Deploying Avaya Aura® System Manager

Release 7.0.1
Issue 2
August 2016

© 2015-2016, 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=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 8
Purpose 8
Prerequisites 8
Change history 8
Warranty 9
Chapter 2: Architecture overview 10
System Manager overview 10
Avaya Aura® Virtualized Appliance overview 10
Avaya Aura® Virtualized offers 10
Avaya Virtualized Appliance overview 11
Appliance Virtualization Platform overview 11
Avaya Aura® Virtualized Environment overview 13
Avaya Pod Fx for Enterprise Communications 13
Avaya Aura® virtualized software 14
Methods of System Manager OVA file deployment 15
Virtual machine management 15
Topology 16
Virtualized components 17
OVA deployment order 18
Deployment guidelines 18
Chapter 3: Planning and preconfiguration 20
Prerequisites 20
Upgrade worksheet 21
Supported servers 22
Server hardware and resources for VMware 22
Configuration tools and utilities 22
Customer configuration data 22
System Manager footprint hardware resource matrix 24
Adjusting the System Manager virtual machine properties 25
Software requirements 25
Installing the Solution Deployment Manager client on your computer 26
Accessing the Solution Deployment Manager client dashboard 29
Accessing Solution Deployment Manager 29
Deploying the Utility Services OVA file 29
Installing software patches 31
Chapter 4: Deploying System Manager on the Avaya-provided server 34
Deployment checklist 34
Installing service packs and software patches on System Manager by using the Solution Deployment Manager client 36

Uploading a file to the software library ... 37
Managing the location ... 39
Viewing a location ... 39
Adding a location ... 39
Editing the location ... 40
Deleting a location ... 40
VM Management field descriptions ... 40
New and Edit location field descriptions ... 45
Managing the host ... 46
Adding an ESXi host ... 46
Editing an ESXi host ... 47
Installing the Appliance Virtualization Platform patch from Solution Deployment Manager ... 47
Changing the network parameters for an Appliance Virtualization Platform host ... 49
Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager ... 50
Changing the password for an Appliance Virtualization Platform host ... 53
Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager ... 54
Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI ... 54
Changing the IP address and default gateway of the host ... 55
Shutting down the Appliance Virtualization Platform host ... 56
Restarting the Appliance Virtualization Platform host ... 57
Deleting an ESXi host ... 57
Mapping the ESXi host to an unknown location ... 57
New and Edit host field descriptions ... 58
Change Network Parameters field descriptions ... 58
Host Network / IP Settings field descriptions ... 59
Change Password field descriptions ... 60
Update field descriptions ... 61
Managing the virtual machine ... 61
Deploying the System Manager OVA file by using the Solution Deployment Manager client ... 61
Editing a virtual machine ... 63
Starting a virtual machine from Solution Deployment Manager ... 64
Stopping a virtual machine from Solution Deployment Manager ... 64
Restarting a virtual machine from Solution Deployment Manager ... 65
VM Deployment field descriptions ... 65
Update Static Routing field descriptions ... 69
Installed Patches field descriptions ... 69
Update VM field descriptions ... 70
Reestablish Connection field descriptions ... 70
Additional Solution Deployment Manager functionality ... 71
Certificate validation ... 71

Monitoring a host and virtual machine ... 76
Managing vCenter ... 77
Viewing the job history of virtual machine operations ... 81
Job History field descriptions ... 81
Network Parameters and Configuration Parameters field descriptions ... 82
Chapter 5: Deploying System Manager on VMware by using the vSphere client ... 84
Deployment of cloned and copied OVAs ... 84
Installing the System Manager OVA file by using vSphere Client ... 84
Installing the System Manager OVA file by using vCenter ... 94
Starting the System Manager virtual machine ... 98
Chapter 6: Post Installation Verification ... 100
Postinstallation steps ... 100
Verifying the installation of System Manager ... 100
Installing language pack on System Manager ... 100
Chapter 7: Configuration ... 102
Configuring Out of Band Management on System Manager ... 102
Configuring Out of Band Management on System Manager in the Geographic Redundancy setup ... 103
Enabling Multi Tenancy on Out of Band Management-enabled System Manager ... 104
configureOOBM command ... 105
Configuring the virtual machine automatic startup settings ... 106
SAL Gateway ... 107
Configuring hardware resources to support VE footprint flexibility ... 108
Virtualized Environment footprint flexibility ... 108
Reconfiguring hardware resources for flexible footprint ... 108
Capability and scalability specification ... 109
Geographic Redundancy configuration ... 111
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup ... 111
Prerequisites for System Manager on VMware in the Geographic Redundancy setup ... 112
Key tasks for Geographic Redundancy ... 113
Configuring Geographic Redundancy ... 114
Enabling the Geographic Redundancy replication ... 116
Disabling the Geographic Redundancy replication ... 117
Activating the secondary System Manager server ... 118
Deactivating the secondary System Manager server ... 119
Restoring the primary System Manager server ... 120
Converting the primary System Manager server to the standalone server ... 122
Geographic Redundancy field descriptions ... 122
GR Health field descriptions ... 124
Chapter 8: Maintenance ... 127
Backup and restore of the System Manager data ... 127
Creating a data backup on a remote server ... 127

Creating a data backup on a local server ... 128
Restoring a backup from a remote server ... 128
Restoring data backup from a local server ... 130
Backup and Restore field descriptions ... 131
Installing the System Manager service pack or patch from CLI ... 132
Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI ... 132
changeIPFQDN command ... 133
changePublicIPFQDN command ... 134
Configuring the NTP server ... 135
Configuring the time zone ... 135
System Manager command line interface operations ... 136
Generating test alarms ... 138
Test alarms ... 138
Generating the test alarm from the web console ... 138
Generating the test alarm from CLI ... 139
Network Management Systems Destinations ... 140
Adding Network Management Systems Destination ... 140
Chapter 9: Resources ... 141
Documentation ... 141
Finding documents on the Avaya Support website ... 142
Training ... 142
Viewing Avaya Mentor videos ... 143
Appendix A: Best Practices for VMware performance and features ... 145
BIOS ... 145
Intel Virtualization Technology ... 145
Dell PowerEdge Server ... 146
HP ProLiant Servers ... 146
VMware Tools ... 147
Timekeeping ... 147
Configuring the NTP time ... 148
VMware networking best practices ... 149
Storage ... 153
Thin vs. thick deployments ... 153
Best Practices for VMware features ... 154
VMware Snapshots ... 154
VMware Cloning ... 156
VMware High Availability ... 156
VMware vMotion ... 156
Glossary ... 157

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 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:

Issue	Date	Summary of changes
2.0	May 2016	• Added procedures for installing the Release 7.0.1 feature pack on Release 7.0. • Added procedures for the following in VM Management: - Enabling and disabling SSH on Appliance Virtualization Platform. - Changing network settings that includes, changing VLAN ID, NIC speed, and NIC team and unteaming for an Appliance Virtualization Platform host. - Restarting the Appliance Virtualization Platform host. - Shutting down the Appliance Virtualization Platform host. - Viewing the job history of all operations that are performed on VM Management. - Updating the license status of hosts and virtual machines state. - Removing the Appliance Virtualization Platform patch. - Changing the IP address and default gateway of the host. - Validating the certificates. • Added support for Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers.

Warranty

Avaya provides a 90-day limited warranty on the System Manager software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com. For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

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

Starting with Release 7.0, Avaya Aura® supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA) - Avaya-provided server, Avaya Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 5.5.
- Avaya Aura® Virtualized Environment (VE) - Customer-provided VMware infrastructure

The virtualization offers, provides 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 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.

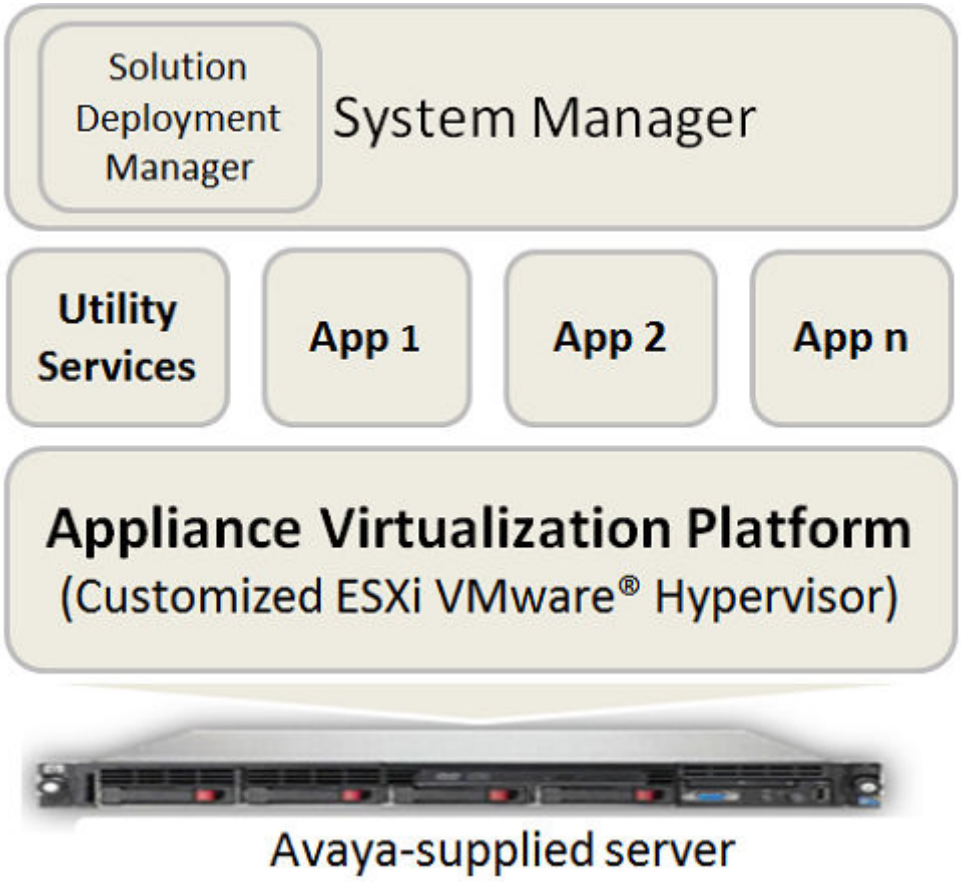
Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya 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, HP ProLiant DL360 G7, HP ProLiant DL360p G8, Dell™ PowerEdge™ R630, and HP ProLiant DL360 G9
- S8300D and S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. 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.



From Release 7.0, Appliance Virtualization Platform replaces System Platform.

Avaya Aura® Release 7.0.1 supports the following applications on Appliance Virtualization Platform:

- Utility Services 7.0.1
- System Manager 7.0.1
- Session Manager 7.0.1
- Branch Session Manager 7.0.1
- Communication Manager 7.0.1
- Application Enablement Services 7.0.1
- WebLM 7.0.1
- Avaya Breeze™ 3.1.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7.0.292 (SP3)
- Avaya Scopia® 8.3.5
- 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.

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 Appliance Virtualization Platform and customer VMware®, and does not include any other industry hypervisor.

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 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.

Title	Description
Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide	Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.
Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide	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.
Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation	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.
Avaya Pod Fx for Enterprise Communications – Release Notes	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.

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 file deployment

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

- For Avaya-appliance deployments, the Solution Deployment Manager client

  For more information, see Deploying the System Manager OVA file by using the Solution Deployment Manager client.

- For customer Virtualized Environment, vSphere or vCentre

  For more information, see Deploying System Manager by using vSphere or Deploying System Manager by using vCenter.

Related links

Deploying the System Manager OVA file using vCenter on page 95
Deploying the System Manager OVA file by using vSphere on page 86
Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 61

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, patch installation, restart, shutdown, and certificate validation of host. 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.

