save**.

   For information, see Add Element field descriptions on page 113.

5. Select the System Manager element.

6. Click **Upgrade**.

7. In **Platform FQDN**, select the required host.

8. Select the datastore on the host, if required.

   The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
9. Click Next.

10. On the OVA tab, click one of the following:

   • **URL**, in the OVA File field, 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 the File Name field, 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.

When you select the OVA, the system:

   • Displays the CPU, memory, and other parameters in the Capacity Details section.

   • Disables the Flexi Footprint field.

11. **(Optional)** In Choose Deployment Type, select ME Deployment, if required.

12. In Flexi Footprint, select the flexi footprint.

13. 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.

14. 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.

15. Click Next.

16. 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”.

17. In the Network Parameters section, select the required Public and Out of Band Management network interface details.

For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

18. Click Upgrade and accept the license terms.

The system takes the backup, shuts down the existing virtual machine, deploys the OVA file, and restores the data on the new virtual machine.

19. 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.

Next steps
Install the valid license file for System Manager Release 8.1.

Related links
Upgrade Management field descriptions on page 115
Upgrade Management field descriptions on page 66

Upgrading System Platform-based System Manager on the same server by using Solution Deployment Manager Client

About this task
The procedure describes the steps to upgrade System Platform-based System Manager to Release 8.1.2 on Appliance Virtualization Platform or VMware virtualized environment.

The procedure covers upgrades on the same server.

Before you begin
• Install Solution Deployment Manager Client.
  For information, see Installing the Solution Deployment Manager client on your computer on page 27.
• Add a location.
  For information, see Adding a location on page 36.
• Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform or ESXi host on page 38.
  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 52.
Important:
- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.

For information about the supported ESXi version, see Supported ESXi version on page 19.

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 8.1.x, then deploy Avaya Aura® Appliance Virtualization Platform and AVP Utilities on a supported server on latest release.

For information about supported servers, see Supported servers for Avaya Aura applications on page 18.

• 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 Elements page, perform the following:
   a. Click Add Elements.
   b. Select System Platform.
   c. In the Required Element Information section, add the System Manager element information.
   d. In the Required C-DOM Information section, add the console domain information.
   e. Click Save.

   For information, see Add Element field descriptions on page 113.
5. Select the System Manager element.
6. Click Upgrade.
7. On the Upgrade Management page, select the Install on Same Host check box.
8. Click Continue.

   The virtual machine shuts down and goes to the paused state.
9. Install the Appliance Virtualization Platform host on the server on which System Platform was running.
10. To resume the upgrade operation, click Upgrade Elements > Resume.
11. In **Platform FQDN**, select the host.
12. Select the datastore on the host, if required.

   The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
13. Click **Next**.
14. On the **OVA** tab, click one of the following:
   - **URL**, in the **OVA File** field, 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 the **File Name** field, 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**.

   When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
15. 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**.
16. 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**.
17. Click **Next**.
18. 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”.

19. In the Network Parameters section, select the required Public and Out of Band Management network interface details.

For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

20. Click Upgrade and accept the license terms.

The system takes the backup, shuts down the existing virtual machine, deploys the OVA file, and restores the data on the new virtual machine.

21. 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.

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

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

23. If the upgrade fails or you want to revert to the old system, click Rollback.

After the rollback operation, you need to re-install System Platform and System Manager, and then restore the backup.

Related links

Upgrade Management field descriptions on page 115
Upgrade Management field descriptions on page 66

Upgrading VMware-based System Manager Release 6.x to Release 8.1.x on the Avaya-provided server

Upgrading VMware-based System Manager 6.x to Release 8.1.2 on a different server by using the Solution Deployment Manager client

About this task

The procedure describes the steps to upgrade VMware-based System Manager 6.x to Release 8.1.2 on different server.
Before you begin

Before upgrading VMware-based System Manager Release 6.x to Release 8.1.x on the Avaya-provided server, you must take a backup of System Manager from the System Manager web console.

- Install Solution Deployment Manager Client.
  For information, see Installing the Solution Deployment Manager client on your computer on page 27.
- Add a location.
  For information, see Adding a location on page 36.
- Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform or ESXi host on page 38.
  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 52.

⚠️ Important:

- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.
  For information about the supported ESXi version, see Supported ESXi version on page 19.
  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 8.1.x, then deploy Avaya Aura® Appliance Virtualization Platform and AVP Utilities on a supported server on latest release.
  For information about supported servers, see Supported servers for Avaya Aura applications on page 18.

- 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**.
   The system displays the Upgrade Elements page.
4. Add the ESXi platform that hosts System Manager Release 6.x, if this is not already added in Application Management.
5. On the Upgrade Elements page, do the following:
   a. Click **Add Elements**, select Virtual Machine Platform (6.x), and add the required host and virtual machine details.
   b. In Required Element Information, enter **SMGR SSH User Name** and **SMGR SSH Password** information.
      The system auto-populates the **SMGR IP** and **SMGR VM Name** details.
      ✪ **Note:**
      After adding the VMware-based System Manager 6.x, do not perform the **Refresh Platform** operation on the associated host of that System Manager. If you perform the **Refresh Platform** operation, the upgrade/migration activity of that VMware-based System Manager 6.x fails.
   c. Click **Save**.

6. If System Manager element is present, select the required element.

7. Click **Upgrade**.

8. In **Platform FQDN**, select the required host.

9. (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 for System Manager on VMware](#) on page 24.

10. Click **Next**.

11. On the **OVA** tab, click one of the following:
   - **URL**, in the **OVA File** field, 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 the **File Name** field, 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**.

   When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
• Disables the **Flexi Footprint** field.

12. 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**.

13. 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**.

14. Click **Next**.

15. In the Config Parameters section, provide the required details.

   ![Note:](image)
   Use the same **Management FQDN** and **Time Zone** as configured on the old System Manager.
   For information, see “Upgrade Management field descriptions”.

16. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
   For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

17. Click **Upgrade** and accept the license terms.
   The system takes the backup, shuts down the existing virtual machine, deploys the OVA file, and restores the data on the new virtual machine.

18. 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.

19. Verify that the new System Manager virtual machine is functional.
   For more information, see “Verifying the functionality of System Manager”.

20. If the upgrade fails or you want to revert to the old system, click **Rollback**.
After the rollback operation, you need to re-install VMware host and System Manager, and then restore the backup.

**Next steps**

Install the valid license file for System Manager Release 8.1.

---

**Upgrading VMware-based System Manager 6.x to Release 8.1.2 on the same server by using Solution Deployment Manager Client**

**About this task**

The procedure describes the steps to upgrade VMware-based System Manager 6.x to Release 8.1.2 on the same server.

**Before you begin**

Before upgrading VMware-based System Manager Release 6.x to Release 8.1.x on the Avaya-provided server, you must take a backup of System Manager from the System Manager web console.

- Install Solution Deployment Manager Client.
  
  For information, see [Installing the Solution Deployment Manager client on your computer](#) on page 27.

- Add a location.
  
  For information, see [Adding a location](#) on page 36.

- Add the ESXi, vCenter, or Appliance Virtualization Platform host.
  
  For information about adding the Appliance Virtualization Platform or ESXi host, see [Adding an Appliance Virtualization Platform or ESXi host](#) on page 38.
  
  For information about adding vCenter, see [Adding a vCenter to Solution Deployment Manager](#) on page 52.

**Important:**

- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.

  For information about the supported ESXi version, see [Supported ESXi version](#) on page 19.

  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 8.1.x, then deploy Avaya Aura® Appliance Virtualization Platform and AVP Utilities on a supported server on latest release.

  For information about supported servers, see [Supported servers for Avaya Aura applications](#) on page 18.
• 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 (SDM) on the desktop.

2. Click **Application Management**.

3. In the lower pane, click **Upgrade Management**.

   The system displays the Upgrade Elements page.

4. On the Upgrade Elements page, do the following:
   
   a. Click **Add Elements**, select Virtual Machine Platform (6.x), and add the required host and virtual machine details.

   b. In Required Element Information, enter **SMGR SSH User Name** and **SMGR SSH Password** information.

      The system auto-populates the **SMGR IP** and **SMGR VM Name** details.

      ✪ **Note:**

      After adding the VMware-based System Manager 6.x, do not perform the **Refresh Platform** operation on the associated host of that System Manager. If you perform the **Refresh Platform** operation, the upgrade/migration activity of that VMware-based System Manager 6.x fails.

   c. Click **Save**.

5. If System Manager element is present, select the required element.

6. Click **Upgrade**.

7. Click **Continue**.

   The virtual machine shuts down and goes to the paused state.

8. Install the Appliance Virtualization Platform host on the server on which VMware was running.

9. To resume the upgrade operation, click **Upgrade Elements > Resume**.

10. In **Platform FQDN**, select the required host.

11. **(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 for System Manager on VMware** on page 24.
12. Click Next.

13. On the OVA tab, click one of the following:
   - **URL**, in the OVA File field, 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 the File Name field, 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.

When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the Flexi Footprint field.

14. 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.

15. 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.

16. Click Next.

17. 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”.

18. In the Network Parameters section, select the required Public and Out of Band Management network interface details.
For Appliance Virtualization Platform, the system pre-populates the data and disables the fields.

19. Click **Upgrade** and accept the license terms.

The system takes the backup, shuts down the existing virtual machine, deploys the OVA file, and restores the data on the new virtual machine.

20. 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.

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

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

22. If the upgrade fails or you want to revert to the old system, click **Rollback**.

After the rollback operation, you need to re-install VMware host and System Manager, and then restore the backup.

