Deploying Avaya Aura® System Manager on VMware® in Virtualized Environment

Release 6.3
January 2015

© 2014 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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

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 Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, 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.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 7
- Related resources 8
  - Documentation 8
  - Training 8
  - Viewing Avaya Mentor videos 9
- Support 10
- Warranty 10

Chapter 2: Architecture overview 11
- Avaya Aura® Virtualized Environment Overview 11
- Topology 12
- VMware components 14
- OVA deployment order 14
- Deployment guidelines 14

Chapter 3: Planning and configuration 16
- Server hardware and resources 16
- Configuration tools and utilities 16
- Customer configuration data 16
- System Manager virtual machine resource requirements 17
- Adjusting the System Manager virtual machine properties 18
- VMware software requirements 19

Chapter 4: Installing the System Manager OVA file 20
- Deployment of cloned and copied OVAs 20
- Methods of System Manager OVA file deployment 20
- Installing the System Manager OVA file by using vSphere Client 20
  - Deployment checklist 20
  - Downloading the authentication file 22
  - Deploying the System Manager OVA file by using vSphere 22
  - Configuring the network parameters from the vSphere console 24
  - Backup Definition parameters 25
  - Installing the authentication file on System Manager 27
  - Installing the System Manager Release 6.3.13 bin file 28
- Installing the System Manager OVA file by using vCenter 29
  - Deployment checklist 29
  - Deploying the System Manager OVA file using vCenter 30
- Starting the System Manager virtual machine 33

Chapter 5: Postinstallation verification 34

Postinstallation steps 34
Verifying the installation of System Manager 34
Chapter 6: Configuration 35
Configuring the virtual machine automatic startup settings 35
SAL Gateway 36
Configuring hardware resources to support VE footprint flexibility 37
Virtualized Environment Footprint Flexibility 37
Reconfiguring hardware resources for flexible footprint 37
System Manager Virtualized Environment footprint hardware resource matrix 38
Capability and scalability specification 38
Geographic Redundancy configuration 40
Prerequisites for System Manager on VMware in the Geographic Redundancy setup 40
Key tasks for Geographic Redundancy 41
Configuring Geographical Redundancy 42
Enabling the Geographic Redundancy replication 44
Disabling the Geographic Redundancy replication 45
Activating the secondary System Manager server 46
Deactivating the secondary System Manager server 47
Restoring the primary System Manager server 47
Converting the primary System Manager server to the standalone server 50
Geographic Redundancy field descriptions 50
GR Health field descriptions 52
Chapter 7: Maintenance 55
Backup and restore System Manager data 55
Creating a data backup on a remote server 55
Creating a data backup on a local server 56
Restoring a backup from a remote server 56
Restoring data backup from a local server 57
Backup and Restore field descriptions 58
Installing the System Manager service pack or patch from CLI 59
Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI 60
changeIPFQDN command 61
Configuring the NTP server 62
Configuring the time zone 62
System Manager command line interface operations 62
Generating test alarms 64
Test alarms 64
Generating the test alarm from the web console 64
Generating the test alarm from CLI 65
Network Management Systems Destinations 66
Adding Network Management Systems Destination 66
Appendix A: Best Practices for VMware performance and features 67
BIOS 67

Intel Virtualization Technology..... 67
Dell PowerEdge Server 68
HP ProLiant Servers..... 68
VMware Tools..... 69
Timekeeping..... 69
Configuring the NTP time..... 70
VMware networking best practices..... 71
Storage..... 75
Thin vs. thick deployments..... 75
Best Practices for VMware features..... 76
VMware Snapshots..... 76
VMware Cloning..... 78
VMware High Availability..... 78
VMware vMotion..... 78
Glossary..... 79

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® System Manager virtual application in Avaya Aura® Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, upgrading, and basic maintenance checklists and procedures.

Intended audience

The primary audience for this document is anyone who is involved with installing, configuring, upgrading, and verifying System Manager on VMware® vSphere™ 5.0, 5.1, or 5.5 Virtualized Environment. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

This document does not include optional or customized aspects of a configuration.

Document changes since last issue

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

- Added support for the deployment on VMware Release ESXi 5.5 in Virtualized Environment.
- Added the procedure for installing the System Manager Release 6.3.13 bin file.
- Added support for EULA prompt during the installation of System Manager bin file on VMware.
- Added that the system displays a message on the web console and command line interface that prompts you to restart the System Manager virtual machine after a patch installation that upgraded the kernel.

Related 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
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.	Sales engineers
Avaya Aura® System Manager Overview and Specification	Describes product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements for Avaya Aura® System Manager.	Sales engineers, Solution architects, Implementation engineers, Support personnel
Administration		
Administering Avaya Aura® System Manager	Describes the procedures to configure System Manager and the managed elements that System Manager supports.	Implementation engineers, Support personnel
Maintenance and Troubleshooting		
Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment	Describes the procedures to upgrade Avaya Aura® System Manager on VMware in Virtualized Environment.	Implementation engineers, Support personnel
Troubleshooting Avaya Aura® System Manager	Describes the procedures to troubleshoot Avaya Aura® System Manager.	Implementation engineers, Support personnel

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging 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
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory

Table continues…

Course code	Course title	Type
1A00236E	Knowledge Access: Avaya Aura® Session Manager and 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 web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

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

Note:

Videos are not available for all products.

Support

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

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

Avaya Aura® Virtualized Environment Overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture. Virtualized Environment 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.
- customers can deploy Avaya products in a virtualized environment on customer-specified servers and hardware.
- business can scale rapidly to accommodate growth and to respond to changing business requirements.

For existing customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to 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 is only for VMware and is not intended to include any other industry hypervisor. Virtualized Environment is inclusive of the Avaya Aura® portfolio.