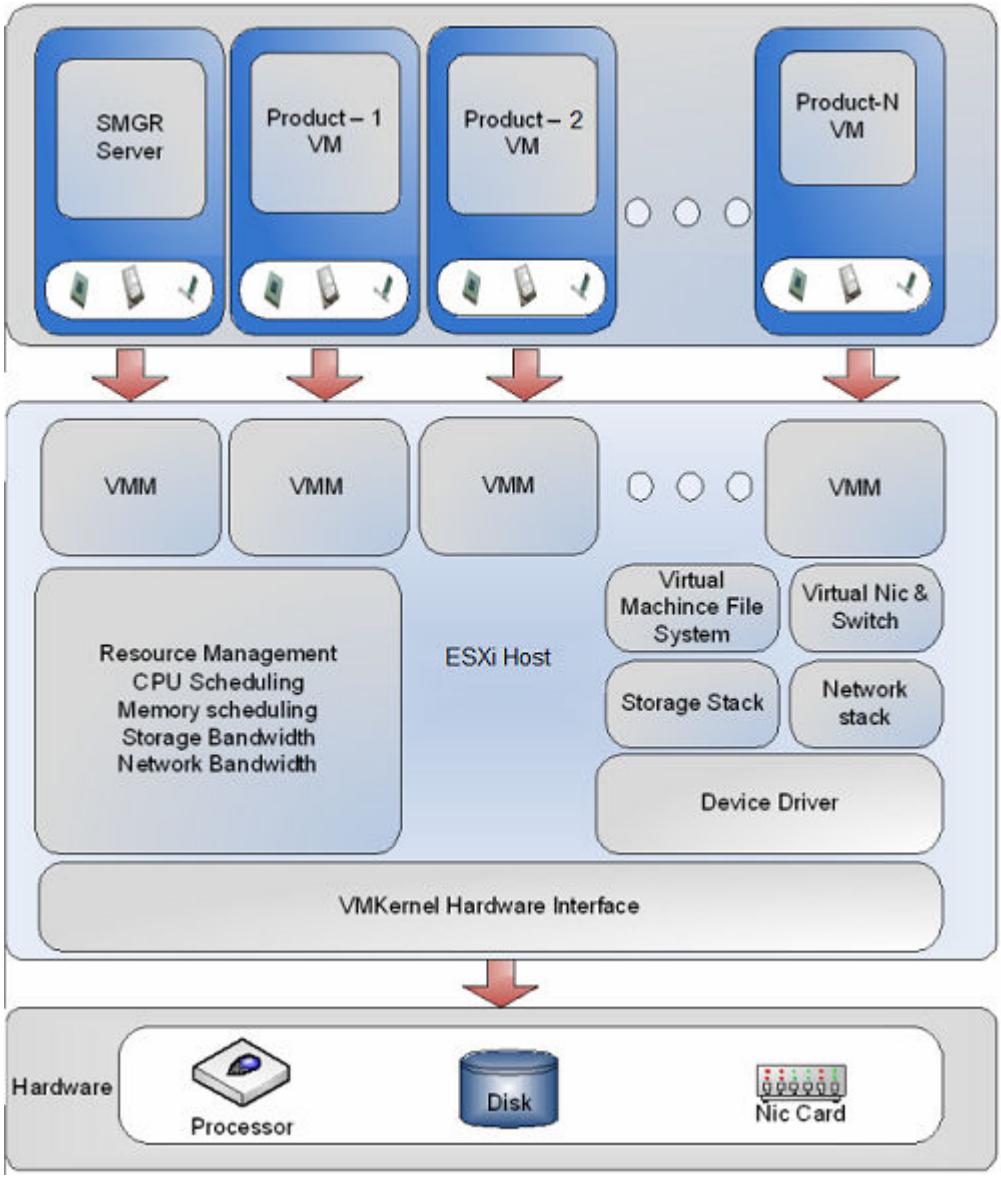
You can deploy the OVA file on the virtual machine by using the System Manager Solution Deployment Manager and the Solution Deployment Manager client.

Related links

Certification validation on page 71

Topology

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



Virtualized components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Table continues…

Software component	Description
vSphere Client	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.
vCenter Server	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.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

OVA deployment order

Deploy the application OVA files in the following order:

- Utility Services
- System Manager
- Session Manager
- Communication Manager
- Application Enablement Services
- SAL
- Communication Manager Messaging
- Presence Services

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

Deployment guidelines

The high-level deployment steps are:

1. Deploy the OVA or OVAs.
2. Configure the application.
3. Verify the installation.

The deployment guidelines for the virtual appliances are:

- 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.

Chapter 3: Planning and preconfiguration

Prerequisites

Serial Number	Prerequisite	Notes
1	Download the following software from the Avaya Support website at http://support.avaya.com: • The System Manager Release 7.0.1 OVA, `SMGR-7.0.0.0.16266-e55-43-29-II.ova` • The `Data_Migration_Utility_7.0.1.0_r96.bin` file • System Manager Release 7.0.1 bin file	
2	Verify that the existing server is compatible with System Manager Release 7.0.1. If the existing server is incompatible, change the server as instructed in the workflow described in this chapter.	Release 7.0.1 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 7.0.1 installation checklist • Upgrade checklist	
4	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	

Table continues…

Serial Number	Prerequisite	Notes
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 roles from the earlier release to System Manager Release 7.0.1.	For more information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager for Release 7.0.1*.

Upgrade worksheet

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

Serial Number	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of System Manager Web Console, enter the IP address of the remote server on which you saved the backup file.
2	**User Name and Password of the remote server**		To gain access to the backup file that is located on a remote server, enter the user name and the password for the account on the System Manager web console.
3	**System Manager command line interface credential**		Open an SSH session and enter `admin` as the user name and password.
4	**Root password of System Manager**		On CLI, to change to root, type the **`su -`** command.
5	**Path and the file name of the backup file on the remote server**		Enter the path and the file name of the backup file.

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 7.0.1:

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

If you must change the server, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9 to install Appliance Virtualization Platform and System Manager Release 7.0.1.

Server hardware and resources 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.

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.

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

Related links

Backup Definition parameters on page 90

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

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
Virtual RAM	9 GB	12 GB	18 GB
Virtual Hard Disk	105 GB	105 GB	250 GB
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager
Common Server R1 support	Yes	No	No
Common Server R2 and R3 support	Yes	Yes	Yes

Table 2: Customer Virtualized Environment

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
CPU reservation	9160 MHz	13740 MHz	18320 MHz
Virtual RAM	9 GB	12 GB	18 GB
Memory reservation	9126 MB	12288 MB	18432 MB
Virtual Hard Disk	105 GB	105 GB	250 GB
Shared NICs	1	1	1
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager

Related links

Adjusting the System Manager virtual machine properties on page 25

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 7.0.x on a customized version of VMware® ESXi 5.5
- Customer-provided Virtualized Environment offer: Supports the following software versions:
  - VMware® vSphere ESXi 5.0
  - VMware® vSphere ESXi 5.1
  - VMware®vSphere ESXi 5.5

- VMware® vSphere ESXi 6.0
- VMware® vCenter Server 5.0
- VMware® vCenter Server 5.1
- VMware® vCenter Server 5.5
- VMware® vCenter Server 6.0

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

Note:

Avaya Aura® Release 7.0 and later does not support ESXi releases earlier than 5.0.

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.

Note:

Click **Next** only once, and wait for the installer to load the next screen.

Before you begin

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel** > **Programs** > **Programs and Features**.

   If you are unable to uninstall, see *Uninstalling the Solution Deployment Manager client*.
2. Ensure that Windows 7 or 8.1 64-bit operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.
3. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

   Tip:

   Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space available.
4. To avoid port conflict, stop any application server that is running on your computer.

Tip:

From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
6. Ensure that ports support Avaya Aura® 7.0.1 supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

   Tip:

   On **Computer**, right-click properties, and perform the following:

   a. In the left navigation pane, click **Advanced system settings**.
   b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.
   c. Verify the system variables.
9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

   On the Avaya PLDS website, at https://plds.avaya.com/, click **Support by Products** > **Downloads**, and provide the product **System Manager**, and version as **7.0.x**.
2. Copy 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`.
3. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
4. On the Welcome page, click **Next**.
5. 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**.
6. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.
7. Click **Next**.

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

       The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.
    c. In **Data Port No**, select the appropriate port from the range 1527 through 1627.
    d. In **Application Port No**, select the appropriate port from the range 443 through 543.
    e. **(Optional)** Click **Reset All to Default**.
10. 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.
11. Click **Install**.
12. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.
13. 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 more information, see “Methods to connect Solution Deployment Manager client to Appliance Virtualization Platform”.

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:

- Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
- Click .

Accessing Solution Deployment Manager

About this task

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

Procedure

Perform one of the following:

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

Deploying the Utility Services OVA file

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. Deploy Utility Services first, install the Release 7.0.1 feature pack, 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 to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.
   c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

   The page displays the capacity details.
6. Click **Next**.
7. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Flexi Footprint**, select the footprint size that the application supports.
      - **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
      - **Default**: For all other server platforms.
8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
9. In the Network Parameters section, ensure that the following fields are preconfigured:
   - **Public**
   - **Services**: Only for Utility Services

- **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. Install the Release 7.0.1 feature pack.
15. Reboot the Utility Services virtual machine.

Next steps

1. Deploy System Manager and install the Release 7.0.1 feature pack.
2. To activate the serviceability agent registration, reset the Utility Services virtual machine.
3. Deploy all other Avaya Aura® applications one at a time.

Installing software patches

About this task

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

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 displays .
16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

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

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

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

19. Click **Schedule**.

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

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

Chapter 4: Deploying System Manager on the Avaya-provided server

Deployment checklist

You can set up Geographic Redundancy on the system after you deploy the System Manager OVA file. For more information, see the Geographic Redundancy configuration section.

Use the following checklist to deploy the System Manager Release 7.0 virtual application by using the Solution Deployment Manager client.

#	Action	Link/Notes	✔
1	Download the following software from the Avaya Support website at http://support.avaya.com: • OVA files for Utility Services and System Manager For System Manager, `SMGR-7.0.0.0.16266-e55-43-29-II.ova` or `SMGR-PROFILE3-7.0.0.0.16266-e55-43-29-II.ova`, the System Manager Release 7.0.1 high capacity OVA. • The `System Manager 7.0.1 bin` file • The Solution Deployment Manager client, `Avaya_SDMClient_win64_7.0.1.0.0620319_44.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…

#	Action	Link/Notes	✔
3	For Avaya Aura® Virtualized Appliance deployments, install the supported server. Appliance Virtualization Platform is preinstalled on the server.	Supported servers on page 22	
4	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.	-	
5	Ensure that the following is accessible: • Hostnames • Out of Band Management considerations • Network configuration data such as naming conventions, IP address, netmask and gateway	-	
6	(Optional) Download the authentication file from http://rfa.avaya.com.	Downloading the authentication file on page 86	
7	Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.		
8	Add a location.	Adding a location on page 39	
9	Add the Appliance Virtualization Platform host.	Adding an ESXi host on page 46	
10	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 on page 29	
11	Install the Utility Services 7.0.1 feature pack.	Installing software patches on page 31	
12	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 61	
13	Install the System Manager Release 7.0.1 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 36	

Table continues…

#	Action	Link/Notes	✔
14	To activate the serviceability agent registration, reset the Utility Services virtual machine.	-	
15	(Optional) After a kernel upgrade, when the system prompts, reboot the System Manager virtual machine.	Starting a virtual machine from Solution Deployment Manager on page 64	
16	Verify the installation of the System Manager virtual machine.	Verifying the installation of System Manager on page 100	
17	(Optional) Install the authentication file on System Manager.	Installing the authentication file on System Manager on page 92	
18	In the settings icon ( ), click **About** to verify that the System Manager version is Release 7.0.1.		

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 <location name> 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.

   Note:

   The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.

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**.

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 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 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 already exist in `versions.xml`, the system does not display the file details. 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 a message about 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 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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. 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 desktop, click the SDM icon (), and then click **VM Management**.
3. On the Location tab, in the Locations section, click **New**.
4. 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.
5. Click **Save**.

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

Related links

New and Edit location field descriptions on page 45

Editing the location

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

Related links

New and Edit location field descriptions on page 45

Deleting a location

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 (), and then click **VM Management**.
3. On the Location tab, in the Locations section, select one or more locations that you want to delete.
4. Click **Delete**.
5. 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

Name	Description
Auto-Reload VM Management Tree	The option to automatically reload the VM Management Tree after the completion of operations such as refreshing virtual machines.

Locations

Name	Description
Location Name	The location name.
City	The city where the host is located.
Country	The country where the host is located.

Button	Description
New	Displays the New Location section where you can provide the details of the location that you want to add.
Edit	Displays the Edit Location section where you can change the details of an existing location.
Delete	Deletes the locations that you select. The system moves the hosts associated with the deleted locations to unknown location.

