© 2015-2020, Avaya Inc.
All Rights Reserved.

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

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

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

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailid=320951281124566561010 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 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 licplicable 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.

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

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

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Terms”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed open source software license terms provided as 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 THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS 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.

Service Provider
The following applies to Avaya Channel Partner's hosting of Avaya products or services. The product or hosted service may use third party components subject to third party terms and require a service provider to be independently licensed directly from the third party supplier. An Avaya Channel Partner’s hosting of Avaya products must be authorized in writing by Avaya and if those hosted products use or embed certain third party software, including but not limited to Microsoft software or codecs, the Avaya Channel Partner is required to independently obtain any applicable license agreements, at the Avaya Channel Partner’s expense, directly from the applicable third party supplier.

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

Deployment checklist.................................................................................................................. 45
Uploading a file to the software library.......................................................................................... 47
**Managing the location** ................................................................................................................ 48
  - Viewing a location...................................................................................................................... 48
  - Adding a location...................................................................................................................... 48
  - Editing the location.................................................................................................................. 49
  - Deleting a location................................................................................................................... 49
  - VM Management field descriptions.......................................................................................... 50
  - New and Edit location field descriptions.................................................................................. 55
**Managing the host** ....................................................................................................................... 56
  - Adding an Appliance Virtualization Platform or ESXi host....................................................... 56
  - Editing an ESXi host................................................................................................................ 58
  - Upgrading Appliance Virtualization Platform from Solution Deployment Manager............ 58
  - Changing the network parameters for an Appliance Virtualization Platform host.............. 60
  - Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager........................................................................................................ 62
  - Changing the password for an Appliance Virtualization Platform host................................ 65
  - Generating the Appliance Virtualization Platform kickstart file............................................. 66
  - Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager.................................................................................................................. 68
  - Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI........................................................................................................................................ 69
  - Changing the IP address and default gateway of the host......................................................... 70
  - Appliance Virtualization Platform license................................................................................ 71
  - Shutting down the Appliance Virtualization Platform host..................................................... 74
  - Restarting Appliance Virtualization Platform or an ESXi host................................................ 74
  - Removing an ESXi host............................................................................................................. 75
  - Configuring the login banner for the Appliance Virtualization Platform host........................ 75
  - Mapping the ESXi host to an unknown location..................................................................... 76
  - Applying third-party AVP certificates......................................................................................... 76
  - Deleting the virtual machine snapshot by using Solution Deployment Manager.................... 79
  - New and Edit host field descriptions........................................................................................ 80
  - Change Network Parameters field descriptions...................................................................... 81
  - Host Network / IP Settings field descriptions.......................................................................... 82
  - Change Password field descriptions....................................................................................... 83
  - Update Host field descriptions................................................................................................ 84
**Managing the virtual machine** .................................................................................................... 84
  - Deploying the System Manager OVA file by using the Solution Deployment Manager client... 84
  - Editing a virtual machine.......................................................................................................... 87
  - Starting a virtual machine from Solution Deployment Manager............................................ 88
  - Stopping a virtual machine from Solution Deployment Manager.......................................... 88
  - Restarting a virtual machine from Solution Deployment Manager.......................................... 89
  - Common causes for VM deployment failure............................................................................. 89
  - VM Deployment field descriptions........................................................................................... 90
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment checklist</td>
<td>119</td>
</tr>
<tr>
<td>Deploying the System Manager OVA by using vSphere Web Client</td>
<td>121</td>
</tr>
<tr>
<td>Deploying the application OVA using vSphere Web Client by accessing the host directly</td>
<td>123</td>
</tr>
<tr>
<td>Network and configuration field descriptions</td>
<td>125</td>
</tr>
<tr>
<td>Deployment of cloned and copied OVAs</td>
<td>130</td>
</tr>
<tr>
<td>Installing the System Manager Release 7.1.3 bin file</td>
<td>130</td>
</tr>
<tr>
<td>Starting the System Manager virtual machine</td>
<td>131</td>
</tr>
<tr>
<td>Postinstallation steps</td>
<td>132</td>
</tr>
<tr>
<td>Verifying the installation of System Manager</td>
<td>132</td>
</tr>
<tr>
<td>Installing language pack on System Manager</td>
<td>132</td>
</tr>
<tr>
<td>Enhanced Access Security Gateway (EASG) overview</td>
<td>133</td>
</tr>
<tr>
<td>Managing EASG from CLI</td>
<td>133</td>
</tr>
<tr>
<td>Viewing the EASG certificate information</td>
<td>134</td>
</tr>
<tr>
<td>EASG site certificate</td>
<td>134</td>
</tr>
<tr>
<td>Configuring Out of Band Management on System Manager</td>
<td>136</td>
</tr>
<tr>
<td>Configuring Out of Band Management on System Manager in the Geographic Redundancy setup</td>
<td>137</td>
</tr>
<tr>
<td>Enabling Multi Tenancy on Out of Band Management-enabled System Manager</td>
<td>138</td>
</tr>
<tr>
<td>configureOOBM command</td>
<td>139</td>
</tr>
<tr>
<td>Configuring the virtual machine automatic startup settings on VMware</td>
<td>139</td>
</tr>
<tr>
<td>SAL Gateway</td>
<td>140</td>
</tr>
<tr>
<td>Configuring hardware resources to support VE footprint flexibility</td>
<td>140</td>
</tr>
<tr>
<td>Virtualized Environment footprint flexibility</td>
<td>140</td>
</tr>
<tr>
<td>Reconfiguring hardware resources for flexible footprint</td>
<td>141</td>
</tr>
<tr>
<td>Capability and scalability specification</td>
<td>142</td>
</tr>
<tr>
<td>Geographic Redundancy configuration</td>
<td>143</td>
</tr>
</tbody>
</table>
Appendix A: Best Practices for VMware performance and features

BIOS .................................................................................................................. 175
Intel Virtualization Technology ........................................................................ 175
Dell PowerEdge Server .................................................................................... 176
HP ProLiant Servers ....................................................................................... 176
VMware Tools ................................................................................................ 177
Timekeeping .................................................................................................. 177
Configuring the NTP time ............................................................................. 178
VMware networking best practices ............................................................... 179
Storage ........................................................................................................... 183
Thin vs. thick deployments ........................................................................... 183
Best Practices for VMware features .............................................................. 184
VMware Snapshots ....................................................................................... 184
VMware Cloning ........................................................................................... 186
VMware High Availability .............................................................................. 186
Chapter 1: Introduction

Purpose

This document contains Avaya Aura® System Manager installation, configuration, initial administration, and basic maintenance checklist and procedures for Avaya-appliance and customer Virtualized Environment deployment methods.

This document is intended for people who install and configure a verified Avaya Aura® System Manager reference configuration at a customer site.

Prerequisites

Before you deploy or upgrade the product, ensure that you have the following knowledge, skills, and tools:

Knowledge
- Avaya Aura® releases
- Linux® operating system
- VMware® and virtualized environment

Skills
- VMware® and virtualized environment

Tools
- Avaya supported servers or VMware® supported servers
- Solution Deployment Manager client if System Manager is unavailable or unreachable
- System Manager virtual machine resource requirements for each profile.
- 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>10</td>
<td>May 2020</td>
<td>Updated the section: <strong>Storage</strong> on page 183</td>
</tr>
<tr>
<td>9</td>
<td>November 2018</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Deploying the application OVA using vSphere Web Client by accessing the host directly</strong> on page 123</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>VM Deployment field descriptions</strong> on page 90</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>System Manager command line interface operations</strong> on page 164</td>
</tr>
<tr>
<td>8</td>
<td>July 2018</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Methods of System Manager OVA deployment</strong> on page 18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>System Manager footprint hardware resource matrix</strong> on page 27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Deployment checklist</strong> on page 119</td>
</tr>
<tr>
<td>7</td>
<td>May 2018</td>
<td>For Release 7.1.3, added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Deleting the virtual machine snapshot by using Solution Deployment Manager</strong> on page 79</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Snapshot Manager field descriptions</strong> on page 80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Virtual machine report</strong> on page 98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>generate_report.sh command</strong> on page 98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Generating a virtual machine report</strong> on page 99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Viewing the status of the virtual machine report</strong> on page 99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Aborting the virtual machine report generation</strong> on page 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Release 7.1.3, updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Appliance Virtualization Platform overview</strong> on page 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Software requirements</strong> on page 29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>VM Management field descriptions</strong> on page 50</td>
</tr>
<tr>
<td>6</td>
<td>March 2018</td>
<td>Updated the <strong>System Manager command line interface operations</strong> on page 164 section.</td>
</tr>
<tr>
<td>5</td>
<td>January 2018</td>
<td>Added the <strong>Common causes for VM deployment failure</strong> on page 89 section.</td>
</tr>
<tr>
<td>Issue</td>
<td>Date</td>
<td>Summary of changes</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 4     | December 2017 | For Release 7.1.2, added the following sections:  
• Appliance Virtualization Platform license on page 71  
• Configuring WebLM Server for an Appliance Virtualization Platform host on page 72  
• WebLM Configuration field descriptions on page 73  
For Release 7.1.2, updated the following sections:  
• Software requirements on page 29  
• Edit Upgrade Configuration field descriptions on page 36  
• Upgrading Appliance Virtualization Platform from Solution Deployment Manager on page 58  
• Create AVP Kickstart field descriptions on page 66  
• Update Host field descriptions on page 84 |
| 3     | August 2017  | For Release 7.1.1, updated the following sections:  
• Adding an Appliance Virtualization Platform or ESXi host on page 56  
• Deployment checklist on page 45  
• Adding a vCenter to Solution Deployment Manager on page 107  
• New vCenter and Edit vCenter field descriptions on page 110  
• System Manager command line interface operations on page 164 |
| 2     | July 2017    | Updated the following sections:  
• configureOOBM command on page 139  
• System Manager command line interface operations on page 164  
• Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI on page 69  
• VM Deployment field descriptions on page 90  
• Restoring the primary System Manager server on page 152 |
| 1     | May 2017     | Release 7.1 document.
Chapter 2: Architecture overview

System Manager overview

Avaya Aura® System Manager is a central management system that provides a set of shared management services and a common console. All shared and element specific management for Avaya Aura® applications that System Manager supports is done from the common console. System Manager provides the following key capabilities:

- Centralized software management solution to support deployments, migrations, upgrades, and updates to the suite of Avaya Aura® applications
- Avoid duplicate data entry through shared management services
- Centralized access to all Avaya Aura® applications through a browser-based Avaya management console with single sign on
- Optimize IT skill sets with consistency of management functions across Avaya solutions
- Integration with enterprise IT infrastructure, such as identity management, authentication, authorization, security, and enterprise directory

You can download System Manager from the Avaya Support website at http://support.avaya.com or order the System Manager software DVD.

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized offers

Avaya Aura® Release 7.0 and later supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.0.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

The virtualization offers provide the following benefits:

- Simplifies IT management using common software administration and maintenance.
• Requires fewer servers and racks which reduces the footprint.
• Lowers power consumption and cooling requirements.
• Enables capital equipment cost savings.
• Lowers operational expenses.
• Uses standard operating procedures for both Avaya and non-Avaya products.
• Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
• Business can scale rapidly to accommodate growth and to respond to changing business requirements.

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized Appliance is a turnkey solution. Avaya provides the hardware, all the software including the VMware hypervisor and might also offer the customer support of the setup. Virtualized Appliance offer is different from Avaya Aura® Virtualized Environment, where Avaya provides the Avaya Aura® application software and the customer provides and supports the VMware hypervisor and the hardware on which the hypervisor runs.

Deployment considerations

• Deployment on the Appliance Virtualization Platform server is performed from the System Manager Solution Deployment Manager or the Solution Deployment Manager standalone Windows client.
• Avaya provides the servers, Appliance Virtualization Platform, which includes the VMware ESXi hypervisor.

Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

• Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
• S8300D and S8300E

⚠️ Note:


⚠️ Note:

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for
Communication Manager LSP and Branch Session Manager with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to the Release 7.1.3.

Consider the following options if the higher capacity is required from the S8300D:

- Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before.
- Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: [https://downloads.avaya.com/css/P8/documents/101048606](https://downloads.avaya.com/css/P8/documents/101048606).

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.
You can deploy the following applications on Appliance Virtualization Platform:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

**Note:**

For deploying Avaya Aura® applications on Appliance Virtualization Platform only use Solution Deployment Manager.

---

**Avaya Aura® Virtualized Environment overview**

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

The Virtualized Environment project applies only for Avaya Aura® Appliance Virtualization Platform and customer VMware®, and does not include any other industry hypervisor.
Avaya Aura® Virtualized Appliance overview

Note:
This document uses the following terms, and at times, uses the terms interchangeably.
• server and host
• reservations and configuration values

Deployment considerations
The following manage the deployment to the blade, cluster, and server:
• Avaya Aura® Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
• VMware® vCenter and VMware® vSphere

Avaya Pod Fx for Enterprise Communications
Avaya Pod Fx for Enterprise Communications is an alternative deployment option for Avaya Aura® Virtualized Environment applications.

Avaya Pod Fx is a full-stack turnkey solution that combines storage arrays from EMC, virtualization software from VMware, and networking, management, and real-time applications from Avaya.

Avaya Pod Fx accelerates deployment of Avaya Aura® applications and simplifies IT operations.

Documentation
The following table lists the Avaya Pod Fx for Enterprise Communications documents. These documents are available on the Avaya support website at http://support.avaya.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide</td>
<td>Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide</td>
<td>Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Avaya Pod Fx. This guide explains how to access and use the applications in the POS management suite.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation</td>
<td>Identifies the Avaya Pod Fx customer documentation. Also includes the documentation for the Avaya and non-Avaya products that are included in the Avaya Pod Fx solution.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Release Notes</td>
<td>Describes fixed and known issues for Avaya Pod Fx. This document does not describe issues associated with each component in the Avaya Pod Fx. For information on the specific components, see the component Release Notes.</td>
</tr>
</tbody>
</table>

Avaya Aura® Virtualized Appliance overview

Note:
This document uses the following terms, and at times, uses the terms interchangeably.
• server and host
• reservations and configuration values

Deployment considerations
The following manage the deployment to the blade, cluster, and server:
• Avaya Aura® Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
• VMware® vCenter and VMware® vSphere

Avaya Pod Fx for Enterprise Communications
Avaya Pod Fx for Enterprise Communications is an alternative deployment option for Avaya Aura® Virtualized Environment applications.

Avaya Pod Fx is a full-stack turnkey solution that combines storage arrays from EMC, virtualization software from VMware, and networking, management, and real-time applications from Avaya.

Avaya Pod Fx accelerates deployment of Avaya Aura® applications and simplifies IT operations.

Documentation
The following table lists the Avaya Pod Fx for Enterprise Communications documents. These documents are available on the Avaya support website at http://support.avaya.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide</td>
<td>Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide</td>
<td>Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Avaya Pod Fx. This guide explains how to access and use the applications in the POS management suite.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation</td>
<td>Identifies the Avaya Pod Fx customer documentation. Also includes the documentation for the Avaya and non-Avaya products that are included in the Avaya Pod Fx solution.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Release Notes</td>
<td>Describes fixed and known issues for Avaya Pod Fx. This document does not describe issues associated with each component in the Avaya Pod Fx. For information on the specific components, see the component Release Notes.</td>
</tr>
</tbody>
</table>

Avaya Aura® Virtualized Appliance overview

Note:
This document uses the following terms, and at times, uses the terms interchangeably.
• server and host
• reservations and configuration values

Deployment considerations
The following manage the deployment to the blade, cluster, and server:
• Avaya Aura® Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
• VMware® vCenter and VMware® vSphere

Avaya Pod Fx for Enterprise Communications
Avaya Pod Fx for Enterprise Communications is an alternative deployment option for Avaya Aura® Virtualized Environment applications.

Avaya Pod Fx is a full-stack turnkey solution that combines storage arrays from EMC, virtualization software from VMware, and networking, management, and real-time applications from Avaya.

Avaya Pod Fx accelerates deployment of Avaya Aura® applications and simplifies IT operations.

Documentation
The following table lists the Avaya Pod Fx for Enterprise Communications documents. These documents are available on the Avaya support website at http://support.avaya.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide</td>
<td>Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide</td>
<td>Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Avaya Pod Fx. This guide explains how to access and use the applications in the POS management suite.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation</td>
<td>Identifies the Avaya Pod Fx customer documentation. Also includes the documentation for the Avaya and non-Avaya products that are included in the Avaya Pod Fx solution.</td>
</tr>
<tr>
<td>Avaya Pod Fx for Enterprise Communications – Release Notes</td>
<td>Describes fixed and known issues for Avaya Pod Fx. This document does not describe issues associated with each component in the Avaya Pod Fx. For information on the specific components, see the component Release Notes.</td>
</tr>
</tbody>
</table>
Avaya Aura® virtualized software

Software delivery
The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS) and the Avaya support site. Each OVA contains the following components:

- The application software and operating system.
- Preinstalled VMware tools.
- Preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Note:
The customer provides the servers and the VMware® infrastructure, that includes VMware® licenses.

Patches and upgrades
A minimum patch level can be required for each supported application. For more information about the application patch requirements, see the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Important:
Do not upgrade the VMware tools software that is packaged with each OVA unless Avaya instructs you to upgrade. The supplied version is the supported release and has been thoroughly tested.

Performance and capacities
The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:
Modifying configuration values might have a direct impact on the performance, capacity, and stability of the virtual machine. Customer must understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) might not be able to assist in fully resolving a problem if the virtual hardware or resource allocation has been changed to unsupported values for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

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

- For Avaya-appliance deployments, use the Solution Deployment Manager client
For information, see Deploying the System Manager OVA file by using the Solution Deployment Manager client.

- For customer Virtualized Environment on VMware, use vSphere Web Client or vCentre

For more information, see Deploying System Manager on VMware.

⚠️ Note:

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

Related links

- Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 84
- Deploying the System Manager OVA by using vSphere Web Client on page 121
- Deploying the application OVA using vSphere Web Client by accessing the host directly on page 123

---

**Virtual machine management**

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

VM Management provides the following capabilities:

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

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

Related links

- Certification validation on page 101
Topology

The following is an example of a deployment infrastructure for System Manager on VMware.