Note:

This document uses the following terms, and at times, uses the terms interchangeably.

- server and host
- reservations and configuration values

Customer deployment

Deployment into the blade, cluster, and server is managed by vCenter Server and vSphere Client.

The customer provides the servers and the VMware infrastructure including the VMware licenses.

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.
- pre-installed VMware tools.
- preset configuration details for
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Patches and upgrades

A minimum patch level can be required for each supported application. For more information regarding 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 instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Performance and capacities

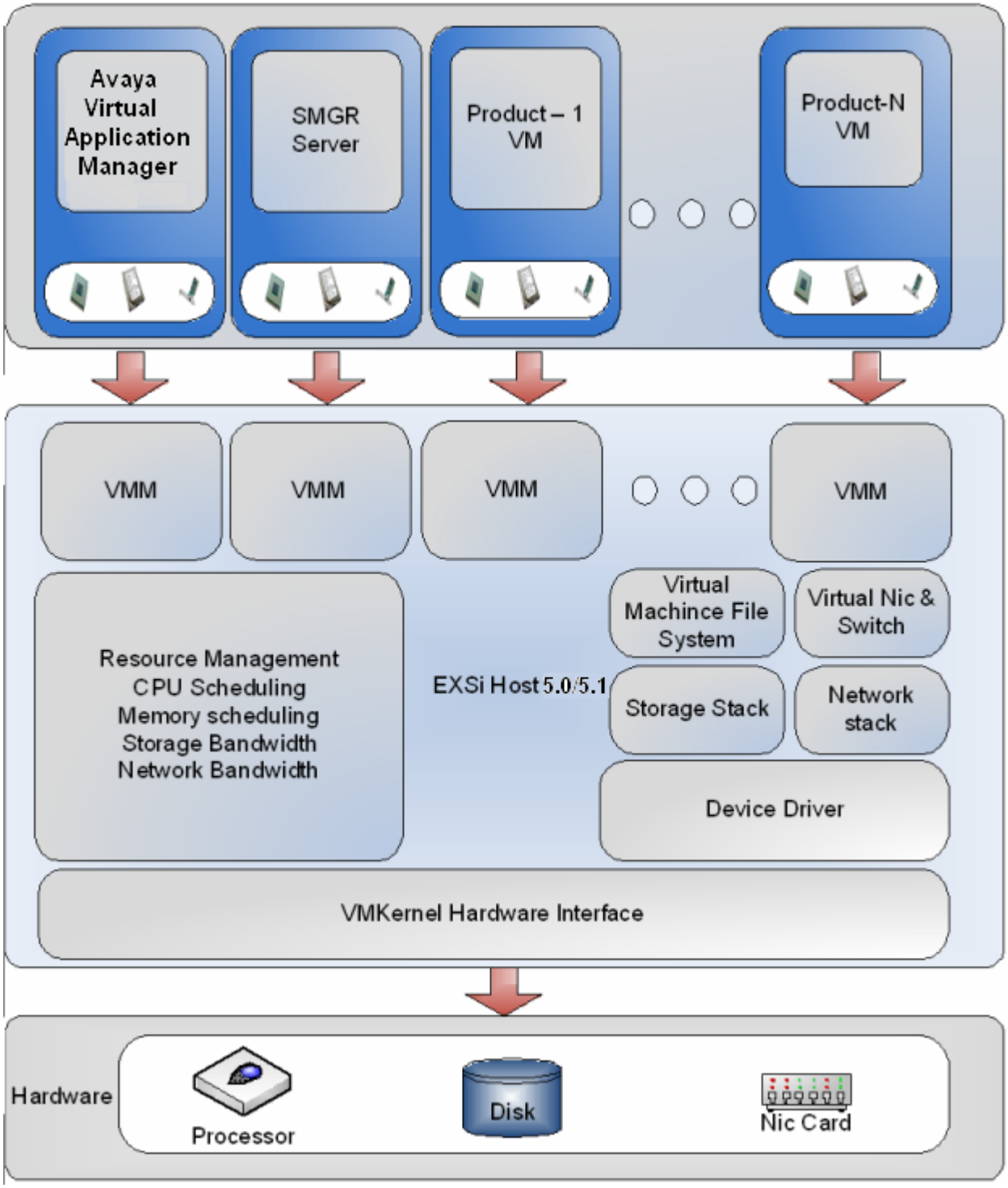
The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

Modifying these values can have a direct impact on the performance, capacity, and stability of the virtual machine. It is the responsibility of the customer to understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) may 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.

Topology

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


Avaya Virtual Application Manager
SMGR Server
Product – 1 VM
Product-N VM
VMM
VMM
VMM
VMM
Resource Management
CPU Scheduling
Memory scheduling
Storage Bandwidth
Network Bandwidth
EXSi Host 5.0/5.1
Virtual Machince File System
Virtual Nic & Switch
Storage Stack
Network stack
Device Driver
VMKernel Hardware Interface
Hardware
Processor
Disk
Nic Card

VMware components

VMware 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.
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.

OVA deployment order

Deploy the application OVA files in the following order:

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

After the application OVA files have been deployed, you can deploy Agile Communication Environment™, SAL, 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 configuration

Server hardware and resources

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

System Manager OVA includes the VMware tools. The tools are a suite of utilities that enhance the performance of the guest operating system and improve the management of the virtual machine.

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. Ensure that the license file copies are accessible.

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
Network Configuration	IP address		172.16.1.10
	Default netmask		255.255.0.0
	Default 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.

