



Deploying Avaya Aura[®] Session Manager using VMware[®] in the Virtualized Environment

Release 6.3
Issue 6
November 2014

© 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](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.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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.

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.

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.

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

Avaya® and Avaya Aura® are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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	9
Viewing Avaya Mentor videos	10
Support	11
Warranty	11
Chapter 2: Architecture overview	12
Avaya Aura® Virtualized Environment Overview	12
Avaya Collaboration Pod for Enterprise Communications	13
VMware components	14
VMware software requirements	14
Server hardware and resources	15
Chapter 3: Planning and configuration	16
Planning checklist	16
Capacity limits	17
Alternative H.323 Endpoint administration considerations and impacts	18
Customer configuration data	19
SAL Gateway	20
Chapter 4: Deploying the Session Manager OVA	21
Deployment guidelines	21
Deployment of cloned and copied OVAs	21
Session Manager Deployment checklist	22
Verifying configuration for deployment	23
Methods for deploying the Session Manager OVA	23
Deploying using vSphere Client connected to vCenter	23
Deploying using vSphere Client connected directly to VMware host	24
Reconfiguring hardware resources for flexible footprint	26
Configuring the virtual machine automatic startup settings	27
Configuring Session Manager	28
Chapter 5: Post-installation verification	30
Post-installation checklist	30
Using the hardware_info command	30
Verifying the Session Manager as a VMware instance	31
Verifying the connections	31
Chapter 6: Upgrading Session Manager on VMware	32

Upgrade checklist.....	32
Verifying the Enrollment Password status.....	34
Upgrading the operating system.....	34
Upgrading Session Manager using a DVD.....	35
Using Network transfer.....	36
Upgrading Session Manager VMware Tools.....	36
Authentication files for Session Manager.....	37
Creating an authentication file for a Session Manager.....	38
Installing an authentication file.....	39
Chapter 7: Migrating Session Manager	40
Migration checklist.....	40
Using the GUI to shut down or reboot the server.....	41
Using the CLI to shut down or reboot the server.....	42
Chapter 8: Maintenance and administration procedures.....	43
Adding Session Manager as a SIP entity.....	43
Accepting new service.....	43
Denying new service.....	44
Creating a snapshot.....	44
Deleting a snapshot.....	45
Restoring a snapshot.....	46
Downloading software from PLDS.....	46
Powering On Session Manager	47
Troubleshooting a Session Manager virtual machine that is unable to power on.....	48
Running maintenance tests.....	48
Session Manager Service Pack and patch updates.....	49
Session Manager Backup and Restore.....	49
Accessing the Backup and Restore service.....	49
Backup and Restore field descriptions.....	50
Verifying the Active Call Count.....	51
Verifying data replication.....	51
Troubleshooting Data Replication.....	51
Viewing Security Module status.....	52
Troubleshooting Security Module Sanity failure.....	52
Viewing the Session Manager Entity Link Connection Status.....	53
Viewing the SIP Monitoring Status Summary page.....	53
Appendix A: Best Practices for VMware performance and features.....	54
BIOS.....	54
Intel Virtualization Technology.....	54
Dell PowerEdge Server	55
HP ProLiant Servers.....	55
Timekeeping.....	56
VMware Tools.....	57
VMware networking best practices.....	57

Separating Session Manager management and Security Module traffic.....	61
Storage.....	62
Thin vs. thick deployments.....	62
Best Practices for VMware features.....	63
VMware High Availability.....	63
VMware vMotion.....	63
VMware Snapshots.....	64
Appendix B: Product notifications.....	66
Viewing PCNs and PSNs.....	66
Registering for product notifications.....	67
Glossary.....	68

Chapter 1: Introduction

Purpose

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

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

Intended audience

The primary audience for this document is anyone who installs, configures, and upgrades Session Manager on VMware® in an Avaya Aura® Virtualized Environment.