Virtualized components

<table>
<thead>
<tr>
<th>Software component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Host</td>
<td>The physical machine running the ESXi Hypervisor software.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Software component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Hypervisor</td>
<td>A platform that runs multiple operating systems on a host computer at the same time.</td>
</tr>
<tr>
<td>vSphere Client</td>
<td>vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface. The installable vSphere Client is not available in vSphere 6.5 and later releases.</td>
</tr>
<tr>
<td>vSphere Web Client</td>
<td>Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.</td>
</tr>
<tr>
<td>vSphere Client (HTML5)</td>
<td>vSphere Client (HTML5) is available in vSphere 6.5. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.</td>
</tr>
<tr>
<td>Appliance Virtualization Platform</td>
<td>Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.</td>
</tr>
<tr>
<td>Solution Deployment Manager</td>
<td>Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.</td>
</tr>
<tr>
<td>Open Virtualization Appliance (OVA)</td>
<td>The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.</td>
</tr>
</tbody>
</table>

**OVA deployment order**

Deploy the application OVA files in the following order:

- Utility Services
- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- SAL
- Communication Manager Messaging
- Avaya Aura® Media Server
• Avaya Breeze™ 3.3.x with Presence Services

After the application OVA files have been deployed, you can deploy Agile Communication Environment™ and, WebLM in any order.

---

Deployment guidelines

• Deploy as many virtual appliances on the same host as possible.

• Deploy the virtual appliances on the same cluster if the cluster goes beyond the host boundary.

• Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.

• Create a tiered or segmented cluster infrastructure that isolates critical applications, such as Avaya Aura® applications, from other virtual machines.

• Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.

• Do not oversubscribe resources. Oversubscribing affects performance.

• Monitor the server, host, and virtual appliance performance.

⚠️ Important:

The values for performance, occupancy, and usage can vary greatly. The blade server might run at 5% occupancy, but a virtual machine might run at 50% occupancy. Note that a virtual machine behaves differently when the CPU usage is higher.
### Prerequisites

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the System Manager software from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</td>
<td>See “Software details of System Manager”.</td>
</tr>
</tbody>
</table>
| 2             | Verify that the existing server is compatible with System Manager Release 7.1.3. If the existing server is incompatible, change the server as instructed in the workflow described in this chapter. | Release 7.0 and later supports the following servers:  
• Dell™ PowerEdge™ R610  
• HP ProLiant DL360 G7  
• Dell™ PowerEdge™ R620  
• HP ProLiant DL360p G8  
• Dell™ PowerEdge™ R630  
• HP ProLiant DL360 G9 |
| 3             | Keep the following checklists:  
• The System Manager Release 7.1.3 installation checklist  
• Upgrade checklist |
| 4             | Keep the following information handy to create a backup on the remote server:  
• IP address  
• Directory  
• User Name  
• Password |
| 5             | 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 System Manager Release 7.1.3. | For more information about managing users and custom roles, see *Administering Avaya Aura® System Manager*. |
Upgrade worksheet

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

<table>
<thead>
<tr>
<th>Serial Number</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>
</tbody>
</table>

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 7.0 and later:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9

For fresh installations, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9.
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).

Latest software updates and patch information

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

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

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

Software details of System Manager

You can download the following software from the Avaya PLDS website at [http://plds.avaya.com/](http://plds.avaya.com/).

<table>
<thead>
<tr>
<th>Product name</th>
<th>Release version and Service pack</th>
<th>OVA details</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Manager</td>
<td>Release 7.1.3</td>
<td>• <strong>Profile 1 and Profile 2:</strong> SMGR-7.1.0.0.1125193-e65-50.ova</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Profile 3:</strong> SMGR-PROFILE3-7.1.0.0.1125193-e65-50.ova</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Patch:</strong> System_Manager_7.1.3.0_r713007763.bin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Data Migration Utility:</strong> datamigration-146.bin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Solution Deployment Manager:</strong> Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip contains Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe</td>
</tr>
</tbody>
</table>
Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring System Manager open virtual application (OVA):

- Solution Deployment Manager client running on your computer
- A remote computer running the VMware vSphere Client
- A browser for accessing the System Manager web interface
- An SFTP client for Windows, for example WinSCP
- An SSH client, for example, PuTTy

Customer configuration data

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.

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

**Important:**

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

<table>
<thead>
<tr>
<th>Required data</th>
<th>Value for the system</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (Out of Band Management) and Public network configuration</td>
<td>IP address</td>
<td>172.16.1.10</td>
</tr>
<tr>
<td>Configure Public network details only when Out of Band Management is enabled.</td>
<td>Netmask</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td></td>
<td>DNS Server IP address</td>
<td>172.16.1.2</td>
</tr>
<tr>
<td></td>
<td>Short hostname</td>
<td>myhost. The host name must be a valid short name.</td>
</tr>
<tr>
<td></td>
<td>Domain name</td>
<td>mydomain.com</td>
</tr>
<tr>
<td></td>
<td>Default search list</td>
<td>mydomain.com</td>
</tr>
<tr>
<td></td>
<td>NTP server</td>
<td>172.16.1.100</td>
</tr>
<tr>
<td></td>
<td>Time zone</td>
<td>America/Denver</td>
</tr>
</tbody>
</table>

*Note:*

System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.

Table continues…
System Manager footprint hardware resource matrix

The following table describes the resource requirements to support different profiles for System Manager in Avaya-Appliance offer and customer Virtualized Environment.

Table 1: Avaya Appliance Virtualization Platform

<table>
<thead>
<tr>
<th>VMware resource</th>
<th>Profile-1</th>
<th>Profile-2</th>
<th>Profile-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Reserved</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Minimum vCPU Speed</td>
<td>2290 MHz</td>
<td>2290 MHz</td>
<td>2290 MHz</td>
</tr>
<tr>
<td>Virtual RAM</td>
<td>8916 MB</td>
<td>12 GB</td>
<td>18 GB</td>
</tr>
<tr>
<td>Virtual Hard Disk</td>
<td>105 GB</td>
<td>105 GB</td>
<td>250 GB</td>
</tr>
<tr>
<td>Number of users</td>
<td>Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager</td>
<td>&gt;35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager</td>
<td>&gt;35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager</td>
</tr>
<tr>
<td>Common Server R1 support</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Common Server R2 and R3 support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: Customer Virtualized Environment

<table>
<thead>
<tr>
<th>VMware resource</th>
<th>Profile-1</th>
<th>Profile-2</th>
<th>Profile-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Reserved</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>VMware resource</td>
<td>Profile-1</td>
<td>Profile-2</td>
<td>Profile-3</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Minimum vCPU Speed</td>
<td>2290 MHz</td>
<td>2290 MHz</td>
<td>2290 MHz</td>
</tr>
<tr>
<td>CPU reservation</td>
<td>9160 MHz</td>
<td>13740 MHz</td>
<td>18320 MHz</td>
</tr>
<tr>
<td>Virtual RAM</td>
<td>9 GB</td>
<td>12 GB</td>
<td>18 GB</td>
</tr>
<tr>
<td>Memory reservation</td>
<td>9216 MB</td>
<td>12288 MB</td>
<td>18432 MB</td>
</tr>
<tr>
<td>Virtual Hard Disk</td>
<td>105 GB</td>
<td>105 GB</td>
<td>250 GB</td>
</tr>
<tr>
<td>Shared NICs</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IOPS</td>
<td>-</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>Number of users</td>
<td>Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager</td>
<td>&gt;35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager</td>
<td>&gt;35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager</td>
</tr>
</tbody>
</table>

Related links

Adjusting the System Manager virtual machine properties on page 28

### Adjusting the System Manager virtual machine properties

**About this task**

If the system encounters CPU resource limitations, the system displays a message similar to *Insufficient capacity on each physical CPU*. To correct the CPU limitation, you require to adjust the virtual machine properties.

If the CPU adjustments you make does not correct the virtual machine start up conditions, you must further reduce the CPU speed. Use the same procedure to reduce the values for other virtual machine resources.

Do not modify the resource settings, for example, remove the resources altogether. Modifying the allocated resources can have a direct impact on the performance, capacity, and stability of the System Manager virtual machine. To run the System Manager virtual machine at full capacity, the resource size requirements must be met; removing or greatly downsizing reservations could put the resource size requirement at risk.

⚠️ **Important:**

Any deviation from the requirement is at your own risk.

**Procedure**

1. Right click on the virtual machine and select **Edit Settings**....

   The system displays the Virtual Machine Properties dialog box.

2. Click the **Resources** tab.

   In the left pane, the system displays the details for CPU, memory, disk advanced CPU, and advanced memory.
3. Select CPU.

4. In the Resource Allocation area, in the Reservation field, perform one of the following to start the virtual machine:
   - Adjust the slider to the appropriate position.
   - Enter the exact value.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 7.1.2 and later on a customized version of VMware® ESXi 6.0.
- Customer-provided Virtualized Environment offer: Supports the following software versions:
  - VMware® vSphere ESXi 5.5
  - VMware® vSphere ESXi 6.0
  - VMware® vSphere ESXi 6.5
  - VMware® vSphere ESXi 6.7
  - VMware® vCenter Server 5.5
  - VMware® vCenter Server 6.0
  - VMware® vCenter Server 6.5
  - VMware® vCenter Server 6.7


Note:

- vSphere ESXi 6.7 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.7.
- vSphere ESXi 6.5 is supported for Avaya Aura® Release 7.1 and later. Avaya Aura® Release 7.0.x and earlier does not support vSphere ESXi 6.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.
- Avaya Aura® Release 7.1 and later does not support vSphere ESXi 5.0 and 5.1.
Installing the Solution Deployment Manager client on your computer

About this task

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

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

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

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

Procedure

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

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

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

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

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

   The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click Next.

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

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

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

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

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

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

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

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

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

      You can save the artifacts in the specified directory.

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

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

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

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

      **Note:**

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

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

11. Click **Next**.

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

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

13. Click **Install**.

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

   The installer creates a shortcut on the desktop.

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

**Next steps**

- Configure the laptop to get connected to the services port if you are using the services port to install.

- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.
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, perform one of the following:

- On your computer, click **Start > All Programs > Avaya**, and click **SDM Client > Avaya SDM Client**.
- On your desktop, click ![SDM Client icon](SDM-client.png).

## Accessing Solution Deployment Manager

### About this task

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

### Procedure

Perform one of the following:

- If System Manager is not already deployed, double-click the Solution Deployment Manager client.
- If System Manager is available, on the web console, click **Services > Solution Deployment Manager**.
Deploying the Utility Services OVA file through System Manager Solution Deployment Manager

About this task

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

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

Before you begin

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

Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click New.
   
   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In Select Location, select a location.
   b. In Select Host, select a host.
   
   The system displays the host name in the Host FQDN field.
5. In Data Store, select a data store, if not displayed upon host selection.
   
   The page displays the capacity details.
6. Click Next.
7. In the Deploy OVA section, perform the following:
   a. In Select Software Library, select the local or remote library where the OVA file is available.
   
      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
b. In **Select OVA**, select the OVA file that you want to deploy.

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

- **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
- **Default**: For all other server platforms.

8. Click **Next**.

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

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

   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled

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

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

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

11. Click **Deploy**.

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

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

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

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

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

14. Reboot the Utility Services virtual machine.

**Next steps**

1. To activate the serviceability agent registration, reset the Utility Services virtual machine.

2. Deploy all other Avaya Aura® applications one at a time.

---

**Installing software patches**

**About this task**

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

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

**Before you begin**

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

**Procedure**

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

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

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

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

14. Click **Schedule**.

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

15. To view the update status, click ✔.

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

   When the update is complete, the **Update status** and **Last Action Status** fields display ✔.

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

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

   The page displays all software patches that you can commit.

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

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

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

19. Click **Schedule**.

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

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

    🟢 **Note:**

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

---

**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</td>
<td>The ESXi 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>• List of hosts that you added from VM Management</td>
</tr>
<tr>
<td>Migrate With AVP Install</td>
<td>The option to migrate System Platform-based system and Communication Manager Release 5.2.1 bare metal system to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.</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 populations 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 Communication Manager and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

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

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-populate Data</td>
<td>The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. For Communication Manager Messaging, the button is unavailable and you must fill in all details. For Communication Manager Messaging you must provide a new IP address.</td>
</tr>
<tr>
<td>CM IPv4 Address</td>
<td>The IP address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Netmask</td>
<td>The network mask of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv4 Gateway</td>
<td>The default gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Address</td>
<td>The IPv6 address of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>CM IPv6 Gateway</td>
<td>The IPv6 default gateway of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>Out of Band Management IPv4 Address</td>
<td>The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management Netmask</td>
<td>The subnetwork mask of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Address</td>
<td>The IPv6 address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Network Prefix</td>
<td>The IPv6 network prefix of the virtual machine for out of band management.</td>
</tr>
<tr>
<td>CM Hostname</td>
<td>The hostname of the Communication Manager virtual machine.</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>The DNS IP address of the virtual machine.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search Domain List</td>
<td>The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).</td>
</tr>
<tr>
<td>WebLM Server IPv4 Address</td>
<td>The IP address of WebLM. The field is mandatory.</td>
</tr>
<tr>
<td>CM Privileged Administrator User Login</td>
<td>The login name for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td>CM Privileged Administrator User Password</td>
<td>The password for the privileged administrator. You can change the value at any point of time.</td>
</tr>
<tr>
<td>Flexi Footprint</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>Public</td>
<td>The port number that you must assign to public port group.</td>
</tr>
<tr>
<td>Out of Band Management</td>
<td>The port number that is assigned to the out of band management port group. The field is available only when you select a different host.</td>
</tr>
<tr>
<td>Private</td>
<td>Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.</td>
</tr>
<tr>
<td>Services</td>
<td>The port number that is assigned to the services port. The system displays this field when Utility Services is available.</td>
</tr>
<tr>
<td>Duplication link</td>
<td>The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process. The field is available only for the Communication Manager duplex configuration and when you select a different host.</td>
</tr>
<tr>
<td>Datastore</td>
<td>The datastore on the target ESXi host. The field is available only when you select a different host.</td>
</tr>
</tbody>
</table>

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

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

### AVP Configuration: Existing Machine Details

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

### AVP Configuration: Configuration Details

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

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

**Enable: (Recommended)**

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

**Disable**

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

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the changes that you made to the Edit Upgrade Configuration page.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the changes that you made to the Edit Upgrade Configuration page.</td>
</tr>
</tbody>
</table>
# Chapter 4: Deploying System Manager on the Avaya-provided server

## Deployment checklist

Use the following checklist to deploy the System Manager Release 7.1.3 virtual application by using the Solution Deployment Manager client.

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Link/Notes</th>
</tr>
</thead>
</table>
| 1  | Download the following software from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com):  
  • OVA files for Utility Services and System Manager  
  For System Manager, SMGR-7.1.0.0.1125193-e65-50.ova or SMGR-PROFILE3-7.1.0.0.1125193-e65-50.ova, the System Manager high capacity OVA.  
  • The System Manager Release 7.1.3 bin file.  
  • The Solution Deployment Manager client,  
  Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip | ✔ |
| 2  | Upload the software that is required for deployment on the computer on which the Solution Deployment Manager client is installed. For example, OVA file, firmware, software patches, service packs, and images. | - |

*Table continues...*
<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>For Avaya Aura® Virtualized Appliance deployments, install the supported server. Appliance Virtualization Platform is preinstalled on the server.</td>
<td>Supported servers on page 24</td>
</tr>
<tr>
<td>4</td>
<td>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. Ensure that the license file copies are accessible.</td>
<td>-</td>
</tr>
</tbody>
</table>
| 5  | Ensure that the following information is handy:  
   • FQDN/IP address, netmask, and gateway  
   • Out of Band Management configuration details.                                                                 | -                                                                        |
| 6  | Install the Avaya_SDMClient_win64_7.1.3.0.0330162_32.exe file.                                                                                                                                         |                                                                          |
| 7  | Add a location.                                                                                                                                                                                          | Adding a location on page 48                                             |
| 8  | Add the Appliance Virtualization Platform host.                                                                                                                                                          | Adding an Appliance Virtualization Platform or ESXi host on page 56      |
| 9  | Deploy Utility Services OVA, and select the appropriate footprint size and the service mode.                                                                                | While deploying OVA, provide the IP address of System Manager that you want to deploy. Deploying the Utility Services OVA file through System Manager Solution Deployment Manager on page 33 |
| 10 | Deploy the System Manager OVA file and provide the network parameters and configuration parameters.                                                                                                   | Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 84 |
| 11 | Install the System Manager Release 7.1.3 bin file. The patch installation takes about 60–65 minutes to complete.                                                                                         | Installing service packs and software patches on System Manager by using the Solution Deployment Manager client on page 100 |

**Note:**

You can install the System Manager Release 7.1.3 bin file during the deployment or after completing the System Manager OVA deployment.
<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>To activate the serviceability agent registration, reset the Utility Services virtual machine.</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>(Optional) After a kernel upgrade, when the system prompts, reboot the System Manager virtual machine.</td>
<td>Starting a virtual machine from Solution Deployment Manager on page 88</td>
</tr>
<tr>
<td>14</td>
<td>Verify the deployment of the System Manager virtual machine.</td>
<td>Verifying the installation of System Manager on page 132</td>
</tr>
<tr>
<td>15</td>
<td>In the settings icon (前列), click About to verify that the System Manager version is Release 7.1.3.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Uploading a file to the software library**

**About this task**

Use the procedure to upload software files, such as OVA, images, and firmware that are required during the deployment, migration, upgrade, and update of Avaya Aura® applications.

**Before you begin**

- Start an SSH session.
- On Download Management page, click **Refresh Families**.
- When you add or update details in the `versions.xml` file, click **Refresh Families** again to get the updated information.

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. From the System Manager command line interface, copy the required OVA file to the `/swlibrary/staging/sync/` location that you had created in System Manager.

   ❗ Note:

   You require admin privileges to access the `/swlibrary/staging/sync/` location.

   The system displays the file that you copied in the Sync Files from directory section.
5. Provide the following information:

   - **MD5 Checksum**: The value mentioned in the source or original location of the file.
   - **Software Library**: The local or remote software library.
• Product Family

Note:
For SAL, in **Product Family**, **Device Type**, and **Software Type** fields, select **Others**.

• Device Type
• Software Type

If the file is already in *versions.xml*, the system populates the information.

If the file does not exist in *versions.xml*, the system does not display the file details. Therefore, you cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from VM Management.

6. Select the file.
7. Click **Sync**.

In File Sync Started Message, the system displays the status of the schedule of the job.

8. Click **OK**.

When the job completes, the system displays the file in the Software Library Files section.

9. To check the status of the job, click **Services > Scheduler > Pending Jobs**.

When the job is complete, the system displays the file in the Software Library Files area and removes from Sync Files from directory.