Table continues…

	Required data	Value for the system	Example Value
			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 25

System Manager virtual machine resource requirements

The Avaya Aura® System Manager virtual machine requires the following set of resources to be available on the ESXi host before deployment:

VMware resource	Minimum value
CPU core	4

Table continues…

VMware resource	Minimum value
CPU reservation	9600 MHz
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHz
Memory	9 GB
Memory reservation	9 GB
Storage reservation	72 GB
Shared NIC(s)	1

If the host does not have the minimum resources to allocate to the virtual machine, the system does not start the System Manager virtual machine.

Related Links

Adjusting the System Manager virtual machine properties on page 18

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.

VMware software requirements

The following VMware software versions are supported:

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

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

Note:

System Manager does not support ESXi releases earlier than 5.0.

Chapter 4: Installing the System Manager OVA file

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.

Methods of System Manager OVA file deployment

Deploy the System Manager OVA file by using one of the following methods:

- Using vSphere
- Using vCenter

Related Links

Deploying the System Manager OVA file using vCenter on page 30
Deploying the System Manager OVA file by using vSphere on page 22

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 `System_Manager_6.3.13_r5003336.bin` file. For more information, see the Geographic Redundancy configuration section.

Note:

If the System Manager virtual machine is already on Release 6.3 or later, install the `System_Manager_6.3.13_r5003336.bin` file to upgrade the system to Release 6.3.13.

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

#	Action	Link/Notes	✔
1	Download the `SMGR-6.3.0.8.5682-e50-68.ova` file and the `System_Manager_6.3.13_r5003336.bin` file from the Avaya Support website at http://support.avaya.com.	-	
2	Install vSphere Client 5.0, 5.1 or 5.5.	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 network configuration data is accessible.	Customer configuration data on page 16	
5	(Optional) Download the authentication file from http://rfa.avaya.com.	Downloading authentication file on page 22	
6	Install the System Manager OVA file.	Deploying the OVA file using vSphere on page 22	
7	Configure the System Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 35	
8	Start the System Manager virtual machine.	Starting SMGR on page 33	
9	Configure the network parameters by using CLI.	Configuring the network parameters from CLI on page 24	
10	Verify the installation of the System Manager virtual machine.	Verifying the deployment of SMGR on page 34	
11	(Optional) Install the authentication file on System Manager.	Installing the authentication file on System Manager on page 27	
12	Install the `System_Manager_6.3.13_r5003336.bin` file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 6.3.13 bin file on page 28	

Table continues…

#	Action	Link/Notes	✔
13	From the **About** link in the settings icon (), verify that the System Manager version is Release 6.3.13.	-	
14	(Optional) Reconfigure the hardware resources for flexible footprint.	Reconfiguring hardware resources for flexible footprint on page 37	

Downloading the authentication file

Procedure

1. To gain access to the Avaya RFA Home page, enter 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 `SP System Platform/VE VMware`.
6. In the **Release** field, click `6.x`.
7. Click **Next**.
8. Click **New System - Product: SP System Platform Release: 6.x**.
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.

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 Host page, select the required data store and then click **Next**.
11. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
12. 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 from the list.

    For example, click VM Network 2.
13. Click **Next**.
14. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.
15. To start the System Manager virtual machine, 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 CLI.

  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.
- Install the `System_Manager_6.3.13_r5003336.bin` file.

Related Links

Configuring the network parameters from the vSphere console on page 24
Installing the System Manager Release 6.3.13 bin file on page 28
Verifying the installation of System Manager on page 34

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.
- To reach the System Manager CLI, open vSphere Client and click the **Console** tab or the  icon.

About this task

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

Procedure

1. At the prompt, enter the following network parameters:
   - **IP**. The IP address of the System Manager virtual machine.
   - **Netmask**. The subnetwork mask of the System Manager virtual machine.
   - **Short Hostname**. The host name of the System Manager virtual machine. For example, smgrdev.

     Note:

     System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
   - **Domain name**. The domain name of the System Manager virtual machine. For example, platform.mydomain.com.
   - **Default Gateway**. The IP address of the System Manager virtual machine gateway For example, 172.16.1.1.
   - **DNS IP**. Enter one of the following:
     - DNS IP address of the primary System Manager virtual machine. For example, 172.16.1.2.
     - DNS IP addresses of primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
   - **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 with commas (,).
   - **Time Zone**. From the lists that the system displays, select the name of the continent and the name of the country.
2. Enter the following SNMPv3 parameters:
   - **User Name Prefix**

- **Authentication Protocol Password**
- **Privacy Protocol Password**

3. Enter the following details:
   - Virtual FQDN 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 the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.
4. 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.
5. 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.
6. 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

Backup Definition parameters on page 25

Backup Definition parameters

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

Note:

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

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

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

Name	Description
Schedule Backup?	• Yes: To schedule the backup jobs during the System Manager installation. • No: To schedule the backup jobs later. **Note:** If you select No, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through CLI.
Backup Server Login Password	The password to log in to the backup server through CLI.
Re-Type Backup Server Login Password	The password that you re-enter to log in to the backup server through CLI.
Backup Directory Location	The location on the remote backup server.
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.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.

Table continues…

Name	Description
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 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.

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 CLI, 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

Downloading the authentication file on page 22

Installing the System Manager Release 6.3.13 bin file

Before you begin

- Ensure that System Manager is running on Release 6.3.
- To reach the System Manager CLI, 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_6.3.13_r5003336.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 6.3.13 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

Verifying the installation of System Manager on page 34
Starting the System Manager virtual machine on page 33

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 `System_Manager_6.3.13_r5003336.bin` file. For more information, see the Geographic Redundancy configuration section.

If the System Manager virtual machine is already on Release 6.3 or later, install the `System_Manager_6.3.13_r5003336.bin` file to upgrade the system to Release 6.3.13.