---

**Add Element field descriptions**

**System Platform: Required C-DOM information**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-DOM IP/FQDN</td>
<td>The C-DOM IP/FQDN.</td>
</tr>
<tr>
<td>C-DOM SSH User Name</td>
<td>The C-DOM SSH user name.</td>
</tr>
<tr>
<td>C-DOM SSH Password</td>
<td>The C-DOM SSH password.</td>
</tr>
<tr>
<td>C-DOM Root User Name</td>
<td>The C-DOM root user name.</td>
</tr>
<tr>
<td>C-DOM Root password</td>
<td>The C-DOM root password.</td>
</tr>
</tbody>
</table>

**Virtual Machine Platform (6.x): Required Host/VM Details Information**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>The host of the virtual machine.</td>
</tr>
<tr>
<td>Virtual machines</td>
<td>The virtual machine.</td>
</tr>
</tbody>
</table>

**System Platform/Virtual Machine Platform (6.x): Required Element Information**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGR IP</td>
<td>The IP address of System Manager.</td>
</tr>
<tr>
<td>SMGR VM NAME</td>
<td>The name of the System Manager virtual machine.</td>
</tr>
<tr>
<td>SMGR SSH User Name</td>
<td>The SSH user name of System Manager.</td>
</tr>
<tr>
<td>SMGR SSH Password</td>
<td>The SSH password of System Manager.</td>
</tr>
</tbody>
</table>
**Button** | **Description**
---|---
Save | Saves the element that you added

---

## Edit Elements field descriptions

### Required Element information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGR IP</td>
<td>The IP address of System Manager</td>
</tr>
<tr>
<td>SMGR NAME</td>
<td>The name of System Manager virtual machine.</td>
</tr>
<tr>
<td>SMGR SSH User Name</td>
<td>The SSH user name of System Manager</td>
</tr>
<tr>
<td>SMGR SSH Password</td>
<td>The SSH password of System Manager</td>
</tr>
</tbody>
</table>

### Required C-DOM information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-DOM IP/FQDN</td>
<td>The C-DOM IP/FQDN</td>
</tr>
<tr>
<td>C-DOM SSH User Name</td>
<td>The C-DOM SSH user name</td>
</tr>
<tr>
<td>C-DOM SSH Password</td>
<td>The C-DOM SSH password</td>
</tr>
<tr>
<td>C-DOM Root User Name</td>
<td>The C-DOM root user name</td>
</tr>
<tr>
<td>C-DOM Root password</td>
<td>The C-DOM root password</td>
</tr>
</tbody>
</table>

**Button** | **Description**
---|---
Update | Updates the changes to the element.

---

## Install on Same ESXi field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Install on Same Host| The option to select the same or a different server during the upgrade. The options are:  
  • Select: To upgrade on same server.  
  • Clear: To upgrade on a different server.  |
| Platform FQDN       | The fully qualified domain name. For example, platform.mydomain.com.        |
# Upgrade Management field descriptions

## Upgrade Elements

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGR Name</td>
<td>System Manager name.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or the FQDN of System Manager virtual machine.</td>
</tr>
<tr>
<td>C-DOM IP/FQDN</td>
<td>The IP address or the FQDN of console domain.</td>
</tr>
<tr>
<td>Element Type</td>
<td>The type of the element.</td>
</tr>
<tr>
<td>Current Version</td>
<td>The current version of the element.</td>
</tr>
<tr>
<td>Upgrade To Version</td>
<td>The upgrade to version for the element.</td>
</tr>
<tr>
<td>Upgrade Status</td>
<td>The status of the upgrade process. The status can be <strong>Upgrading</strong>, <strong>Completed</strong>, or <strong>Failed</strong>. The <strong>Status Details</strong> link provides more information about the System Manager upgrade.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last upgrade action.</td>
</tr>
<tr>
<td>Related VM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Elements</td>
<td>Displays the Add Element page where you add System Manager.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Displays the Upgrade Management page where you upgrade the System Manager virtual machine.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the Edit Element page where you can change the details of System Manager that you added.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the System Manager virtual machine.</td>
</tr>
<tr>
<td>Commit</td>
<td>Saves the changes and upgrades the System Manager virtual machine.</td>
</tr>
<tr>
<td>Rollback</td>
<td>Reverts the upgrade of the System Manager virtual machine.</td>
</tr>
</tbody>
</table>
Chapter 9: Upgrading to System Manager Release 8.1.x by using CLI

Checklist for upgrading to System Manager Release 8.1.x from CLI

Checklist for upgrading VMware-based System Manager to Release 8.1.2 by using CLI

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Record the number of users and number of roles. You require this information later to verify that the upgrade is successful</td>
<td>For more information about managing users and custom roles, see Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>3</td>
<td>Record the System Manager FQDN and Time Zone.</td>
<td>See Customer configuration data for System Manager on page 22.</td>
</tr>
<tr>
<td>4</td>
<td>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.</td>
<td>Do this, if you have the System Manager Release 6.3.8 or later system and Avaya Breeze® platform is configured.</td>
</tr>
<tr>
<td>5</td>
<td>Ensure that the server is compatible with System Manager Release 8.1.2.</td>
<td>For Appliance Virtualization Platform, see Supported servers on page 17. For the Customer-provided Virtualized Environment offer, see: Software requirements on page 19</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Create a backup of System Manager.</td>
<td>Creating a data backup on a remote server on page 32</td>
</tr>
<tr>
<td>7</td>
<td>Turn off the old System Manager application.</td>
<td>Note: To migrate or upgrade from an earlier release (starting from Release 7.x and above) to Release 8.1.x, 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.</td>
</tr>
<tr>
<td>8</td>
<td>On the ESXi server, deploy the System Manager OVA file.</td>
<td>Use the same FQDN as that of the existing System Manager.</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
<td>System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.</td>
</tr>
<tr>
<td>9</td>
<td>Copy the data migration utility, the Release 8.1.2 bin file, and the backup file to the /swlibrary location on System Manager Release 8.1.2.</td>
<td>To copy files, use the tools, such as SCP, WinSCP, and FileZilla.</td>
</tr>
<tr>
<td>10</td>
<td>Create the snapshot of the System Manager application.</td>
<td>Creating the System Manager virtual machine snapshot on page 34</td>
</tr>
<tr>
<td>11</td>
<td>Verify that the new System Manager application is functional.</td>
<td>Verifying the functionality of System Manager on page 150</td>
</tr>
<tr>
<td>12</td>
<td>Verify the software version of the current System Manager.</td>
<td>Verifying the current software version on page 31</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>After deploying the System Manager OVA, run <code>upgradesmgr</code> 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.</td>
<td>Upgrading to System Manager Release 8.1.2 from CLI on page 120</td>
</tr>
<tr>
<td>14</td>
<td>Verify that the new System Manager application is functional.</td>
<td>Verifying the functionality of System Manager on page 150</td>
</tr>
<tr>
<td>15</td>
<td>Reinstall the license files because after the data migration the existing license files become invalid.</td>
<td>-</td>
</tr>
<tr>
<td>16</td>
<td>Copy the Avaya Breeze® platform snap-in <code>svar</code> files that you saved earlier to the Release 8.1.2 system.</td>
<td>-</td>
</tr>
</tbody>
</table>

---

**Checklist for upgrading VMware-based System Manager in the Geographic Redundancy setup to Release 8.1.2 by using CLI**

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager data migration utility, patch, and required OVA files from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>For the latest service packs and software patches, see Avaya Aura® release notes on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Disable the Geographic Redundancy replication.</td>
<td>See Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>3</td>
<td>Create a backup of primary System Manager and copy to the remote server.</td>
<td>Creating a data backup on a remote server on page 32</td>
</tr>
<tr>
<td>4</td>
<td>Turn off or remove the System Manager application.</td>
<td>-</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Deploy the System Manager OVA file. <strong>Note:</strong> After you deploy the Release 8.1 .ova file and before you perform operations such as configuring Geographic Redundancy and changing the IP or FQDN, you must run the data migration utility.</td>
<td>See “Deploying System Manager in Virtualized Environment”.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that the System Manager installation is successful and post-installation verification is complete.</td>
<td>Verifying the functionality of System Manager on page 150</td>
</tr>
<tr>
<td>7</td>
<td>Copy the data migration utility, the Release 8.1.2 bin file, and the backup file to the <code>/swlibrary</code> location on System Manager Release 8.1.2.</td>
<td>To copy files, use the tools, such as SCP, WinSCP, and FileZilla.</td>
</tr>
<tr>
<td>8</td>
<td>Create the snapshot of the System Manager application.</td>
<td>Creating the System Manager virtual machine snapshot on page 34</td>
</tr>
<tr>
<td>9</td>
<td>Run the data migration utility and provide the backup file and the Release 8.1.2 bin file.</td>
<td>Upgrading to System Manager Release 8.1.2 from CLI on page 120</td>
</tr>
<tr>
<td>10</td>
<td>Verify that the data is successfully migrated to Release 8.1.2.</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>Convert the primary System Manager server that is upgraded to the latest release to the standalone server.</td>
<td>See Administering Avaya Aura® System Manager.</td>
</tr>
<tr>
<td>12</td>
<td>Reinstall the license files because after the data migration, the existing license files become invalid.</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>Turn off or remove the System Manager application.</td>
<td>-</td>
</tr>
<tr>
<td>14</td>
<td>Deploy the System Manager OVA file.</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Verify that the System Manager installation is successful and post-installation verification is complete.</td>
<td>See “Deploying System Manager in Virtualized Environment”.</td>
</tr>
<tr>
<td>16</td>
<td>Install the System Manager Release 8.1.2 bin file. The patch installation takes about 45 minutes to complete.</td>
<td>-</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Create the snapshot of the System Manager application.</td>
<td><a href="#">Creating the System Manager virtual machine snapshot</a> on page 34</td>
</tr>
<tr>
<td>18</td>
<td>Configure CRL download on the secondary System Manager server.</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td>19</td>
<td>Configure Geographic Redundancy on the secondary System Manager server with the details of the primary System Manager server that you converted to standalone.</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td>20</td>
<td>Add the primary System Manager server CA certificate to the secondary System Manager trust store.</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td>21</td>
<td>On the primary System Manager server, enable the Geographic Redundancy replication.</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td>22</td>
<td>Once the system verification is successful, log off from the system, and remove the snapshot of the primary and secondary servers.</td>
<td>-</td>
</tr>
</tbody>
</table>

---

**Upgrading to System Manager Release 8.1.2 from CLI**

**About this task**

Use the procedure to upgrade System Manager from Release 6.2.x, 6.3.x, 7.x, 8.0.x to Release 8.1.2 running on VMware by using Command Line Interface.

When you upgrade System Manager to Release 8.1.x 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**

ℹ️ **Important:**

- If the application is running on the ESXi version that is not supported with Release 8.1.x, then first upgrade the ESXi to a supported ESXi version.

  For information about the supported ESXi version, see [Supported ESXi version](#) on page 19.

  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. Shut down the old System Manager.

5. Deploy the System Manager OVA on the supported ESXi version.
   
   For information about the supported ESXi version, see Supported ESXi version on page 19.