--

**Managing the location**

**Viewing a location**

**Procedure**

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

   The Locations section lists all locations.

**Adding a location**

**About this task**

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

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

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

Related links
New and Edit location field descriptions on page 55

---

Editing the location

Procedure

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

Related links
New and Edit location field descriptions on page 55

---

Deleting a location

Procedure

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

   The system does not delete the virtual machines that are running on the host, and moves the host to Unknown location host mapping > Unknown location.
## VM Management field descriptions

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

### Locations

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

### Button

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Displays the New Location section where you can provide the details of the location that you want to add.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the Edit Location section where you can change the details of an existing location.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the locations that you select. The system moves the hosts associated with the deleted locations to unknown location.</td>
</tr>
</tbody>
</table>

### Hosts

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The name of the host.</td>
</tr>
<tr>
<td>Host IP</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Host FQDN</td>
<td>FQDN of the host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the host.</td>
</tr>
<tr>
<td>vCenter FQDN</td>
<td>FQDN of vCentre.</td>
</tr>
<tr>
<td>Current Action</td>
<td>The operation that is currently being performed on the host.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last completed operation on the host.</td>
</tr>
<tr>
<td>License Status</td>
<td>The status of the license.</td>
</tr>
<tr>
<td>Host Version</td>
<td>The host version.</td>
</tr>
<tr>
<td>Offer Type</td>
<td>The host type. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>AVP</strong>: Appliance Virtualization Platform host</td>
</tr>
<tr>
<td></td>
<td>• <strong>Customer VE</strong>: customer-provided VMware ESXi host</td>
</tr>
</tbody>
</table>
### SSH Status

The SSH service status. The values are enabled and disabled.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSH Status</strong></td>
<td>The SSH service status. The values are enabled and disabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Certificate</strong></td>
<td>The certificate status of the Appliance Virtualization Platform host. The values are:</td>
</tr>
<tr>
<td></td>
<td>• ✔: The certificate is added in Solution Deployment Manager and correct.</td>
</tr>
<tr>
<td></td>
<td>• ✗: The certificate is not accepted or invalid.</td>
</tr>
<tr>
<td></td>
<td>You can click View for details of the certificate status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vCenter Certificate</strong></td>
<td>The certificate status of the ESXi host. The values are:</td>
</tr>
<tr>
<td></td>
<td>• ✔: The certificate is correct.</td>
</tr>
<tr>
<td></td>
<td>The system enables all the options in More Actions that apply to VMware ESXi host.</td>
</tr>
<tr>
<td></td>
<td>• ✗: The certificate is not accepted or invalid.</td>
</tr>
<tr>
<td></td>
<td>You can click View for details of the certificate status.</td>
</tr>
</tbody>
</table>

**Note:**

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

### Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto Refresh</strong></td>
<td>The option to automatically refresh the page with the latest changes. For example, the page updates:</td>
</tr>
<tr>
<td></td>
<td>• The VM state when a virtual machine changes</td>
</tr>
<tr>
<td></td>
<td>• The license status or certificate status of host when host changes</td>
</tr>
<tr>
<td></td>
<td>The system refreshes the data every minute.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td>Displays the New Host section where you can provide the details of the host that you want to add.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Displays the Host Information section where you can change the details of an existing host.</td>
</tr>
<tr>
<td><strong>Remove</strong></td>
<td>Removes the hosts that you select only from the Solution Deployment Manager client. The system moves the hosts associated with the deleted locations to unknown location.</td>
</tr>
<tr>
<td><strong>Change Network Params &gt; Change Host IP Settings</strong></td>
<td>Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Network Params &gt; Change Network Settings</strong></td>
<td>Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Refreshes the status of the hosts.</td>
</tr>
<tr>
<td><strong>More Actions &gt; AVP Update/Upgrade Management</strong></td>
<td>Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>More Actions &gt; Change Password</strong></td>
<td>Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>More Actions &gt; SSH &gt; Enable SSH</strong></td>
<td>Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays <em>SSH enabled successfully.</em></td>
</tr>
<tr>
<td><strong>More Actions &gt; SSH &gt; Disable SSH</strong></td>
<td>Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays <em>Disabling SSH for AVP host with &lt;IP address&gt; &lt;FQDN&gt;, &lt;username&gt;.</em></td>
</tr>
<tr>
<td><strong>More Actions &gt; Syslog config &gt; Push</strong></td>
<td>Displays the Push Syslog Configuration section where you can push the syslog configuration on the virtual machine host. Also Syslog is only for Appliance Virtualization Platform. You can select multiple Hosts and Push syslog configuration on selected hosts.</td>
</tr>
<tr>
<td><strong>More Actions &gt; Syslog config &gt; View</strong></td>
<td>Displays the View Syslog Configuration section where you can view syslog profiles of selected the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>More Actions &gt; Syslog config &gt; Delete</strong></td>
<td>Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.</td>
</tr>
<tr>
<td><strong>More Actions &gt; Lifecycle Actions &gt; Host Restart</strong></td>
<td>Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.</td>
</tr>
<tr>
<td><strong>More Actions &gt; Lifecycle Actions &gt; Host Shutdown</strong></td>
<td>Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Button Description

- **More Actions > AVP Cert. Management > Generate/Accept Certificate**
  - Displays the Certificate dialog box where you can manage certificates for the host.
  - Depending on the host type, the options are:
    - **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only.
    - **Accept Certificate**: To accept a valid certificate for the host or vCenter.
    - **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate.

- **More Actions > AVP Cert. Management > Manage Certificate**
  - Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected host.

- **More Actions > AVP Cert. Management > Generic CSR**
  - Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.

- **More Actions > Snapshot Manager**
  - Displays the Snapshot Manager dialog box from where you can view and delete the virtual machine snapshot.

- **More Actions > WebLM Configuration**
  - Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.

- **More Actions > Set Login Banner**
  - Displays the Message of the Day dialog box from where you can push the login banner text to the selected host.

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

### Virtual Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>VM IP</td>
<td>The IP address of the virtual machine.</td>
</tr>
<tr>
<td>VM FQDN</td>
<td>FQDN of the virtual machine.</td>
</tr>
<tr>
<td>VM IPv6</td>
<td>The IPv6 address of the virtual machine, if any.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM App Name</td>
<td>The name of the application virtual machine. For example, Session Manager.</td>
</tr>
<tr>
<td>VM App Version</td>
<td>The version of the application virtual machine. For example, 7.1.</td>
</tr>
<tr>
<td>VM State</td>
<td>The state of the virtual machine. The states are <strong>Started</strong> and <strong>Stopped</strong>.</td>
</tr>
<tr>
<td>Current Action Status</td>
<td>The status of the current operation. The statuses are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deploying</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Starting</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Stopping</strong></td>
</tr>
<tr>
<td></td>
<td>The <strong>Status Details</strong> link provides the details of the operation in progress.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last action performed on the virtual machine.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The hostname of the VMware host or Appliance Virtualization Platform host on which the virtual machine resides.</td>
</tr>
<tr>
<td>Trust Status</td>
<td>The status of the connection between System Manager and the virtual machine.</td>
</tr>
<tr>
<td></td>
<td>The status can be <strong>Success</strong> or <strong>Failed</strong>.</td>
</tr>
<tr>
<td></td>
<td>When the connection between System Manager and the virtual machine establishes, <strong>Trust Status</strong> changes to <strong>Success</strong>.</td>
</tr>
<tr>
<td></td>
<td>Only when the trust status is <strong>Success</strong>, you can perform other operations.</td>
</tr>
<tr>
<td>Data Store</td>
<td>The data store name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Displays the VM Deployment section where you can provide the host and deploy an application.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the VM Deployment section where you can change the details of a virtual machine.</td>
</tr>
<tr>
<td>Delete</td>
<td>Turns off the virtual machines and deletes the selected virtual machine from host and Solution Deployment Manager Client.</td>
</tr>
<tr>
<td>Start</td>
<td>Starts the selected virtual machines.</td>
</tr>
<tr>
<td>Stop</td>
<td>Stops the selected virtual machines.</td>
</tr>
<tr>
<td>Show Selected</td>
<td>Displays only the selected virtual machines.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Actions &gt; Restart</td>
<td>Starts the selected virtual machines that were stopped earlier.</td>
</tr>
<tr>
<td>More Actions &gt; Refresh VM</td>
<td>Updates the status of the virtual machines.</td>
</tr>
<tr>
<td>More Actions &gt; Re-establish connection</td>
<td>Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the <strong>Trust Status</strong> changes to <strong>Success</strong>.</td>
</tr>
<tr>
<td>More Actions &gt; Update Static Routing</td>
<td>Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.</td>
</tr>
<tr>
<td>More Actions &gt; Syslog config &gt; Push</td>
<td>Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected virtual machine.</td>
</tr>
<tr>
<td>More Actions &gt; Syslog config &gt; View</td>
<td>Displays the View Syslog Configuration section where you can view all configured syslog profiles.</td>
</tr>
<tr>
<td>More Actions &gt; Syslog config &gt; Delete</td>
<td>Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.</td>
</tr>
</tbody>
</table>

---

**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>
</tbody>
</table>

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

<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 an standalone ESXi host to System Manager Solution Deployment Manager or to the Solution Deployment Manager client, add the standalone ESXi host using its FQDN only.

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

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

Before you begin
A location must be available.
Procedure

1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> section, click Add.
4. In the New Host section, provide the Host name, IP address or FQDN, user name, and password.
5. Click Save.

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

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

7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select the required virtual machine.
   b. Click More Actions > Re-establish connection.
      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click More Actions > Refresh VM.

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

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

Next steps

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

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

Related links
New and Edit host field descriptions on page 80
Generating and accepting certificates on page 103

Editing an ESXi host

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

Related links
New and Edit host field descriptions on page 80

Upgrading Appliance Virtualization Platform from Solution Deployment Manager

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

Note:
• From System Manager Solution Deployment Manager, you cannot update Appliance Virtualization Platform that hosts this System Manager.
• When you update Appliance Virtualization Platform, the system shuts down all the associated virtual machines and restarts the Appliance Virtualization Platform host. During the update process, the virtual machines will be out of service. Once Appliance Virtualization Platform update is complete, the system restarts the virtual machines.
• If you are upgrading or updating the Appliance Virtualization Platform host, then you must not restart, shutdown, upgrade, or install the patch on the virtual machine that is hosted on the same Appliance Virtualization Platform host.
If you are deploying or upgrading a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.

If you are installing a patch on a virtual machine then you must not restart, shutdown, or upgrade the Appliance Virtualization Platform host on which the same virtual machine is hosted.

- If you are using services port to update or upgrade Appliance Virtualization Platform, connect the system directly with the Appliance Virtualization Platform services port (Gateway 192.168.13.1). If you connect the system using the Utility Services services port (Gateway 192.11.13.1), the Appliance Virtualization Platform update or upgrade fails.

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

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

**Procedure**
1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions > AVP Update/Upgrade Management**.
4. On the Update Host page, click **Select Patch from Local SMGR**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.
   For example, the absolute path on your computer can be **C:\tmp\avp\upgrade-avaya-avp-7.1.2.0.0.xx.zip**.
   In the Hosts for Selected Location <location name> section, the system displays the update status in the **Current Action** column.
6. On the AVP Update/Upgrade - Enhanced Access Security Gateway (EASG) User Access page, read the following messages, and do one of the following:

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

**Disable:**

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

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

Avaya recommends to enable EASG.

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

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

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

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

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

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

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

**Next steps**

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

**Related links**

- [Update Host field descriptions](#) on page 84

---

**Changing the network parameters for an Appliance Virtualization Platform host**

**About this task**

Use this procedure to change the network parameters of Appliance Virtualization Platform after deployment. You can change network parameters only for the Appliance Virtualization Platform host.
**Note:**
If you are connecting to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. Therefore, after the IP address changes, close Solution Deployment Manager, and restart Solution Deployment Manager by using the new IP address to reconnect.

**Procedure**

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

**Note:**
An Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

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

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

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

6. Click **Save**.
   The system updates the Appliance Virtualization Platform host information.

**Related links**

[Change Network Parameters field descriptions](#) on page 81
Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager

About this task

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

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

⚠️ Note:

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

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

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

Procedure

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

2. In VM Management Tree, select a location.

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

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

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

5. To change VLAN ID, perform the following:
   a. To expand the Standard Switch: vSwitch<n> section, click 
      ![click icon](image)
      The section displays the vSwitch details.
   b. Click on the VLANID link or the edit icon (📝).
      The system displays the Port Group Properties page where you can edit the VLAN ID port group property.
   c. In **VLAN ID**, select an ID from the available values.
      For more information about the value, see NIC teaming.
   d. Click **OK**.

The system displays the new VLAN ID.

**Note:**

You can change the services port VLAN ID for S8300D servers only through Solution Deployment Manager.
6. To change the NIC speed, perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.
      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.
      For more information, see VLAN ID assignment.
   The system displays the updated NIC speed in the **Speed** column.

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

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

7. To change the NIC teaming, perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.
      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or unteaming, select the vmnic and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.
      For more information, see NIC teaming modes.
   d. Click **OK**.
      The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.
   e. To check the status of the vmnic, click **NIC team/ unteam**.

8. To get the latest data on host network IP settings, click **Refresh** 🔄.
   The system displays the current status of the vmnic.

**Note:**
You cannot perform NIC teaming for S8300D and S8300E servers.

Related links

Host Network / IP Settings field descriptions on page 82
Changing the password for an Appliance Virtualization Platform host

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

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

Related links
Password policy on page 65
Change Password field descriptions on page 83

Password policy
The password must meet the following requirements:
• Must contain at least eight characters.
• Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.
• Must not contain an uppercase letter at the beginning and a digit or a special character at the end.

Examples of invalid passwords:
• Password1: Invalid. Uppercase in the beginning and a digit at the end.
• Password1!: Uppercase in the beginning and a special character at the end.

Example of a valid password: myPassword!1ok

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

Ensure that you keep the admin password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.
Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Generate AVP Kickstart**.
3. On **Create AVP Kickstart**, enter the appropriate information, and click **Generate Kickstart File**.

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

Create AVP Kickstart field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose AVP Version</td>
<td>The field to select the release version of Appliance Virtualization Platform.</td>
</tr>
<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></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>yes</strong>: To enable the IPv6 format.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no</strong>: To disable the IPv6 format.</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 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>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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 S8300D and E only)</td>
<td>VLAN ID for S8300D and S8300E servers. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use Public VLAN ID only on S8300D and S8300E servers.</td>
</tr>
<tr>
<td>Out of Band Management Setup</td>
<td>The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • yes: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • no: To disable Out of Band Management. The default option.</td>
</tr>
<tr>
<td>OOBM vLAN ID (Used on S8300D and E only)</td>
<td>Out of Band Management VLAN ID for S8300D. Use OOBM VLAN ID only on the S8300D server. • For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.</td>
</tr>
</tbody>
</table>
### Name | Description
---|---
**AVP Super User Admin Password** | Admin password for Appliance Virtualization Platform. 
The password must contain 8 characters and can include alphanumeric characters and @!$. 
You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

**Confirm Password** | Admin password for Appliance Virtualization Platform.

**Enable Stricter Password (14 char pass length)** | The check box to enable or disable the stricter password. 
The password must contain 14 characters.

**WebLM IP/FQDN** | The IP Address or FQDN of WebLM Server.

**WebLM Port Number** | The port number of WebLM Server. The default port is 52233.

### Button | Description
---|---
**Generate Kickstart File** | Generates the Appliance Virtualization Platform kickstart file and the system prompts you to save the file on your local computer.

#### Related links
- [Generating the Appliance Virtualization Platform kickstart file](#) on page 66

---

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

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

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

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

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

Before you begin
Start an SSH session.

Procedure
1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. Navigate to the $MGMT_HOME/infra/bin/avpSSHUtility location.

3. Type ./enableDisableSSHOnAVP.sh. The system displays the following options:
   • Enable SSH on the Appliance Virtualization Platform host.
   • Disable SSH on the Appliance Virtualization Platform host.
   • Check the SSH status on the Appliance Virtualization Platform host.

4. To enable SSH, perform the following:
   a. At the prompt, type 1 and press Enter.
   b. Type the IP address of the Appliance Virtualization Platform host.
   c. Type the time in minutes.

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

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

      For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.

5. To disable SSH, perform the following:
   a. At the prompt, type 2 and press Enter.
b. Type the IP address of the Appliance Virtualization Platform host.

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

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

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

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

---

**Changing the IP address and default gateway of the host**

**About this task**

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

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

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

**Before you begin**

Connect the computer to the services port.

**Procedure**

1. Using an SSH client, log in to the Appliance Virtualization Platform host.

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

   ```
esxcli network ip interface ipv4 set -i vmk0 -I <old IP address of the host> -N <new IP address of the host> -t static
   
   For example:
   
esxcli network ip interface ipv4 set -i vmk0 -I 135.27.162.121 -N 255.255.255.0 -t static
   ```

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

   For example:

   ```
esxcfg-route 135.27.162.1
   ```

3. Enable SSH on the Appliance Virtualization Platform host and run the `. / serverInitialNetworkConfig` command.
For more information, see Configuring servers preinstalled with Appliance Virtualization Platform.

---

**Appliance Virtualization Platform license**

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

<table>
<thead>
<tr>
<th>Server type</th>
<th>Appliance Virtualization Platform license feature keyword</th>
<th>Appliance Virtualization Platform license feature display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Avaya S8300D</td>
<td>VALUE_AVP_1CPU_EMBD_SRV</td>
<td>Maximum AVP single CPU Embedded Servers</td>
</tr>
<tr>
<td>• Avaya S8300E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Server Release 1</td>
<td>• VALUE_AVP_1CPU_CMN_SR</td>
<td>• Maximum AVP single CPU Common Servers</td>
</tr>
<tr>
<td>• HP ProLiant DL360 G7</td>
<td>• VALUE_AVP_2CPU_CMN_SR</td>
<td>• Maximum AVP dual CPU Common Servers</td>
</tr>
<tr>
<td>• Dell™ PowerEdge™ R610</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Server Release 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HP ProLiant DL360p G8</td>
<td></td>
<td></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>
</tbody>
</table>

To configure the Appliance Virtualization Platform license file:

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

**Note:**

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

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

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

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

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

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

**Note:**

Restricted administrative actions for:

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

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

**Appliance Virtualization Platform licensing alarms**

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

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

**Before you begin**

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

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

Procedure

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

WebLM Configuration field descriptions

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

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

Procedure

1. Perform one of the following:
   - On the System Manager Web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
   - On the desktop, click the SDM icon (SDM), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Hosts** tab, in the Hosts for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Shutting down the Appliance Virtualization Platform host

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

Procedure

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

Restarting Appliance Virtualization Platform or an ESXi host

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

Procedure

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

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

Removing an ESXi host

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

Configuring the login banner for the Appliance Virtualization Platform host

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Host tab, in Hosts for Selected Location <location name>, select one or more Appliance Virtualization Platform hosts on which you want to configure the message.
4. Click More Actions > Push Login Banner.