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

#	Action	Link/Notes	✔
1	Download the `SMGR-6.3.0.8.5682-e50-68.ova` file and the `System_Manager_6.3.13_r5003336.bin` file 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.	

Table continues…

#	Action	Link/Notes	✔
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 network configuration data is accessible.	Customer configuration data on page 16	
5	(Optional) Download the authentication file from http://rfa.avaya.com.	Downloading authentication file on page 22	
6	Install the `SMGR-6.3.0.8.5682-e50-68.ova` file and provide network parameters for System Manager.	Deploying the OVA file using vCenter on page 30	
7	Configure the System Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 35	
8	Start the System Manager virtual machine.	Starting System Manager on page 33	
9	Verify the installation of the System Manager virtual machine.	Verifying the deployment of System Manager on page 34	
10	(Optional) Install the authentication file on System Manager.	Installing the authentication file on System Manager on page 27	
11	Install the `System_Manager_6.3.13_r5003336.bin` file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 6.3.13 bin file on page 28	
12	From the **About** link in the settings icon (), verify that the System Manager version is Release 6.3.13.		
13	(Optional) Reconfigure the hardware resources for flexible footprint.	Reconfiguring hardware resources for flexible footprint on page 37	

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. In the **Inventory Location** area, select the datacenter and click **Next**.
10. If the cluster exists, select the cluster and click **Next**.
11. Select the specific host within the cluster and click **Next**.
12. On the Storage page, select the required data store and 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 from the list.

    For example, click VM Network 2.
15. On the Properties page:
    a. Configure the following network parameters:
       - **IP**. The IP address of the System Manager virtual machine.
       - **Netmask**. The Subnet mask of the System Manager virtual machine.
       - **Default Gateway**. The IP address of your default gateway.
       - **DNS IP**. The IP address of your DNS server. Separate IP addresses with commas (,).
       - **Short Hostname**. The hostname of the System Manager virtual machine. For example, smgrdev.

         Note:

         System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
       - **Domain Name**. The domain name of the System Manager virtual machine. For example, platform.mydomain.com.
       - **Default Search List**. The search list of domain names. Separate IP addresses with commas (,).

- **NTP Server IP or FQDN**. The IP address or FQDN of the NTP server. Separate IP addresses or FQDNs with commas (,).
- **Time Zone**. The time zone. Select a time zone from the list.
- **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 the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

b. Configure the following SNMPv3 parameters:

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

c. **(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.

16. Click **Next**.
17. 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.

18. To start the System Manager virtual machine, 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.
19. Click the **Console** tab and verify that the system startup is successful.

Next steps

- Verify the deployment of the System Manager OVA file.
- Install the `System_Manager_6.3.13_r5003336.bin` file.

Related Links

Installing the System Manager Release 6.3.13 bin file on page 28
Verifying the installation of System Manager on page 34
Backup Definition parameters on page 25

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.

Chapter 5: Postinstallation 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

You must perform the following verification procedure after you install System Manager Release 6.3.13 and configure System Manager.

Before you begin

Log on to the System Manager web console by using admin credentials.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`.

   The system must display the System Manager web console.

2. On the upper-right corner, click  and **About**.

   The system displays the About SMGR window with the build details.

3. Verify the version number of System Manager.

Chapter 6: Configuration

Configuring the virtual machine automatic startup settings

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

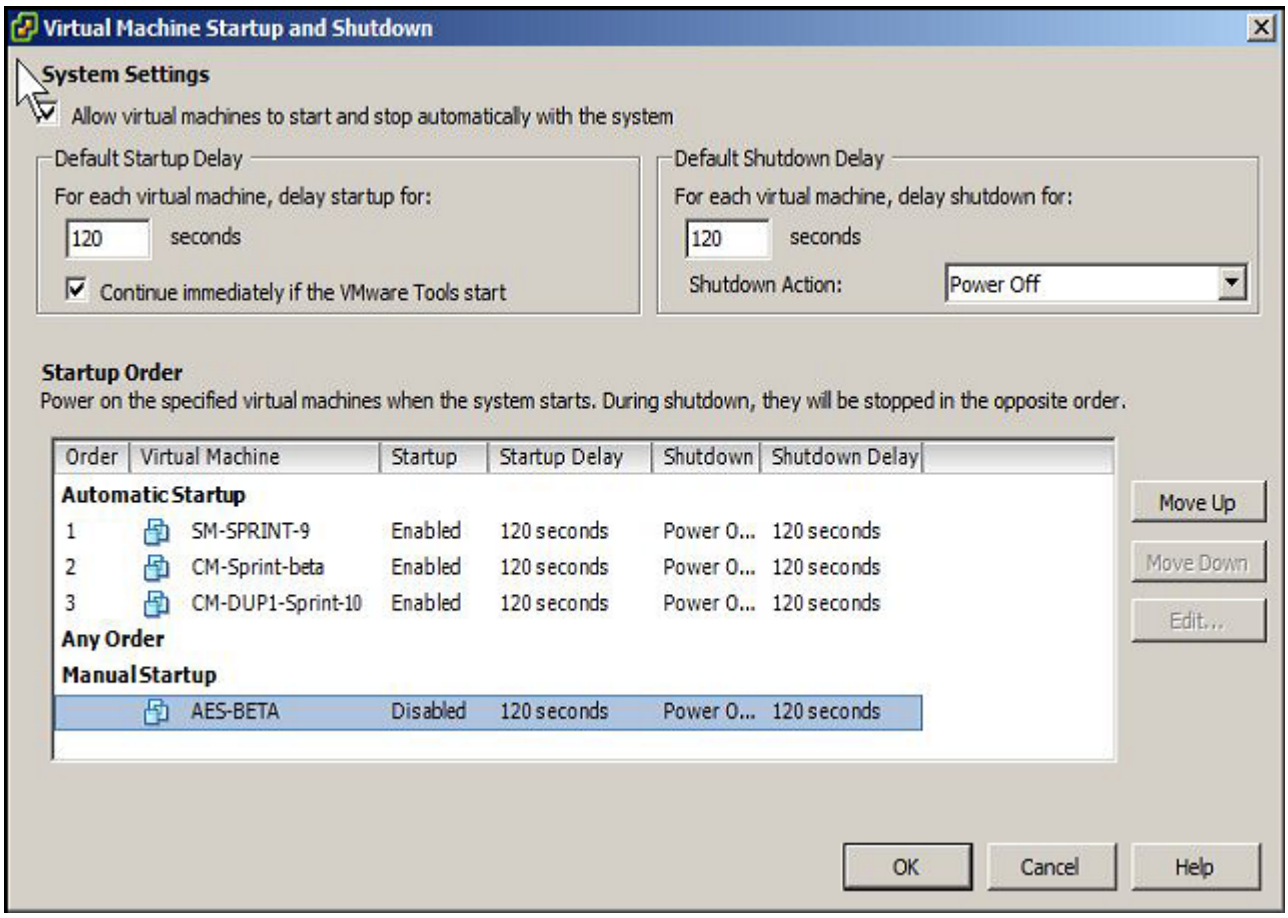
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