   For information about deploying System Manager on VMware, see Deploying the System Manager OVA by using vSphere Web Client on page 174 and Deploying the System Manager OVA using vSphere Web Client by accessing the host directly on page 176.

   Deployment of the System Manager OVA using vSphere Web Client by accessing the ESXi host 6.7 directly might fail. Therefore, to deploy the System Manager OVA, use vCenter 6.7 (flex) or Solution Deployment Manager Client.

   **Important:**
   
   It is recommended to use the same network parameters and system parameters that you recorded on the existing system. However, 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 22.

6. Copy the following files to the /swlibrary location on System Manager.
   
   - Data Migration Utility (datamigration-8.1.0.0.7-28.bin)
   - Latest patch (System_Manager_8.1.2.0_r812011097.bin)
   - System Manager backup file that you created in Step 3.

7. Do the following:
   
   a. Create a VMware 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.

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

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

For example, */swlibrary/System_Manager_R8.1.0.0.xxxxxxxxxx.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.
```

8. 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.

Once 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.
9. Perform one of the following:
   • If the upgrade or patch installation is successful, log off from the system, and remove the snapshot.

   **Note:**
   Snapshots occupy the system memory and degrades 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. The system creates a `LogsBackup_xx_xx_xx_xx_xxxxxx.tar.gz` file at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

**Next steps**

Install the valid license file for System Manager Release 8.1.x.

---

### Updating the System Manager Release 8.1 or 8.1.1 to Release 8.1.2

**About this task**

Use this procedure to update System Manager from Release 8.1 or 8.1.1 to Release 8.1.2 that is non-file encryption system.

**Note:**

For upgrading a non-file encryption System Manager Release 8.1 or 8.1.1 to file system encryption System Manager Release 8.1.2, see the “Upgrading the data from non-file encryption System Manager Release 8.1 or 8.1.1 to file system encryption System Manager Release 8.1.2” section.

**Before you begin**

• Ensure that System Manager is running on Release 8.1 or Release 8.1.1.

• Download the patch file from the Avaya Support website at [http://support.avaya.com/](http://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 CLI user credentials.

2. At the prompt, run the following command:

   ```bash
   SMGRPatchdeploy <absolute path to the bin file>
   ```
The system displays the license information.

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

---

**Updating the System Manager Release 8.1 or 8.1.1 to Release 8.1.2 in the Geographic Redundancy setup**

**About this task**

Use this procedure to update System Manager from Release 8.1 or 8.1.1 in the Geographic Redundancy setup to Release 8.1.2 that is non-file encryption system in the Geographic Redundancy setup.

**Before you begin**

- Ensure that System Manager is running on Release 8.1 or Release 8.1.1 in the Geographic Redundancy setup.
- Download the patch file from the Avaya Support website at [http://support.avaya.com/](http://support.avaya.com/) and copy the file to the `/swlibrary` location on System Manager.
- Calculate the MD5sum of the downloaded files and ensure that it has the same value as given on the Avaya PLDS website.
- You can update the primary and secondary System Manager servers in any order. However, you should not update the primary and secondary System Manager servers simultaneously. At a time, install the patch on one server.
- Activate the secondary System Manager server only after installing the patch.

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

**Procedure**

1. Disable the Geographic Redundancy replication on the primary System Manager server.
   
   For information about disabling Geographic Redundancy replication, see *Administering Avaya Aura® System Manager*.

2. Create the snapshot of the primary and secondary System Manager servers.
   
   This activity might impact the service.

   You must take the snapshot only after disabling the Geographic Redundancy replication.

3. Log in to the System Manager command line interface with CLI user credentials that you created at the time of application deployment.
4. To install the patch on the primary System Manager server, do the following:
   a. At the System Manager CLI, run the following command:

   ```bash
   $SMGRPatchdeploy <absolute path to the bin file>
   ```

   System Manager displays the license information.

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

   The patch installation takes about 45 minutes to complete.

   You can monitor the progress of the System Manager patch installation from the `/var/log/Avaya/SMGR_Patch.log` file.

   Once the patch is successful, the system displays the following message:

   `<Day Month Date HH:MM:SS IST Year #### ########>Patch execution completed Successfully.`

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

5. Verify the software version of the System Manager application.
   For information, see “Verifying the current software version”.

6. To install the patch on the secondary System Manager server, do the following:
   a. At the System Manager CLI, run the following command:

   ```bash
   $SMGRPatchdeploy <absolute path to the bin file>
   ```

   System Manager displays the license information.

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

   The patch installation takes about 45 minutes to complete.

   You can monitor the progress of the System Manager patch installation from the `/var/log/Avaya/SMGR_Patch.log` file.

   Once the patch is successful, the system displays the following message:

   `<Day Month Date HH:MM:SS IST Year #### ########>Patch execution completed Successfully.`

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

7. On the primary System Manager server, enable the Geographic Redundancy replication.
   For information about enabling Geographic Redundancy replication, see *Administering Avaya Aura® System Manager*. 
8. Verify the software version of the System Manager application.
   For information, see “Verifying the current software version”.

9. Perform one of the following:
   • If the patch installation is successful, log off from the system, and remove the snapshot.
     
     **Note:**
     Snapshots occupy the system memory and degrades 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, 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 at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.
Chapter 10: Upgrading System Manager to Release 8.1.x on Kernel-based Virtual Machine

Migration path

You can migrate to System Manager Release 8.1.2 on KVM from the following:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/KVM in customer-provided Virtualized Environment or on AWS/Google Cloud/Microsoft Azure on IaaS or on Software-only environment.
- System Manager Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.x on System Platform.

Migrating to System Manager Release 8.1.2 on KVM

About this task

Use the procedure to migrate System Manager from Release 6.x, 7.x, or 8.0.x to System Manager Release 8.1.2 on KVM.

Before you begin

- Ensure that System Manager is running.
- Download the required software files.

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. Record the network parameters and system parameters, such as virtual FQDN (vFQDN), IP Address, and Netmask of the old system.
4. 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.

5. Log in to the System Manager command line interface of the old system.

6. Shut down the old System Manager.

7. Deploy the System Manager Release 8.1 application for KVM.

   For information about deploying System Manager on Kernel-based Virtual Machine, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.

   **Important:**
   You can use the same network parameters and system parameters that you recorded on the old system or you can use the different network parameters to configure the new system.

8. Log in to the System Manager command line interface of the new system.

9. Copy the following files to the `/swlibrary` location on System Manager.
   - Data Migration Utility (`datamigration-8.1.0.0.7-28.bin`)
   - Latest patch (`System_Manager_8.1.2.0_r812011097.bin`)
   - System Manager backup file that you created in Step 4.

10. Do the following:
    a. Create a VMware 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.
    f. In **Enter the patch file**, type the absolute path of the patch file:

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

       For example, `/swlibrary/System_Manager_R8.1.0.0.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.

11. 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.

Once 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.

12. Verify the software version of the new System Manager.

Next steps
Install the valid license file for System Manager Release 8.1.x.

License management

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

• If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, all applications
that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 7.1.1 and later, KVM supports the WebLM that is integrated with System Manager.

- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, but only the KVM supported applications move to KVM, then you do not have to regenerate the license for those applications that move to KVM.

- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to KVM, then all the licenses need to migrate to the centralized System Manager Release 7.1.1 and later with integrated WebLM in KVM and the supported KVM applications that move need to regenerate the license files.
Chapter 11: Upgrading System Manager to Release 8.1.x on IaaS

Upgrade path for AWS
You can upgrade to System Manager Release 8.1.x on AWS from:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- System Manager Release 7.x on AWS.
- System Manager Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.x on System Platform.

Upgrade path for Google Cloud Network
You can upgrade to System Manager Release 8.1.x on Google Cloud Network from:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- System Manager Release 7.x on AWS.
- System Manager Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.x on System Platform.
Upgrade path for Microsoft Azure

You can upgrade to System Manager Release 8.1.x on Microsoft Azure from:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- System Manager Release 7.x on AWS.
- System Manager Release 7.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.x on System Platform.

Upgrading to System Manager Release 8.1.2 on IaaS

About this task

Use the procedure to:

- Migrate System Manager from Release 6.x or 7.x to System Manager Release 8.1.2 on IaaS offer.
- Upgrade the System Manager Release 7.x AWS instance to the System Manager Release 8.1.2 AWS instance.

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. Log in to the System Manager command line interface of the old system.
5. Shut down the old System Manager.
6. Perform the following steps based on your IaaS offer:
<table>
<thead>
<tr>
<th>IaaS offer</th>
<th>Choice Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>a. Convert the System Manager Release 8.1 AWS OVA to AMI.</td>
</tr>
<tr>
<td></td>
<td>✪ Note:</td>
</tr>
<tr>
<td></td>
<td>For information about converting System Manager AWS OVA to AMI, see <em>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</em>.</td>
</tr>
<tr>
<td></td>
<td>b. Deploy the System Manager Release 8.1 AMI.</td>
</tr>
<tr>
<td></td>
<td>✪ Note:</td>
</tr>
<tr>
<td></td>
<td>For information about deploying the System Manager AMI, see <em>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</em>.</td>
</tr>
<tr>
<td></td>
<td>✪ Important:</td>
</tr>
<tr>
<td></td>
<td>If you are using the AWS offer for Software-only environment, see the section “Upgrading System Manager to Release 8.1 on Software-only environment”.</td>
</tr>
<tr>
<td>Google Cloud Network</td>
<td>Deploy the System Manager Release 8.1 application.</td>
</tr>
<tr>
<td></td>
<td>✪ Note:</td>
</tr>
<tr>
<td></td>
<td>For information, see <em>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</em>.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Deploy the System Manager Release 8.1 application.</td>
</tr>
<tr>
<td></td>
<td>✪ Note:</td>
</tr>
<tr>
<td></td>
<td>For information, see <em>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</em>.</td>
</tr>
</tbody>
</table>

7. Log in to the System Manager command line interface of the new system.

8. Copy the following files to the `/swlibrary` location on System Manager.
   - Data Migration Utility (`datamigration-8.1.0.0.7-28.bin`)
   - Latest patch (`System_Manager_8.1.2.0_r812011097.bin`)
   - System Manager backup file that you created in Step 3.

9. Do the following:
   a. Create a VMware 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.

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

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

For example, `/swlibrary/System_Manager_R8.1.0.0.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.
```

10. 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.