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

The system updates the login banner on the selected Appliance Virtualization Platform hosts.
Mapping the ESXi host to an unknown location

About this task

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

Procedure

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

Applying third-party AVP certificates

Applying third-party Appliance Virtualization Platform certificates

About this task

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

Before you begin

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

Procedure

1. On the System Manager web console, click Services \(\Rightarrow\) Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. To generate CSR, do the following:
   - Click More Actions \(\Rightarrow\) AVP Cert. Management \(\Rightarrow\) Manage Certificate.
b. In the Load AVP host certificate dialog box, select one or more Appliance Virtualization Platform hosts.

c. Click **View/Generate CSR**.
   
The system displays the View/Generate CSR dialog box.

d. Add or edit the details of the generic CSR.
   
   For more information, see “Creating or editing generic CSR”.

e. Click **Generate CSR**.
   
The system generates CSR for the Appliance Virtualization Platform host.

f. To view the status, in the **Upgrade Status** column, click **Status Details**.
   
The time required for the complete process varies depending on the data on System Manager.

5. To download CSR, do the following:

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

b. Click **Download CSR**.

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

d. To view the status, in the **Upgrade Status** column, click **Status Details**.
   
The time required for the complete process varies depending on the data on System Manager.

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

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

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

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

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

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

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

e. Click **Push Certificate**.

f. To view the status, in the **Upgrade Status** column, click **Status Details**.
   
The time required for the complete process varies depending on the data on System Manager.
Creating or editing generic CSR

About this task

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

Procedure

1. In VM Management Tree, select a location.
2. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click More Actions > AVP Cert. Management > Generic CSR.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click Create/Edit CSR and then click OK.

Next steps

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

Load AVP host certificate field descriptions

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

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

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

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

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

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

Procedure

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

2. In VM Management Tree, select a location.

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

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

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

Related links

- [Snapshot Manager field descriptions](#) on page 80
### Snapshot Manager field descriptions

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

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

### Related links

- [Deleting the virtual machine snapshot by using Solution Deployment Manager](#)
  on page 79

### New and Edit host field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>The location where the host is available. The field is read only.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The hostname of Appliance Virtualization Platform or the ESXi host.</td>
</tr>
<tr>
<td>Host FQDN or IP</td>
<td>The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name to log in to Appliance Virtualization Platform or the ESXi host.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>For Appliance Virtualization Platform, provide the admin credentials that you configured while generating the Kickstart file.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to log in to Appliance Virtualization Platform or the ESXi host.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the host information and returns to the Hosts for Selected Location &lt;location name&gt; section.</td>
</tr>
</tbody>
</table>

### Change Network Parameters field descriptions

#### Network Parameters

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change IPv4 Gateway</td>
<td>Makes the IPv4 Gateway field available, and displays <strong>Save IPv4 Gateway</strong> and <strong>Cancel IPv4 Gateway Change</strong> buttons.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change IPv6 Gateway</td>
<td>Makes the IPv6 Default Gateway field available, and displays Save IPv6 Default Gateway and Cancel IPv6 Default Gateway Change buttons.</td>
</tr>
<tr>
<td>Save IPv4 Gateway</td>
<td>Saves the gateway IPv4 address value that you provide.</td>
</tr>
<tr>
<td>Cancel IPv4 Gateway Change</td>
<td>Cancels the changes made to the IPv4 gateway.</td>
</tr>
<tr>
<td>Save IPv6 Default Gateway</td>
<td>Saves the default IPv6 gateway address value that you provide.</td>
</tr>
<tr>
<td>Cancel IPv6 Default Gateway Change</td>
<td>Cancels the changes made to the IPv6 default gateway.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes that you made to network parameters.</td>
</tr>
</tbody>
</table>

---

**Host Network / IP Settings field descriptions**

### Port Groups

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✏ or VLAN ID link</td>
<td>Displays the Port Group Properties page where you configure VLAN ID.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Displays the VLAN ID. The options are:</td>
</tr>
<tr>
<td></td>
<td>• None (0)</td>
</tr>
<tr>
<td></td>
<td>• 1 to 4093</td>
</tr>
<tr>
<td></td>
<td>The field displays only unused IDs.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves the changes.</td>
</tr>
</tbody>
</table>

### NIC speed

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the NIC speed.</td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• Autonegotiate</td>
</tr>
<tr>
<td></td>
<td>• 10,Half</td>
</tr>
<tr>
<td></td>
<td>• 10,Full</td>
</tr>
<tr>
<td></td>
<td>• 100,Half</td>
</tr>
<tr>
<td></td>
<td>• 100,Full</td>
</tr>
<tr>
<td></td>
<td>• 1000,Full</td>
</tr>
</tbody>
</table>

**OK** Saves the changes.

### NIC teaming

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

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

### Change Password field descriptions

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</td>
<td>Saves the new password.</td>
</tr>
</tbody>
</table>
**Update Host field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch location</td>
<td>The location where the Appliance Virtualization Platform patch is available. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Select Patch from Local SMGR:</strong> To use the Appliance Virtualization Platform patch that is available on the local System Manager.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Select Patch from software library:</strong> To use the Appliance Virtualization Platform patch that is available in the software library.</td>
</tr>
<tr>
<td>Ignore Signature Validation</td>
<td>Ignores the signature validation for the patch.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>If the Appliance Virtualization Platform patch is unsigned, you must select the <strong>Ignore signature validation</strong> check box.</td>
</tr>
<tr>
<td>Select patch file</td>
<td>The absolute path to the Appliance Virtualization Platform patch file.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>Update Host</td>
<td>Installs the patch on the Appliance Virtualization Platform host.</td>
</tr>
</tbody>
</table>

---

**Managing the virtual machine**

**Deploying the System Manager OVA file by using the Solution Deployment Manager client**

**About this task**

Use the procedure to create a virtual machine on the Appliance Virtualization Platform host or on the ESXi host, and deploy OVA for System Manager virtual machine by using the Solution Deployment Manager client.

**Before you begin**

- Install the Solution Deployment Manager client on your computer.
- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
• Deploy Utility Services.

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. In VM Management Tree, select a host.

3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click New.
   The system displays the VM Deployment section.

4. In the Select Location and Host section, do the following:
   a. In Select Location, select a location.
   b. In Select Host, select a host.
      The system displays the host name in the Host FQDN field.

5. In Data Store, select a data store, if not displayed upon host selection.
   The page displays the capacity details.

6. Click Next.

7. To get the OVA file, select the OVA tab, and do one of the following:
   • Click URL, in OVA File, type the absolute path to the System Manager OVA file, and click Submit.
   • Click S/W Library, in File Name, select the System Manager OVA file.
   • Click Browse, select the required OVA file from a location on the computer, and click Submit File.

8. In Flexi Footprint, select one of the following:
   • SMGR Profile 3 Max User 250K: To support 250000 users. This configuration requires 8 vCPUs and 18 GB memory.
   • SMGR Profile 2 Max User 250K: To support 250000 users. This configuration requires 6 vCPUs and 12 GB memory.
   • SMGR Profile 1 Max User 35K: To support 35000 users. This configuration requires 4 vCPUs and 9 GB memory.

9. (Optional) To install the System Manager bin file, click Service or Feature Pack, and enter the appropriate parameters.
   • Click URL, and provide the absolute path to the latest service or feature pack.
   • Click S/W Library, and select the latest service or feature pack.
   • Click Browse, and select the latest service or feature pack.
   You can install the System Manager Release 7.1.3 bin file now or after completing the System Manager OVA deployment.
If you do not provide the System Manager Release 7.1.3 bin file at the time of deploying the System Manager OVA, the system displays the following message:

Installation of the latest System Manager patch is mandatory. Are you sure you want to skip the patch installation? If Yes, ensure to manually install the System Manager patch later.

10. Click **Next**.

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

11. In the Network Parameters section, ensure that page displays the following preconfigured fields:
   - **Public**
   - **Out of Band Management**: When Out of Band Management is enabled.

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

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

   For each application that you deploy, fill the appropriate fields.

13. Click **Deploy**.

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

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

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

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

**Next steps**

To configure System Manager, log on to the System Manager Web console. At your first log in, change the System Manager Web console credentials.

Update the user password for the system to synchronize the data from applications.

When System Manager is operational, you can use Solution Deployment Manager from System Manager to deploy all other Avaya Aura® applications or continue to use the Solution Deployment Manager client.

**Related links**

- [Uploading a file to the software library](#) on page 47
- [VM Deployment field descriptions](#) on page 90
Editing a virtual machine

Before you begin

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

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.
   The system displays the Edit VMs section.
4. **(Optional)** Click **Change Flexi Footprint** and do the following:
   a. Click **Change flexi footprint value**.
   b. In **Flexi Footprint**, select a footprint that the application supports.
   
   **Important:**
   Each application must ensure that only the supported flexible footprint is selected.
5. To update the IP address and FQDN of the virtual machine, perform the following:
   a. Click **More Actions > Re-establish connection.**
   
   **Note:**
   To update IP address or FQDN for Utility Services, establish trust on all virtual machines that are running on the host on which Utility Services resides.
   b. Click **More Actions > Refresh VM.**
   
   **Note:**
   To update IP address or FQDN for Utility Services, refresh all virtual machines that are running on the host on which Utility Services resides.
   c. Click **Update IP/FQDN in Local Inventory.**
d. Click **Update VM IP/FQDN**.

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

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

6. Click **Save**.

### Starting a virtual machine from Solution Deployment Manager

**Procedure**

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

2. From the virtual management tree, select a host to which you added virtual machines.

3. On the Virtual Machines tab, select one or more virtual machines that you want to start.

4. Click **Start**.

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

### Stopping a virtual machine from Solution Deployment Manager

**About this task**

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

**Procedure**

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

2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.

3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.

4. Click **Stop**.

   In **VM State**, the system displays **Stopped**.
Restarting a virtual machine from Solution Deployment Manager

Before you begin

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

Procedure

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

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

Common causes for VM deployment failure

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

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

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

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

You can check the deployment status in the Current Action Status column on the Virtual Machine tab.
# VM Deployment field descriptions

## Select Location and Host

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Location</td>
<td>The location name. The field is display-only.</td>
</tr>
<tr>
<td>Select Host</td>
<td>The hostname of the Appliance Virtualization Platform that you must select.</td>
</tr>
<tr>
<td>Host FQDN</td>
<td>The FQDN of the Appliance Virtualization Platform host. The field is display-only.</td>
</tr>
<tr>
<td>Data Store</td>
<td>The data store for the virtual machine. The page populates the capacity details in the Capacity Details section.</td>
</tr>
<tr>
<td>VM Name</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>ME Deployment</td>
<td>The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.</td>
</tr>
</tbody>
</table>

## OVA Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The option to specify the URL from where you can get the OVA file.</td>
</tr>
<tr>
<td>Browse</td>
<td>The option to specify the location from where you can get the OVA file.</td>
</tr>
</tbody>
</table>
| Select OVA         | The absolute path to the .ova file of the virtual machine that you must provide. For example, C:\Program Files\SDM\smgr_7.x.ova  
                    | The field is available only when you click **Browse**.                                                                                     |

**Note:**

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

When you select **OVA from software library**, you can select the .ova file of the virtual machine that you want to deploy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit File</td>
<td>The field is available only when you click <strong>Browse</strong>. Selects the .ova file of the virtual machine that you want to deploy.</td>
</tr>
<tr>
<td>OVA from software library</td>
<td>The option to specify the software library where the OVA file is saved.</td>
</tr>
</tbody>
</table>
| Select Software Library | The default path provided during the installation of the Solution Deployment Manager client. The default path is C:\Program Files \Avaya\SDMClient\Default_Artifacts.  
                             | The field is available only when you click **OVA from software library**                                                                      |

*Table continues...*
Flexi Footprint

The footprint size supported for the selected host. The options are:

- **SMGR Profile 3 Max User 250K**: To support 250,000 users. This configuration requires 8 vCPUs and 18 GB memory.
- **SMGR Profile 2 Max User 250K**: To support 250,000 users. This configuration requires 6 vCPUs and 12 GB memory.
- **SMGR Profile 1 Max User 35K**: To support 35,000 users. This configuration requires 4 vCPUs and 9 GB memory.

**Important:**
Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.

For more information about the resource requirements to support different profiles for System Manager in Avaya-Appliance offer and customer Virtualized Environment, see *Avaya Aura® System Manager Overview and Specification*.

### Configuration Parameters

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

### Management Network Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management IPv4 Address (or Out of Band Management IPv4 Address)</strong></td>
<td>The IPv4 address of the System Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.</td>
</tr>
<tr>
<td><strong>Management Netmask</strong></td>
<td>The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.</td>
</tr>
<tr>
<td><strong>Management Gateway</strong></td>
<td>The gateway IPv4 address to assign to the System Manager virtual machine.</td>
</tr>
<tr>
<td><strong>IP Address of DNS Server</strong></td>
<td>The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td><strong>Management FQDN</strong></td>
<td>The FQDN to assign to the System Manager virtual machine. Note: System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.</td>
</tr>
</tbody>
</table>

Note:

IPv6 Address

The IPv6 address of the System Manager virtual machine for out of band management. The field is optional.

IPv6 Network prefix

The IPv6 subnetwork mask to assign to the System Manager virtual machine. The field is optional.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Default Search List</td>
<td>The search list of domain names. The field is optional.</td>
</tr>
<tr>
<td>NTP Server IP/FQDN</td>
<td>The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.</td>
</tr>
</tbody>
</table>

**Public Network Settings**

*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>Public IP Address</td>
<td>The IPv4 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public Netmask</td>
<td>The IPv4 subnetwork mask to assign to System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Public Gateway</td>
<td>The gateway IPv4 address to assign to the System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Public FQDN</td>
<td>The FQDN to assign to the System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Address</td>
<td>The IPv6 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Network Prefix</td>
<td>The IPv6 subnetwork mask to assign to System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.</td>
</tr>
</tbody>
</table>
## 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 virtual machine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.</td>
</tr>
<tr>
<td></td>
<td>• VFQDN is a mandatory field.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>• VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.</td>
</tr>
<tr>
<td></td>
<td>• You must keep VFQDN domain value same as of FQDN domain value.</td>
</tr>
<tr>
<td></td>
<td>• If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>• In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.</td>
</tr>
<tr>
<td></td>
<td>• After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to the System Manager virtual machine with administrator privilege credentials.</td>
</tr>
<tr>
<td></td>
<td>2. Run the <code>changeVFQDN</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>When you run the <code>changeVFQDN</code> 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>
</tr>
<tr>
<td>Virtual Domain</td>
<td>The virtual domain name of the System Manager virtual machine.</td>
</tr>
</tbody>
</table>

## SNMPv3 Parameters

<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>
</tbody>
</table>

*Table continues…*
### SNMPv3 User Authentication Protocol Password

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>• <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>Note:</td>
<td>If you select <strong>No</strong>, the system does not display the remaining fields.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. 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>
**Network Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.</td>
</tr>
<tr>
<td>Out of Band Management</td>
<td>The port number that you must assign to the Out of Band Management port group. The field is mandatory.</td>
</tr>
</tbody>
</table>

**Button**

<table>
<thead>
<tr>
<th>Deploy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the EULA acceptance screen. To accept EULA and start the deployment process, click Accept.</td>
</tr>
</tbody>
</table>

**Update Static Routing field descriptions**

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

<table>
<thead>
<tr>
<th>Update</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Updates the static IP address for routing.</td>
</tr>
</tbody>
</table>

**Installed Patches field descriptions**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to be performed</td>
<td>The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong>: Displays all the software patches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Commit</strong>: Displays the software patches that you can commit.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rollback</strong>: Displays the software patches that you can rollback.</td>
</tr>
</tbody>
</table>
## Update VM field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>The System Manager virtual machine name</td>
</tr>
<tr>
<td>VM IP</td>
<td>The IP address of System Manager</td>
</tr>
<tr>
<td>VM FQDN</td>
<td>FQDN of System Manager</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name</td>
</tr>
<tr>
<td>Select bin file from Local SMGR</td>
<td>The option to select the software patch or service pack for System Manager.</td>
</tr>
<tr>
<td></td>
<td>The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.</td>
</tr>
<tr>
<td></td>
<td>This option is available only on the Solution Deployment Manager client.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Auto commit the patch

The option to commit the software patch or service pack automatically. If the check box is clear, you must commit the patch from More Actions > Installed Patches.

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

---

### Reestablish Connection field descriptions

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

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

---

### Virtual machine report

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

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

⚠️ **Important:**

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

#### generate_report.sh command

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

**Syntax**

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

Generating a virtual machine report

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

Procedure
1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the /swlibrary/reports/ directory.
3. Type the ./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password> command:
   For example: ./generate_report.sh -g -u admin -p password
   The system displays the following message: Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].
4. To proceed with report generation, type Y, and press Enter.
   The system generates the report in the .csv format in the /swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv folder.

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

Viewing the status of the virtual machine report

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

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

Aborting the virtual machine report generation

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

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

The system aborts the virtual machine report generation process.

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 on the desktop.
2. Click VM Management.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Location section, select System Manager on which you want to install the patch.
5. (Optional) If updating from a different client, perform the following:
   a. Click More Actions > Re-establish connection.
b. Click on Refresh VM.

c. To view the status, in the Current Action column, click Status Details.

d. Proceed with the next step.

6. Click More Actions > Update VM.

The system displays the System Manager Update dialog box.

7. In Select bin file from Local SDM Client, provide the absolute path to the software patch or service pack.

小心：

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.

8. (Optional) Click the Auto commit the patch check box.

9. Click Install.

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

10. 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.

11. 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.

---

**Additional Solution Deployment Manager functionality**

**Certificate validation**

**Certification validation**

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.
The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

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

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

**Note:**

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

- Log Certificate Validation Events

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

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.

- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

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

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

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

**Note:**

Solution Deployment Manager:

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

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

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

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

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

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

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

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

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
5. On the Certificate window, do the following:
   a. Click Generate Certificate.
      Note: You can generate certificate only for the Appliance Virtualization Platform host.
   b. Click Accept Certificate.