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

A Secure Access Link (SAL) Gateway is required 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 the SAL Gateway OVA using vCenter through a vSphere client. You can also deploy the SAL Gateway OVA directly to the ESXi server through a vSphere client.

For more information about the 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 Environment applications provide a fixed profile based on maximum capacity requirements. However, many customers require only a fraction of the maximum capacity.

Certain applications in the Virtualized Environment solution 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 38

Reconfiguring hardware resources for flexible footprint

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

Before you begin

Install the System Manager Release 6.3.13 patch.

Procedure

1. Connect to the host or cluster by using the VMware vSphere client.
2. Log in 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

Installing the System Manager Release 6.3.13 bin file on page 28
System Manager Virtualized Environment footprint hardware resource matrix on page 38
Capability and scalability specification on page 38

System Manager Virtualized Environment footprint hardware resource matrix

The following table describes the resource requirements to support the different profiles for System Manager.

Footprint	# of CPUs	RAM in GB/MB	Maximum # of users
Profile 1	4 (9600 MHz)	9 / 9216	> 35K to 250K
Profile 2	3 (7200 MHz)	7 / 7168	Up to 35K

Capability and scalability specification

The following table contains the values of the profiles supported for the System Manager Virtualized Environment flexible footprint.

Parameters/Profile	Profile 2 footprint	Profile 1 footprint
Number of administrator logins	35	250
Number of simultaneous logins	10	50
Number of endpoints (all types)	35000	250,000
Number of SIP endpoints	35000	125,000
Number of end users	35000	250,000
Number of messaging mailboxes	35000	250,000
Number of contacts per user	250	250
Number of public contacts	1000	1000
Number of personal contact lists, per user	1	1
Number of members in a personal contact list	250	250
Number of groups	100	300
Number of members in a group	400	400
Number of elements	3500	25,000
Number of Communication Managers	10 CM/35K Users	500/250K Users
Number of Session Managers	10 SM/35K Users	12/250K Users
Number of Branch Session Managers	35 BSM/35K Users	250/250K Users
Number of IP Office	280/35K Users	2000/250K Users
Collaboration Environment (CE)	10/35K Users	10/35K Users
Number of Conferencing	1/35K Users	1/250K Users
Messaging	1/35K Users	1/250K WebLMUsers
Presence Services	4/35K Users	32/250K Users
MMCS	1/35K Users	1/250K Users
CS 1000	1/35K Users	1/250K Users
Number of roles	100	200
Number of roles, per user	20	20
Number of licensing clients	3500	3500
Number of Local WebLMs per Master WebLM	20	20
Number of trust management clients	2,500	2,500
Number of Active Alarms	75000	75000
Number of Cleared Alarms	75000	75000
Number of SAL Agents	45	250
Number of Logs	300,000	500,000
Number of Replica Nodes in Data Replication Service	45	250
Number of Scheduler Jobs	3000	5000
Number of total/concurrent Scheduler Jobs	100/60	250/90

Table continues…

Number of concurrent DRS clients	10	25
Concurrent Communication Manager Sync	10	30

Geographic Redundancy configuration

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 System Platform environment. For example, the primary System Manager on 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 be able to 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.

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 Geographical 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 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:

      As 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 steps:
     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 steps:
     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 50
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 40

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.

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:

   As 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 45
Geographic Redundancy field descriptions on page 50

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 44
Geographic Redundancy field descriptions on page 50

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:

As 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 47
Geographic Redundancy field descriptions on page 50

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 46
Geographic Redundancy field descriptions on page 50