Once 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.`

11. Verify the software version of the new System Manager.

**Next steps**

Install the valid license file for System Manager Release 8.1.x.
License management

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

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 8.0 and later, AWS supports the WebLM that is integrated with System Manager.

- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, but only the AWS supported applications move to AWS, then you do not have to regenerate the license for those applications that move to AWS.

- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to AWS, then all the licenses need to migrate to the centralized System Manager Release 8.0 and later with integrated WebLM in AWS and the supported AWS applications that move need to regenerate the license files.
Chapter 12: Upgrading System Manager to Release 8.1.x on Software-only environment

Upgrade path for Software-only environment

You can upgrade to System Manager Release 8.1.x on Software-only environment from:

- Release 8.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware/ KVM in customer-provided Virtualized Environment or on AWS/ Google Cloud/ Microsoft Azure on IaaS or on Software-only environment.
- System Manager Release 7.x on Appliance Virtualization Platform on Avaya provided server or on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment.
- System Manager Release 6.x on System Platform.

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 7.x to System Manager Release 8.1.2 on Software-only environment.

⚠️ Note:

Follow this procedure to upgrade to Release 8.1 on Hyper-V systems.

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 7.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”.

• 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 7.x 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**.

---

**Upgrading from System Platform based System Manager to Software-only environment by using the Solution Deployment Manager client**

**Before you begin**

- Install the Solution Deployment Manager client.
- Add a location.
- 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 ([SDM](#)) on the desktop.
2. Click **Application Management**.
3. In the lower pane, click Upgrade Management.

4. On the Upgrade Elements page, perform the following:
   a. Click Add Elements.
   b. Select System Platform.
   c. In the Required Element Information section, add the System Manager element information.
   d. In the Required C-DOM Information section, add the console domain information.
   e. Click Save.
   
   For information, see Add Element field descriptions on page 113.

5. Select the System Manager element.

6. Click Upgrade.

7. On Select Platform, select the Software Only check box.

8. Click Continue.

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

9. Click the Refresh icon until the Upgrade Status changes to Upgrading (PAUSED)...RESUME state.

10. Manually install and configure the RHEL OS with the same IP address of the old System Manager virtual machine.

11. 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.

12. 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.
   - 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.

13. Click Save.

14. Click Upgrade Management > Upgrade Elements and, then click RESUME displayed under the Upgrade Status column.

15. 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**.

16. Click **Next**.

17. 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**.

18. 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.

19. 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.

20. Click **Next**.

21. In **Flexi Footprint**, select the footprint size for the application.

22. 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**.

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

The system displays the Environment Check Output window.

24. Click **Next**.

25. On the Configuration Parameters page, provide all the information required.

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

26. Click **Upgrade**.

27. On the EULA Acceptance window, click **Accept**.

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

28. 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.

29. To view details, click **Status Details**.
Chapter 13: Changing over to Cold Standby server

Cold standby server as failover server for System Manager

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 primary 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 primary, Node A, and cold standby, Node B, servers are identical and have the same IP address, host name, and VFQDN. When the primary server is running, you must turn off the standby server.
2. Deploy System Manager on the primary and standby server.
3. Ensure that the system date is identical on both the servers.
4. Using the remote backup capability of System Manager Element Manager, create a regular backup of the System Manager database of the primary server so that you have the latest data for a cold standby procedure when the primary server fails.
   Create the backup of the database on a remote computer or on an external storage device such as a tape drive and DVD using VMware. When the primary server fails, use the backup to restore the database on the standby server.

Setting up a Cold Standby server

Before you begin

Ensure that the primary server, also called Node A, is turned off.
Procedure

1. Turn on the 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 database backup that you took from the Node A on Node B by using the backup and restore utility of System Manager Element Manager provided with System Manager. For more information, see Restoring a backup from a remote server on page 146.

4. When System Manager becomes operational, run repair on all the replica nodes to ensure the replicas have data that is consistent with the data restore on System Manager.

5. To repair the nodes: A, B, and C, perform the following steps:
   a. Log on to the System Manager Web console with administrator privilege credentials.
   b. Click Services > Replications to open the replication page.
   c. Select all the replica groups and click Repair. The repair time of all the nodes depends on the number of nodes and the size of data populated in the System Manager database.

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.
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:
   - Deselect the **Use Global Backup Encryption Password** check box.
   System Manager displays the following fields:
   - **Backup Encryption Password**
   - **Confirm Backup Encryption Password**
   - In **Backup Encryption Password**, type the encryption password.
   - 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!!**

---

**Scheduling 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. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

**About this task**

Use this functionality to schedule a data backup on a remote server. If you do not schedule a System Manager backup on a remote server every 7 days, the system generates an alarm.

**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:
   - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
   - 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. Click **Schedule**.

6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range

7. Click **Commit**.

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

---

**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 xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 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. Deselect 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 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.

Implementing the cold standby procedure on another computer

About this task

When you implement the System Manager cold standby procedure on a different computer, the system does not process the previously installed license file because the MAC address changes for the new computer.

Procedure

1. 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 MAC address.

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

3. Click Services > Licenses > Install licenses.

4. Click Browse and select the newly generated license file.

5. Click Install.

6. Verify that the system successfully installed the new license file.

7. Perform Steps 1 through 6 for each product.
Chapter 14: Post-upgrade Verification

Post-upgrade checklist

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that System Manager is installed properly after the upgrade.</td>
<td>See <a href="#">Verifying the functionality of System Manager</a> on page 150.</td>
</tr>
<tr>
<td>2</td>
<td>Install the license file.</td>
<td>See <a href="#">Installing a license file</a> on page 162.</td>
</tr>
<tr>
<td>3</td>
<td>Verify that the number of user profiles remains same before and</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td></td>
<td>after the upgrade.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Add or edit user from user profile, if required.</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td>5</td>
<td>Verify that Communication Manager and Session Manager are</td>
<td>See <a href="#">Administering Avaya Aura® System Manager</a>.</td>
</tr>
<tr>
<td></td>
<td>synchronized with the System Manager.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Install software patches and service packages that are entitled for</td>
<td>See <a href="#">Installing software patches</a> on page 151.</td>
</tr>
<tr>
<td></td>
<td>an Avaya Aura® application, and commit the patches that you installed.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Install mandatory System Manager patch.</td>
<td>See <a href="#">Installing the mandatory System Manager Release 8.1.2 patch</a> on page 78</td>
</tr>
<tr>
<td>8</td>
<td>Install the language pack to get localization support, if required.</td>
<td>See <a href="#">Installing language pack on System Manager</a> on page 163.</td>
</tr>
<tr>
<td>9</td>
<td>Delete the virtual machine snapshots, if required.</td>
<td>See <a href="#">Deleting the virtual machine snapshot from the Appliance Virtualization Platform host</a> on page 164 and <a href="#">Deleting the virtual machine snapshot from the vCenter managed host or standalone host</a> on page 165.</td>
</tr>
<tr>
<td>10</td>
<td>Configure the EASG settings, if required.</td>
<td>See <a href="#">Managing EASG from CLI</a> on page 165.</td>
</tr>
</tbody>
</table>
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 6.x or 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

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

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

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

Before you begin
• Perform 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 display ✓.

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

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

The page displays all software patches that you can commit.

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

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

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

19. Click **Schedule**.

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

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

**Note:**

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

Edit Upgrade Configuration has following tabs:

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

**Element Configuration: General Configuration Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>The system name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>Operation</td>
<td>The operation that you want to perform on the device. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Upgrade/Migration</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td>ESXi/AVP host/Platform</td>
<td>The host on which you want to run the device. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Same Box</td>
</tr>
<tr>
<td></td>
<td>• Software Only</td>
</tr>
<tr>
<td></td>
<td>• List of hosts that you added from Application Management</td>
</tr>
<tr>
<td>New Target ESXi/AVP host/Platform</td>
<td>The new target host on which you want to run the device.</td>
</tr>
<tr>
<td>Migrate With AVP Install</td>
<td>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.</td>
</tr>
<tr>
<td>Upgrade Source</td>
<td>The source where the installation files are available. The options are:</td>
</tr>
<tr>
<td></td>
<td>• SMGR_DEFAULT_LOCAL</td>
</tr>
<tr>
<td></td>
<td>• Remote Software Library</td>
</tr>
<tr>
<td>Upgrade To</td>
<td>The OVA file to which you want to upgrade.</td>
</tr>
<tr>
<td></td>
<td>When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.</td>
</tr>
<tr>
<td>Service/Feature Pack for auto-install after upgrade/ migration</td>
<td>The service pack or feature pack that you want to install.</td>
</tr>
</tbody>
</table>

**Element Configuration: Upgrade Configuration Details**

The page displays the following fields when you upgrade AE Services and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto Commit</strong></td>
<td>The option to automatically commit the upgrade.</td>
</tr>
<tr>
<td><strong>Existing Administrative User</strong></td>
<td>The user name with appropriate admin privileges.</td>
</tr>
<tr>
<td><strong>Existing Administrative Password</strong></td>
<td>The password of the administrator.</td>
</tr>
<tr>
<td><strong>Pre-populate Data</strong></td>
<td>The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>The IP address of the AE Services virtual machine.</td>
</tr>
<tr>
<td><strong>DNS Search Path</strong></td>
<td>The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).</td>
</tr>
<tr>
<td><strong>Password for cust</strong></td>
<td>The password of the cust user.</td>
</tr>
<tr>
<td><strong>Password for root</strong></td>
<td>The password of the root user.</td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td>The timezone of the virtual machine.</td>
</tr>
<tr>
<td><strong>NTP server(s)</strong></td>
<td>The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
</tbody>
</table>
| **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.                                                                                               |

*Table continues...*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Netmask</strong></td>
<td>The network mask of AE Services virtual machine.</td>
</tr>
<tr>
<td><strong>Private IP Address</strong></td>
<td>This field is optional and can be configured to be used for private network.</td>
</tr>
<tr>
<td><strong>Private Netmask</strong></td>
<td>This field is optional, and can be configured to be used for private network.</td>
</tr>
<tr>
<td><strong>Out of Band Management Netmask</strong></td>
<td>The subnet mask of the virtual machine for out of band management.</td>
</tr>
<tr>
<td><strong>Out of Band Management IP Address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Flexi Footprint</strong></td>
<td>The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>The port number that you must assign to public port group.</td>
</tr>
<tr>
<td><strong>Out of Band Management</strong></td>
<td>The port number that is assigned to the out of band management port group.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
<tr>
<td><strong>Datastore</strong></td>
<td>The datastore on the target ESXi host.</td>
</tr>
<tr>
<td></td>
<td>The field is available only when you select a different host.</td>
</tr>
</tbody>
</table>
## Element Configuration: Data Encryption