Hosts

Name	Description
Host Name	The name of the ESXi host.
Host IP	The IP address of the ESXi host.
Host FQDN	FQDN of the ESXi host.
vCenter IP/FQDN	The IP address or FQDN of vCentre.
Current Action	The operation that is currently being performed on the ESXi host.
Last Action	The last completed operation on the ESXi host.
License Status	The status of the license.
Host Version	The ESXi host version. The options are 5.5, 5.1, and 5.0. 6.0 only for VMware ESXi host.
Offer Type	The ESXi host type. The options are: • **AVP**: Appliance Virtualization Platform host • **Customer VE**: customer-provided VMware ESXi host
SSH Status	The SSH service status. The values are: • **enabled** • **disabled**

Table continues…

Name	Description
Host Certificate	The certificate status of the Appliance Virtualization Platform host. The values are: • ✔: The certificate is added in Solution Deployment Manager and correct. • ⊗: The certificate is not accepted or invalid. You can click **View** for details of the certificate status.
vCenter Certificate	The certificate status of the ESXi host. The values are: • ✔: The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • ⊗: The certificate is not accepted or invalid. You can click **View** for details of the certificate status.

Note:

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

Button	Description
Auto Refresh	The option to automatically refresh the page with the latest changes. For example, the page updates: • The VM state when a virtual machine changes • The license status or certificate status of host when host changes The system refreshes the data every minute.
Add	Displays the New Host section where you can provide the details of the host that you want to add.
Edit	Displays the Host Information section where you can change the details of an existing host.
Remove	Removes the hosts that you select. The system moves the hosts associated with the deleted locations to unknown location.
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.

Table continues…

Button	Description
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **Update**	Displays the Update host page where you can select the file for updating the Appliance Virtualization Platform host.
More Actions > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays `SSH enabled successfully`.
More Actions > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.
More Actions > **Host Restart**	Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Host Shutdown**	Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **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.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.

Table continues…

Name	Description
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.0.0.0.
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the VMware host or Appliance Virtualization Platform host
Trust Status	The status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store with the available size.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machines.
Start	Starts the selected virtual machines.
Stop	Stops the selected virtual machines.
Show Selected	Displays only the selected virtual machines.

Table continues…

Button	Description
More Actions > **Restart**	Starts the selected virtual machines that were stopped earlier.
More Actions > **Refresh VM**	Updates the status of the virtual machines.
More Actions > **Reestablish Connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.

New and Edit location field descriptions

Required Location Information

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

Optional Location Information

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

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

Managing the host

Adding an 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.

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Hosts for Selected Location <location name> section, click **New**.
5. In the New Host section, provide the following:

   Host name, IP address, user name, and password.
6. Click **Save**.
7. On the Certificate dialog box, click **Accept Certificate**.

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

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **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.

Related links

New and Edit host field descriptions on page 58
Generating and accepting certificates on page 72

Editing an ESXi host

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 (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host that you want to update.
5. Change the ESXi host information.
6. Click **Save**.

   The system updates the ESXi host information.

Related links

New and Edit host field descriptions on page 58

Installing the Appliance Virtualization Platform patch from Solution Deployment Manager

About this task

Install the Release 7.0.1 feature pack on the existing Appliance Virtualization Platform Release 7.0 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Note:

From System Manager Solution Deployment Manager, you cannot update an Appliance Virtualization Platform that hosts this System Manager.

Do not use this procedure for installing the Appliance Virtualization Platform patch on an S8300D server.

Before you begin

1. Add a location.
2. Add a host.
3. Enable the SSH service on the Appliance Virtualization Platform host.
4. Stop all virtual machines that are running 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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the **Host** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **Update**.
5. On the Update Host page, click **Select patch from local SDM client machine**.
6. 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 `/tmp/avp/avaya-avp-7.0.0.1.0.5.zip`.

   In the Hosts for Selected Location <location name> section, the system displays the update status in the **Current Action** column.
7. To view the details, in the **Current Action** column, click **Patching**.

   Host Patching 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 virtual machines that were running on the Appliance Virtualization Platform host does not automatically start, manually start the machines.

Related links

Update field descriptions on page 61

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 58

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:

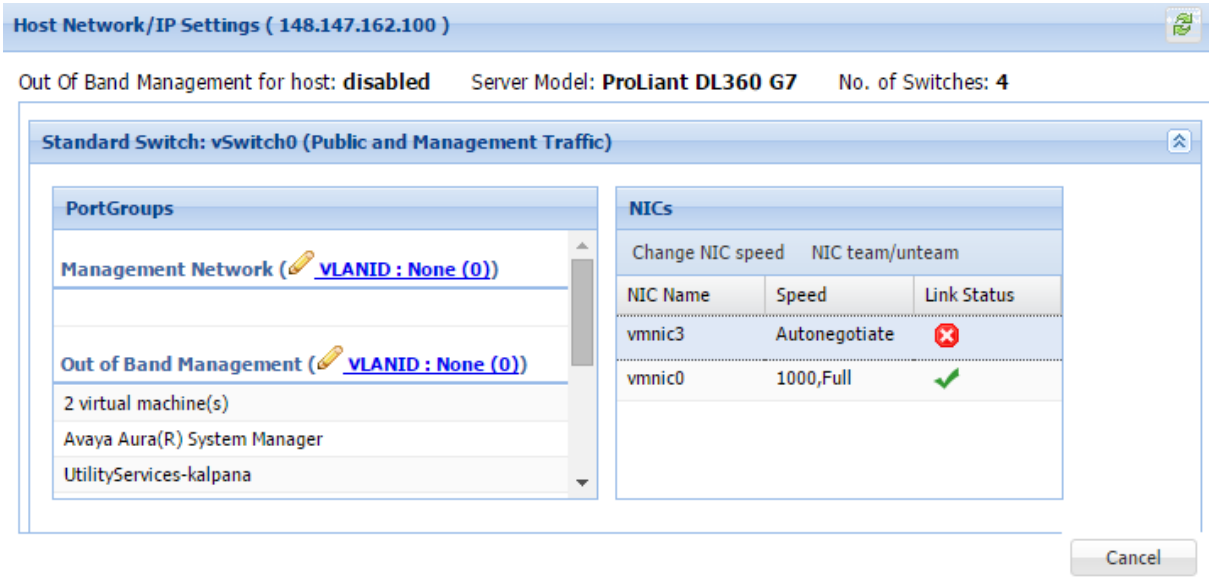
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fails because 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 Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.

4. Click **Change Network params** > **Change Network Settings**.



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

You can configure port groups for the following switches:

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

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

      The section displays the vSwitch details.

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

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

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

      For more information about the value, see NIC teaming.

   d. Click **OK**.

The system displays the new VLAN ID.

Note:

You can change the services port VLAN ID for S8300D servers only through Solution Deployment Manager.

6. To change the NIC speed, perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.

      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.

      For more information, see VLAN ID assignment.

   The system displays the updated NIC speed in the **Speed** column.

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

   Note:

   You can change the speed only for common servers. You cannot change the speed for S8300D and S8300E servers.
7. To change the NIC teaming, perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.

      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or 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 59

Changing the password for an Appliance Virtualization Platform host

About this task

You can change the password only for the Appliance Virtualization Platform host. This is the password for the user that you provide when adding the Appliance Virtualization Platform host.

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 (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **More Actions** > **Change Password**.
5. In the Change Password section, enter the current password and the new password.

   For more information about password rules, see “Password policy”.
6. Click **Change Password**.

   The system updates the password of the Appliance Virtualization Platform host.

Related links

Password policy on page 53
Change Password field descriptions on page 60

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 root password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.

Related links

Changing the password for an Appliance Virtualization Platform host on page 53

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. Select an Appliance Virtualization Platform host.
5. To enable SSH, click **More Actions** > **Enable SSH**.

   The system displays `enabled` in the **SSH status** column.
6. To disable SSH, click **More Actions** > **Disable SSH**.

   The system displays `disabled` 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 as root.
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.

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
5. Click **More Actions** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting the Appliance Virtualization Platform host

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 (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
5. Click **More Actions** > **Host Restart**.

   The system restarts the Appliance Virtualization Platform host and virtual machines.

Deleting an ESXi host

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 (), and then click **VM Management**.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select one or more hosts that you want to delete.
4. Click **Delete**.
5. On the Delete confirmation page, click **Yes**.

Mapping the ESXi host to an unknown location

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In the left navigation pane, click the **Unknown location host mapping** link.

4. In the Host Location Mapping section, select an ESXi host and click **Edit**.

   The system displays the Host Information page.

5. Select a location to which you want to map the ESXi host.
6. Click **Submit**.

   The system displays the ESXi host in the selected location.

New and Edit host field descriptions

Name	Description
Location	The location where the host is availabe. The field is read only.
Host Name	The hostname of Appliance Virtualization Platform or the ESXi host. For example, smgrdev.
Host FQDN or IP	The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.
User Name	The user name to log in to Appliance Virtualization Platform or the ESXi host. **Note:** For Appliance Virtualization Platform, provide the root login and password that you configured in the spreadsheet.
Password	The password to log in to Appliance Virtualization Platform or the ESXi host.

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

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IP	The IP address of the Appliance Virtualization Platform host

Table continues…

Name	Description
Subnet Mask	The subnet mask the Appliance Virtualization Platform host
Host Name	The host name the Appliance Virtualization Platform host
Domain Name	The domain name the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
Gateway	The gateway IP address. The field is available only when you click **Change Gateway**.

Button	Description
Change Gateway	Makes the **Gateway** field available, and displays **Save Gateway** and **Cancel Gateway Change** buttons.
Save Gateway	Saves the gateway IP address value that you provide.
Cancel Gateway Change	Cancels the changes made to the gateway.

Button	Description
Save	Saves the changes that you made to network parameters.

Host Network / IP Settings field descriptions

Port Groups

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

Name	Description
or **VLAN ID** link	Displays the Port Group Properties page where you configure VLAN ID.
VLAN ID	Displays the VLAN ID. The options are: • **None (0)** • **1 to 4093** The field displays only unused IDs.
OK	Saves the changes.

NIC speed

Button	Description
Change NIC speed	Displays the vmnic<n> dialog box.

Name	Description
Configured speed, Duplex	Displays the NIC speed. The options are: • **Autonegotiate** • **10,Half** • **10,Full** • **100,Half** • **100,Full** • **1000,Full**
OK	Saves the changes.

NIC teaming

Button	Description
NIC team/unteam	Displays the Out of Band Management Properties vSwitch<n> dialog box.

Button	Description
Move Up	Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.
Move Down	Moves the VMNIC from active to standby adapter or from standby to unused adapter.
Refresh	Refreshes the page.
OK	Saves the changes.

Change Password field descriptions

Name	Description
Current Password	The password for the user you input when adding the host.
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Update field descriptions

Name	Description
Patch location	The location where the Appliance Virtualization Platform patch is available. The options are: • **Select Patch from Local SMGR**: To use the Appliance Virtualization Platform patch that is available on the local System Manager. • **Select Patch from software library**: To use the Appliance Virtualization Platform patch that is available in the software library.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Installs the patch on the Appliance Virtualization Platform host.

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 Appliance Virtualization Platform or 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.

   c. In **Host FQDN**, type the virtual machine name.

5. In **Data Store**, select a data store.

   The page displays the capacity details.

6. Click **Next**.

7. In the Deploy OVA section, do the following:

   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      To deploy the OVA by using the Solution Deployment Manager client, you can use the default software library that is set during the client installation.

   b. In **Select OVAs**, select the OVA file that you want to deploy.

   c. In **Flexi Footprint**, select one of the following:

      - **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.

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 page displays the following preconfigured fields:

   - **Public**
   - **Out of Band Management**: When Out of Band Management is enabled.

10. 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.

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.

Next steps

- Install the System Manager Release 7.0.1 patch file.
- 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 37
VM Deployment field descriptions on page 65

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. 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 location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.

   The system displays the Edit VMs section.
4. **(Optional)** Click **Change Flexi Footprint** and do the following:
   a. Click **Change flexi foot print value**.
   b. In **Flexi Footprint**, select a foot print 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`.

VM Deployment field descriptions

Select Location and Host

Name	Description
Select Location	The location name. The field is display-only.
Select Host	The hostname of the Appliance Virtualization Platform that you must select. For example, smgrdev.
Host FQDN	FQDN of the Appliance Virtualization Platform host. The field is display-only.
VM Name	The name of the virtual machine.

Table continues…

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Deploy OVA

Name	Description
Provide OVA path	The option to specify the location from where you can get the OVA file.
Select OVA File	The absolute path to the `.ova` file of the virtual machine that you must provide. For example, `C:\Program Files\SDM\smgr_7.ova` The field is available only when you click **Provide OVA path**.
Submit	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Provide OVA path**.
OVA from SW Library	The option to specify the software library where the OVA file is saved.
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 SW Library**
File Name	The `.ova` file that you want to deploy. The field is available only when you click **OVA from SW Library**.
Select Flexi Footprint	The footprint size supported for the selected host. The options are: • System Manager Profile 2 Max User 250K: To support 250000 users. This configuration requires 6 vCPUs and 12 GB memory. • System Manager Profile 1 Max User 35K: To support 35000 users. This configuration requires 4 vCPUs and 9 GB memory.