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

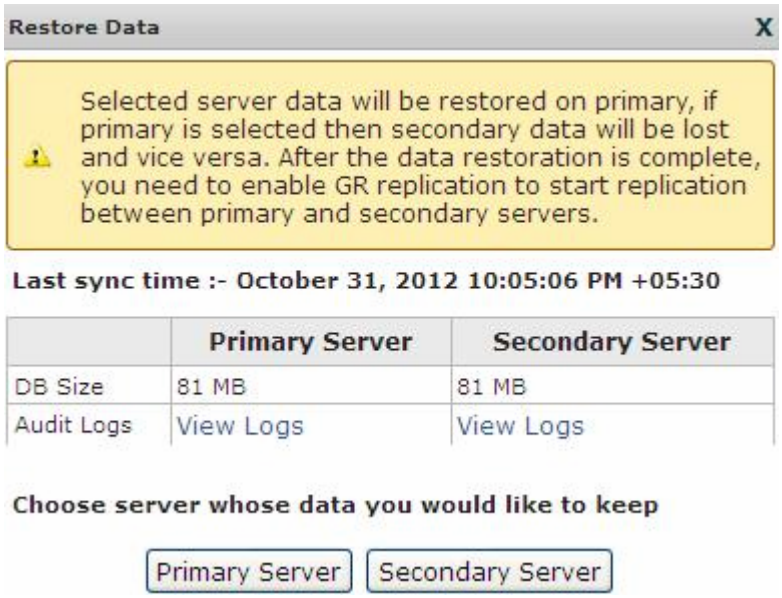
1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:
   - **Primary Server**

     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.
      - As 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 44
Deactivating the secondary System Manager server on page 47
Geographic Redundancy field descriptions on page 50

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 Geographical Redundancy on page 42
Enabling the Geographic Redundancy replication on page 44
Geographic Redundancy field descriptions on page 50

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 7: Maintenance

Backup and restore System Manager data

Creating a data backup on a remote 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 **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 58

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 58

Restoring a backup from a remote server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 **Remote**.
4. In the **Parameterized Restore** tab, perform one of the following:
   - Provide the name of the file that you must restore, the file transfer protocol, the remote server IP, 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.
   - 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. In the Backup List, view the list of the remote backups that are created by using the SFTP and SCP protocols.

   If the location of a backup file is modified, in the **Parameterized Restore** tab, specify the correct location of the backup file in the **File Name** field. You can select only one file at a time.

6. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

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

7. Click **Continue**.

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

Result

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

Related Links

Backup and Restore field descriptions on page 58

Restoring data backup from a local server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 complete path of the file 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 58

Backup and Restore field descriptions

Use this page to view the details of backup files or the files you require to restore.

Name	Description
Operation	Specifies the type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, specifies the name of the backup file. • For the restore operation, specifies the name of the file you want to restore.

Table continues…

Name	Description
Path	• For the backup operation, specifies the path of the backup file. • For the restore operation, specifies the path of the file you want to restore.
Status	Indicates the status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	Displays the error details of the backup or restore operation that has failed.
Operation Time	Specifies the time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	Displays the user who performed the operation.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Installing the System Manager service pack or patch from CLI

Before you begin

- To reach the System Manager CLI, 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

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

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

Related Links

System Manager command line interface operations on page 62

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

Before you begin

- To reach the System Manager CLI, 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.

About this task

Important:

- After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.
- Do not change the network settings from vSphere Client when the virtual machine is in the power off mode.
- The FQDN value must be unique and different from the virtual FQDN value of System Manager.

Procedure

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.

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 61
System Manager command line interface operations on page 62

changeIPFQDN command

Use the **changeIPFQDN** command to change the IP address, FQDN, DNS address, Gateway, Netmask address for System Manager, and the search list for the DNS address.