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption</td>
<td>Enables or disables the data encryption.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• 1: To enable the data encryption.</td>
</tr>
<tr>
<td></td>
<td>• 2: To disable the data encryption.</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On Solution Deployment Manager:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On vCenter or ESXi:</strong> When the Data Encryption field is set to 1, enter the encryption passphrase in the Password and Confirm Password fields.</td>
</tr>
</tbody>
</table>

| 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…*
### 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

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

### AVP Configuration: Existing Machine Details

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

### AVP Configuration: Configuration Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Source</td>
<td>The source where the installation files are available. The options are:</td>
</tr>
<tr>
<td></td>
<td>• SMGR_DEFAULT_LOCAL</td>
</tr>
<tr>
<td></td>
<td>• Remote Software Library</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade To</td>
<td>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.</td>
</tr>
<tr>
<td>Dual Stack Setup (with IPv4 and IPv6)</td>
<td>Enables or disables the fields to provide the IPv6 addresses.</td>
</tr>
<tr>
<td>AVP Management IPv4 Address</td>
<td>IPv4 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP IPv4 Netmask</td>
<td>IPv4 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP Gateway IPv4 Address</td>
<td>IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.</td>
</tr>
<tr>
<td>AVP Hostname</td>
<td>Hostname for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td></td>
<td>The hostname:</td>
</tr>
<tr>
<td></td>
<td>• Can contain alphanumeric characters and hyphen</td>
</tr>
<tr>
<td></td>
<td>• Can start with an alphabetic or numeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain at least 1 alphabetic character</td>
</tr>
<tr>
<td></td>
<td>• Must end in an alphanumeric character</td>
</tr>
<tr>
<td></td>
<td>• Must contain 1 to 63 characters</td>
</tr>
<tr>
<td>AVP Domain</td>
<td>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.</td>
</tr>
<tr>
<td>IPv4 NTP server</td>
<td>IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com</td>
</tr>
<tr>
<td>Secondary IPv4 NTP Server</td>
<td>Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.</td>
</tr>
<tr>
<td>Main IPv4 DNS Server</td>
<td>Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.</td>
</tr>
<tr>
<td>Secondary IPv4 DNS server</td>
<td>Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.</td>
</tr>
<tr>
<td>AVP management IPv6 address</td>
<td>IPv6 address for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP IPv6 prefix length</td>
<td>IPv6 subnet mask for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td>AVP gateway IPv6 address</td>
<td>IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.</td>
</tr>
<tr>
<td>IPv6 NTP server</td>
<td>IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td>Secondary IPv6 NTP server</td>
<td>Secondary IPv6 address or FQDN of customer NTP server.</td>
</tr>
<tr>
<td>Main IPv6 DNS server</td>
<td>Main IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary IPv6 DNS server</td>
<td>Secondary IPv6 address of customer DNS server. One DNS server entry in each line.</td>
</tr>
<tr>
<td>Public vLAN ID (Used on S8300E only)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Stricter Password (14 char pass length)</td>
<td>The check box to enable or disable the stricter password. The password must contain at least 14 characters.</td>
</tr>
<tr>
<td>AVP Super User Admin Password</td>
<td>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.</td>
</tr>
<tr>
<td>Enhanced Access Security Gateway (EASG)</td>
<td>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.</td>
</tr>
<tr>
<td>WebLM IP/FQDN</td>
<td>The IP Address or FQDN of WebLM Server.</td>
</tr>
<tr>
<td>WebLM Port Number</td>
<td>The port number of WebLM Server. The default port is 52233.</td>
</tr>
</tbody>
</table>
### 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 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 6.3.x, 7.0.x or 8.0.x

**About this task**

If you are using third-party certificates on System Manager Release 6.3.x, 7.0.x or 8.0.x and want to upgrade to System Manager Release 8.1, use the following procedure:
Procedure

1. Deploy the new System Manager Release 8.1 OVA using the same IP/FQDN and virtual FQDN values that are on System Manager Release 6.3.x, 7.0.x or 8.0.x.

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 can fail.

---

Using third-party certificates while upgrading from System Manager Release 6.2.x or earlier

About this task

If you are using third-party certificates on System Manager Release 6.2.x or earlier and want to upgrade to System Manager Release 8.1.x, use the following procedure. This procedure provides two ways to upgrade.

• Option 1:

1. Generate a new third-party CA-issued identity certificate with certificate attributes as described in the “Identity Certificate attributes” section of Avaya Aura® System Manager Certificate Management for System Manager 8.1.x and install it on the existing 6.2 system.

   The VFQDN used here must be configured at the time of deploying the System Manager 8.1 OVA.

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 can fail.

3. Deploy the new System Manager Release 8.1 OVA using the same IP/FQDN and virtual FQDN values that are on the old System Manager Release 6.2.x or earlier system.

   Release 6.2.x and earlier systems do not have a virtual FQDN. Therefore, at the time of deploying System Manager Release 8.1 OVA, use the same virtual FQDN value that you used while generating the new identity certificate.

• Option 2:

1. Revert to System Manager CA-issued certificate on Release 6.2.x.

2. Upgrade to System Manager Release 8.1 system.

3. Install the new third-party CA-issued certificate.

   For more information, see Avaya Aura® System Manager Certificate Management for System Manager 8.1.x.
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
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.

Before you begin
- 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter license path</td>
<td>The complete path where the license file is saved.</td>
</tr>
<tr>
<td>Browse</td>
<td>The option to browse and select the license file.</td>
</tr>
<tr>
<td>Avaya Global License Terms &amp; Conditions</td>
<td>Avaya license terms and conditions that the user must agree to continue the license file installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Installs the product license file.</td>
</tr>
</tbody>
</table>

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/8.1.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/8.1.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 JBoss service. 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 Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`
2. To log in to the Appliance Virtualization Platform host, provide the credentials.

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

4. Select the virtual machine, click **Actions > Snapshots > Manage snapshots**.
   The system displays the Manage snapshots - <Virtual machine name> dialog box.

5. Select the snapshot and click **Delete snapshot**.
   The system deletes the selected snapshot.

---

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

**Procedure**

1. Log in to the vSphere Web client for the vCenter managed host or the standalone host.

2. Depending on the host, perform one of the following
   
   a. On the vCenter managed host, select the host, and then select the virtual machine.
   
   b. On the Standalone host, select the virtual machine.

3. Right-click the selected virtual machine, click **Snapshot > Snapshot Manager**.
   The system displays the Snapshot for the <Virtual machine name> dialog box.

4. Select the snapshot and click **Delete**.
   The system deletes the selected snapshot.

---

### Enhanced Access Security Gateway overview

#### 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, 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: \texttt{EASG\textsc{status}}.
   The system displays the status of EASG.

2. To enable EASG, do the following:
   a. Run the command: \texttt{EASG\textsc{manage} --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 \url{https://grt.avaya.com}) to be eligible for Avaya remote connectivity. Please see the Avaya support site (\url{https://support.avaya.com/registration}) for additional information for registering products and establishing remote access and alarming.
    b. When the system prompts, type \texttt{yes}.
      The system displays the message: EASG Access is enabled.

3. To disable EASG, do the following:
   a. Run the command: \texttt{EASG\textsc{manage} --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 \texttt{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: \texttt{EASG\textsc{productcert} --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/response.

Managing site certificates

Before you begin

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

Procedure

1. 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 that are 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 that are currently installed on the system.
Chapter 15: 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.
4. Perform one of 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. Deselect 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 on the **Services > Configurations > Settings > SMGR > SMGR Element Manager** page.

**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. Deselect 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 xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 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.
4. (Optional) To restore encrypted backup using encryption password, do the following:
   a. Deselect 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 on the Services > Configurations > Settings > SMGR > SMGR Element Manager page.

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. Deselect 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

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

*Table continues…*
### Common upgrade procedures

#### Methods of System Manager deployment

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

- For Avaya-appliance deployments, see *Deploying Avaya Aura® System Manager in Virtual Appliance*.
- For customer Virtualized Environment, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.
- For Infrastructure as a Service Environment deployments, see *Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment*.
- For Software-Only Environment deployments, see *Deploying Avaya Aura® System Manager in Software-Only Environment*.

**Note:**

The deployment of the System Manager OVA by using the Appliance Virtualization Platform web interface and vSphere Client is not supported.
Deploying System Manager in Virtualized Environment

Deploying the System Manager OVA by using vSphere Web Client

Before you begin

• Access vCenter Server by using vSphere Web Client.
• Download the Client Integration Plug-in.

Procedure

1. On the web browser, type the following URL: https://<vCenter FQDN or IP Address>/vsphere-client/.

2. To log in to vCenter Server, do the following:
   a. In User name, type the user name of vCenter Server.
   b. In Password, type the password of vCenter Server.

3. Right-click the ESXi host and select Deploy OVF Template.
   The system displays the Deploy OVF Template dialog box.

4. On the Select 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 Locate file, click Browse, and navigate to the OVA file.

5. Click Next.

6. On the Select name and location page, do the following:
   a. In Name, type a name for the virtual machine.
   b. In Browse, select a datacenter.

7. Click Next.

8. On the Select a resource page, select a host, and click Next.


10. To accept the End User License Agreement, on the Accept license agreements page, click Accept.

11. Click Next.

12. On the Select configuration page, in Configuration, select the required profile.

13. Click Next.

14. On the Select storage page, in Select virtual disk format, click the required disk format.

15. Click Next.
16. On the Select networks page, select the destination network for each source network.

17. Click **Next**.

18. 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 178.

   ! **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.

19. Click **Next**.

20. On the Ready to complete page, review the settings, and click **Finish**. Wait until the system deploys the OVA file successfully.

21. 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.

   When the system starts for the first time, configure the parameters for System Manager. For instructions, see “Network and configuration field descriptions”.

22. 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 message: `exit status of eject command is 0`.

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 using vSphere Web Client by accessing the host directly**

**Before you begin**
- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.
- This procedure is applicable for ESXi 6.5 u2 onwards.