Table continues…

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

Configuration Parameters

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

Name	Description
Management IP Address (Out of Band Management IP Address)	The IP 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.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.
Management Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
Management Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP or 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.

Network Parameters

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

Table continues…

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

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. For example, grsmgr.
Virtual Domain	The virtual domain name of the System Manager virtual machine. For example, dev.com.

SNMPv3 Parameters

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

Public Network Settings

Name	Description
Public IP Address	The IP address to enable public access to different interfaces.
Public Netmask	The subnetwork mask to assign to System Manager virtual machine.
Public Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
Public Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

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

Update Static Routing field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
Utility Services IP	The IP address of Utility Services

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

Button	Description
Action to be performed	The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are: • **All**: Displays all the software patches. • **Commit**: Displays the software patches that you can commit. • **Rollback**: Displays the software patches that you can rollback.
Get Info	Displays software patches, service packs, and feature packs that you installed.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

Name	Description
VM Name	The name of the System Manager virtual machine on which you want to install the patch.
VM IP	The IP address of System Manager on which you want to install the patch.
Patch Name	The software patch name that you want to install.
Patch Type	The patch type. The options are service pack and software patch.
Patch Version	The software patch version.
Patch State	The software patch state. The states are: • Activated

Table continues…

Name	Description
	• Deactivated • Removed • Installed
Patch Status	The software patch status.

Update VM field descriptions

Name	Description
VM Name	The System Manager virtual machine name
VM IP	The IP address of System Manager
VM FQDN	FQDN of System Manager
Host Name	The host name
Select bin file from Local SMGR	The option to select the software patch or service pack for System Manager. 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. This option is available only on the Solution Deployment Manager client.
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**.

Button	Description
Install	Installs the software patch or service pack on System Manager.

Reestablish Connection field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
User Name	The user name
Password	The password

Button	Description
Reestablish Connection	Establishes connection between System Manager and the virtual machine.

Additional Solution Deployment Manager functionality

Certificate validation

Certification validation

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

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
- 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 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
- Does not validate certificates for hosts that vCenter manages

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 directly log on to the host and confirm that the details in the `/etc/vmware/ssl/rui.crt` file match the details displayed on the screen.

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
5. Click **More Actions** > **Generate/Accept Certificate**.
6. 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 ESXi host on page 46
Generating new self-signed certificates for the ESXi host on page 75

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 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 7.0.1 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 75

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Host tab, in the Host for Selected Location <location name>, select a host.
5. **(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**.
6. 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”.
7. 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 75
Generating and accepting certificates on page 72

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. Click the Monitor Hosts tab.
4. In 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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. Click the Monitor VMs tab.
4. 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.
5. 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 5.0, 5.1, 5.5, and 6.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

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

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In the lower pane, click **Map vCenter**.
4. On the Map vCenter page, click **Add**.
5. In the New vCenter section, provide the following vCenter information:
   - **vCenter FQDN**

     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.
   - **User Name**
   - **Password**
   - **Authentication Type**
6. Click **Save**.
7. 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 78
Map vCenter field descriptions on page 79
New vCentre and Edit vCentre field descriptions on page 79

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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In the lower pane, click **Map vCenter**.
4. On the Map vCenter page, select a vCenter server and click **Edit**.
5. In the Edit vCenter section, change the vCenter information as appropriate.
6. If vCenter is migrated from earlier release, on the Certificate page, click **Accept Certificate**, and click **Save**.
7. 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. On the desktop, click the SDM icon (), and then click **VM Management**.
3. In the lower pane, click **Map vCenter**.
4. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
5. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

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

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

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

New vCentre and Edit vCentre field descriptions

Name	Description
vCenter FQDN	FQDN of vCenter.

Table continues…

Name	Description
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter

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

Managed Hosts

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

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	The version of the ESXi host. The options are: 5.0, 5.1, 5.5, and 6.0.

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

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 (), 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.

Job History field descriptions

Name/Button	Description
Operation	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.
Submit	Provides details of jobs that you selected.

History

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

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.

Name	Description
Configuration Parameters	
Communication Manager IP	IP address of Communication Manager. **Note:** A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine.
TImezone setting	The selected timezone setting for the Utility Services virtual machine.
NTP Server IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management. **Note:** **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.
Utility Services Mode	The mode in which you want to deploy Utility Services. The options are: • **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services. 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.

Table continues…

Name	Description
	• **Utility Servers 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. • **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. **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. Utility Services provides application routing between the physical port and virtual applications.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirmation password	The confirmation password.
Network Parameters	
Default Gateway	The IP address of the default gateway. Required field unless you use DHCP.
DNS	The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP.
Public IP address	The IP address for this interface. Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.

Chapter 5: Deploying System Manager on VMware by using the vSphere client

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.

Related links

Starting the System Manager virtual machine on page 98

Installing the System Manager OVA file by using vSphere Client

Deployment checklist

You can set up Geographic Redundancy on the system after the installation of the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and the Release 7.0.1 bin file. For more information, see the Geographic Redundancy configuration section.

Use the following checklist to deploy the System Manager Release 7.0.1 vAppliance by using vSphere.

#	Action	Link/Notes	✔
1	Download the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and System Manager Release 7.0.1 bin files from the Avaya Support website at http://support.avaya.com.	-	
2	Upload the required software that are required for deployment and upgrade operations to the local or remote software library of System Manager. For example,	Uploading a file to the software library on page 37	

Table continues…

#	Action	Link/Notes	✔
	OVA, firmware, software patches, service packs, and images.		
3	Install vSphere Client 5.0, 5.1 or 5.5.	Download the third-party client from the VMware website.	
4	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.	-	
5	Ensure that the following is accessible: • Hostnames • Out of Band Management considerations • Network configuration data such as naming conventions, IP address, netmask and gateway	Customer configuration data on page 22	
6	(Optional) Download the authentication file from http://rfa.avaya.com.	Downloading the authentication file on page 86	
7	Install the System Manager OVA file.	Deploying the System Manager OVA file by using vSphere on page 86	
8	Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 7.0.1 bin file on page 93	
9	Configure the System Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 106	
10	Start the System Manager virtual machine.	Starting the System Manager virtual machine on page 98	
11	Configure the network parameters by using command line interface.	Configuring the network parameters from the vSphere console on page 88	
12	Verify the installation of the System Manager virtual machine.	Verifying the installation of System Manager on page 100	
13	(Optional) Install the authentication file on System Manager.	Installing the authentication file on System Manager on page 92	
14	In the settings icon ( ), click **About** to verify that the System Manager version is Release 7.0.1.	-	
15	(Optional) Reconfigure the hardware resources for flexible footprint.	Reconfiguring hardware resources for flexible footprint on page 108	

Related links

Deployment of cloned and copied OVAs on page 84
Key tasks for Geographic Redundancy on page 113

Downloading the authentication file

Procedure

1. To gain access to the Avaya RFA Home page, type http://rfa.avaya.com in the web browser.
2. Log on to the RFA Home page.
3. Click **Start the AFS Application**.
4. On the license page, click **I Agree**.
5. In the **Product** field, select `Avaya Aura System Manager`.
6. In the **Release** field, click `7.x`.
7. Click **Next**.
8. To create a new authentication file, perform one of the following:
   - For new installation, click **New System - Product: Avaya Aura System Manager Release: 7.x**.
   - For an upgrade system, click **Upgrade or Re-deliver for Existing System or re-deliver for existing system - Product: Avaya Aura System Manager Release: 7.x**, and type the authentication file ID.
9. Click **Next**.
10. In the **Enter the fully qualified domain name** field, type FQDN or retain the default value.
11. Click **Download file to my PC** or **Download file via email**.

    Depending on the selection, the system downloads the authentication file on your computer or sends the file through email.

Related links

Deployment of cloned and copied OVAs on page 84

Deploying the System Manager OVA file by using vSphere

Before you begin

Install vSphere Client.

Procedure

1. Start vSphere Client.
2. Enter the IP address and the user credentials for the ESXi host.

   Ignore any security warning that the system displays.
3. On vSphere Client, click **File** > **Deploy OVF Template**.

4. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, enter the path to the `.ova` file.
   - Click **Browse** and navigate to the `.ova` file from the local computer, network share, CD-ROM, or DVD.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, change the name for the virtual machine.
9. Click **Next**.
10. On the Deployment Configuration page, in the **Configuration** field, click one of the following:
    - **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.
11. Click **Next**.
12. On the Storage page, select the required data store and then click **Next**.
13. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
14. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network for the Out of Band Management interface and Public interface.
15. Click **Next**.
16. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.
17. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - 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.

Next steps

- When the system starts for the first time, configure the parameters for System Manager. For instructions, see Configuring the network parameters from the vSphere console.

  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.

- Verify the deployment of the System Manager OVA file.

Related links

Deployment of cloned and copied OVAs on page 84
Configuring the network parameters from the vSphere console on page 88
Verifying the installation of System Manager on page 100

Configuring the network parameters from the vSphere console

Before you begin

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

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

About this task

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

Procedure

1. At the prompt, enter the following management network parameters:
   - **Management IP Address (or Out of Band Management IP address)**: The Management or Out of Band Management IP address to assign to the System Manager virtual machine.
   - **Management Netmask**: The subnetwork mask to assign to the Management interface of the System Manager virtual machine.
   - **Management Gateway**: The gateway IP address to assign to the Management interface of the System Manager virtual machine. For example, 172.16.1.1.
   - **IP Address of DNS Server**: The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
   - **Management Short Hostname**: The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

     Note:

     System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
   - **Management Domain Name**: The domain name to assign to the System Manager virtual machine. For example, smgrdev.com.
   - **Default Search List**: The search list of domain names. The field is optional.

- **NTP Server IP or FQDN**: The IP address or FQDN of the NTP server. This is an optional field. Separate the IP addresses or FQDNs 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.

2. At the prompt, enter the following public network parameters:
   - **Public IP Address**: The IP address for the Public interface of the System Manager virtual machine.
   - **Public Netmask**: The subnetwork mask to assign to the Public interface of the System Manager virtual machine.
   - **Public Gateway**: The gateway IP address to assign to the Public interface of the System Manager virtual machine. For example, 172.16.1.1.
   - **Public Hostname**: The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
   - **Public Domain Name**: The domain name to assign to the System Manager virtual machine. For example, smgrdev.dev.

   Note:

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

3. Enter the following SNMPv3 parameters:
   - **User Name Prefix**: For example, global.
   - **Authentication Protocol Password**: For example, globalpass.
   - **Privacy Protocol Password**: For example, globalpass.
4. Enter the following virtual FQDN details of the System Manager virtual machine:
   - Virtual host name. For example, grsmgr.
   - Virtual domain name. For example, dev.com.

   Note:

   - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
   - VFQDN is a mandatory field.
   - Do not add VFQDN entries in the DNS configuration.
   - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
   - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.

- After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:

  a. Log in to the System Manager virtual machine as root user.

  b. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

5. Type the backup definition parameters for the System Manager virtual machine to schedule the remote backup during the System Manager installation. For information, see Backup Definition parameters.

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

6. To confirm the network parameters, type `Y`.

   The system starts the configuration of the network parameters. The deployment process takes about 30–40 minutes to complete.

   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.

7. On the web browser, enter `https://FQDN/SMGR` to gain access to the System Manager web console.

   The system displays the System Manager web console.

Related links

Deployment of cloned and copied OVAs on page 84
Backup Definition parameters on page 90

Backup Definition parameters

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

Note:

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

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

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

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later.

Table continues…

Name	Description
	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.
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 7 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.

Table continues…

Name	Description
Backup Start Hour	The hour in which the backup must start. The value must be 6 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.

Related links

Deployment of cloned and copied OVAs on page 84

Installing the authentication file on System Manager

Avaya BusinessPartner or the Avaya representative provides the authentication file to the customer and the customer can install the authentication file during the deployment of the OVA file if required.

Before you begin

- 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 on System Manager.
- Log in to the System Manager virtual machine as craft, init, inads, or admin to update the ASG file.
- Download the authentication file from http://rfa.avaya.com.

Procedure

1. Copy the authentication file to the `/tmp` directory on the server by using the program such as WinSCP.

   Note the name of the authentication file. For example, `AF-7000438702-121024-172934.xml`.

2. Type `cd /tmp` to navigate to the `tmp` directory.
3. Type `ls`.

   The system lists the authentication file if present.