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

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

Related links
Adding an Appliance Virtualization Platform or ESXi host on page 56
Generating new self-signed certificates for the ESXi host on page 105

Updating the certificate on the ESXi host from VMware

About this task
Use the procedure to update the ESXi host certificate.
For information about updating vCenter certificates, see the VMware documentation.

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

**Procedure**

1. Start vSphere Web Client, and log in to the ESXi host as admin or root user.
2. Ensure that the domain name and the hostname of the ESXi host is set correctly and matches the FQDN that is present on the DNS servers, correct the entries to match if required.
   
   For security reason, the common name in the certificate must match the hostname to which you connect.
3. To generate new certificates, type `/sbin/generate-certificates`.
   
   The system generates and installs the certificate.
4. Restart the ESXi host.
5. *(Optional)* Do the following:
   
   a. Move the ESXi host to the maintenance mode.
   
   b. Install the new certificate.
   
   c. From the Direct Console User Interface (DCUI), restart management agents.

   **Note:**

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

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

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

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

**Related links**

[Generating new self-signed certificates for the ESXi host](on page 105)

**Managing certificates for existing hosts**

**About this task**

By default, the certificate status of the host or vCenter that is migrated from earlier release is invalid. To perform any operation on the host from Solution Deployment Manager, you require a valid certificate. Therefore, you must get the valid certificate and accept the certificate.
Depending on the host type and the validity of the certificate, use appropriate steps to generate the certificate, and then accept the certificate.

**Before you begin**

Require permissions to add a host to generate certificates.

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select a host.
4. *(Optional)* On an Appliance Virtualization Platform host, click **More Actions > Generate/ Accept Certificate**, and on the Certificate dialog box, do one of the following:
   - If the certificate is valid, click **Accept Certificate**.
   - If the certificate is invalid, click **Generate Certificate**, and then click **Accept Certificate**.
5. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions > Generate/ Accept Certificate**, and click **Accept Certificate**.
   - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.
     For more information, see “Generating new self-signed certificates for the ESXi host”.
6. For vCenter, do the following:
   a. Click **Map vCenter**, select the vCenter server, and click **Edit**.
   b. In the Certificate dialog box, accept certificate, and click **Save**.

**Related links**

- [Generating new self-signed certificates for the ESXi host](#) on page 105
- [Generating and accepting certificates](#) on page 103

**Generating new self-signed certificates for the ESXi host**

**About this task**

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

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

**Before you begin**

Start an SSH session on the ESXi host.
Procedure

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

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

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

3. To generate new certificates, type `/sbin/generate-certificates`.
4. Restart the ESXi host.
   
   The generation process places the certificates places in the correct location.

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

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

Next steps

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

---

Monitoring a host and virtual machine

Monitoring a host

Procedure

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

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

Procedure

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

Managing vCenter

Adding a vCenter to Solution Deployment Manager

About this task

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

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
   b. In **User Name**, type user name to log in to vCenter.
c. In **Password**, type password to log in to vCenter.

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

e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.
   
   PSC must have a valid certificate.
   
   The system enables **PSC IP or FQDN** and you must provide the IP or FQDN of PSC.

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

5. Click **Save**.

6. On the certificate dialog box, click **Accept Certificate**.
   
   The system generates the certificate and adds vCenter.
   
   In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Related links

- [Editing vCenter](#) on page 108
- [Map vCenter field descriptions](#) on page 109
- [New vCenter and Edit vCenter field descriptions](#) on page 110

**Editing vCenter**

**Before you begin**

Ensure that you have the required permissions.

**Procedure**

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

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

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

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

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

6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   
   * Select an ESXi host and click the edit icon (✏).
   
   * Select one or more ESXi hosts, select the location, and click **Bulk Update** and click **Update**.
If you do not click Commit after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables. Click Commit to get an updated list of managed and unmanaged hosts.

Deleting vCenter from Solution Deployment Manager

Before you begin
Ensure that you have the required permissions.

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

Map vCenter field descriptions

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

Note: Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.

| License | The license type of the vCenter server.                                   |
| Status  | The license status of the vCenter server.                                |
| Certificate Status | The certificate status of the vCenter server. The values are:
|                    | • ✓: The certificate is correct.                                         |
|                    | • ✗: The certificate is not accepted or invalid.                          |

<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>Button</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Generate/Accept Certificate</td>
<td>Displays the certificate dialog box where you can generate and accept certificate for vCenter. For vCenter, you can only accept certificate. You cannot generate certificate.</td>
</tr>
<tr>
<td>Add</td>
<td>Displays the New vCenter page, where you can add a new ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays the Edit vCenter page, where you can update the details and location of ESXi hosts.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the ESXi host.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Updates the list of ESXi hosts in the Map vCenter section.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP/FQDN</td>
<td>The name of the ESXi host.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The IP address of the ESXi host.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the ESXi host.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The IPv6 address of the ESXi host.</td>
</tr>
<tr>
<td>Edit</td>
<td>The option to edit the location and host.</td>
</tr>
<tr>
<td>Bulk Update</td>
<td>Provides an option to change the location of more than one ESXi hosts.</td>
</tr>
</tbody>
</table>

**Note:** You must select a location before you click **Bulk Update**.

| Update             | Saves the changes that you make to the location or hostname of the ESXi host. |
| Commit             | Commits the changes that you make to the ESXi host with location that is managed by vCenter. |

Unmanaged Hosts

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

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

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

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

Viewing the job history of virtual machine operations

**Procedure**

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

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

3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

The page displays the details of jobs that you selected.

**Related links**

- [Job History field descriptions](#) on page 112

### Job History field descriptions

<table>
<thead>
<tr>
<th>Name/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.</td>
</tr>
<tr>
<td>Submit</td>
<td>Provides details of jobs that you selected.</td>
</tr>
</tbody>
</table>

### History

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>The unique name of the virtual machine management job.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or host name of the virtual machine or the host where the operation is performed.</td>
</tr>
<tr>
<td>Operation</td>
<td>The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the job.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The start time of the job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The end time of the job.</td>
</tr>
</tbody>
</table>

**Related links**

- [Viewing the job history of virtual machine operations](#) on page 111

---

### Managing syslog profiles

#### Adding a remote Syslog server profile

**About this task**

Use this procedure to configure a remote Syslog server details in System Manager such that it receives to receive system logs from Appliance Virtualization Platform hosts.
Before you begin
To view the Syslog data from the Appliance Virtualization Platform host or application, ensure that:
  • The firewall on the Syslog server is configured correctly.
  • The Syslog service on the server is running.

Procedure
1. On the System Manager web console, click Services > Solution Deployment Manager, and then click VM Management.
2. Click VM Management.
3. In the lower pane, click Configure Remote Syslog Profile.
4. Click Add.
5. In the Add Syslog Receiver dialog box, add the details of the Syslog server, such as profile name, IP address or FQDN, and port.
6. In TCP/UDP, click TCP or UDP.
7. If the remote host is TLS based, do the following:
   a. Select TLS based Remote Host.
   b. Click Browse and select a certificate file that you want to upload.
8. Click Save.

Syslog Receiver Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>The name of the Syslog server configuration.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or host name of the Syslog server configuration.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number of the Syslog server configuration.</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>The type of port used for the Syslog server configuration.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td>TLS based Remote Host</td>
<td>The option to select if the remote host is TLS based.</td>
</tr>
<tr>
<td>Select Certificate</td>
<td>The field to upload a certificate for the TLS based remote host.</td>
</tr>
<tr>
<td></td>
<td>This option is available only if the TLS based Remote Host is selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Displays the Add Syslog Receiver dialog box where you can add the Syslog server configuration.</td>
</tr>
</tbody>
</table>
### Pushing a system log to Syslog servers

**About this task**

Use this procedure to send an Appliance Virtualization Platform host’s log files to Syslog servers.

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions > Syslog config > Push**.
5. In the Push Syslog Configuration dialog box, select the required Syslog profile, and click **Push**.

   The system sends the system log to the selected Syslog server.

### Viewing configured Syslog servers

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Hosts tab, in the Hosts for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions > Syslog config > View**.
5. In the View Syslog Configuration dialog box, select the required Syslog profile to view it.

### Deleting configured Syslog servers

**Procedure**

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

4. Click More Actions > Syslog config > Delete.

5. In the Delete Syslog Configuration dialog box, select the required Syslog profile and click Delete.

6. On the confirmation dialog box, click Yes.

---

**Network Parameters and Configuration Parameters field descriptions**

☆ **Note:**

During the Utility Services deployment, if you do not know the Communication Manager IP Address, System Manager IP Address, or Enrollment Password, then use the dummy values. Dummy values must pass validation. Use the localhost default 127.0.0.1 for the IP address, and Dummy as the password.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking Properties</td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>Linux hostname or fully qualified domain name for Utility Services virtual machine.</td>
</tr>
<tr>
<td></td>
<td>☆ <strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The host name is regardless of the interface that is used to access. The Public interface is the default interface.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The IP address for this interface.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Public Netmask</td>
<td>The netmask for this interface.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Public Default Gateway</td>
<td>The IP address of the default gateway.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td></td>
<td>☆ <strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The default gateway should be configured for the Public network. You can use the ovf_set_static command to allow a static route to be assigned to the OOBM network, enabling OOBM network to reach a second subnet.</td>
</tr>
<tr>
<td>Public IPv6 address</td>
<td>The IP address for this interface.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Public IPv6 Prefix</td>
<td>The netmask for this interface.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Default IPv6 Gateway</td>
<td>The IP address of the default gateway.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td>Out of Band Management IP Address</td>
<td>The IP address for this interface.</td>
</tr>
<tr>
<td>Out of Band Management Netmask</td>
<td>The netmask for this interface.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Address</td>
<td>The IPv6 address for this interface. This field is optional.</td>
</tr>
<tr>
<td>Out of Band Management IPv6 Prefix</td>
<td>The IPv6 prefix for this interface. This field is optional.</td>
</tr>
<tr>
<td>Network Time Protocol IP</td>
<td>IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.</td>
</tr>
<tr>
<td>Timezone setting</td>
<td>The selected timezone setting for the Utility Services virtual machine.</td>
</tr>
<tr>
<td>DNS</td>
<td>The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma.</td>
</tr>
<tr>
<td></td>
<td>Required field unless you use DHCP.</td>
</tr>
<tr>
<td></td>
<td>You can specify up to three DNS Servers.</td>
</tr>
<tr>
<td>Name</td>
<td>Primary WebLM IP address for Licensing. A valid Utility Services license is required for all deployment types and modes other than deployment on Appliance Virtualization Platform.</td>
</tr>
<tr>
<td>Primary System Manager IP address for application registration</td>
<td>The IP address of System Manager that is required for application registration.</td>
</tr>
<tr>
<td>Enrollment Password</td>
<td>The enrollment password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The confirmation password.</td>
</tr>
<tr>
<td>Application Properties</td>
<td></td>
</tr>
<tr>
<td>Communication Manager IP</td>
<td>IP address of Communication Manager.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.</td>
</tr>
</tbody>
</table>

Table continues…
Utility Services Mode

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

• **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform.

  You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed.

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

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

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

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

**Note:**

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

• **Services Port Only**

• **Hardened Mode services port only**

**Note:**

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

Utility Services can gain access to the hypervisor and all virtual machines through the IP address 192.11.13.6. Utility Services provides application routing between the physical port and virtual applications.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of Band Management Mode</td>
<td>The Out of Band Management mode in which you want to deploy. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>OOBM_Enabled</strong>: To enable Out of Band Management.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OOBM_Disabled</strong>: To disable Out of Band Management.</td>
</tr>
<tr>
<td></td>
<td>🌟 <strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>OOBM_Disabled</strong> is the default setting. If the mode is set to <strong>OOBM_Disabled</strong>, then you do not need to configure Out of Band Management.</td>
</tr>
</tbody>
</table>

Deploying System Manager on the Avaya-provided server

May 2020

Deploying Avaya Aura® System Manager

Comments on this document? infodev@avaya.com
# Chapter 5: Deploying System Manager on VMware

## Deployment checklist

Use the following checklist to deploy the System Manager Release 7.1.3 OVA by using vSphere Web Client.

**Note:**
- Deployment of the System Manager OVA by using vSphere Client is not supported.
- 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.

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>, download the SMGR-7.1.0.0.1125193-e65-50.ova OVA or System Manager high capacity SMGR-PROFILE3-7.1.0.0.1125193-e65-50.ova OVA and System Manager Release 7.1.3 bin files.</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Upload the required software that are required for deployment and upgrade operations to the local or remote software library of System Manager. For example, OVA, firmware, software patches, service packs, and images.</td>
<td><a href="#">Uploading a file to the software library on page 47</a></td>
</tr>
<tr>
<td>3</td>
<td>Install vSphere Client 5.5, 6.0, 6.5, and 6.7. Gain access to vCenter and vSphere Web Client.</td>
<td>Download from the VMware website. <strong>Note:</strong> With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>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. Ensure that the license file copies are accessible.</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Ensure that the following information is handy:</td>
<td>Customer configuration data on page 26</td>
</tr>
<tr>
<td></td>
<td>• FQDN/IP address, netmask, and gateway</td>
<td>“Out of Band Management configuration”</td>
</tr>
<tr>
<td></td>
<td>• Out of Band Management configuration details.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Deploy the System Manager OVA file.</td>
<td>• Deploying the System Manager OVA by using vSphere Web Client on page 121</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deploying the application OVA using vSphere Web Client by accessing the host directly on page 123</td>
</tr>
<tr>
<td>7</td>
<td>You can perform one of the following to start the virtual machine.</td>
<td>Configuring the virtual machine automatic startup settings on VMware on page 139</td>
</tr>
<tr>
<td></td>
<td>• Configure the System Manager virtual machine to start automatically after the deployment.</td>
<td>Deploying the application OVA using vSphere Web Client by accessing the host directly on page 123</td>
</tr>
<tr>
<td></td>
<td>• Start the System Manager virtual machine.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Configure the network parameters by using command line interface.</td>
<td>Network and configuration field descriptions on page 125</td>
</tr>
<tr>
<td>9</td>
<td>Verify the deployment of the System Manager virtual machine.</td>
<td>Verifying the installation of System Manager on page 132</td>
</tr>
<tr>
<td>10</td>
<td>In the settings icon ( ), click About to verify that the System Manager version is Release 7.1.3.</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>(Optional) Reconfigure the hardware resources for flexible footprint.</td>
<td>Reconfiguring hardware resources for flexible footprint on page 141</td>
</tr>
<tr>
<td>12</td>
<td>Install the System Manager Release 7.1.3 bin file.</td>
<td>Installing the System Manager Release 7.1.3 bin file on page 130</td>
</tr>
<tr>
<td></td>
<td>The patch installation takes about 60–65 minutes to complete.</td>
<td></td>
</tr>
</tbody>
</table>
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. In 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, perform one of the following steps:
   • 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, perform 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, in the Accept license agreements page, click Accept.

11. Click Next.

12. On the Select configuration page, from Configuration, select one of the following:
   • SMGR Profile 3 Max User 250K: To support 250000 users. This configuration requires 8 vCPUs and 18 GB memory.
   • SMGR Profile 2 Max User 250K: To support 250000 users. This configuration requires 6 vCPUs and 12 GB memory.
• **SMGR Profile 1 Max User 35K**: To support 35000 users. This configuration requires 4 vCPUs and 9 GB memory.

13. Click **Next**.

14. On the Select storage page, in **Select virtual disk format**, select **Thick provision lazy zeroed**.

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 information about the configuration and network parameters, see “VM Deployment field descriptions”.

   ✪ **Note**:
   
   • If you do not provide the details in the mandatory fields, you cannot power 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 information about the parameters, 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.

Related links

Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 84
Deploying the application OVA using vSphere Web Client by accessing the host directly on page 123

Deploying the application OVA using vSphere Web Client by accessing the host directly

About this task

Use this procedure for deploying application OVA on ACP 130. This same procedure is applicable for ESXi 6.5 u2 onwards.

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 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:
   a. Type a name for the virtual machine.
   b. 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:
   a. From **Network mappings**, select the required network.
   b. From **Disk provisioning**, select **Thick provision lazy zeroed**.
   c. From **Deployment type**, select profile.
      
      For more information about supported footprints, see “Supported footprints of Communication Manager on VMware”.
   d. 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.

17. To start the virtual machine, if application 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 application virtual machine.

When the system starts for the first time, configure the parameters for application.

18. Click **Actions > Console**, select the open console type, verify that the system startup is successful, then input the application configuration parameters.

**Related links**

- [Deploying the System Manager OVA file by using the Solution Deployment Manager client](#) on page 84
- [Deploying the System Manager OVA by using vSphere Web Client](#) on page 121

---

### Network and configuration field descriptions

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

**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 virtual machine for out of band management. The field is optional. |
| **IPv6 Network prefix**                                        | The IPv6 subnetwork mask to assign to the System Manager virtual machine. The field is optional.       |
| **IPv6 Gateway**                                               | The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.       |
| **Default Search List**                                        | The search list of domain names. The field is optional.                                              |

*Table continues…*
### 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 virtual machine 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 virtual machine. The field is optional.</td>
</tr>
<tr>
<td><strong>Public Gateway</strong></td>
<td>The gateway IPv4 address to assign to the System Manager virtual machine. The field is optional.</td>
</tr>
<tr>
<td><strong>Public FQDN</strong></td>
<td>The FQDN to assign to the System Manager virtual machine. 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 virtual machine. 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 virtual machine. The field is optional.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Hostname</td>
<td>The virtual hostname of the System Manager virtual machine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.</td>
</tr>
<tr>
<td></td>
<td>• VFQDN is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>• By default, VFQDN entry gets added in the <code>/etc/hosts</code> file during installation. Do not remove VFQDN entry from the <code>/etc/hosts</code> file.</td>
</tr>
<tr>
<td></td>
<td>• VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.</td>
</tr>
<tr>
<td></td>
<td>• You must keep VFQDN domain value same as of FQDN domain value.</td>
</tr>
<tr>
<td></td>
<td>• If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>• In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.</td>
</tr>
<tr>
<td></td>
<td>• After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to the System Manager virtual machine with administrator privilege credentials.</td>
</tr>
<tr>
<td></td>
<td>2. Run the <code>changeVFQDN</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>When you run the <code>changeVFQDN</code> 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>
</tr>
<tr>
<td>Virtual Domain</td>
<td>The virtual domain name of the System Manager virtual machine.</td>
</tr>
<tr>
<td></td>
<td><strong>Table continues…</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Description</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 of contents

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confirm Password</strong></td>
<td>The password that you retype to confirm the SNMPv3 user authentication protocol.</td>
</tr>
<tr>
<td><strong>SNMPv3 User Privacy Protocol Password</strong></td>
<td>The password for SNMPv3 user privacy.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>The password that you must provide to confirm the SNMPv3 user privacy protocol.</td>
</tr>
<tr>
<td><strong>SMGR command line user name</strong></td>
<td>The user name of the System Manager CLI user.</td>
</tr>
<tr>
<td><strong>SMGR command line user password</strong></td>
<td>The password for the System Manager CLI user.</td>
</tr>
<tr>
<td><strong>SMGR command line user password</strong></td>
<td>The password that you must provide to confirm the System Manager CLI user authentication.</td>
</tr>
</tbody>
</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. |
| **File Transfer Protocol** | The protocol that you can use to create the backup. The values are SCP and SFTP. |

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

<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`. |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
Deployment of cloned and copied OVAs

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA on the virtual machine. At this time, Avaya only supports the deployment of new OVAs.