**Procedure**
1. On the Web browser, type the host URL: `https://<Host FQDN or IP Address>/ui`.
2. Enter login and password.
3. Right-click an ESXi host and select **Create/Register VM**.
   - The system displays the New virtual machine dialog box.
4. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
5. Click **Next**.
6. On the Select OVF and VMDK file page, do the following:
   - Type a name for the virtual machine.
   - Click to select files or drag and drop the OVA file from your local computer.
7. Click **Next**.
8. On the Select storage page, select a datastore, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I Agree**.
10. Click **Next**.
11. On the Deployment options page, perform the following:
    - From **Network mappings**, select the required network.
    - From **Disk provisioning**, select the required disk format.
    - From **Deployment type**, select profile.
    - Uncheck **Power on automatically**.
12. Click **Next**.
13. On the Additional settings page, click **Next**.

14. On the Ready to complete page, review the settings, and click **Finish**.

   Wait until the system deploys the OVA file successfully.

15. To edit the virtual machine settings, click VM radio option and perform the following:

   • Click **Actions > Edit Settings** to edit the required parameters.
   
   • Click **Save**.

   **Note:**

   Ensure that the virtual machine is powered down to edit the settings.

16. To ensure that the virtual machine automatically starts after a hypervisor reboot, click VM radio option, and click **Actions > Autostart > Enable**.

   **Note:**

   If you do not enable autostart, you must manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.

17. To start the System Manager virtual machine, if System Manager is not already powered on perform 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 178.

18. 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 message: `exit status of eject command is 0`.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Management IPv4 Address** (or Out of Band Management IPv4 Address) | The IPv4 address of the System Manager application for out of band management.  
The field is 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. The field is optional.                                                                                                |
| **IPv6 Network prefix**                                             | The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.                                                                                                               |
| **IPv6 Gateway**                                                    | The gateway IPv6 address to assign to the System Manager application. The field is optional.                                                                                                                |
| **Default Search List**                                             | The search list of domain names. The field is optional.                                                                                                                                                     |
| **NTP Server IP/FQDN**                                              | The IP address or FQDN of the NTP server. The field is optional.                                                                                                                                              |
| **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.                                                     |

★ Note:

   You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public IP Address</strong></td>
<td>The IPv4 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td><strong>Public Netmask</strong></td>
<td>The IPv4 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td><strong>Public Gateway</strong></td>
<td>The gateway IPv4 address to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td><strong>Public FQDN</strong></td>
<td>The FQDN to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td><strong>Public IPv6 Address</strong></td>
<td>The IPv6 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td><strong>Public IPv6 Network Prefix</strong></td>
<td>The IPv6 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td><strong>Public IPv6 Gateway</strong></td>
<td>The gateway IPv6 address to assign to the System Manager application. The field is optional.</td>
</tr>
</tbody>
</table>
### Virtual Hostname
- **Description:** 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
- **Description:** The virtual domain name of the System Manager application.

### SNMPv3 User Name Prefix
- **Description:** The prefix for SNMPv3 user.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Hostname</td>
<td>The virtual hostname of the System Manager application.</td>
</tr>
<tr>
<td>SNMPv3 User Name Prefix</td>
<td>The prefix for SNMPv3 user.</td>
</tr>
<tr>
<td>SNMPv3 User Authentication Protocol Password</td>
<td>The password for SNMPv3 user authentication.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the SNMPv3 user authentication protocol.</td>
</tr>
<tr>
<td>SNMPv3 User Privacy Protocol Password</td>
<td>The password for SNMPv3 user privacy.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you must provide to confirm the SNMPv3 user privacy protocol.</td>
</tr>
<tr>
<td>SMGR command line user name</td>
<td>The user name of the System Manager CLI user.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>SMGR command line user password</td>
<td>The password for the System Manager CLI user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you retype to confirm the System Manager CLI user authentication.</td>
</tr>
<tr>
<td>Schedule Backup?</td>
<td>• <strong>Yes:</strong> To schedule the backup jobs during the System Manager installation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No:</strong> To schedule the backup jobs later.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If you select <strong>No</strong>, the system does not display the remaining fields.</td>
</tr>
<tr>
<td>Backup Server IP</td>
<td>The IP address of the remote backup server.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The IP address of the backup server must be different from the System Manager IP address.</td>
</tr>
<tr>
<td>Backup Server Login Id</td>
<td>The login ID of the backup server to log in through the command line interface.</td>
</tr>
<tr>
<td>Backup Server Login Password</td>
<td>The SSH login password to log in to the backup server from System Manager through the command line interface.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password that you reenter to log in to the backup server through the command line interface.</td>
</tr>
<tr>
<td>Backup Directory Location</td>
<td>The location on the remote backup server.</td>
</tr>
<tr>
<td>File Transfer Protocol</td>
<td>The protocol that you can use to create the backup. The values are SCP and SFTP.</td>
</tr>
</tbody>
</table>
### 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.
The system generates an alarm if you do not schedule a System Manager backup every seven days.

### 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.

### 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

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

Pix Note:

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Customer Root Account for this Application</td>
<td>Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <strong>Accept</strong>. When you accept the root access statement, the system displays the <strong>Customer Root Password</strong> and <strong>Re-enter Customer Root Password</strong> fields.</td>
</tr>
<tr>
<td>Customer Root Password</td>
<td>The root password for the application</td>
</tr>
<tr>
<td>Re-enter Customer Root Password</td>
<td>The root password for the application</td>
</tr>
</tbody>
</table>

Data Encryption

Pix Note:

- From Release 8.1.2, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.
### Name: 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.

---

Comments on this document? infodev@avaya.com
### 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 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”.

### Table: Require Encryption Passphrase at Boot-Time

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Require Encryption Passphrase 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 Passphrase 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. |
If you do not schedule a System Manager backup every 7 days, the system 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.

   The system 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 message: exit status of eject command is 0.
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Transfer Protocol</td>
<td>The protocol that you can use to create the backup. The values are SCP and SFTP.</td>
</tr>
<tr>
<td>Repeat Type</td>
<td>The type of the backup. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Hourly</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
<tr>
<td>Backup Frequency</td>
<td>The frequency of the backup taken for the selected backup type.</td>
</tr>
<tr>
<td></td>
<td>The system generates an alarm if you do not schedule a System Manager backup every seven days.</td>
</tr>
<tr>
<td>Backup Start Year</td>
<td>The year in which the backup must start. The value must be greater than or equal to the current year.</td>
</tr>
<tr>
<td>Backup Start Month</td>
<td>The month in which the backup must start. The value must be greater than or equal to the current month.</td>
</tr>
<tr>
<td>Backup Start Day</td>
<td>The day on which the backup must start. The value must be greater than or equal to the current day.</td>
</tr>
<tr>
<td>Backup Start Hour</td>
<td>The hour in which the backup must start.</td>
</tr>
<tr>
<td></td>
<td>The value must be six hours later than the current hour.</td>
</tr>
<tr>
<td>Backup Start Minutes</td>
<td>The minute when the backup must start. The value must be a valid minute.</td>
</tr>
<tr>
<td>Backup Start Seconds</td>
<td>The second when the backup must start. The value must be a valid second.</td>
</tr>
</tbody>
</table>

**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.
**Note:**

On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the `changeIPFQDN` command, the system changes the host ID of System Manager and invalidate 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 < >
```

<table>
<thead>
<tr>
<th>#</th>
<th>Option</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP</td>
<td>The new Management IPv4 address of System Manager.</td>
<td><code>changeIPFQDN -IP 10.11.12.13</code></td>
</tr>
<tr>
<td>2</td>
<td>FQDN</td>
<td>The new Management FQDN of System Manager.</td>
<td><code>changeIPFQDN -FQDN a.mydomain.smgr.com</code></td>
</tr>
<tr>
<td>3</td>
<td>GATEWAY</td>
<td>The new Management Gateway IPv4 address of System Manager.</td>
<td><code>changeIPFQDN -GATEWAY 10.11.1.1</code></td>
</tr>
<tr>
<td>4</td>
<td>NETMASK</td>
<td>The new Management netmask address of System Manager.</td>
<td><code>changeIPFQDN -NETMASK 255.255.203.0</code></td>
</tr>
<tr>
<td>5</td>
<td>DNS</td>
<td>The new Management DNS address of System Manager.</td>
<td><code>changeIPFQDN -DNS 10.11.1.2</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can provide multiple DNS addresses. Separate each address by a comma.</td>
<td><code>changeIPFQDN -DNS 10.11.12.5,10.11.12.3</code></td>
</tr>
<tr>
<td>6</td>
<td>SEARCH</td>
<td>The new search list of domain names.</td>
<td><code>changeIPFQDN -SEARCH smgr.com</code></td>
</tr>
<tr>
<td>8</td>
<td>IPV6GW</td>
<td>The new Management Gateway IPv6 address of System Manager.</td>
<td><code>changeIPFQDN -IPV6GW 2001:b00d::1</code></td>
</tr>
<tr>
<td>9</td>
<td>IPV6PREFIX</td>
<td>The new Management netmask prefix of System Manager. The default value is 64.</td>
<td><code>changeIPFQDN -IPV6PREFIX 64</code></td>
</tr>
</tbody>
</table>

**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
```
Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI

About this task

Use this procedure to change the network configuration parameters for Public interface and Management interface when OOBM is enabled.

⚠️ Important:

- Do not change the network settings from vSphere Web Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the Console tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

❌ Note:

Delete the snapshot after the System Manager operation is complete.

Procedure

1. To configure Management network parameters, type `changeIPFQDN -IP <IPv4 address> -FQDN <FQDN> -GATEWAY <Gateway IPv4 address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6 Gateway address> -IPV6PREFIX <IPv6 prefix>`.

   For information, see `changeIPFQDN`.

2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN> -PublicGATEWAY <Gateway IP address> -PublicNETMASK <Netmask address>`.

   For information, see `changePublicIPFQDN`.

Next steps

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*. 
Installing the System Manager service pack or patch from CLI

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the icon.
  - Use PuTTY.

- Log in to System Manager with administrator privilege credentials.
- Take a snapshot of the System Manager virtual machine.

**Procedure**

**Type** `SMGRPatchdeploy <absolute path to the service pack or patch for System Manager>`.

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

**Next steps**

Delete the snapshot after you verify the System Manager functionality.