4. Type `updateASG`.
5. At the prompt, enter the absolute path to the ASG XML file to install the authentication file.

   For example, `/tmp/AF-7000438702-121024-172934.xml`.

   The system displays the message similar to the following:

```
5bd1875ce6dd8a293cd12f1ed2b34c9808e5641f38a85c5a3fbbb7010d0639de2807e11f84551fc1abcee
Mon Mar 4 14:21:02 IST 2013: ASG auth file has changed. Loading new auth file
Loading file /tmp/asg_auth_file.xml
Skipping certificate installation on System Platform
Mon Mar 4 14:21:02 IST 2013: ASG auth file load complete with status: 0
```

Related links

Deployment of cloned and copied OVAs on page 84
Downloading the authentication file on page 86

Installing the System Manager Release 7.0.1 bin file

Before you begin

- Ensure that System Manager is running on Release 7.0.1.
- 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 on System Manager.
- Log in to the System Manager virtual machine as admin.
- Download the `System_Manager_7.0.1.0_r701064859.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/home/admin` location on System Manager.

About this task

If you fail to install the Release 7.0.1 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:

   ```
   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

1. Verify the patch installation.
   - 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.

2. Shut down the System Manager virtual machine.
3. Turn on the System Manager virtual machine.

   System Manager takes about 15 minutes to start.

Related links

Deployment of cloned and copied OVAs on page 84

Installing the System Manager OVA file by using vCenter

Deployment checklist

You can set up Geographic Redundancy on the system after the installation of the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and the Release 7.0.1 bin file. For more information, see the Geographic Redundancy configuration section.

Use the following checklist for deploying the System Manager vAppliance using vCenter.

#	Action	Link/Notes	✔
1	Download the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and System Manager Release 7.0.1 bin files from the Avaya Support website at http://support.avaya.com.	-	
2	Install vSphere Client 5.0, 5.1, or 5.5 and gain access to vCenter.	Download the third-party client from the VMware website.	
3	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.	-	
4	Ensure that the following is accessible:	Customer configuration data on page 22	
5	(Optional) Download the authentication file from http://rfa.avaya.com.	Downloading authentication file on page 86	
6	Install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file and provide network parameters for System Manager.	Deploying the OVA file using vCenter on page 95	

Table continues…

#	Action	Link/Notes	✔
7	Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 7.0.1 bin file on page 93	
8	Configure the System Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 106	
9	Start the System Manager virtual machine.	Starting the System Manager virtual machine on page 98	
10	Verify the installation of the System Manager virtual machine.	Verifying the installation of System Manager on page 100	
11	(Optional) Install the authentication file on System Manager.	Installing the authentication file on System Manager on page 92	
12	In the settings icon ( ), click **About** to verify that the System Manager version is Release 7.0.1.		
13	(Optional) Reconfigure the hardware resources for flexible footprint.	Reconfiguring hardware resources for flexible footprint on page 108	

Related links

Deployment of cloned and copied OVAs on page 84

Deploying the System Manager OVA file using vCenter

Before you begin

- Install vSphere client.
- Install vCenter server and connect vSphere Client to vCenter.

Procedure

1. Start vSphere Client.
2. Enter the IP address and the user credentials for the vCenter server.

   Ignore any security warning that the system displays.
3. On vSphere Client, click **File** > **Deploy OVF Template**.
4. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, enter the path to the `.ova` file.
   - Click **Browse** and navigate to the `.ova` file from the local computer, network share, CD-ROM, or DVD.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.

7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, change the name for the virtual machine.
9. On the Deployment Configuration page, in the **Configuration** field, click one of the following:
   - **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.
10. Click **Next**.
11. In the **Inventory Location** area, select the datacenter and click **Next**.
12. If the cluster exists, select the cluster and click **Next**.
13. Select the specific host within the cluster and click **Next**.
14. On the Storage page, select the required data store and click **Next**.
15. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
16. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network for the Out of Band Management interface and Public interface.
17. On the Properties page:
    a. At the prompt, enter the following management network parameters:
       - **Management IP Address (or Out of Band Management IP address)**: The Management or Out of Band Management IP address to assign to the System Manager virtual machine.
       - **Management Netmask**: The subnetwork mask to assign to the Management interface of the System Manager virtual machine.
       - **Management Gateway**: The gateway IP address to assign to the Management interface of the System Manager virtual machine. For example, 172.16.1.1.
       - **IP Address of DNS Server**: The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
       - **Management Hostname**. The fully qualified domain name to assign to the Management interface of the System Manager virtual machine. For example, bouldervm1.smgrpub.com.
       - **Default Search List**: The search list of domain names. The field is optional.
       - **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.

b. At the prompt, enter the following public network parameters:

- **Public IP Address**: The IP address for the Public interface of the System Manager virtual machine.
- **Public Netmask**: The subnetwork mask to assign to the Public interface of the System Manager virtual machine.
- **Public Gateway**: The gateway IP address to assign to the Public interface of the System Manager virtual machine. For example, 172.16.1.1.
- **Public Hostname**: The fully qualified domain name to assign to the Public interface of the System Manager virtual machine. For example, bouldervm2.smgrdev.com.
- **Virtual FQDN** for the System Manager virtual machine.
  - Virtual short hostname. For example, grsmgr.
  - Virtual domain. For example, dev.com.
    - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
    - VFQDN is a mandatory field.
    - Do not add VFQDN entries in the DNS configuration.
    - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
    - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
    - After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
      a. Log in to the System Manager virtual machine as root user.
      b. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

Note:

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

c. Configure the following SNMPv3 parameters:

- **User Name Prefix**: For example, global.
- **Authentication Protocol Password**: For example, globalpass.
- **Privacy Protocol Password**: For example, globalpass.

d. **(Optional)** Select the **Schedule SMGR backup** check box to schedule the System Manager backup and configure the backup definition input parameters. For information, see Backup Definition parameters.

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.
- The system does not validate the backup definition data that you provide. If the data is invalid, the system does not schedule the backup.

18. Click **Next**.
19. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.

    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.
20. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

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

Next steps

Verify the deployment of the System Manager OVA file.

Related links

Deployment of cloned and copied OVAs on page 84
Verifying the installation of System Manager on page 100
Backup Definition parameters on page 90

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 template file.

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.

Related links

Deployment of cloned and copied OVAs on page 84

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 7.0.1 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 as admin.

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.

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.
3. To add the IP address and subnet ranges in the Management IP range, type `configureOOBM -AddIPtoManagementIPRange`.

   You can now gain access to System Manager from the network.

Related links

configureOOBM command on page 105

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 105

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. You can also add, delete, list the IP address or subnet range for Management and Public network.

Syntax

```
configureOOBM [-EnableOOBM|-DisableOOBM|-ListManagementIPRange|AddIPtoManagementIPRange|
DeleteIPFromManagementIPRange|enableMultitenancyInPublicInterface]
```

Option	Description
EnableOOBM	Enables Out of Band Management on System Manager virtual machine. With **EnableOOBM**, the additional Ethernet interface is configured, network configuration is updated, and firewall rules are set.
DisableOOBM	Disables Out of Band Management on System Manager virtual machine. With **DisableOOBM**, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.
ListManagementIPRange	Lists all IP addresses and subnet range that are available for the Management interface.
AddIPtoManagementIPRange	Adds the IP address or a subnet range to the Management IP address list and reconfigures the firewall rule with the updated list of IP addresses and subnet ranges.
DeleteIPfromManagementIPRange	Deletes IP address or a subnet range from the Management IP address list and reconfigures the firewall rule with the updated list of IP addresses and subnet ranges.
EnableMultitenancyInPublicInterface	Enables Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Example

```
configureOOBM AddIPtoManagementIPRange w.x.y.z/p.q.r.s
```

Where w.x.y.z is the IP address of the subnet or individual machine, and p.q.r.s is the netmask. For example:

```
configureOOBM AddIPtoManagementIPRange 10.10.2.0/255.255.255.0
configureOOBM DeleteIPFromManagementIPRange 10.10.2.0/255.255.255.0
```

Configuring the virtual machine automatic startup settings

About this task

This procedure does not apply for deployments and upgrades of applications running on Appliance Virtualization Platform.

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

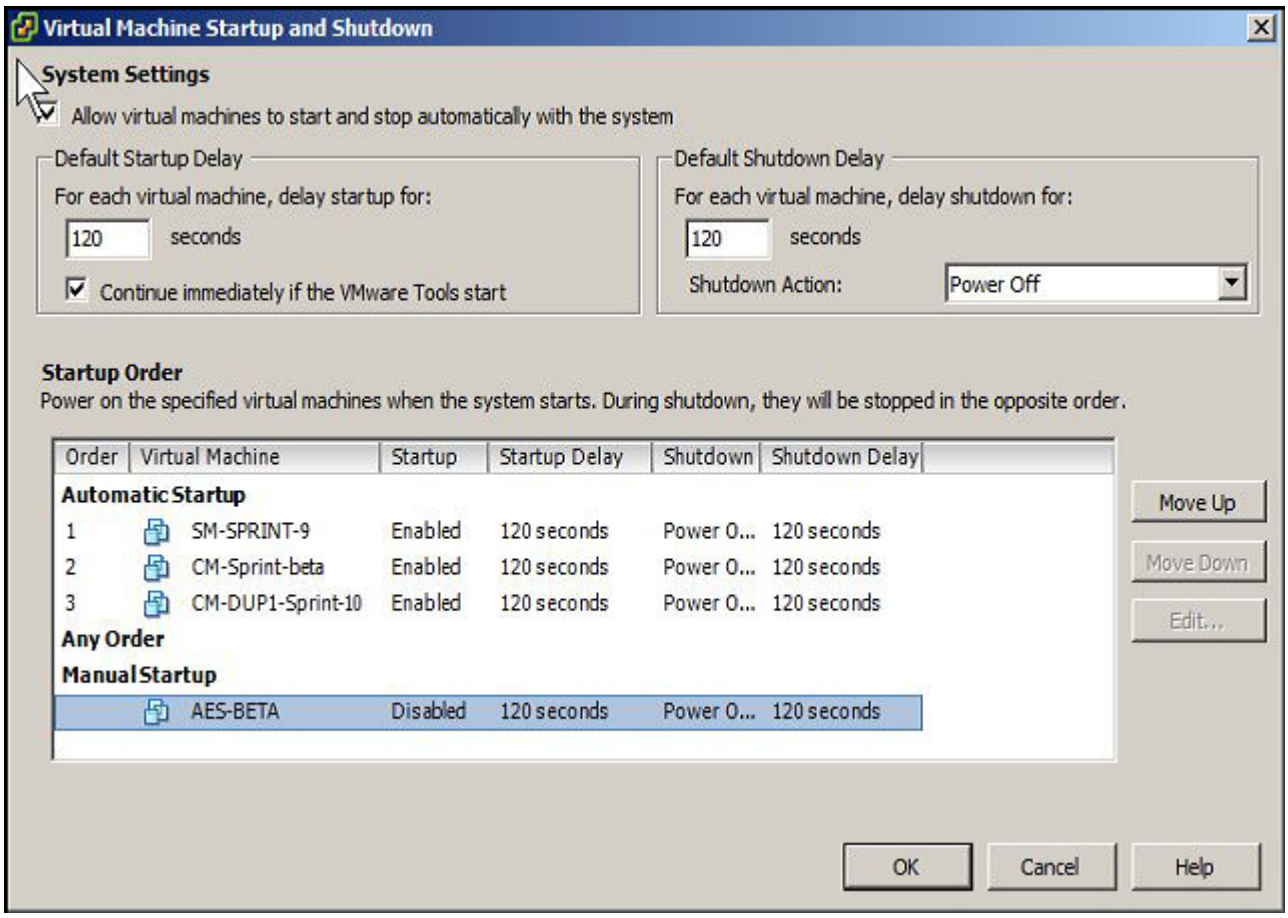
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper-right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine to the **Automatic Startup** section.
8. Click **OK**.

Example

The following is an example of the **Virtual Machine Startup/Shutdown** screen.



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 SALGateway 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
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

Related links

Capability and scalability specification on page 109

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.
16. Power on the virtual machine.

Related links

System Manager footprint hardware resource matrix on page 24
Capability and scalability specification on page 109

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.

Capacity	Maximum limit	Notes
Administrator logins	250	
Simultaneous logins	50	
Total administered endpoints of all types	250,000	The total number of endpoints are defined in Home/Elements/ Communication Manager/ Endpoints / Manage Endpoints

Table continues…

Capacity	Maximum limit	Notes
		Endpoint page in System Manager.
Total administered users defined in the System Manager database	250,000	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.
Messaging mailboxes	250,000	
Contacts per user	250	
Public contacts	1000	
Personal contact lists per user	1	
Members in a personal contact list	250	
Groups	300	
Members in a group	400	
Elements	25,000	
Communication Manager and/or CS 1000	500	Capacity counts against the total number of elements.
Session Managers	28	
Branch Session Manager	500	
IP Office	2000	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.
IP Office Unified Communication Module (UCM) or Application servers as part of Branch deployments	2000	
Roles	200	
Roles per user	20	
Licensing clients	1000	
Concurrent License requests per WebLM	300	
license requests during any 9 minute window per WebLM	50,000	
Local WebLM	22	

Table continues…

Capacity	Maximum limit	Notes
Trust management clients	2500	
Tenants (System Manager Multi Tenant)	250	

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”.

- 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 Geographic Redundancy 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 that is available on the primary System Manager server.
  - During the system maintenance or during the upgrades, Geographic Redundancy replication is disabled. You must enable the replication after the maintenance activity is complete and you configure Geographic Redundancy on the system.

    Note:

    If the heartbeat between the two System Manager servers, in which the Geographic Redundancy replication is enabled, stops because of network connectivity failure or because of the failure of one of the server, 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 relevant 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 GR 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 122
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 112

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 117
Geographic Redundancy field descriptions on page 122

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 116
Geographic Redundancy field descriptions on page 122

Activating the secondary System Manager server

Before you begin

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

About this task

Note:

- 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.

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 secondary the 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.

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.

Related links

Deactivating the secondary System Manager server on page 119
Geographic Redundancy field descriptions on page 122

Deactivating the secondary System Manager server

Before you begin

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

About this task

Note:

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.

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 118
Geographic Redundancy field descriptions on page 122

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.

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 operation is complete. You can ignore this error message.

Procedure

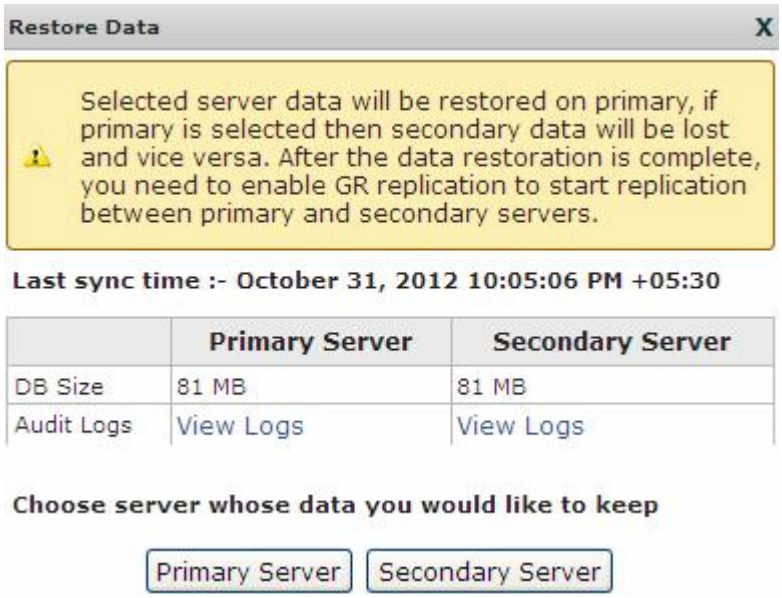
1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:
   - **Primary Server**

     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 as root.
   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

After the data restoration is complete, 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 116
Deactivating the secondary System Manager server on page 119
Geographic Redundancy field descriptions on page 122

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 114
Enabling the Geographic Redundancy replication on page 116
Geographic Redundancy field descriptions on page 122

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.

Name	Description
Convert to Standalone	Converts to a standalone server. The system displays the **Convert to Standalone** button only when the replication is disabled.
Configure	Configures Geographic Redundancy. The system displays the **Configure** button only on the standalone System Manager server.
Reconfigure	Configures Geographic Redundancy. The system displays the **Reconfigure** button only on the secondary System Manager server.

Secondary Server Configured

You can use the **Enable Replication**, **Disable Replication**, and **Restore Data** buttons only from the primary System Manager server.

Button	Description
Enable Replication	Continuously replicates the data between the primary and the secondary System Manager server. The system displays the **Enable Replication** button after the following events: • State of Geographic Redundancy is Disable. • Geographic Redundancy configuration. • Restoration of the primary Geographic Redundancy server is complete.
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.

Table continues…

Field name	Description
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

Name	Description
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.
Activate Secondary Server	Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails or the data network splits. **Note:** • The system displays **Activate Secondary Server** only on the secondary System Manager server. • The system displays the **Activate Secondary Server** or the **Deactivate Secondary Server** button on the page.
Deactivate Secondary Server	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. **Note:** The system displays **Deactivate Secondary Server** only on the secondary System Manager server.

Table continues…

Name	Description
Service Name	Displays the name of the service for which the system provides the status of the health.
View Detail	Click **View Graph**. • 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 **Generate** to view health details in a graph. 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. • For file replication, the system displays the last replication time and the size of the lag.

HeartBeat status

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.

Name	Description
Service Name	The name of the monitored service. The services are: • **System Health**: The heartbeat status indicates if the primary or the secondary System Manager server can communicate with the peer System Manager server over the network. • **Database Replication**: 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. • **Application System Health**: The heartbeat status indicates if the application server of primary or secondary System Manager can query the application server of the peer System Manager. • **File Replication**: The heartbeat status indicates if the configuration files are getting replicated between the primary and the secondary System Manager server. • **Directory Replication**: The heartbeat status indicates if the data stored in the internal LDAP server is getting replicated in the respective System Manager server.

Table continues…

Name	Description
Last Successful Heartbeat Time	The last time the heartbeat was successful for the monitored service.
Last Missed Heartbeat Time	The last time when the monitored service missed the heartbeat.
View Details	The **View Graph** link to view the health status of the monitored service over a period of time. To configure the time period, click **Edit Dates**. The graph displays the status in 0 and 1. • 0 indicates that the monitored service is either stopped or failed at that point of time • 1 indicates that the monitored service is running at that point of time.

Chapter 8: Maintenance

Backup and restore of the System Manager data

Creating a data backup on a remote server

Before you begin

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

Note:

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

Procedure

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

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. 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!!`

Related links

Backup and Restore field descriptions on page 131

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!!`

Related links

Backup and Restore field descriptions on page 131

Restoring a backup from a remote server

About this task

Note:

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

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 software patch installed.

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

Procedure

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

  The backup integrity check feature of 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.

Related links

Backup and Restore field descriptions on page 131

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:

   The backup integrity check feature of 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.

Related links

Backup and Restore field descriptions on page 131

Backup and Restore field descriptions

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

Button	Description
Backup	Opens the Backup page from where you can backup the System Manager data.
Restore	Opens the Restore page from where you can restore the data to System Manager.

Installing the System Manager service pack or patch from CLI

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the  icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Take a snapshot of the System Manager virtual machine.

Procedure

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

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

Next steps

Delete the snapshot after you verify the System Manager functionality.

Related links

System Manager command line interface operations on page 136

Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI

About this task

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

Important:

- Do not change the network settings from vSphere Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.
- After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
  1. Log in to the System Manager virtual machine as root user.

2. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

Before you begin

- 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 on System Manager.
- Log in to the System Manager virtual machine as admin.
- Create the System Manager virtual machine snapshot.

Note:

Delete the snapshot after the System Manager operation is complete.

Procedure

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

   For information, see changeIPFQDN command.

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

   For information, see changePublicIPFQDN command.

Next steps

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

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

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

Related links

changeIPFQDN command on page 133
changePublicIPFQDN command on page 134
System Manager command line interface operations on page 136

changeIPFQDN command

Use the **changeIPFQDN** command to change the Management IP address when Out of Band Management is enabled. With this command you can change the IP address, FQDN, DNS address,

Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address.

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

Syntax

```
changeIPFQDN -IP < >  -FQDN < > -GATEWAY < >-NETMASK < > -DNS < > -SEARCH < >
```

#	Option	Description	Usage
1	IP	The new Management IP address of System Manager.	**changeIPFQDN -IP 10.11.12.13**
2	FQDN	The new Management FQDN of System Manager.	**changeIPFQDN -FQDN a.mydomain.smgr.com**
3	GATEWAY	The new Management Gateway address of System Manager.	**changeIPFQDN -GATEWAY 10.11.1.1**
4	NETMASK	The new Management netmask address of System Manager.	**changeIPFQDN -NETMASK 255.255.203.0**
5	DNS	The new Management DNS address of System Manager. You an provide multiple DNS addresses. Separate each address by a comma.	**changeIPFQDN -DNS 10.11.1.2** **changeIPFQDN -DNS 10.11.12.5,10.11.12.3**
6	SEARCH	The new search list of domain names.	**changeIPFQDN -SEARCH smgr.com**

Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK
255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

changePublicIPFQDN command

Use the **changePublicIPFQDN** command to change the Public IP address when Out of Band Management is enabled. With this command, you can change the IP address, FQDN, Gateway, and Netmask address for Public network configuration of System Manager.

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

Syntax

```
changePublicIPFQDN -publicIP < > -publicFQDN < > -publicGATEWAY < > -publicNETMASK < >
```

#	Option	Description	Usage
1	publicIP	The new Public IP address of System Manager.	**changePublicIPFQDN -IP 10.11.12.13**
2	publicFQDN	The new Public FQDN of System Manager.	**changePublicIPFQDN -FQDN a.mydomain.smgr.com**
3	publicGATEWAY	The new Public Gateway address of System Manager.	**changePublicIPFQDN -GATEWAY 10.11.1.1**
4	publicNETMASK	The new Public netmask address of System Manager.	**changePublicIPFQDN -NETMASK 255.255.203.0**

Example

You can provide options in any combination that the system supports:

```
changePublicIPFQDN -publicIP 10.11.y.z -publicFQDN a.domain.weblm.com -publicGATEWAY
10.11.1.1 -publicNETMASK 255.255.255.0
```

```
changePublicIPFQDN -publicFQDN a.domain.weblm.com -publicGATEWAY 10.11.1.1
```