Installing the System Manager Release 7.1.3 bin file

**Before you begin**
- Ensure that System Manager is running on Release 7.1.3.
- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 📲 icon.
  - Start an SSH session on System Manager.
- Log in to the System Manager virtual machine with administrator privilege credentials.
- Download the `System_Manager_7.1.3.0_r713007763.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.

**About this task**

If you fail to install the Release 7.1.3 bin file for System Manager, the Virtualized Environment-specific functionality might be unavailable in System Manager.

**Procedure**

1. Create the System Manager virtual machine snapshot.
   - **Note:**
     
     This activity might impact the service.

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 60–65 minutes to complete.
   - If the installation is successful, the system displays a warning message on the web console and on the command line interface to restart System Manager if kernel is updated.
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.

- 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.

---

Starting the System Manager virtual machine

The system packages System Manager and other products for VMware in the .OVA package format. You can install the OVA file using vSphere Client.

**Before you begin**

Deploy the System Manager OVA.

**Procedure**

On vSphere Client, start the System Manager virtual machine by using one of the following:

- 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.
Chapter 6: Post Installation Verification

Postinstallation steps

Procedure
Recreate all licenses with the new host ID format, and install the new license files.

System Manager on VMware uses a new host ID format for Avaya WebLM server. Therefore, all licenses previously installed becomes invalid. For instructions to install the license file, see Managing licenses in Administering Avaya Aura® System Manager.

Verifying the installation of System Manager

About this task
Perform the following verification procedure after you install System Manager Release 7.1.3 and configure System Manager.

Procedure
1. On the web browser, type https://<fully qualified domain name of System Manager>, and ensure that the system displays the System Manager web console.
2. On the upper-right corner, click and click About.
   The system displays the About SMGR window with the build details.
3. Verify the System Manager version number.

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.
Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Run the command: `#service jboss stop`.
3. Once the system stops the JBoss service, run the command: `sh $MGMT_HOME/CommonConsole/script/LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
4. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection, otherwise the process gets killed and the installation fails.

*Note:*

During this activity, the system 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.

---

**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: `EASGStatus`.
   
   The system displays the status of EASG.

2. To enable EASG, do the following:
   
   a. Run the command: `EASGManage --enableEASG`.
The system displays the following message.

By enabling Avaya Services Logins you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

The product must be registered using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity. Please see the Avaya support site (https://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

b. When the system prompts, type yes.

The system displays the message: EASG Access is enabled.

3. To disable EASG, do the following:

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

The system displays the following message.

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

b. When the system prompts, type yes.

The system displays the message: EASG Access is disabled.

---

**Viewing the EASG certificate information**

**Procedure**

1. Log in to the application CLI interface.

2. Run the command: `EASGProductCert --certInfo`.

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

---

**EASG site certificate**

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate...
will only allow access to systems on which it has been installed, and will only allow access to the
given Avaya technician and cannot be used by anyone else to access the system including other
Avaya technicians. Once this is done, the technician logs in with the EASG challenge/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 7: Configuration

Configuring Out of Band Management on System Manager

About this task

If you do not configure Out of Band Management during the deployment of System Manager OVA from Solution Deployment Manager on an Avaya-provided server, you can use the configureOOBM command to configure Out of Band Management anytime after the deployment.

Before you begin

- Enable Out of Band Management on Appliance Virtualization Platform.
- Install System Manager on the Appliance Virtualization Platform host on which Out of Band Management is installed.
- Ensure that IP address or hostname of Public network and Management network are different.

If both are in the same network, Out of Band Management configuration might not function as expected.
- Log in to System Manager by using an SSH client utility.

When you enable Out of Band Management configuration, you might lose the connection as the system does a network restart. You can login to System Manager from the Console of VMware vSphere Client. that is configured to connect to the Appliance Virtualization Platform host server.

Procedure

1. To enable Out of Band Management, type configureOOBM -EnableOOBM.

   The system enables Out of Band Management on the System Manager virtual machine. With EnableOOBM, the system configures the additional Ethernet interface, updates network configuration, and sets the firewall rules.

2. To disable Out of Band Management, type configureOOBM -DisableOOBM.

   The system disables Out of Band Management on the System Manager virtual machine. With DisableOOBM, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.

Related links

configureOOBM command on page 139
Configuring Out of Band Management on System Manager in the Geographic Redundancy setup

About this task

⚠️ Note:

You cannot enable Out of Band Management on secondary System Manager server when Out of Band Management on primary System Manager server is disabled.

Before you begin

Identify one of the following:

- Enable Out of Band Management on both the primary and secondary System Manager server.
- Enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on the secondary System Manager server.
- Disable Out of Band Management on secondary System Manager server.
- Disable Out of Band Management on both the primary and secondary System Manager server.

Procedure

1. To enable Out of Band Management on both primary and secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server and activate the secondary System Manager server.
   c. Enable Out of Band Management on both primary and secondary System Manager server.
   d. Reconfigure the Geographic Redundancy on the secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.

2. To enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server.
   c. Enable Out of Band Management on primary System Manager server.
   d. Once Out of Band Management on primary System Manager server is enabled, reconfigure Geographic Redundancy on secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.
3. To disable Out of Band Management on secondary server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server.
   c. Activate secondary System Manager server and disable Out of Band Management.
   d. Reconfigure primary System Manager server from the web console of the secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.

4. To disable Out of Band Management on both servers, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server and disable Out of Band Management.
   c. Activate secondary System Manager server and disable Out of Band Management.
   d. Reconfigure Geographic Redundancy on secondary System Manager server with old primary System Manager server which is now standalone.
   e. Enable Geographic Redundancy replication on primary System Manager server.

---

**Enabling Multi Tenancy on Out of Band Management-enabled System Manager**

**About this task**

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

**Before you begin**

Start an SSH session.

**Procedure**

1. Log in to System Manager by using the command line utility.
2. Type `opt/vsp/OOBM/ enableMultitenancyInPublicInterface.sh`.

**Related links**

- [configureOOBM command](#) on page 139
configureOOBM command

After the deployment of System Manager, use `configureOOBM` to configure Out of Band Management. You can enable or disable Out of Band Management.

**Syntax**

`configureOOBM [-EnableOOBM|DisableOOBM]`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableOOBM</td>
<td>Enables Out of Band Management on System Manager virtual machine. With <code>EnableOOBM</code>, the additional Ethernet interface is configured, network configuration is updated, and firewall rules are set.</td>
</tr>
<tr>
<td>DisableOOBM</td>
<td>Disables Out of Band Management on System Manager virtual machine. With <code>DisableOOBM</code>, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.</td>
</tr>
</tbody>
</table>

Configuring the virtual machine automatic startup settings on VMware

**About this task**

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software ignores the startup selections.

**Before you begin**

Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

**Procedure**

1. In the Web browser, type the vSphere vCenter host URL.
2. Click **Hosts and Clusters** or **VMs and Templates** icon.
3. In the left pane, select the host where the virtual machine is located.
4. Click **Configure**.
5. Under Virtual Machines, select **VM Startup/Shutdown**, and click **Edit**.
   The system displays the Edit VM Startup and Shutdown window.
6. Select **Automatically start and stop the virtual machines with the system**.
SAL Gateway

You require a Secure Access Link (SAL) Gateway for remote access and alarming. Through SAL, support personnel or tools can gain remote access to managed devices to troubleshoot and debug problems.

A SAL Gateway:

1. Receives alarms from Avaya products in the customer network.
2. Reformats the alarms.
3. Forwards the alarms to the Avaya support center or a customer-managed Network Management System.

You can deploy SAL Gateway OVA:

• On Avaya Aura® Virtualized Appliance by using Solution Deployment Manager
• In the Avaya Aura® Virtualized Environment by using vCenter, vSphere or Solution Deployment Manager

For more information about SAL Gateway, see the Secure Access Link documentation on the Avaya Support website at http://support.avaya.com.

Configuring hardware resources to support VE footprint flexibility

Virtualized Environment footprint flexibility

Virtualized applications provide a fixed profile based on maximum capacity requirements. However, many customers require only a fraction of the maximum capacity.

Certain virtualized applications offer a flexible footprint profile based on the number of users that are supported. The customer can configure VMware CPU and RAM of a virtual machine according to a particular capacity line size requirement.

The applications that currently support Virtualized Environment footprint flexibility are:

• Avaya Aura® System Manager
• Avaya Aura® Communication Manager
Reconfiguring hardware resources for flexible footprint

About this task
Reconfigure the CPU and RAM resources for the System Manager virtual machine.

Procedure
1. Connect to the host or cluster by using the VMware vSphere client.
2. Log in by using the admin login name and password.
3. To power off the virtual machine, perform the following:
   a. Right-click on the virtual machine name.
   b. Select Power > Shut Down Guest.
   c. Click Yes in the Shutdown Confirmation dialog box.
4. On the virtual machine name, right-click and select Edit Settings.
5. Click the Hardware tab.
6. Click Memory and change the Memory Size to the appropriate limit.
   For more information, see System Manager Virtualized Environment footprint hardware resource matrix.
7. Click on the Resources tab.
8. Select Memory and verify the Reservation is set correctly.
9. Clear the unlimited check box and verify the Limit slide is set to the same value as the Reservation.
10. Click the Hardware tab.
11. Select CPUs and change the Number of sockets according to the limit requirement.
   For more information, see System Manager Virtualized Environment footprint hardware resource matrix.
12. Click the Resources tab.
13. Select CPUs and verify that the Reservation is set correctly.
14. Clear the unlimited check box and verify that the Limit slide is set to the same value as the Reservation field.
15. Click OK and wait until the virtual machine completes the reconfiguration process.

**Related links**
- [System Manager footprint hardware resource matrix](#) on page 27
- [Capability and scalability specification](#) on page 142

---

### Capability and scalability specification

The table provides the maximum capacities supported for each element type.

**Note:**

Because only one System Manager is available with each Avaya Aura® deployment, the solution number is not the sum of all supported elements listed in the table.

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Maximum limit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator logins</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Simultaneous logins</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Total administered endpoints of all types</td>
<td>250,000</td>
<td>The total number of endpoints are defined in Home/Elements/Communication Manager/Endpoints / Manage Endpoints Endpoint page in System Manager.</td>
</tr>
<tr>
<td>Total administered users defined in the System Manager database</td>
<td>250,000</td>
<td>The total number of administered users with an Identity is configured in System Manager, and might not have a communication profile defined. Users are defined in the Home/Users/Manage Users Users page System Manager.</td>
</tr>
<tr>
<td>Messaging mailboxes</td>
<td>250,000</td>
<td></td>
</tr>
<tr>
<td>Contacts per user</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Public contacts</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>Personal contact lists per user</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Members in a personal contact list</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>Members in a group</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>Elements</td>
<td>25,000</td>
<td></td>
</tr>
<tr>
<td>Communication Manager and/or CS 1000</td>
<td>500</td>
<td>Capacity counts against the total number of elements.</td>
</tr>
</tbody>
</table>

*Table continues…*
## Geographic Redundancy configuration

### Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup

In a Geographic Redundancy setup, ensure that the two standalone running on Appliance Virtualization Platform that you designate as primary and secondary servers meet the following requirements:

- Must contain similar hardware and operating system architecture.

**Note:**

For more information, see “Hardware resource and parameter for the Geographic Redundancy setup”.

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Maximum limit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Managers</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Branch Session Manager</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>IP Office</td>
<td>2000</td>
<td>To support central licensing of 2,000 IP Office 9.x, local WebLM licensing servers that are slaved to System Manager licensing are required. See the IP Office 9.x product offer and System Manager WebLM for details.</td>
</tr>
<tr>
<td>IP Office Unified Communication Module (UCM) or Application servers as part of Branch deployments</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Roles per user</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Licensing clients</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>Concurrent License requests per WebLM</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>license requests during any 9 minute window per WebLM</td>
<td>50,000</td>
<td></td>
</tr>
<tr>
<td>Local WebLM</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Trust management clients</td>
<td>2500</td>
<td></td>
</tr>
<tr>
<td>Tenants (System Manager Multi Tenant)</td>
<td>250</td>
<td></td>
</tr>
</tbody>
</table>
• Must contain the same version of the Avaya Virtualization Platform software that includes software packs.

🌟 Note:

System Manager does not support the mixed Virtualized Environment and Appliance Virtualization Platform environment. For example, the primary System Manager on Appliance Virtualization Platform and the secondary System Manager on VMware ESXi.

• Must contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 1, the secondary System Manager must also contain Profile 1.

• Must contain the same version of the System Manager software that includes service pack and software patches.

• Must contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.

• Must communicate with each other over the network using the IP address and FQDN.

• Must have synchronized network time.

• Must use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the /etc/hosts file on the primary and secondary System Manager servers.

• Must ensure that the required ports are open to support the Geographic Redundancy feature. For port usage information, see Avaya Port Matrix: Avaya Aura® System Manager on the Avaya Support website at http://support.avaya.com/.

• Must ensure that the minimum data pipe between the primary and the secondary System Manager server is T1. T1 provides 1.544 Mbps.

• Must ensure that the network latency is less than 500 ms.

---

**Prerequisites for System Manager on VMware in the Geographic Redundancy setup**

In a Geographic Redundancy-enabled system running on VMware, ensure that System Manager that you designate as primary and secondary systems meet the following requirements:

• Must be on VMware environment.

🌟 Note:

System Manager does not support the mixed VMware and Appliance Virtualization Platform environment. For example, the primary System Manager on Appliance Virtualization Platform and the secondary System Manager on VMware ESXi.
• Must contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 1, the secondary System Manager must also contain Profile 1.

• Must contain the same version of the System Manager software that includes service pack and software patches.

• Must contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.

• Must communicate with each other over the network using the IP address and FQDN.

• Must have synchronized network time.

• Must use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the /etc/hosts file on the primary and secondary System Manager servers.

• Must ensure that the required ports are open to support the Geographic Redundancy feature. For port usage information, see Avaya Port Matrix: Avaya Aura® System Manager on the Avaya Support website at http://support.avaya.com/.

• Must ensure that the network latency is less than 500 ms.

• Must ensure that the minimum data pipe between the primary and the secondary System Manager server is T1. T1 provides 1.544 Mbps.

---

**Key tasks for Geographic Redundancy**

**Prerequisites**

Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

**Key tasks**

Only the system administrator can perform Geographic Redundancy-related operations.

• Configure Geographic Redundancy.

  Configure Geographic Redundancy to handle the situation when the primary System Manager server fails or when the managed element loses connectivity to the primary System Manager server.

  **Important:**

  During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

• Enable the Geographic Redundancy replication between the two servers.
Enable the replication in the following scenarios:

- After you configure the two standalone System Manager servers for Geographic Redundancy, you must enable the Geographic Redundancy replication between the two servers to ensure that the secondary System Manager server contains the latest copy of the data from the primary System Manager server.

- During the system maintenance or upgrades, Geographic Redundancy replication must be disabled. After maintenance activity is complete, you must enable Geographic Redundancy replication if it was manually or automatically disabled due to the maintenance activity.

**Note:**

If the heartbeat between the two System Manager servers in which the Geographic Redundancy replication is enabled stops due to network connectivity failure or the server failure, the system automatically disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes. If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers. If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.

- After the primary System Manager server recovers from failure.

**Important:**

During the bulk activities such as import, export, and full synchronization of Communication Manager, the system might disable the Geographic Redundancy replication for reasons, such as the size of the data involved in the bulk activity and the bandwidth between the primary and the secondary System Manager server. After you complete the bulk activity, enable the Geographic Redundancy replication if the replication is disabled.

- Disable the Geographic Redundancy replication between the two servers.

Disable the Geographic Redundancy replication before you start the maintenance activities such as upgrades, installation of software patches or hot fixes. If the primary and the secondary System Manager servers disconnect from each other for more than the threshold period, the system automatically disables the Geographic Redundancy replication. The default threshold period is 5 minutes.

- Activate the secondary System Manager server.

Activate the secondary System Manager server in the following scenarios:

  - The primary System Manager becomes nonoperational.
  - The enterprise network splits.

- Deactivate the secondary System Manager server.

Deactivate the secondary System Manager server in the following situations:

  - The primary System Manager server becomes available.
  - The element network restores from the split.

- Restore the primary System Manager server.
After you activate the secondary System Manager server, to return to the active-standby mode, you must restore the primary System Manager server. You can choose to restore from the primary System Manager or the secondary System Manager server.

**Note:**
The system does not merge the data from the primary and secondary server.

- Reconfigure Geographic Redundancy.

  You can reconfigure Geographic Redundancy when the secondary System Manager is in the standby mode or active mode. The reconfiguration process copies the data from the primary System Manager server to the secondary System Manager server.

- Convert the primary System Manager server to the standalone server.

  Perform this procedure to convert the primary System Manager server in the Geographic Redundancy-enabled system to a standalone server or if you have to configure a new secondary server.

For detailed instructions to complete each task, see the appropriate section in this document.

---

**Configuring Geographic Redundancy**

**Before you begin**

- For the new installation of System Manager, ensure that you change the default password for the system administrator user.

- Ensure that you change CLI passwords on primary and secondary System Manager servers.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

**About this task**

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

**Important:**

- During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

- After the Geographic Redundancy configuration is complete, the credentials used for logging in to the secondary System Manager becomes identical to the login credentials of the primary System Manager.
Procedure

1. Log on to the System Manager web console of the standalone server that you require to designate as the secondary server and perform the following:
   a. On the System Manager web console, click Services > Geographic Redundancy.
   b. Click Configure.
   c. In the dialog box, provide the details of the primary System Manager server in the following fields:
      • Primary Server Username
        Enter the system administrator user name that you use to log on to the primary System Manager server.
      • Primary Server Password
        Enter the system administrator password that you use to log on to the primary System Manager server.
      • Primary Server IP
      • Primary Server FQDN
   d. Click OK.