**Related links**

- [System Manager command line interface operations](#) on page 192
# System Manager command line interface operations

<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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 system, if you change the IP Address of System Manager by using the changeIPFQDN command, the system changes the host ID of System Manager and invalidate 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>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>changePublicIPFQDN</td>
<td>-publicIP &lt;new IP address for System Manager&gt;</td>
<td>Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.</td>
<td>- changePublicIPFQDN -publicIP &lt;new Public IP address&gt; -publicFQDN &lt;new fully qualified domain name for System Manager&gt; -publicGATEWAY &lt;new Gateway address for System Manager&gt; -publicNETMASK &lt;new netmask address for System Manager&gt;</td>
</tr>
<tr>
<td>3</td>
<td>upgradeSMGR</td>
<td>&lt;absolute path to the dmutility.bin&gt; -m -v</td>
<td>Upgrades System Manager using the data migration utility.</td>
<td>upgradeSMGR dmutility *.bin -m -v</td>
</tr>
<tr>
<td>4</td>
<td>SMGRPatchdeploy</td>
<td>&lt;absolute path to the System Manager service pack or the software patch&gt;</td>
<td>Installs the software patch or the service pack for System Manager.</td>
<td>SMGRPatchdeploy &lt;absolute path to SMGRservicepackName&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Copy the System Manager service pack or patches that you must install to /swlibrary.</td>
</tr>
<tr>
<td>5</td>
<td>configureTimeZone</td>
<td>Time zone that you select</td>
<td>Configures the time zone with the value that you select.</td>
<td>configureTimeZone</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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 | EASGSiteCert Manage|            | To manage EASG Certificates. |                                                                     |
| 15 | editHosts          |            | To modify the /etc/hosts file.|                                                                     |
| 16 | swversion          |            | Displays the System Manager software information. |                                                                      |
| 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… |
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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 primary server>  
  -NEWFQDN <New FQDN of primary server>  

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>smgr</td>
<td></td>
<td>Starts, stops, and checks the status of Jboss service.</td>
<td>smgr start/stop/status</td>
</tr>
<tr>
<td>20</td>
<td>smgr-db</td>
<td></td>
<td>Starts, stops, and checks the status of postgresql.service.</td>
<td>smgr-db start/stop/status</td>
</tr>
<tr>
<td>21</td>
<td>toggleWeblmOldCert</td>
<td></td>
<td>Replaces identity certificate with old certificate.</td>
<td>toggleWeblmOldCert</td>
</tr>
<tr>
<td>22</td>
<td>getUserAuthCert</td>
<td></td>
<td>Generates a user specific certificate for System Manager to facilitate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>certificate-based authentication.</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>changeCipherSuiteList</td>
<td></td>
<td>Configures cipher suite mode for System Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To configure strict cipher suite list:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>changeCipherSuiteList STRICT_CIPHER_SUITE_LIST</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To configure relax cipher suite list:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>changeCipherSuiteList RELAX_CIPHER_SUITE_LIST</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>collectLogs</td>
<td></td>
<td>Collects the required logs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To collect all the logs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>collectLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To collect all the logs along with backup:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>collectLogs -Db</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To collect all the logs along with CND data:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>collectLogs -CND</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>rebootVM</td>
<td></td>
<td>Reboots the System Manager virtual machine.</td>
<td>Type y or n to reboot the System Manager virtual machine.</td>
</tr>
<tr>
<td>#</td>
<td>Command</td>
<td>Parameters</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>powerOffVM</td>
<td></td>
<td>Power off the System Manager virtual machine.</td>
<td>Type y or n to power off the System Manager virtual machine.</td>
</tr>
<tr>
<td>27</td>
<td>sudo /bin/spotify</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the Spotify service.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>sudo /bin/spotify</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the Spotify service.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>sudo /bin/spotify</td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the Spotify service.</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>encryptionPassphrase</td>
<td>[add</td>
<td>change</td>
<td>remove</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>encryptionRemoteKey</td>
<td>[add</td>
<td>remove</td>
<td>list]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>encryptionRemoteKey remove</strong>: To remove remote key server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>encryptionRemoteKey list</strong>: To display the remote key server and slot assignment.</td>
</tr>
<tr>
<td>32</td>
<td>encryptionLocalKey</td>
<td>[enable</td>
<td>disable]</td>
<td>To enable and disable the local key store.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>encryptionLocalKey disable</strong>: To disable local key store.</td>
</tr>
<tr>
<td>33</td>
<td>encryptionStatus</td>
<td></td>
<td>Displays information about encryption on the system.</td>
<td><strong>encryptionStatus</strong> displays information about encryption on the system.</td>
</tr>
</tbody>
</table>
### 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](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® System Manager Overview and Specification</td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Administering Avaya Aura® System Manager</td>
<td>Administering System Manager applications and install patches on System Manager applications.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Avaya Aura® System Manager Certificate Management</td>
<td>Understand certificate management.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Using</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using the Solution Deployment Manager client</td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td>Avaya Aura® System Manager Solution Deployment Manager Job-Aid</td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading Avaya Aura® System Manager</td>
<td>Upgrade the Avaya Aura® System Manager application to Release 8.1.x.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® System Manager in Virtual Appliance</td>
<td>Deploy System Manager applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® System Manager in Virtualized Environment</td>
<td>Deploy System Manager applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</td>
<td>Deploy System Manager applications in Infrastructure as a Service Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying Avaya Aura® System Manager in Software-Only Environment</td>
<td>Deploy System Manager applications in Software-Only Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

## Finding documents on the Avaya Support website

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
   - The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   - For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

## Accessing the port matrix document

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - Application & Technical Notes
   - Design, Development & System Mgt
   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

---

**Avaya Documentation Portal navigation**

Customer documentation for some programs is now available on the Avaya Documentation Portal at [https://documentation.avaya.com](https://documentation.avaya.com).

⚠️ **Important:**

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open [https://support.avaya.com](https://support.avaya.com).

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (⭐).

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

Navigate to the **My Content > Watch list** menu, and do the following:
- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page. As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

• Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.

• Send feedback on a section and rate the content.

**Note:**

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

---

**Training**

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you log into the website, enter the course code or the course title in the Search field and click Go to search for the course.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20460W</td>
<td>Virtualization and Installation Basics for Avaya Team Engagement Solutions</td>
</tr>
<tr>
<td>20970W</td>
<td>Introducing Avaya Device Adapter</td>
</tr>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.1</td>
</tr>
<tr>
<td>71200V</td>
<td>Integrating Avaya Aura® Core Components</td>
</tr>
<tr>
<td>72200V</td>
<td>Supporting Avaya Aura® Core Components</td>
</tr>
<tr>
<td>20130V</td>
<td>Administering Avaya Aura® System Manager Release 8.1</td>
</tr>
<tr>
<td>21450V</td>
<td>Administering Avaya Aura® Communication Manager Release 8.1</td>
</tr>
</tbody>
</table>

---

**Viewing Avaya Mentor videos**

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

**About this task**

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

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

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

In the right pane, the page displays a list of available videos.

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

🌟 Note:

Videos are not available for all products.

---

**Support**

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

**Related links**

Using the Avaya InSite Knowledge Base on page 204

---

**Using the Avaya InSite Knowledge Base**

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

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

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

2. Log on to the Avaya website with a valid Avaya user ID and password. The system displays the Avaya Support page.
4. In Enter Product Name, enter the product, and press Enter.
5. Select the product from the list, and select a release.
6. Click the Technical Solutions tab to see articles.
7. Select relevant articles.

Related links
Support on page 204
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, data migration utility, 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.

For upgrading System Manager, use Solution Deployment Manager Client. For upgrading 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:
  - System Platform to AVP/VMware
  - AVP to VMware
  - VMware to AVP

  For upgrading System Manager, use Solution Deployment Manager Client. For upgrading 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, kernel patches, 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.
customer configuration data ........................................ 22

data
  Backup Definition Parameters ........................................ 22
  network configuration .................................................. 22
  SNMP parameters .......................................................... 22
  FQDN ................................................................. 22
data backup
  remote server .......................................................... 32, 144, 168
  data backup; schedule ................................................. 145
  data backup from local server ..................................... 171
data encryption
  overview .................................................................. 57
data migration
  from System Manager configured with Geographic Redundancy .......... 74, 98
  data migration checklist ............................................. 98
  data migration from 6.x ............................................... 95
  data migration utility .................................................. 13
  Data Migration utility .................................................. 120
deleting
  location ................................................................. 36
  snapshot from standalone host ..................................... 165
deleting a location ....................................................... 36
deleting vCenter .......................................................... 54
deploy application ....................................................... 35
deploying System Manager OVA
  using vSphere Web Client ......................................... 174
deploy System Manager ................................................ 173
deploy System Manager OVA
  direct host ............................................................. 176
  vSphere Web Client ................................................... 176
documentation
  System Manager ....................................................... 200
documentation portal ................................................... 202
  finding content ........................................................ 202
  navigation ............................................................... 202
download software ..................................................... 44

E

EASG
  certificate information .............................................. 166
  disabling ............................................................... 165
  enabling ............................................................... 165
  status ..................................................................... 165
  EASG site certificate ................................................ 167
edit
  application ............................................................. 45
  edit application ........................................................ 45
editing
  location ................................................................. 36
  vCenter ................................................................. 53
editing the location ................................................... 36
editing vCenter .......................................................... 53

Edit Location .......................................................... 37
Edit Platform ........................................................... 44
Edit Upgrade Configuration
  AVP Configuration .................................................. 153
  Element Configuration ............................................. 153
Edit vCenter
  element
    add ....................................................................... 113
  elements
    refresh ............................................................... 30
Enhanced Access Security Gateway
  EASG overview ........................................................ 165
ESXi host
  adding ..................................................................... 38
  removing ............................................................... 44
  restarting ............................................................... 43
ESXi version
  Avaya Aura® application .......................................... 19

F

field description
  edit elements ........................................................... 114

field descriptions
  Add Platform .......................................................... 44
  Edit Location ........................................................ 37
  Edit Platform ........................................................ 44
  Map vCenter .......................................................... 54
  New Location ......................................................... 37
  WebLM Configuration .............................................. 42
  finding content on documentation portal ..................... 202
  finding port matrix ............................................... 201
  first boot
    network and configuration ..................................... 178
  footprint hardware matrix
    System Manager on Appliance Virtualization Platform .... 23
    System Manager on VMware .................................... 24
  FQDN ................................................................. 190
  changeIPFQDN ...................................................... 188