```
changePublicIPFQDN -publicIP 10.11.y.z
```

Configuring the NTP server

Before you begin

- 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 on System Manager.
- Log in to the System Manager virtual machine as admin.

Procedure

Type `configureNTP <IP address of NTP server>`.

Related links

System Manager command line interface operations on page 136

Configuring the time zone

Procedure

1. Type `configureTimeZone`.
2. Select the time zone from the list.

   For example, America/Denver.

Related links

System Manager command line interface operations on page 136

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	`change IPFQDN`	• `-IP <new Management interface or Out of Bound Management IP address for System Manager>` • `-FQDN <new Management or Out of Bound Management fully qualified domain name for System Manager>` • `-GATEWAY <new Management interface or Out of Bound Management Gateway address for System Manager>` • `-NETMASK <new Management interface or Out of Bound 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 Bound Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• `changeIPFQDN -IP <new IP address>` • `changeIPFQDN -FQDN <new fully qualified domain name>` • `changeIPFQDN -IP <new IP address> -GATEWAY <new Gateway address for System Manager> -SEARCH <new search list for DNS address>`
1	`change Public IPFQDN`	• `-publicIP <new IP address for System Manager>` • `-publicFQDN <new fully qualified domain name for System Manager>` • `-publicGATEWAY <new Gateway address for System Manager>`	Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.	• `changePublicIPFQDN -publicIP <new Public IP address>` • `changePublicIPFQDN -publicFQDN <new fully qualified domain name for public interface>` • `changePublicIPFQDN -publicIP <new`

Table continues…

#	Command	Parameters	Description	Usage
		• **-publicNETMASK <new netmask address for System Manage>**		**Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>**
2	**upgradeSMGR**	**<absolute path to the dmutility.bin> -m -v -V -H**	Upgrades System Manager using the data migration utility.	**upgradeSMGR dmutility *.bin -m -v -V -H**
3	**SMGRPatchdeploy**	**<absolute path to the System Manager service pack or the software patch>**	Installs the software patch or the service pack for System Manager.	**SMGRPatchdeploy <absolute path to /home/admin/ <SMGRservicepackName>** **Note:** Copy the System Manager service pack or patches that you must install to `/home/admin/`.
4	**updateASG**	**<absolute path to the ASG XML file>**	Updates the ASG XML file.	**updateASG <absolute path to the ASG XML file>**
5	**configureTimeZone**	**Time zone that you select**	Configures the time zone with the value that you select.	**configureTimeZone** **Select a time zone. For example, America/Denver**
6	**configureNTP**	**<IP address of NTP server>**	Configures the NTP server details.	**configureNTP <IP address of NTP server>** Separate IP addresses or hostnames of NTP servers with commas (,).
7	**createCA**		Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size. For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	**createCA** You must provide the desired Common Name (CN)

Generating test alarms

Test alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the test alarm to the ADC.

Test Alarm Event

Test Alarm property	Value
Alarm.Message	Test alarm
Alarm.Severity	Minor
Alarm.Status	Raised
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_GEN_0001

Test Clear Event

Test Clear Event property	Value
Alarm.Message	Clear event for test alarm
Alarm. Severity	Indeterminate
Alarm.Status	Cleared
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_CLR_0000

Related links

Generating the test alarm from the web console on page 138
Generating the test alarm from CLI on page 139

Generating the test alarm from the web console

About this task

You can generate test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.

3. In the **Agent List** section, select one or more agents for which you want to generate alarms.
4. Click **Generate Test Alarm**.

   The system generates the alarm.
5. To view the alarm, click **Events** > **Alarms**.

   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.

Generating the test alarm from CLI

Procedure

1. Log in to the computer on which you installed System Manager.
2. At the command prompt, perform the following:
   a. To check the status of SAL Agent, type `service spiritAgent status` and press `Enter`.

      The system displays `SPIRIT Agent is running`.

      Note:

      If the system displays `SPIRIT Agent is not running`, then start SAL Agent.

   b. To start SAL Agent, type `service spiritAgent start` and press `Enter`.

      The `utils` directory contains SAL Agent command line utilities.
3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/`and press `Enter`.
4. Perform one of the following:
   - To generate the test alarm for System Manager, type `sh generateTestAlarm.sh`, and press `Enter`.
   - To generate the clear alarm for System Manager, type `sh generateTestAlarm.sh -c`, and press `Enter`.
5. Perform one of the following:
   - To generate the test alarm for a different product, type `sh generateTestAlarm.sh -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.
   - To generate the clear alarm for a different product, type `sh generateTestAlarm.sh -c -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.

     Here, *LOG_LOCATION* is one of the log files that the SAL agent tails for this product, and `PRODUCT_TYPE` is the log product type that you configured for this product in the SAL agent.

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

- SAL Gateway (mandatory)
- System Manager trap listener
- Third-party NMS
- Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with the SAL Gateway as a trap destination. You can configure the serviceability agent by using the System Manager web console. You must also configure Session Manager as a managed device on the SAL Gateway. Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager for Release 7.0.1*.

Adding Network Management Systems Destination

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see “Managing Serviceability Agents” in *Administering Avaya Aura® System Manager for Release 7.0.1*.

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.

Title	Description	Audience
Overview		
Avaya Aura® Virtualized Environment Solution Description	Understand high-level solution and functionality.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering		
Administering Avaya Aura® System Manager for Release 7.0.1	Perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators
Using		
Using the Solution Deployment Manager client	Deploy Avaya Aura® applications and install patches on Avaya Aura® applications.	System administrators
Maintaining and Troubleshooting		
Upgrading Avaya Aura® System Manager to Release 7.0.1	Upgrade the Avaya Aura® System Manager virtual application to Release 7.0.1.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 142

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 141

Training

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

Course code	Course title	Type
2007V/W	What is New in Avaya Aura® Release 7.0.1	AvayaLive™ Engage Theory
2008V/W	What is New in Avaya Aura® Application Enablement Services 7.0	AvayaLive™ Engage Theory
2009V/W	What is New in Avaya Aura® Communication Manager 7.0	AvayaLive™ Engage Theory

Table continues…

Course code	Course title	Type
2010V/W	What is New in Avaya Aura® Presence Services 7.0	AvayaLive™ Engage Theory
2011/V/W	What is New in Avaya Aura® Session Manager Release 7.0.1 and Avaya Aura® System Manager Release 7.0.1	AvayaLive™ Engage Theory
2012V	Migrating and Upgrading to Avaya Aura® Platform 7.0	AvayaLive™ Engage Theory
2013V	Avaya Aura® Release 7.0.1 Solution Management	AvayaLive™ Engage Theory
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation	ALE License
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura® Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

- In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

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

Note:

Videos are not available for all products.

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 http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.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:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls 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. 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

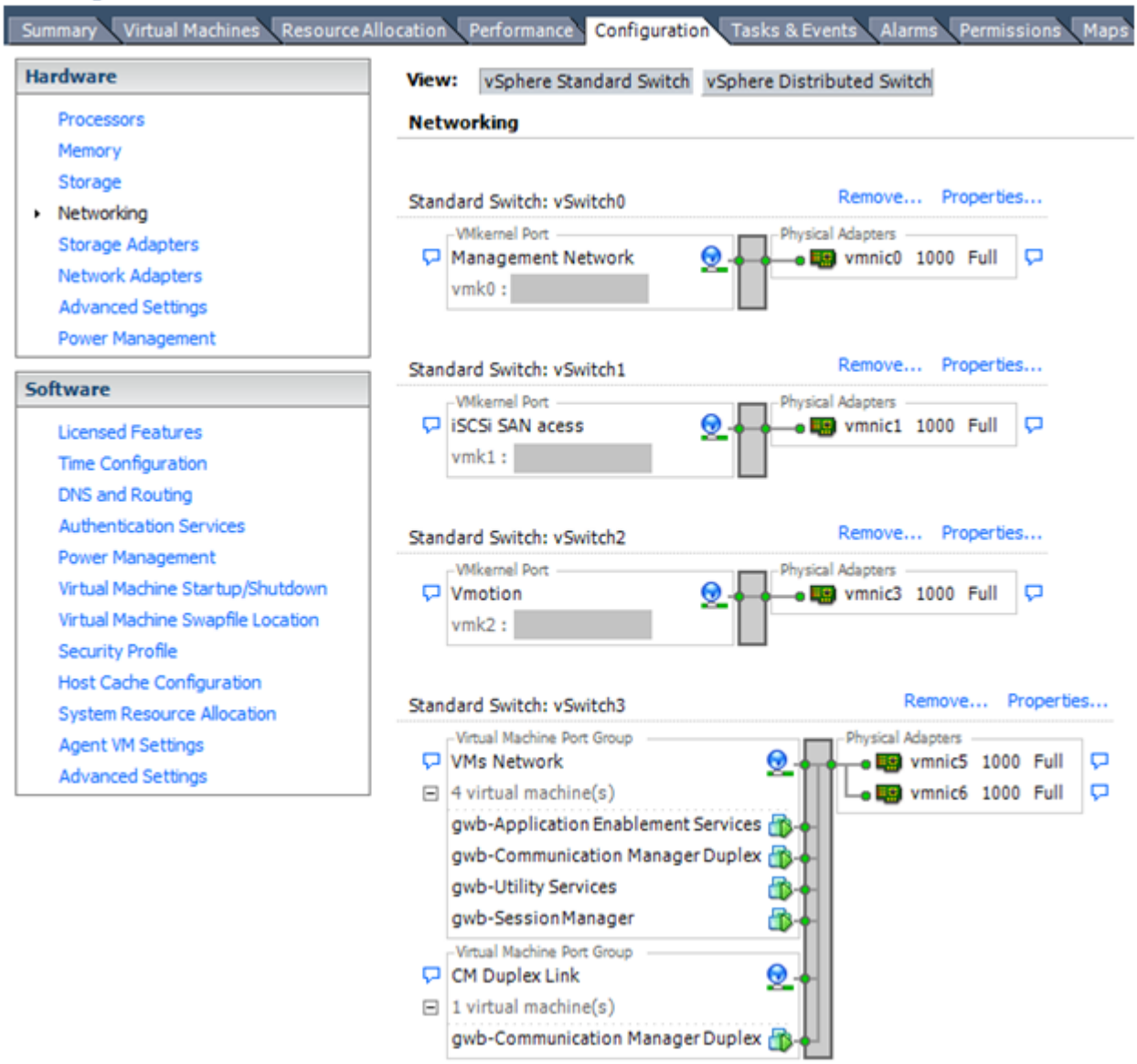
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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:

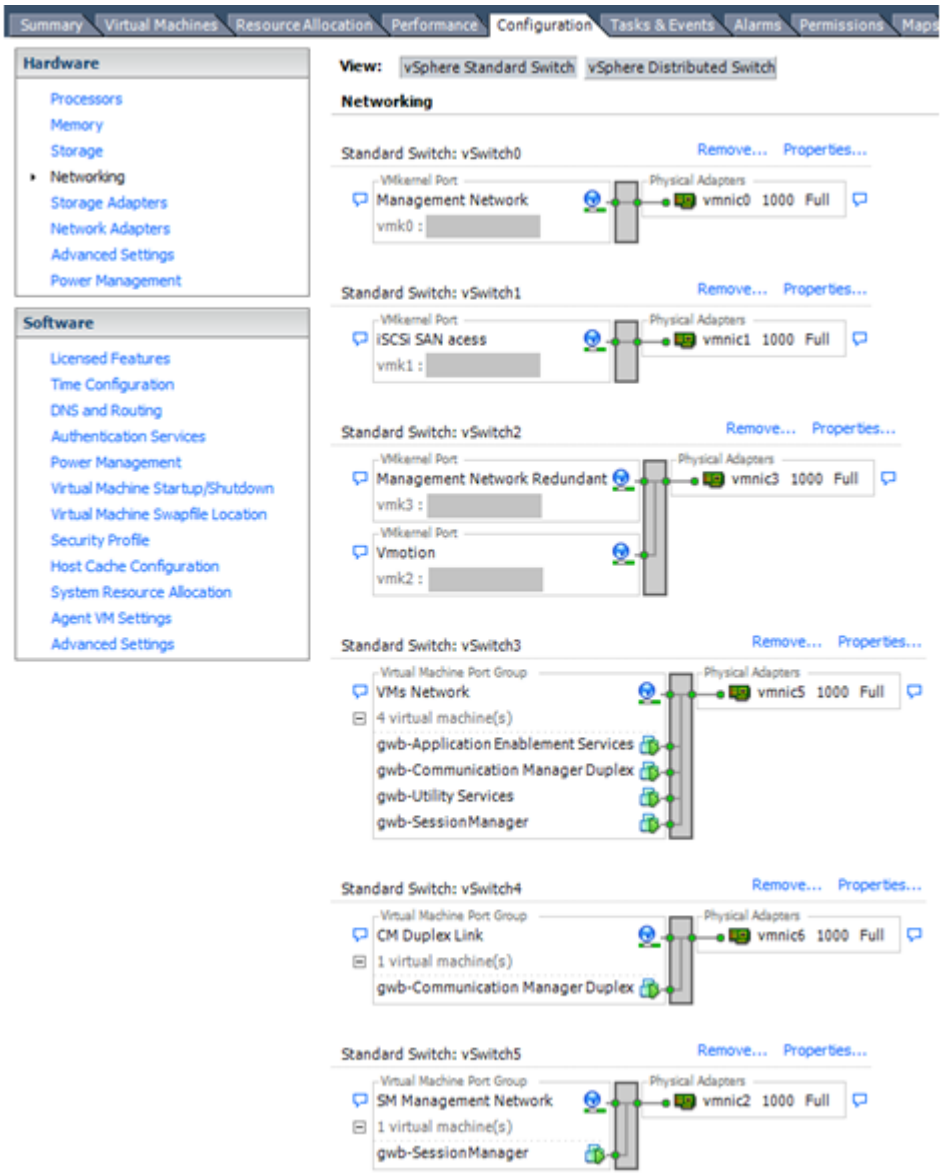
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides 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

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere® 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
Performance Best Practices for VMware vSphere® 6.0	http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware vSphere 6.0 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Storage

When you deploy Avaya Aura® System Manager in Virtualized Environment, observe the following set of storage recommendations:

- Always deploy System Manager with a thickly provisioned disk.
- For best performance, use System Manager only on disks local to the ESXi Host, or Storage Area Network (SAN) storage devices. Do not store System Manager on an NFS storage system.

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

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

VMware Cloning

System Manager does not support VMware Cloning.

VMware High Availability

InVirtualized 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

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Appliance Virtualization Platform	Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. 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. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.
Application	A software solution development by Avaya that includes a guest operating system.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
Blade	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.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	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.

MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	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.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make 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 a downloadable interface for administering vCenter Server and ESXi.

Index

Special Characters

/sbin/generate-certificates 75

A

access Solution Deployment Manager 29
access Solution Deployment Manager client 29
activate
    secondary server 118
add
    virtual machine 65
adding
    Appliance Virtualization Platform host 46
    AVP host 46
    ESXi host 46
    location 39
    vCenter to SDM 77
adding certificates
    available hosts 74
    existing hosts 74
    migrated hosts 74
adding ESXi host 46
adding location 39
adding location to host 78
adding vCenter to SDM 77
add NMS destination 140
add virtual machine 65
adjust System Manager VM properties 25
AFS file 86
    download 86
Appliance Virtualization Platform 10, 11, 50, 54, 59
    change password 53
    restarting 57
    shutting down 56
    update 47, 61
Appliance Virtualization Platform host Gateway
    change 49
    edit 49
Appliance Virtualization Platform host IP address
    change 49
    edit 49
Appliance Virtualization Platform host password
    changing 53
Appliance Virtualization Platform network parameters 49
Appliance Virtualization Platform overview 11
architecture 10
authentication file
    download 86
    install 92
automatic restart
    virtual machine 106