   The configuration process takes about 30 minutes. However, the duration might vary depending on the size of the data on the primary System Manager server,

   Note:
   Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

   The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

2. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:
   • Log on to the web console of the primary System Manager server and perform the following:
      a. On the System Manager web console, click Services > Geographic Redundancy.
      b. Refresh the GR Health page.

      If Enable is available, the configuration is complete.

   Note:
   Log off and log on to the primary System Manager server to view the updated status of Geographic Redundancy health.
• Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:
  
a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

  The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

  ```
  SMGR :: operationStatus=success
  SMGR :: Quantum has been successfully configured as a secondary.
  ```

Next steps
On the web console of the primary System Manager server, enable the Geographic Redundancy replication.

Related links
- [Converting the primary System Manager server to the standalone server](#) on page 154
- [Prerequisites for System Manager on VMware in the Geographic Redundancy setup](#) on page 144

---

### Enabling the Geographic Redundancy replication

Enable the Geographic Redundancy replication between the two servers to ensure that the data gets continuously replicated between the primary and secondary System Manager servers.

**Before you begin**

• Log on to the System Manager web console of the primary server.
• Ensure that CLI passwords on primary and secondary System Manager servers do not expire.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

**About this task**

⚠️ Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

**Procedure**

1. On the System Manager web console, click Services > Geographic Redundancy.
2. Click Enable Replication.

  The system displays the progress information in the Enable GR Status section.
Note:
Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

If the enabling process is successful, the system displays the Geographic Redundancy replication status as Enabled. If the process fails, the system displays an error message with the replication status as Failed on the primary the System Manager web console. The primary server remains in the failed state while the secondary server rolls back to the previous state. Verify if the system has raised an alarm for a temporary network connectivity failure. Retry when the network connectivity is restored. If the problem persists, contact Avaya service personnel.

Related links
- Disabling the Geographic Redundancy replication on page 150
- Geographic Redundancy field descriptions on page 155

Disabling the Geographic Redundancy replication

Before you begin
Log on to the System Manager web console of the primary server.

Procedure
1. On the System Manager web console, click Services > Geographic Redundancy.
2. Click Disable Replication.
3. In the dialog box, click Yes.

The system displays the progress information in the Disable GR Status section.

If the disabling process is successful, the system displays the Geographic Redundancy replication status as Disabled. The system stops replicating the data from the primary and secondary System Manager server. If the disabling process fails, the system displays an error message on the web console of the primary System Manager.

Related links
- Enabling the Geographic Redundancy replication on page 149
- Geographic Redundancy field descriptions on page 155

Activating the secondary System Manager server

About this task
- When you activate the secondary System Manager server, the system stops replicating the data from the primary System Manager server to the secondary System Manager server. During activation, you cannot gain access to the web console of the secondary System Manager server for some time.
• In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

**Before you begin**
Log on to the System Manager web console of the secondary server.

**Procedure**
1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Click **Activate Secondary Server**.
   The system displays the Geographic Redundancy (GR) Health Current status dialog box.
3. In the Select the reason for activation, choose one of the following options:
   • **Primary Down**: When the primary System Manager server becomes nonoperational, the server hardware is faulty and unusable or the application server fails to recover.
   • **Network Split**: When the enterprise network splits and servers fail to communicate with each other.
   • **Maintenance**: When the maintenance activities such as backup, restore, upgrade, and shutdown are in progress.
   • **Other**: Any other reason where the primary System Manager server becomes unusable and needs the secondary System Manager server to become operational.
4. Click **Yes**.
   The system displays the initialization of the activation process.
5. Click **Yes**.
   The activation process takes about 15–20 minutes to complete.

   If the activation process fails, the system displays an error message on the secondary System Manager web console and rolls back to the previous state. If the activation process is successful, the secondary System Manager server changes to the active mode and provides complete System Manager functionality.

   Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

**Related links**
- [Deactivating the secondary System Manager server](#) on page 151
- [Geographic Redundancy field descriptions](#) on page 155

---

**Deactivating the secondary System Manager server**

**Before you begin**
Log on to the System Manager web console of the secondary server.
Procedure

1. On the System Manager web console, click Services > Geographic Redundancy.

2. Click Deactivate Secondary Server.

   The system displays the Deactivate Secondary Server dialog box and the progress while performing the deactivation process.

3. Click OK.

   If the deactivation process is complete, the secondary System Manager server goes to the standby mode. If the deactivation process fails, the system displays an error message on the secondary System Manager web console and the server remains in the active mode.

Next steps

Restore primary System Manager. For instructions, see Restoring the primary System Manager server.

Related links

Activating the secondary System Manager server on page 150
Geographic Redundancy field descriptions on page 155

Restoring the primary System Manager server

Before you begin

Log on to the System Manager web console of the primary server.

About this task

You can restore the data when the secondary System Manager server is active or in the standby mode. However, for minimum system nonfunctional time during data restoration or an emergency or both, you can restore the data when the secondary System Manager server is active.

Important:

After you restore the system with the secondary System Manager data, if you want to revert to the primary System Manager data, you can restore to the primary System Manager data using the procedure in Step 4. However, you must restore to the primary System Manager data, before you enable the Geographic Redundancy replication. After you enable the Geographic Redundancy replication, you cannot restore to the primary System Manager server data.

Procedure

1. On the System Manager web console, click Services > Geographic Redundancy.

2. Click Restore Data.

3. On the Restore GR dialog box, select a server whose data you want to retain:

   - Primary Server

      The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.
Select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between activation and deactivation and the administrator wants to retain those changes even after restoring the data using Restore Data.

• Secondary Server

The system restores the data from the secondary server on the primary System Manager server. The System Manager web console is unavailable for some time. The time that the system takes to restore depends on the network speed and the size of the data that the system must restore.

After the system recovery, select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between the system recovery and the deactivation and if you want to retain the changes from the secondary System Manager server after restoring the data by using Restore Data.

The system displays the Restore Status dialog box.

The system displays the restore operation status and the status of the primary and the secondary System Manager server.

**Important:**

After you restore the data, all changes that you make on the secondary System Manager server that is active will not be available on the primary System Manager server.

4. If you later decide to revert to the database of the primary System Manager server, perform the following steps after the restore is complete:
   a. Using the command line interface, log in to System Manager of the primary server with administrator privilege CLI user credentials.
b. Change to the $MGMT_HOME/geo/bin directory.

c. Type `sh backupandrestore.sh recovery secondaryIP secondaryFQDN`.

When the script completes, System Manager restarts and contains the data from the primary System Manager server that was available before you restored with the secondary System Manager data.

**Note:**

- To restore with the secondary System Manager server data again, activate and deactivate the secondary System Manager server.
- Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

**Next steps**

Verify the data and deactivate the secondary System Manager server if the server is active during the restoration process.

Enable the Geographic Redundancy replication to synchronize the primary and secondary System Manager servers.

**Related links**

- [Enabling the Geographic Redundancy replication](#) on page 149
- [Deactivating the secondary System Manager server](#) on page 151
- [Geographic Redundancy field descriptions](#) on page 155

### Converting the primary System Manager server to the standalone server

**Before you begin**

- Log on to the System Manager web console of the primary server.
- Disable the Geographic Redundancy replication if you have not already disabled.

**Procedure**

1. On the System Manager web console, click **Services > Geographic Redundancy**.

2. Select the primary System Manager server, and click **Convert To Standalone**.

   The system displays a dialog box.

3. Click **OK**.

   If the conversion is successful, the system displays **Converted to Standalone successfully** and converts the primary System Manager server to a standalone server.

   The system displays the status of the server as **Unconfigured** on the Manage Elements page. The administrator can configure the server when required.
Related links

- Configuring Geographic Redundancy on page 147
- Enabling the Geographic Redundancy replication on page 149
- Geographic Redundancy field descriptions on page 155

Geographic Redundancy field descriptions

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

**Primary Server Details**

The system displays the IP address and the FQDN of the primary System Manager server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convert to Standalone</td>
<td>Converts to a standalone server.</td>
</tr>
<tr>
<td></td>
<td>The system displays the Convert to Standalone</td>
</tr>
<tr>
<td></td>
<td>button only when the replication is disabled.</td>
</tr>
<tr>
<td>Configure</td>
<td>Configures Geographic Redundancy.</td>
</tr>
<tr>
<td></td>
<td>The system displays the Configure button only on</td>
</tr>
<tr>
<td></td>
<td>the standalone System Manager server.</td>
</tr>
<tr>
<td>Reconfigure</td>
<td>Configures Geographic Redundancy.</td>
</tr>
<tr>
<td></td>
<td>The system displays the Reconfigure button only</td>
</tr>
<tr>
<td></td>
<td>on the secondary System Manager server.</td>
</tr>
</tbody>
</table>

**Secondary Server Configured**

You can use the Enable Replication, Disable Replication, and Restore Data buttons only from the primary System Manager server.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Replication</td>
<td>Continuously replicates the data between the primary and the secondary</td>
</tr>
<tr>
<td></td>
<td>System Manager server.</td>
</tr>
<tr>
<td></td>
<td>The system displays the Enable Replication button after the following</td>
</tr>
<tr>
<td></td>
<td>events:</td>
</tr>
<tr>
<td></td>
<td>• State of Geographic Redundancy is Disable.</td>
</tr>
<tr>
<td></td>
<td>• Geographic Redundancy configuration.</td>
</tr>
<tr>
<td></td>
<td>• Restoration of the primary Geographic Redundancy server is complete.</td>
</tr>
</tbody>
</table>

Table continues…
## Button | Description
---|---
Disable Replication | Stops replicating the data between the primary and the secondary System Manager server. The system displays the **Disable Replication** button when the state of Geographic Redundancy is Enable.

### Restore Data
- Recovers the server after the failback.
- The system displays the **Restore Data** button when the secondary System Manager server is deactivated.

## Field name | Description
---|---
IP | Displays the IP address of the secondary System Manager server.
FQDN | Displays FQDN of the secondary System Manager server.
Replication Status | Displays the status of replication. The values are Disabled and Enabled.
Last Action | Displays the last action that you performed on the secondary System Manager server.
Last Action Status | Displays the status of the last action that you performed on the secondary System Manager server.

### GR Health field descriptions
The information available on the GR Health page is read-only.

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

#### GR Health

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| GR Health Status | Displays the health status of the monitored services. The page displays:

- ▢, if the monitored service stops.
- ✔, if the monitored service is running.
- ✗, if the monitored service fails to run. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activate Secondary Server</strong></td>
<td>Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails or the data network splits.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>• The system displays <strong>Activate Secondary Server</strong> only on the secondary System Manager server.  \</td>
</tr>
<tr>
<td></td>
<td>• The system displays the <strong>Activate Secondary Server</strong> or the <strong>Deactivate Secondary Server</strong> button on the page.</td>
</tr>
<tr>
<td><strong>Deactivate Secondary Server</strong></td>
<td>Click to make the primary System Manager resume operation. You use this option when the primary System Manager server restores operation or recovers from a network failure.</td>
</tr>
<tr>
<td></td>
<td>The system displays <strong>Deactivate Secondary Server</strong> only on the secondary System Manager server.</td>
</tr>
<tr>
<td><strong>Service Name</strong></td>
<td>Displays the name of the service for which the system provides the status of the health.</td>
</tr>
<tr>
<td><strong>View Detail</strong></td>
<td>Click <strong>View Graph</strong>.</td>
</tr>
<tr>
<td></td>
<td>• For database and directory replication, the system displays the graph for default interval. If no graph is present for the default interval, using the calendar, you can set the period for which you require to check the health status, and click <strong>Generate</strong> to view health details in a graph.</td>
</tr>
<tr>
<td></td>
<td>For database replication, the system displays graphs for time lag and the size lag. For directory replication, the system displays graph for time lag only.</td>
</tr>
<tr>
<td></td>
<td>• For file replication, the system displays the last replication time and the size of the lag.</td>
</tr>
</tbody>
</table>

**HeartBeat status**

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Name</strong></td>
<td>The name of the monitored service. The services are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System Health</strong>: The heartbeat status indicates if the primary or the secondary System Manager server can communicate with the peer System Manager server over the network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Database Replication</strong>: The heartbeat status indicates if the data stored in the System Manager database is getting replicated between the primary and the secondary System Manager server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Application System Health</strong>: The heartbeat status indicates if the application server of primary or secondary System Manager can query the application server of the peer System Manager.</td>
</tr>
<tr>
<td></td>
<td>• <strong>File Replication</strong>: The heartbeat status indicates if the configuration files are getting replicated between the primary and the secondary System Manager server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Directory Replication</strong>: The heartbeat status indicates if the data stored in the internal LDAP server is getting replicated in the respective System Manager server.</td>
</tr>
<tr>
<td><strong>Last Successful Heartbeat Time</strong></td>
<td>The last time the heartbeat was successful for the monitored service.</td>
</tr>
<tr>
<td><strong>Last Missed Heartbeat Time</strong></td>
<td>The last time when the monitored service missed the heartbeat.</td>
</tr>
<tr>
<td><strong>View Details</strong></td>
<td>The <strong>View Graph</strong> link to view the health status of the monitored service over a period of time. To configure the time period, click <strong>Edit Dates</strong>. The graph displays the status in 0 and 1.</td>
</tr>
<tr>
<td></td>
<td>• 0 indicates that the monitored service is either stopped or failed at that point of time.</td>
</tr>
<tr>
<td></td>
<td>• 1 indicates that the monitored service is running at that point of time.</td>
</tr>
</tbody>
</table>
Chapter 8: Maintenance

Backup and restore

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

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

*Note:*

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

**Procedure**

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

*Important:*

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page,
Creating a data backup on a local server

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 the File name field, enter the backup file that you want to create.
5. 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. 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.

5. 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.

6. 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**

**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. 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.

6. 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>
<tbody>
<tr>
<td>Operation</td>
<td>The type of operation. The values are:</td>
</tr>
<tr>
<td></td>
<td>• Backup</td>
</tr>
<tr>
<td></td>
<td>• Restore</td>
</tr>
<tr>
<td>File Name</td>
<td>• For the backup operation, the name of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• For the restore operation, the name of the backup file that was used for the restore.</td>
</tr>
<tr>
<td>Path</td>
<td>• For the backup operation, the path of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• For the restore operation, the path of the backup file that was used for the restore.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the backup or restore operation. The values are:</td>
</tr>
<tr>
<td></td>
<td>• SUCCESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• PLANNED</td>
</tr>
<tr>
<td></td>
<td>• RUNNING</td>
</tr>
</tbody>
</table>

| Status Description | The error details of the backup or restore operation that has failed.                                                                          |
| Operation Time     | The time of the backup or restore operation.                                                                                                                                                              |
| Operation Type     | Defines whether the backup or restore operation is local or remote.                                                                               |
| User               | The user who performed the operation.                                                                                                          |

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>Opens the Backup page from where you can backup the System Manager data.</td>
</tr>
<tr>
<td>Restore</td>
<td>Opens the Restore page from where you can restore the data to System Manager.</td>
</tr>
</tbody>
</table>
# 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 - GATEWAY <new Gateway address for System Manager>`  
• `changeIPFQDN - 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;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-publicFQDN &lt;new fully qualified domain name for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -publicFQDN &lt;new fully qualified domain name for public interface&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-publicGATEWAY &lt;new Gateway address for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -publicGATEWAY &lt;new Public Gateway address for System Manager&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-publicNETMASK &lt;new netmask address for System Manager&gt;</td>
<td></td>
<td>• changePublicIPFQDN -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>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Select a time zone. For example, America/Denver</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>6</td>
<td>configureNTP</td>
<td>&lt;IP address of NTP server&gt;</td>
<td>Configures the NTP server details.</td>
<td>configureNTP &lt;IP address of NTP server&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Separate IP addresses or hostnames of NTP servers with commas (,).</td>
</tr>
<tr>
<td>7</td>
<td>createCA</td>
<td></td>
<td>Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.</td>
<td>createCA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>You must provide the desired Common Name (CN).</td>
</tr>
<tr>
<td>8</td>
<td>configureOOBM</td>
<td></td>
<td>Enables or disables the Out of Band Management configuration.</td>
<td>• To enable Out of Band Management:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>configureOOBM -- EnableOOBM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• To disable Out of Band Management:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>configureOOBM -- DisableOOBM</td>
</tr>
<tr>
<td>9</td>
<td>enableOOBMMultiTenancy</td>
<td></td>
<td>If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>setSecurityProfile</td>
<td></td>
<td>Enabling the commercial and military grade hardening.</td>
<td>• Enabling commercial grade hardening:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>setSecurityProfile --enable-commercial-grade</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Enabling military grade hardening:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>setSecurityProfile --enable-military-grade</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>11</td>
<td>EASGManage</td>
<td></td>
<td>Enables or disables EASG.</td>
<td>• EASGManage --enableEASG</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• EASGManage --disableEASG</td>
</tr>
<tr>
<td>12</td>
<td>EASGStatus</td>
<td></td>
<td>Displays the status of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EASG.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>EASGProductCert</td>
<td></td>
<td>Displays the EASG</td>
<td>EASGProductCert --certInfo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>certificate details.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>EASGSiteCert</td>
<td></td>
<td>To manage EASG Certificates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>editHosts</td>
<td></td>
<td>To modify the /etc/hosts file.</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>swversion</td>
<td></td>
<td>Displays the System Manager software information.</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>changeVFQDN</td>
<td></td>
<td>To change the System Manager Virtual FQDN.</td>
<td>changeVFQDN&lt;br&gt;• Type the System Manager Virtual FQDN.</td>
</tr>
</tbody>
</table>