Syntax

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

#	Option	Description	Usage
1	IP	The new IP address of System Manager.	**changeIPFQDN -IP 10.11.12.13**
2	FQDN	The new FQDN of System Manager.	**changeIPFQDN -FQDN a.mydomain.smgr.com**
3	GATEWAY	The new Gateway address of System Manager.	**changeIPFQDN -GATEWAY 10.11.1.1**
4	NETMASK	The new netmask address of System Manager.	**changeIPFQDN -NETMASK 255.255.203.0**
5	DNS	The new 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
```

Configuring the NTP server

Before you begin

- To reach the System Manager CLI, 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 62

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 62

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	**changeIPFQDN**	• **-IP <new IP address for System Manager>** • **-FQDN <new fully qualified domain name for System Manager>** • **-GATEWAY <new Gateway address for System Manager>**	Updates the existing 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**

Table continues…

#	Command	Parameters	Description	Usage
		• **-NETMASK <new netmask address for System Manage>** • **-DNS <new DNS address for System Manager>** • **-SEARCH <new search list for DNS address>**		**for System Manager> -SEARCH <new search list for DNS address>**
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**
5	**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 (,).

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 64
Generating the test alarm from CLI on page 65

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 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 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*.

Adding Network Management Systems Destination

You can add an NMS destination using 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 Chapter “Managing Serviceability Agents” in *Administering Avaya Aura® System Manager guide*.

Appendix A: 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.

- 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.

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.

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

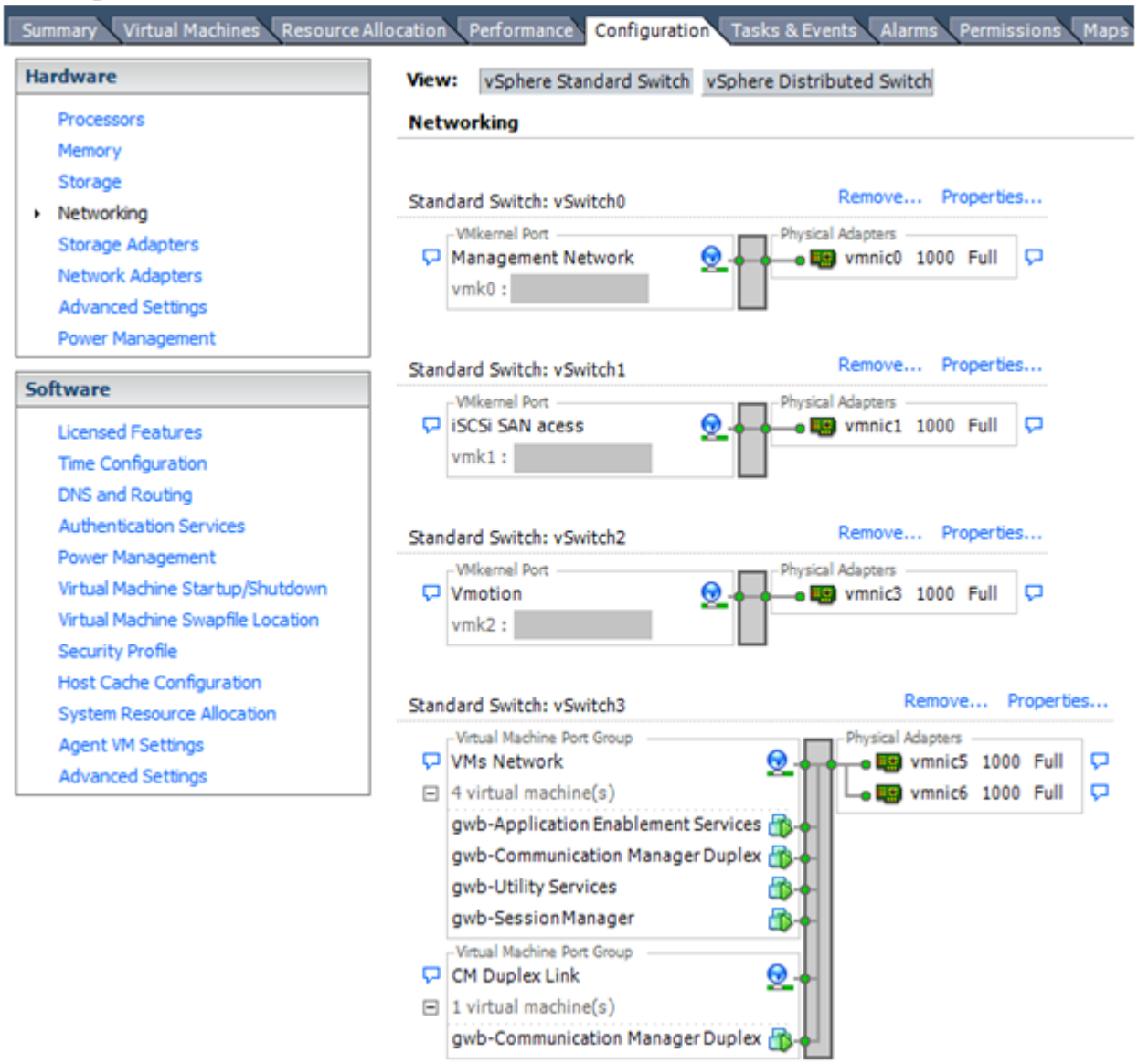
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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 VMkernal 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:

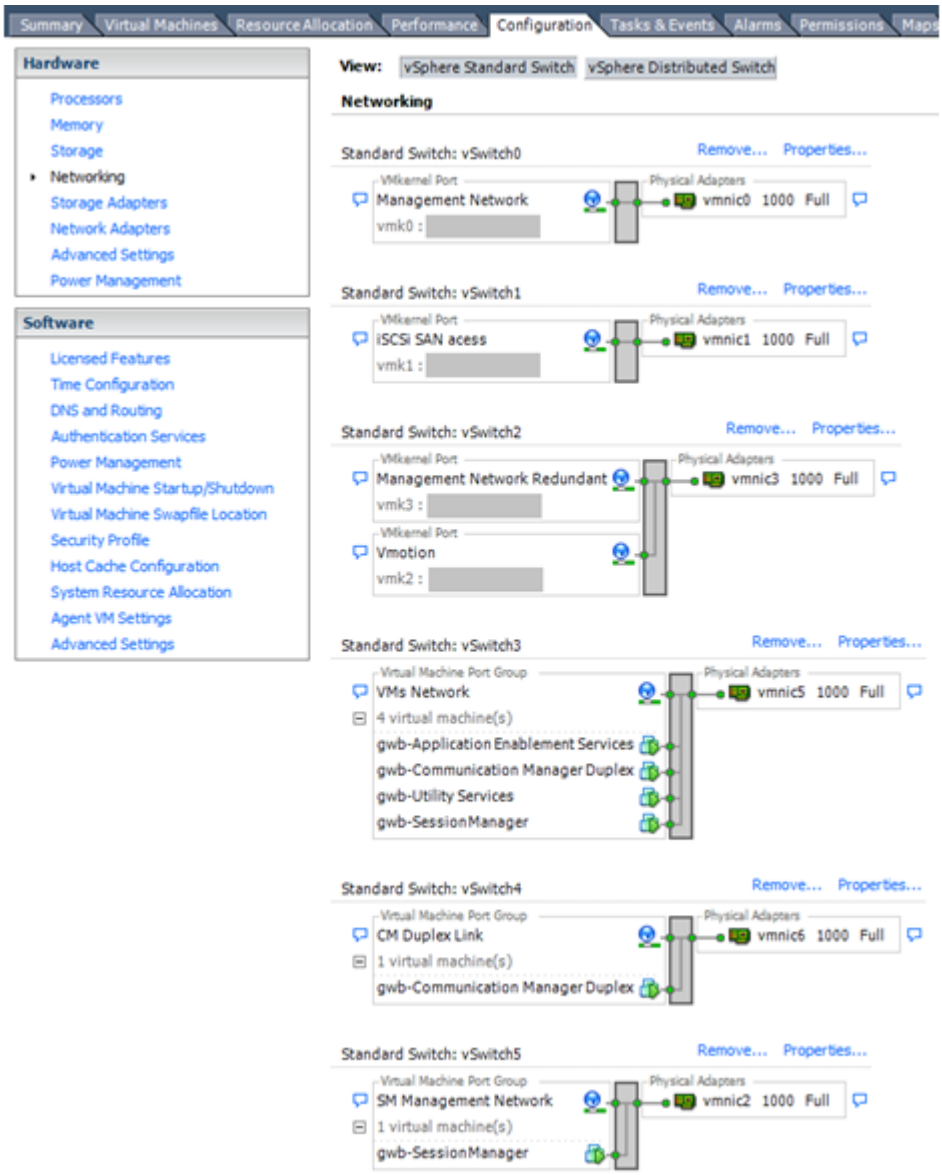
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides 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™ 5.0	Performance Best Practices for VMware vSphere™ 5.0
Performance Best Practices for VMware vSphere™ 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
VMware vSphere 5.0 Basics	VMware vSphere Basics - ESXi 5.0
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-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 all of 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 all of the space. 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 of the 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 off of 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, a warning is displayed in the UI.

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.
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

A

activate
secondary server 46
add NMS destination 66
adjust System Manager VM properties 18
AFS file 22
authentication file 22
install 27
automatic restart
virtual machine 35
Avaya Aura products
license file 16

B

backup
remote server 55
Backup and Restore page 58
Backup Definition parameters 25
best practices
performance and features 67
VMware networking 71
BIOS 67
BIOS for HP servers 68
BIOS settings
for Dell servers 68

C

capability and scalability specification 38
change
DNS 60, 62
FQDN 60
FQDN from CLI 62
Gateway 60, 62
IP address 60
IP address from CLI 62
Netmask 60, 62
search list 60, 62
change FQDN from CLI 62
change IP address from CLI 62
changeIPFQDN command, ... 61
checklist
deployment procedures 20, 29
clones
deployment 20
Cloning 78
command
changeIPFQDN 61
configureTimeZone 62