Avaya Aura applications deployment order 18
Avaya Aura products
    license file 22
Avaya Aura Virtualized Appliance offer 11
Avaya Aura Virtualized Software 14
Avaya virtualization platform 11
Avaya Virtualized offers 10
Avaya Virtualized Software 14

B

backup
    remote server 127
Backup and Restore page 131
Backup Definition parameters 90
best practices
    performance and features 145
    VMware networking 149
BIOS 145
BIOS for HP servers 146
BIOS settings
    for Dell servers 146

C

capability and scalability specification, ... 109
certificates
    accepting 72
    generating 72
certificate update
    ESXi host 73
    vCenter 73
    VMware documentation 73
Certification validation 71
change
    Appliance Virtualization Platform host IP address 49
    DNS 132, 136
    FQDN 132
    FQDN from CLI 136
    Gateway 132, 136
    Host/ IP Settings 50
    IP address 132
    IP address from CLI 136
    Netmask 132, 136
    network settings 59
    Network Settings 50
    search list 132, 136
change FQDN from CLI 136
Change Gateway 58
change IP address for AVP host 49
change IP address from CLI 136
changeIPFQDN 136
Change IP FQDN 63
changeIPFQDN command, ... 133

change Netmask for Appliance Virtualization Platform host 49
Change Network Params 49
changePublicIPFQDN 136
changePublicIPFQDN command, ...134
changing
IP address and default gateway 55
changing Appliance Virtualization Platform host password . 53
checklist
deployment procedures 84
System Manager deployment 34
System Manager deployment using vCentre 94
clones
deployment 84
Cloning 156
Collaboration Pod 13
command
AddIPtoManagementIPRange 105
AddIPtoPublicIPRange 105
changeIPFQDN 133
changePublicIPFQDN 134
configureOOBM 105
configureTimeZone 135
DeleteIPfromManagementIPRange 105
DeleteIPfromPublicIPRange 105
enableMultitenancyInPublicInterface 105
ListManagementIPRange 105
ListPublicIPRange 105
updateASG 92
Communication Manager update 31
components
virtualized 17
VMware 17
configuration data
customer 22
configuration tools and utilities 22
configure 148
backup definition 90
configure network parameters from command line interface 88
configureNTP 135, 136
configureTimeZone 135, 136
configuring
Geographical Redundancy 114
virtual machine automatic restart 106
configuring NTP server 135
configuring Out of Band Management 105
configuring Out of Band Management on System Manager 102, 103
configuring time zone 135
convert
to stand-alone 122
correcting ESXi host certificate 73
courses 142
create
virtual machine 61
createCA 136
creating data backup on remote server 127
creating system data backup on a local server 128
customer configuration data 22
customer VMware 13

D

data
Backup Definition Parameters 22
network configuration 22
SNMP parameters 22
VFQDN 22
data backup
create 128
remote server 127
data backup from local server 130
data migration prerequisites 20
deactivate
secondary server 119
deleting
ESXi host 57
location 40
deleting ESXi host 57
deleting location 40
deleting vCenter 78
deploy
product knowledge 8
skills 8
System Manager 61
tools 8
deploy application 15
Deploying an OVA file
utility services 29
deploying copies 84
deploying System Manager 86
deployment
thick 153
thin 153
deployment guidelines 18
deployment order of OVA files 18
deployment procedures
checklist 84, 94
deploy OVA 61
deploy System Manager 34
deploy System Manager ova file 15
deploy System Manager OVA file using vCenter 95
disabling
Geo Redundancy replication 117
SSH on Appliance Virtualization Platform 54
disabling SSH 54
documentation 141
download
AFS file 86
download authentication file 86

E

edit

edit *(continued)*
virtual machine ... 63
Edit Host ... 58
editing
ESXi host ... 47
location ... 40
vCenter ... 78
editing ESXi host ... 47
editing location ... 40
editing vCenter ... 78
Edit Location ... 45
Edit vCenter ... 79
edit virtual machine ... 63
enable
Multitenancy on Out of Band Management-enabled System Manager ... 105
enabling
Geographic Redundancy replication ... 116
SSH on Appliance Virtualization Platform ... 54
Enabling Multi Tenancy on Out of Band Management-enabled System Manager ... 104
enabling SSH ... 54
esxcfg-route ... 55
esxcli network ip interface ipv4 set -i vmk0 -I ... 55
ESXi host
adding ... 46
deleting ... 57
editing ... 47
ESXi host certificate addition ... 74
ESXi host certificate update ... 73
ESXi host map to unknown location ... 57
existing hosts
managing certificates ... 74
existing vCenter
managing certificates ... 74

F

features best practices ... 145
field descriptions
change password ... 60
Edit Host ... 58
Edit Location ... 45
Hosts ... 40
Job History ... 81
Locations ... 40
Map vCenter ... 79
New Host ... 58
New Location ... 45
Virtual Machines ... 40
VM Deployment ... 65
flexible footprint ... 108
configuring hardware resources ... 108
footprint flexibility ... 108
footprint hardware matrix
System Manager ... 24
FQDN ... 132
changeIPFQDN ... 133
changePublicIPFQDN ... 134

G

generate test alarm ... 139
generate test alarms ... 138
generating
certificates ... 72
new self-signed certificates for ESXi host ... 75
generating test alarms ... 138
Geographical Redundancy ... 114
configuring ... 114
Geographic Redundancy ... 112, 119, 120, 122, 124
disable ... 117
enabling ... 116
prerequisites ... 111
Geographic Redundancy field descriptions ... 122
Geographic Redundancy key tasks ... 113
Geo Redundancy ... 118
GR Health field descriptions ... 124
guidelines
deployment ... 18

H

HA ... 156
hardware and software prerequisites on primary and secondary servers ... 111
hardware and software prerequisites on the primary and secondary servers ... 112
hardware resources
configuring for flexible footprint ... 108
hardware supported
System Manager ... 22
High Availability ... 156
host ... 50, 59
monitoring ... 76
Host
update ... 61
Hosts ... 40

I

install
Application Enablement Services ... 26
Avaya Aura applications ... 26
Avaya Aura Media Server ... 26
Avaya Breeze ... 26
Branch Session Manager ... 26
Communication Manager ... 26
patch from CLI ... 136
SAL ... 26
SDM ... 26
service pack from CLI ... 136
Session Manager ... 26

install *(continued)*
Solution Deployment manager client 26
System Manager 26
System Manager patch 93
System Manager service pack from CLI 132
WebLM 26
install authentication file 92
install AVP host patch
Solution Deployment Manager 47
Installed Patches field descriptions 69
installing
Canadian French 100
language pack 100
install new license files 100
install patches 31
install patch from CLI 136
install service pack from CLI 136
install services packs 31
install software patches 31
install System Manager ova file 15
install System Manager OVA file using vCenter 95
Install System Manager patch 70
Intel Virtualization Technology 145
IP address 132
IP address and default gateway
changing 55

J

Job History 81

K

key tasks
Geographic Redundancy 113

L

license file
Avaya Aura products 22
Life cycle management 15
location
adding 39
deleting 40
editing 40
view 39
Locations 40

M

managing certificates migrated hosts 74
map ESXi host to unknown location 57
Map vCenter 77–79
migrated hosts
managing certificates 74
monitoring
host 76
virtual machine 76
VM 76
Multitenancy on Out of Band Management-enabled System Manager 105
Multi Tenancy on Out of Band Management-enabled System Manager 104

N

network management systems destination 140
Network Management Systems Destinations 140
network parameters 88
change 58
Network Parameters and Configuration Parameters
field descriptions 82
New Host 58
new license file 100
New Location 45
New vCenter 79
NMS destination
add 140
NMS destinations 140
NTP server
configure 135
NTP time 148
NTP time source 147

O

offer
Avaya appliance 10
Virtualized Environment 10
Out of Band Management
disable 102, 105
enable 102, 105
Geographic Redundancy 103
OVA deployment order 18
OVA file
deploy 86, 95
overview 13
System Manager 10

P

parameters
backup definition 90
password
change 60
password change
Appliance Virtualization Platform host 53
password policy 53
password rules 53
patch file
install 93
performance best practices 145

perform System Manager tests 100
postinstall
steps 100
power on System Manager VM 98
prerequisites 111–113
data migration 20
product knowledge 8

R

record network parameters details 21
record user name and password 21
reestablish
connection 70
Reestablish Connection 40
related documentation 141
removing location from host 78
removing vCenter 78
resources
server 22
restart
virtual machine 65
restarting, AVP 57
restart virtual machine from SDM 65
restore
primary System Manager 120
restore backup
remote server 128
restore backup from remote server 128
restore data backup 130
restore system backup from local server 130

S

SAL Gateway 107
SDM
installation 26
SDM client dashboard 29
secondary server 118, 119
Select Flexi Footprint 63
self-signed certificates for ESXi host
generate 75
server hardware and resources 22
servers supported 22
Session Manager update 31
shutting down
AVP 56
skills to deploy 8
snapshots 154
SNMP traps 140
software library
software library management 37
viewing a file 37
software requirements 25
Solution Deployment Manager 53, 54
access 29
restart virtual machine 65
start 29
start virtual machine 64
stop virtual machine 64
update Appliance Virtualization Platform host 47
Solution Deployment Manager client
install 26
Solution Deployment Manager client dashboard 29
specification
capability 109
scalability 109
stand-alone 122
start
virtual machine 64
start Solution Deployment Manager 29
start System Manager VM 98
start virtual machine from SDM 64
stop
virtual machine 64
stop virtual machine from SDM 64
storage 153
supported servers 22
System Manager
deploy 61, 86
footprint hardware matrix 24
installing patches 36
resource requirements 24
Solution Deployment Manager 36
topology 16
Virtual Machines 36
VM Management 36
System Manager bin file 93
System Manager deployment
checklist 34
System Manager deployment using vCentre 94
System Manager documentation 141
System Manager installation
verify 100
System Manager ova
deploy 15
System Manager overview 10
System Manager patch 93, 132
System Manager restore 120
System Manager service pack 132
System Manager training 142
System Manager VM management 69
System Manager VM update 70

T

test alarm from CLI
generate 139
test alarms from web console
generate 138
thick deployment 153
thin deployment 153
timekeeping 147
time zone

time zone *(continued)*
configure 135
tools and utilities 22
tools to deploy 8
topology 16

U

unconfigure
Geographic Redundancy 122
Unknown location host mapping 57
update
Appliance Virtualization Platform 61
Appliance Virtualization Platform host 47
Communication Manager 31
Session Manager 31
updateASG 92, 136
update software 31
update static routing 69
Update Static Routing 40
update System Manager VM 70
updating ESXi host or vCenter certificate 73
upgrade
System Manager 136
upgrade worksheet 21

V

vCenter
add 79
adding 77
add location 78
deleting 78
edit 79
editing 78
manage 78
remove location 78
removing 78
unmanage 78
vCenter certificate update 73
vCentre 79
verify
System Manager installation 100
videos 143
view
location 39
viewing job history 81
view location 39
Virtualized Appliance 11
Virtualized components 17
Virtualized Environment 11, 13
virtual machine 86, 95
automatic restart configuration 106
create 61
edit 63
monitoring 76
restart 65
start 64
stop 64
Virtual machine management 15
virtual machine operations
job history 81
Virtual Machines 40
VM connection reestablish 70
VM Deployment 65
vMotion 156
VM properties
adjust 25
VMware Cloning 156
VMware components 17
VMware High Availability 156
VMware networking
best practices 149
VMware server in Geographic Redundancy setup 112
VMware software requirements 25
VMware Tools 147
VT support 145

W

warranty 9
worksheet, upgrade, ... 21