**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: 
```bash
#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: 
```bash
#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: 
```bash
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of the 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></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>19</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></td>
<td>toggleWeblmOldcert</td>
<td></td>
<td>Replaces identity certificate with old certificate.</td>
<td>toggleWeblmOldcert</td>
</tr>
<tr>
<td>21</td>
<td>getUserAuthCert</td>
<td></td>
<td>Generates a user specific certificate for System Manager to facilitate certificate-based authentication.</td>
<td></td>
</tr>
</tbody>
</table>
|   | collectLogs  |            | Collects the required logs.                       | • To collect all the logs: collectLogs  
• To collect all the logs along with backup: collectLogs -Db  
• To collect all the logs along with CND data: collectLogs –CND |
<p>| 23| rebootVM     |            | Reboots the System Manager virtual machine.       | Type y or n to reboot the System Manager virtual machine.           |
| 24| powerOffVM   |            | Power off the System Manager virtual machine.      | Type y or n to power off the System Manager virtual machine.        |
| 25| sudo /bin/systectl (parameter) snmpd | start/stop/restart/status | To start or stop, and to check status of the SNMP service. |                                                                        |
| 26| sudo /bin/systectl (parameter) spiritAgent | start/stop/restart/status | To start or stop, and to check status of the Spirit Agent service. |                                                                        |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Command</th>
<th>Parameters</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td><code>sudo /bin/systemctl (parameter) cnd</code></td>
<td>start/stop/restart/status</td>
<td>To start or stop, and to check status of the CND service.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 9: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Virtualized Environment Solution Description</td>
<td>Understand high-level solution and functionality.</td>
<td>Customers and sales, services, and support personnel</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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administering Avaya Aura® System Manager</td>
<td>Perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports.</td>
<td>System administrators</td>
</tr>
<tr>
<td>Using</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using the Solution Deployment Manager client</td>
<td>Deploy Avaya Aura® applications and install patches on Avaya Aura® applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td>Maintaining and Troubleshooting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading Avaya Aura® System Manager</td>
<td>Upgrade the Avaya Aura® System Manager virtual application to Release 7.1.2.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Troubleshooting Avaya Aura® System Manager</td>
<td>Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.</td>
<td>System administrators and IT personnel</td>
</tr>
</tbody>
</table>

Finding documents on the Avaya Support website

Procedure

2. At the top of the screen, type your username and password and click Login.
3. Click **Support by Product > Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.

5. In **Choose Release**, select an appropriate release number.

6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.

7. Click **Enter**.

---

### Training

The following courses are available on the Avaya Learning website at [http://www.avayalearning.com](http://www.avayalearning.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>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007V/W</td>
<td>What is New in Avaya Aura® Release 7.1.3</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2008V/W</td>
<td>What is New in Avaya Aura® Application Enablement Services 7.0</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2009V/W</td>
<td>What is New in Avaya Aura® Communication Manager 7.0</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2010V/W</td>
<td>What is New in Avaya Aura® Presence Services 7.0</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2011/V/W</td>
<td>What is New in Avaya Aura® Session Manager Release 7.1.3 and Avaya Aura® System Manager Release 7.1.3</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2012V</td>
<td>Migrating and Upgrading to Avaya Aura® Platform 7.0</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>2013V</td>
<td>Avaya Aura® Release 7.1.3 Solution Management</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>1A00234E</td>
<td>Avaya Aura® Fundamental Technology</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>1A00236E</td>
<td>Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals</td>
<td>AvayaLive™ Engage Theory</td>
</tr>
<tr>
<td>5U00106W</td>
<td>Avaya Aura® System Manager Overview</td>
<td>WBT Level 1</td>
</tr>
<tr>
<td>4U00040E</td>
<td>Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation</td>
<td>ALE License</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5U00050E</td>
<td>Knowledge Access: Avaya Aura® Session Manager and System Manager Support</td>
<td>ALE License</td>
</tr>
<tr>
<td>5U00095V</td>
<td>Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting</td>
<td>vILT+Lab Level 1</td>
</tr>
<tr>
<td>5U00097I</td>
<td>Avaya Aura® Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting</td>
<td>vILT+Lab Level 2</td>
</tr>
<tr>
<td>3102</td>
<td>Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam</td>
<td>Exam (Questions)</td>
</tr>
<tr>
<td>5U00103W</td>
<td>Avaya Aura® System Manager 6.2 Delta Overview</td>
<td>WBT Level 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 [http://support.avaya.com](http://support.avaya.com) and perform one of the following actions:
  - In Search, type **Avaya Mentor Videos** to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

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

**Note:**

Videos are not available for all products.
Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

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

The following sections describe the best practices for VMware performance and features.

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-tuning-latency-sensitive-workloads-white-paper.pdf.

The following sections describe the recommended BIOS settings for:

• Intel Virtualization Technology
• Dell PowerEdge Servers
• HP ProLiant Servers

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

• Intel Virtualization Technology
• Intel Extended Memory 64 Technology
• Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.
Note:
The VT setting is locked as either On or Off when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings
Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is enabled. Do not change the default.

Dell PowerEdge Server
When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to Maximum Performance.
- Set the CPU Power and Performance Management Mode to Maximum Performance.
- In Processor Settings, set:
  - Turbo Mode to enable.
  - C States to disabled.

HP ProLiant Servers
The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to Static High Mode.
- Disable Processor C-State Support.
- Disable Processor C1E Support.
- Disable QPI Power Management.
- Enable Intel Turbo Boost.
VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see Overview of VMware Tools at http://kb.vmware.com/kb/340.

⚠️ Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command /usr/bin/vmware-toolbox-cmd timesync status.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine. If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add tinker panic 0 to the first line of the ntp.conf file so that the NTP can adjust to the network time even with large differences.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service
cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

- Verifies if the NTP service is getting time from a network time source.
- Indicates which network time source is in use.
- Displays how closely the guest OS matches the network time.
- Displays how often the guest OS checks the time.

The guest OSpolls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is local, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding `ntpd`. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at [http://kb.vmware.com/kb/1006427](http://kb.vmware.com/kb/1006427). The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

---

**Configuring the NTP time**

**Procedure**

1. Select the ESXi server and click the **Configuration** tab.
2. In the left navigation pane, click **Software > Time Configuration**.
3. At the upper-right side of the Time Configuration page, click **Properties**.
4. On the Time Configuration dialog box, in the NTP Configuration area, perform the following:
   a. Select the **NTP Client Enabled** check box.
   b. Click **Options**.
5. On the NTP Daemon (ntpd) Options dialog box, perform the following:
   a. In the left navigation pane, click **NTP Settings**.
   b. Click **Add**.
c. On the Add NTP Server dialog box, in the NTP Server area, enter the IP address of the NTP server.

d. Click OK.

The date and time of the System Manager virtual machine synchronizes with the NTP server.

6. Select the **Restart NTP service to apply changes** check box.

7. Click OK.

The Time Configuration page displays the date and time, NTP Servers, and the status of the NTP client.

---

**VMware networking best practices**

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type `vmxnet3` for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).
Networking Avaya applications on VMware ESXi – Example 1

This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.

- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.

- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The
Communication Manager software duplication link must meet specific network requirements. For more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:

- The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
- The round-trip delay must be 8 ms or less.
- The round-trip packet loss must be 0.1% or less.
- Both servers duplication ports must be on the same IP subnet.
- You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the list measurements occupancy command and looking at the results under the Static + CPU occupancy heading.
- The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.

• Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.

• Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.
Networking Avaya applications on VMware ESXi – Example 2

This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- **VMware Management Network redundancy**: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.

- **Removal of Teaming for Virtual Machines Network**: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

- **Communication Manager Duplex Link**: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.
• Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

<table>
<thead>
<tr>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Support Notice PSN003556u</td>
<td><a href="https://downloads.avaya.com/css/P8/documents/100154621">https://downloads.avaya.com/css/P8/documents/100154621</a></td>
</tr>
<tr>
<td>Performance Best Practices for VMware vSphere® 5.5</td>
<td><a href="http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf">http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf</a></td>
</tr>
<tr>
<td>VMware vSphere 5.5 Documentation</td>
<td><a href="https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html">https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html</a></td>
</tr>
<tr>
<td>VMware vSphere 6.5 Documentation</td>
<td><a href="http://pubs.vmware.com/vsphere-65/index.jsp">http://pubs.vmware.com/vsphere-65/index.jsp</a></td>
</tr>
<tr>
<td>VMware vSphere 6.0 Documentation</td>
<td><a href="https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html">https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html</a></td>
</tr>
<tr>
<td>VMware Documentation Sets</td>
<td><a href="https://www.vmware.com/support/pubs/">https://www.vmware.com/support/pubs/</a></td>
</tr>
</tbody>
</table>

**Storage**

For best performance, use System Manager on disks local to the ESXi Host, Storage Area Network (SAN) storage devices, or Network File System (NFS) shares. Network storage system performance (IOPS and latency) must not impact the ability of the System Manager virtual machine to perform I/O operations in a timely fashion. CPU I/O wait times of the virtual machine should be zero or very close to zero. Slow network I/O performance can cause serious stability issues with the OS and the System Manager application.

**Thin vs. thick deployments**

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

In contrast, a thin virtual disk does not pre-allocate nspace. Blocks in the VMDK file are not allocated and backed by physical storage until they are written during the normal course of operation. A read to an unallocated block returns zeroes, but the block is not backed with physical
storage until it is written. Consider the following when implementing thin provisioning in your VMware environment:

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

---

**Best Practices for VMware features**

**VMware Snapshots**

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

⚠️ Caution:

**Snapshot operations can adversely affect service.** Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.
Snapshots can:

• Consume large amounts of data resources.
• Increase CPU loads on the host.
• Affect performance.
• Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

• Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
• Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.
• Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
• When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the Take Virtual Machine Snapshot window, clear the Snapshot the virtual machine’s memory check box.
  - Select the Quiesce guest file system (Needs VMware Tools installed) check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
• If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

⚠️ Note:

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

<table>
<thead>
<tr>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
</table>

Table continues…
VMware Cloning

System Manager does not support VMware Cloning.

VMware High Availability

In Virtualized Environment, use the VMware High Availability (HA) method to recover System Manager in the event of ESXi Host failure. For more information, see the High Availability documentation for VMware.

When you use VMware HA with System Manager, the communication between System Manager and Avaya Aura® Communication Manager fails. The virtual machine then starts again on a standby server, and the system starts running.

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or underperforming servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
• Use a dedicated NIC to ensure the best performance.

**Note:**

If System Manager WebLM is being used as a master WebLM server in an enterprise licensing deployment for a product, after migration of virtual machine to another physical server by using vMotion, validate connectivity with added local WebLM servers. This is to ensure that the master WebLM server can communicate with local WebLM servers.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>A software solution development by Avaya that includes a guest operating system.</td>
</tr>
<tr>
<td>Blade</td>
<td>A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.</td>
</tr>
<tr>
<td>EASG</td>
<td>Enhanced Access Security Gateway. The Avaya Services Logins to access your system remotely. The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.</td>
</tr>
<tr>
<td>ESXi</td>
<td>A virtualization layer that runs directly on the server hardware. Also known as a <em>bare-metal hypervisor</em>. Provides processor, memory, storage, and networking resources on multiple virtual machines.</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.</td>
</tr>
<tr>
<td>OVA</td>
<td>Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.</td>
</tr>
<tr>
<td>PLDS</td>
<td>Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.</td>
</tr>
<tr>
<td>Reservation</td>
<td>A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make...</td>
</tr>
</tbody>
</table>
storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.

**Snapshot**
The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.

**Storage vMotion**
A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.

**vCenter Server**
An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.

**virtual appliance**
A virtual appliance is a single software application bundled with an operating system.

**VM**
Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.

**vMotion**
A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.

**VMware HA**
VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.

**vSphere Client**
The vSphere Client is an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based client version is VMware 6.5 and later.
Index

**Special Characters**

/sbin/generate-certificates .................................................. 105

**Numerics**

7.1 ...................................................................................... 113

**A**

aborting
  virtual machine report generation ......................................... 100
access Solution Deployment Manager ........................................... 32
access Solution Deployment Manager client ................................. 32
activating
  secondary server ................................................................... 150
adding
  Appliance Virtualization Platform host ................................... 56
  AVP host ........................................................................... 56
  ESXi host .......................................................................... 56
  location ............................................................................. 48
  syslog server ...................................................................... 112
  vCenter to SDM .................................................................. 107
adding certificates
  available hosts .................................................................. 104
  existing hosts .................................................................. 104
  migrated hosts .................................................................. 104
adding ESXi host .................................................................... 56
adding location ...................................................................... 48
adding location to host ............................................................ 108
adding vCenter to SDM ............................................................ 107
adjust System Manager VM properties ......................................... 28
Appliance Virtualization Host
  configure login banner .......................................................... 75
  push login banner ................................................................ 75
Appliance Virtualization Platform ..............................................
  change password ................................................................... 65
  delete syslog ....................................................................... 114
  generating kickstart file ....................................................... 66
  license file .......................................................................... 71
  push syslog .......................................................................... 114
  restarting ............................................................................ 74
  shutting down ...................................................................... 74
  update .................................................................................. 58, 84
  view syslog ........................................................................... 114
  WebLM Configuration ........................................................... 71
Appliance Virtualization Platform host Gateway
  change .................................................................................. 60
  edit ....................................................................................... 60
Appliance Virtualization Platform host IP address
  change .................................................................................. 60
  edit ....................................................................................... 60
Appliance Virtualization Platform host password
  changing ................................................................................ 65
  Appliance Virtualization Platform host password (continued) 
  changing ................................................................................ 65
  Appliance Virtualization Platform network parameters ........... 60
  applying
    third-party AVP certificates ............................................... 76
    architecture ......................................................................... 13
  automatic restart
    virtual machine .................................................................. 139
  Avaya Aura applications deployment order .................................. 21
  Avaya Aura application upgrade .............................................. 113
Avaya Aura products
  license file ........................................................................... 26
  Avaya Aura Virtualized Appliance offer ................................... 14
  Avaya Aura Virtualized Software ........................................... 18
  Avaya virtualization platform ............................................... 14
  Avaya Virtualized offers ....................................................... 13
  Avaya Virtualized Software ................................................... 18
  AVP license status ............................................................... 74

**B**

backup
  remote server ...................................................................... 159
Backup and Restore page .......................................................... 162
best practices
  performance and features ....................................................... 175
  VMware networking ................................................................ 179
  BIOS .................................................................................. 175
  BIOS for HP servers ................................................................ 176
  BIOS settings for Dell servers ................................................ 176

**C**

capability and scalability specification, ........................................ 142
certificates
  accepting ............................................................................ 103
  generating .......................................................................... 103
  certificate update
    ESXi host .......................................................................... 103
    vCenter ............................................................................ 103
    VMware documentation ..................................................... 103
Certification
  validation ............................................................................. 101
  Certification validation ......................................................... 101
  change
    Appliance Virtualization Platform host IP address ................. 60
    DNS .................................................................................. 164
    FQDN from CLI .................................................................. 164
    Gateway ............................................................................. 164
    Host/ IP Settings ................................................................ 62
    IP address from CLI .......................................................... 164
Index

OVA file deploy ................................................................. 121, 123
overview ................................................................. 16
System Manager .......................................................... 13

P
password change .............................................................. 83
password change
Appliance Virtualization Platform host ......................... 65
password policy .......................................................... 65
password rules ............................................................ 65
patch file
install ................................................................. 130
patch information .......................................................... 25
performance best practices ............................................ 175
perform System Manager tests ........................................ 132
postinstall steps ......................................................... 132
power on System Manager VM ........................................ 131
prerequisites ............................................................. 143–145
data migration .......................................................... 23
product knowledge ..................................................... 10
push login banner on host ............................................. 75
pushing syslog ............................................................ 114

R
record network parameters details ................................... 24
record user name and password ..................................... 24
reestablish connection .................................................. 98
Reestablish Connection .................................................. 50
related documentation .................................................. 171
release notes for latest software patches ......................... 25
removing ESXi host ...................................................... 75
removing ESXi host ...................................................... 75
removing location from host .......................................... 108
removing vCenter ......................................................... 109
resources server .......................................................... 25
restart virtual machine .................................................. 89
restarting
Appliance Virtualization Platform ................................ 74
ESXi host ................................................................. 74
restart virtual machine from SDM ................................. 89
restore primary System Manager .................................... 152
restore backup remote server ........................................ 160
restore backup from remote server ................................. 160
restore data backup ..................................................... 161
restore system backup from local server .......................... 161

S
SAL Gateway .............................................................. 140
SDM
installation ............................................................... 30
SDM client dashboard .................................................. 32
secondary server ......................................................... 150, 151
Select Flexi Footprint ................................................... 87
self-signed certificates for ESXi host
generate ................................................................. 105
servers supported ......................................................... 24
Session Manager update ................................................. 34
shutting down
AVP ................................................................. 74
site certificate
add ........................................................................ 135
delete .................................................................. 135
manage ................................................................ 135
view ..................................................................... 135
skills to deploy ............................................................ 10
Snapshot Manager
virtual machine snapshot ............................................. 79
Snapshot Manager field descriptions ................................ 80
snapshots ................................................................. 184
software library
software library management ........................................ 47
viewing a file ............................................................. 47
software patches ........................................................ 25
software requirements ................................................... 29
Solution Deployment Manager ......................................... 65, 68
access ..................................................................... 32
restart virtual machine ................................................ 89
start ....................................................................... 32
start virtual machine ................................................... 88
stop virtual machine .................................................... 88
update Appliance Virtualization Platform host ................... 58
Solution Deployment Manager client dashboard ................. 32
specification
capability .................................................................. 142
scalability .................................................................. 142
stand-alone ................................................................ 154
start virtual machine .................................................... 88
start Solution Deployment Manager .................................. 32
start System Manager VM .............................................. 131
start virtual machine from SDM ..................................... 88
stop virtual machine .................................................... 88
stop virtual machine from SDM ...................................... 88
storage .................................................................... 183
support .................................................................... 174
supported hardware and resources .................................. 25
supported servers ........................................................ 24
syslog receiver configuration
field descriptions ......................................................... 113
VM Deployment *(continued)*

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>field descriptions</td>
<td>90</td>
</tr>
<tr>
<td>vMotion</td>
<td>186</td>
</tr>
<tr>
<td>VM properties adjust</td>
<td>28</td>
</tr>
<tr>
<td>VMware Cloning</td>
<td>186</td>
</tr>
<tr>
<td>VMware components</td>
<td>20</td>
</tr>
<tr>
<td>VMware High Availability</td>
<td>186</td>
</tr>
<tr>
<td>VMware networking best practices</td>
<td>179</td>
</tr>
<tr>
<td>VMware server in Geographic Redundancy setup</td>
<td>144</td>
</tr>
<tr>
<td>VMware software requirements</td>
<td>29</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>177</td>
</tr>
<tr>
<td>VT support</td>
<td>175</td>
</tr>
</tbody>
</table>

W

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebLM Server on AVP host</td>
<td>72</td>
</tr>
<tr>
<td>worksheet, upgrade</td>
<td>24</td>
</tr>
</tbody>
</table>