updateASG 27
components 14
VMware 14
configuration data
customer 16
configuration tools and utilities 16
configure 70
backup definition 25
Geographical Redundancy 42
configure network parameters from CLI 24
configureNTP 62
configureTimeZone 62
configuring
virtual machine automatic restart 35
configuring NTP server 62
configuring time zone 62
convert
to stand-alone 50
courses 8
creating data backup on remote server 55
creating system data backup on a local server 56
customer configuration data 16

D

data
Backup Definition Parameters 16
network configuration 16
SNMP parameters 16
VFQDN 16
data backup
create 56
remote server 55
data backup from local server 57
deactivate
secondary server 47
deploying copies 20
deploying System Manager OVA file 22
deployment
thick 75
thin 75
deployment guidelines 14
Deployment order of OVA file 14
deployment procedures
checklist 20, 29
deploy ova file 20
deploy System Manager OVA file using vCenter 30
disabling
Geo Redundancy replication 45
download authentication file 22

E

enabling
Geographic Redundancy replication 44

F

features best practices 67
flexible footprint 37
configuring hardware resources 37
footprint flexibility 37
footprint hardware matrix 38
FQDN 60
changeIPFQDN 61

G

generate test alarm 65
generate test alarms 64
generating test alarms 64
Geographical Redundancy 42
Geographic Redundancy 40, 47, 50, 52
disable 45
enable 44
Geographic Redundancy field descriptions 50
Geographic Redundancy key tasks 41
Geo Redundancy 46
GR Health field descriptions 52
guidelines
deployment 14

H

HA 78
hardware and software prerequisites on the primary and secondary servers 40
hardware resources
configuring for flexible footprint 37
High Availability 78

I

install
patch from CLI 62
service pack from CLI 62
System Manager patch 28
System Manager service pack from CLI 59
install authentication file 27
install new license files 34
install patch from CLI 62
install service pack from CLI 62
install System Manager OVA file using vCenter 30
Intel Virtualization Technology 67
IP address 60

K

key tasks
Geographic Redundancy 41

L

license file
Avaya Aura products 16
load matrix 38

N

network management systems destination 66
Network Management Systems Destinations 66
network parameters 24
new license file 34
NMS destination; add 66
NMS destinations 66
NTP server
configure 62
NTP time 70
NTP time source 69

O

OVA deployment order 14
ova file 20
OVA file
deploy 22, 30
overview 11

P

parameters
backup definition 25
patch file
install 28
performance best practices 67
perform the System Manager tests 34
postinstall
steps 34
power on System Manager VM 33
prerequisites 40, 41

R

related documentation 8
requirements
virtual machine resources 17
resource requirements 17
resources
server 16
restore
primary System Manager 47
restoring a backup from a remote server 56
restoring a system backup from a local server 57
restoring backup; remote server 56
restoring data backup 57

S

SAL Gateway 36
secondary server 46, 47
server hardware and resources 16
snapshots 76
SNMP traps 66
specification
    capability and scalability 38
stand-alone 50
start System Manager VM 33
storage 75
support 10
System Manager
    topology 12
System Manager bin file 28
System Manager installation
    verify 34
System Manager patch 28
System Manager restore 47
System Manager service pack 59

T

test alarm from CLI
    generate 65
test alarms from web console
    generate 64
thick deployment 75
thin deployment 75
timekeeping 69
time zone
    configure 62
tools and utilities 16
topology 12
training 8

U

unconfigure
    Geographic Redundancy 50
updateASG 27, 62
upgrade
    System Manager 62

V

verify
    System Manager installation 34
videos 9
virtual machine 22, 30
    automatic restart configuration 35
virtual machine resource requirements 17
vMotion 78
VM properties
    adjust 18
VMware Cloning 78
VMware High Availability 78
VMware networking
    best practices 71
VMware server in Geographic Redundancy setup 40
VMware software requirements 19
VMware Tools 69
VT support 67

W

warranty 10