G

General Configuration Details ........................................ 153
generate_report.sh .................................................... 153

Generating
  virtual machine report ........................................... 49
  Geographic Redundancy setup upgrade ......................... 118

H

hardware supported
  System Manager ..................................................... 17

I

implementing cold standby on another computer ............... 148
InSite Knowledge Base ................................................................. 204
install
Application Enablement Services ............................................... 27
Avaya Aura applications .............................................................. 27
Avaya Aura Media Server ............................................................ 27
Avaya Breeze ............................................................................ 27
Branch Session Manager ............................................................. 27
Communication Manager ......................................................... 27
SAL ......................................................................................... 27
SDM ....................................................................................... 27
Session Manager ..................................................................... 27
Solution Deployment Manager client ......................................... 27
System Manager ...................................................................... 27
System Manager patch ............................................................... 78
System Manager service pack from CLI ..................................... 191
WebLM ................................................................................... 27
installing language pack
Canadian French ....................................................................... 163
install license file ...................................................................... 162
Install License page .................................................................... 163
install on same ESXi .................................................................. 66
Install on Same server ............................................................... 114
install patches ......................................................................... 151
install services packs ............................................................... 151
install software patches ........................................................... 151
install System Manager ............................................................. 173
Install System Manager patches ............................................... 115
inventory
refresh elements ...................................................................... 30
IP address ................................................................................ 190
L
LAC .......................................................................................... 162
latest software patches .............................................................. 19
License Activation Code ........................................................... 162
license file
Avaya Aura products ................................................................ 22
install ...................................................................................... 162
license file installation ............................................................... 163
Licenses .................................................................................. 129, 135
Life cycle management ............................................................ 35
local data backup
create ..................................................................................... 169
location
adding .................................................................................... 36
deleting ................................................................................... 36
editing ..................................................................................... 36
view ......................................................................................... 35
M
Manage
System Manager upgrades .......................................................... 115
Map vCenter ............................................................................. 52-55
My Docs .................................................................................. 202
N
network and configuration
field descriptions .................................................................... 178
network parameters ............................................................... 185
New Location ........................................................................ 37
New vCenter ........................................................................... 55
O
OVA file
deploy ..................................................................................... 176
deploying ................................................................................. 174
P
parameters
backup definition ..................................................................... 187
patch file
install .................................................................................... 78
patch information ................................................................. 19
PCN ......................................................................................... 19
PLDS
finding LAC ........................................................................... 162
port matrix ............................................................................. 201
post-upgrade checklist .......................................................... 149
prerequisites
System Manager upgrade ...................................................... 16
prerequisites for cold standby ............................................... 143
PSN ......................................................................................... 19
R
record network parameters details ......................................... 17
record user name and password ............................................. 17
reestablish
connection ............................................................................ 49
re-establishing trust
application .......................................................................... 47
SDM elements ......................................................................... 47
Solution Deployment Manager elements ................................... 47
re-establishing trust application ............................................ 47
refresh elements in inventory .................................................... 30
release notes for latest software patches ..................................... 19
removing
Appliance Virtualization Platform host ................................... 44
ESXi host ................................................................................. 44
removing location from host .................................................. 53
removing vCenter .................................................................... 54
resources
server .................................................................................... 18
restart
application ............................................................................. 47
restart application from SDM ................................................ 47
restarting
Appliance Virtualization Platform ......................................... 43
restarting (continued)
ESXi host ................................................................. 43
restore backup
remote server ......................................................... 146, 170
restore backup from remote server ...................... 146, 170
restore data backup ................................................... 171
restore system backup from local server .............. 171
restoring backup
from local server ..................................................... 148
restoring backup from local server ....................... 148
run
Data Migration utility ................................................ 120, 127, 132

S
same host installation .................................................. 114
schedule data backup; remote server .................. 145
scheduling a data backup on a remote server .......... 145
SDM
installation .................................................................. 27
SDM elements
re-establishing trust ................................................... 47
searching for content .................................................. 202
Select Flexi Footprint .................................................. 45
servers supported ...................................................... 17
Session Manager update .......................................... 151
setting up a Cold Standby server ......................... 143
sharing content ......................................................... 202
shutting down
AVP ........................................................................ 43
site certificate
add .......................................................................... 167
delete .................................................................... 167
manage .................................................................... 167
view ......................................................................... 167
snapshot from Appliance Virtualization Platform
deleting ................................................................. 164
snapshot from vCenter managed host
deleting ............................................................... 165
Snapshot restore ....................................................... 160
snapshot System Manager virtual machine ............ 34
software
download ................................................................. 44
software details
System Manager ......................................................... 22
software patches ...................................................... 19
software requirements ............................................. 19
Solution Deployment Manager ................................ 31
access .................................................................... 30
restart application ................................................... 47
start ....................................................................... 30
start application ....................................................... 46
stop application ......................................................... 46
Solution Deployment Manager client dashboard ..... 29
Solution Deployment Manager elements
re-establishing trust .................................................. 47
start (continued)
application ............................................................. 46
start application from SDM ...................................... 46
start Solution Deployment Manager ....................... 30
stop
application .............................................................. 46
stop application from SDM ....................................... 46
support ...................................................................... 204
supported hardware and resources ..................... 18
supported servers ................................................... 17
Avaya Aura® application ......................................... 18
supported System Manager upgrade paths ............. 14
System Manager
commands ................................................................ 192
deploy ....................................................................... 173
footprint hardware matrix ....................................... 24
installing patches ...................................................... 76
resource requirements ............................................. 24
Solution Deployment Manager ............................... 76
Virtual Machines ...................................................... 76
VM Management ...................................................... 76
System Manager 6.x data migration ....................... 95
System Manager bin file ......................................... 78
System Manager functionality .................................. 150
System Manager on KVM
CPU, vCPUs, RAM, HDD, NICs, users .................... 25
footprints ................................................................. 25
System Manager patch ............................................ 78, 191
System Manager service pack ............................... 191
System Manager test ................................................ 150
System Manager training ......................................... 203
System Manager upgrade ........................................ 66
to AWS ..................................................................... 132
to Azure ................................................................... 132
to Google Cloud ....................................................... 132
System Manager upgrade paths ............................. 14
System Manager upgrades ...................................... 116
third-party certificate ................................................ 160
System Manager upgrade to KVM ......................... 127
System Manager upgrade to VMware .................... 120
System Manager upgrade using CLI
  to Release 8.1.x .................................................... 118
System Manager virtual machine
  snapshot ................................................................. 34
System Platform-based System Manager upgrade
  on different server .................................................. 100
  on same server ....................................................... 103

T
test
System Manager functionality .................................. 150
third-party certificate ................................................ 160

U
update
Index

update (continued)
  Appliance Virtualization Platform 7.x to 7.x through services port ........................................ 86
  Appliance Virtualization Platform 8.0.x to 8.1.x through services port ........................................ 86
  Communication Manager .................................................. 151
  Session Manager ............................................................. 151
update software ................................................................ 151
update static routing ....................................................... 48
upgrade
  Appliance Virtualization Platform through services port ................................................................. 80
  Branch Session Manager .................................................. 153
  Communication Manager .................................................. 153
  from System Manager configured with Geographic Redundancy .................................................. 74, 98
  prerequisites ..................................................................... 62
  Session Manager ............................................................. 153
  System Manager 8.1.1 to 8.1.2 or later ........................................... 123
  System Manager 8.1.1 to 8.1.2 or later in the Geographic Redundancy setup ................................ 124
  System Manager through services port ......................................................................................... 89
Upgrade Configuration Details ........................................... 153
Upgrade Management .......................................................... 66
upgrade non-file encryption System Manager
  file encryption System Manager ...................................... 58
upgrade order
  Avaya Aura applications .................................................. 20
  Avaya Aura platform .......................................................... 20
  Avaya components ............................................................. 20
  Avaya Components ............................................................. 20
upgrade overview
  System Manager ............................................................... 13
upgrade path
  Amazon Web Services ..................................................... 131
  AWS .............................................................................. 131
  Azure ............................................................................ 132
  Google Cloud ................................................................. 131
  Microsoft Azure ............................................................. 132
  Software-only ................................................................. 136
upgrade paths ..................................................................... 14
upgrade procedures
  checklist ........................................................................... 116
upgrades
  third-party certificate ....................................................... 160
Upgrade System Manager ..................................................... 115
upgrade System Manager in Geographic Redundancy .... 118
upgrade System Manager using data migration utility ................................................................. 120, 127, 132
upgrade worksheet ............................................................. 17
upgrading
  from AVP to Software-only ............................................. 136
  from System Platform to Software-only .............................. 139
  from VMware to Software-only ......................................... 136
Upgrading
  VMware ESXi version ....................................................... 33
upgrading non-file encryption System Manager
  (continued) file encryption System Manager in the Geographic Redundancy setup ......................... 59
  using third-party certificates for upgrade from System Manager Release 6.2.x or earlier ............ 161
  using third-party certificates for upgrade from System Manager Release 6.3.x, 7.0.x or 8.0.x ...... 160
utility
  data migration ................................................................. 13

V

vCenter
  add .................................................................................. 55
  adding ............................................................................... 52
  add location ....................................................................... 53
  deleting ............................................................................... 54
  edit .................................................................................. 55
  editing ............................................................................... 53
  manage ............................................................................. 53
  remove location .................................................................. 53
  removing ............................................................................ 54
  unmanage ......................................................................... 53
vCentre
  field descriptions ............................................................ 54
  verify
    System Manager functionality ......................................... 150
  verify the current software version on System Manager .............................................................. 31
  videos ............................................................................... 203
  view
    location ........................................................................... 35
  viewing
    virtual machine report status ......................................... 50
  Viewing AVP host
    license status .................................................................. 43
  view location ..................................................................... 35
  virtualized environment-based System Manager
    upgrade ............................................................................ 63
  virtual machine
    migration ........................................................................ 188
  virtual machine report
    aborting ........................................................................... 50
    overview .......................................................................... 49
  VM connection reestablish .............................................. 49
  VMware-based System Manager 6.x
    upgrade on different server ........................................... 106
    upgrade on same server .................................................. 110
  VMware software requirements ........................................ 19

W

watch list ............................................................................ 202
WebLM Server on AVP host ................................................. 41
worksheet, upgrade, ................................................................ 17