The audience includes and is not limited to:

- Implementation Engineers
- Field Technicians
- Business Partners
- Solution Providers
- Customers

Document changes since last issue

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

- Added information regarding the alternative method for administering H.323 endpoints.
- Added authentication file information and procedures.
- Updated checklists.

Related resources

Documentation

The following documents are available at <http://support.avaya.com>.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
<i>Avaya Aura® Session Manager Overview and Specification</i>	Describes the key features of Session Manager.	IT management System administrators
<i>Avaya Aura® Virtualized Environment Solution Description</i>	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
<i>Avaya Aura® Session Manager Security Design</i>	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
<i>Avaya Aura® Session Manager 6.3.x Release Notes</i>	Contains enhancements, fixes, and workarounds for the various Session Manager 6.3 releases.	System administrators Services and support personnel
Implementation		
<i>Deploying Avaya Aura® Session Manager</i>	Describes how to install and configure a Session Manager instance.	Services and support personnel
<i>Deploying Avaya Aura® Branch Session Manager</i>	Describes how to install and configure Branch Session Manager.	Services and support personnel
<i>Deploying Avaya Aura® Communication Manager on System Platform</i>	Describes how to install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment</i>	Describes how to deploy the Session Manager virtual application in a VMware environment.	Services and support personnel
Administration		
<i>Administering Avaya Aura® Session Manager</i>	Describes the procedures to administer Session Manager using System Manager.	System administrators
<i>Administering Avaya Aura® Communication Manager Server Options</i>	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides	System administrators

Title	Description	Audience
	information related to Session Manager administration.	
<i>Avaya Aura® Session Manager Case Studies</i>	Provides common administration scenarios.	System administrators
Installation and upgrades		
<i>Installing Service Packs for Avaya Aura® Session Manager</i>	Describes the procedures to install service packs on Session Manager.	Services and support personnel
<i>Installing Patches for Avaya Aura® Session Manager</i>	Describes the procedures to install patches on Session Manager.	Services and support personnel
<i>Installing the Avaya S8800 Server for Avaya Aura® Communication Manager</i>	Describes the installation procedures for the S8800 Server.	Services and support personnel
<i>Installing the Avaya S8510 Server Family and Its Components</i>	Describes the installation procedures for the S8510 Server.	Services and support personnel
<i>Installing the Dell™ PowerEdge™ R610 Server</i>	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
<i>Installing the Dell™ PowerEdge™ R620 Server</i>	Describes the installation procedures for the Dell™ PowerEdge™ R620server.	Services and support personnel
<i>Installing the HP ProLiant DL360 G7 Server</i>	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
<i>Installing the HP ProLiant DL380p G8 Server</i>	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
<i>Upgrading Avaya Aura® Session Manager</i>	Describes the procedures to upgrade a Session Manager to the latest software release.	Services and support personnel
Maintaining		
<i>Maintaining and Troubleshooting Avaya Aura® Session Manager</i>	Describes the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Training

The following courses are available on <https://www.avaya-learning.com>. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support

Course code	Course title
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Avaya Aura® Session Manager 6.2 Delta Overview
5U00104W	Avaya Aura® Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Avaya Aura® Session Manager General Overview
ATC00175OEN	Avaya Aura® Session Manager Rack and Stack
ATU00170OEN	Avaya Aura® Session Manager Technical Overview
ATC01840OEN	Survivable Remote Avaya Aura® Session Manager Administration
3U00100O	Designing Avaya Aura 6.2 Part 1
3U00101O	Designing Avaya Aura 6.2 Part 2

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the Search Channel to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 Note:

Videos are not available for all products.

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 Session Manager. For more information about the terms of the limited warranty, see the sales agreement or other applicable documentation . In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at <https://support.avaya.com> under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

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.

Avaya Collaboration Pod for Enterprise Communications

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

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

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

Documentation

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

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

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.

VMware software requirements

The Avaya Aura® Virtualized Environment supports the following VMware software versions:

- 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 Matrices* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

 Note:

ESXi 4.1 is not supported.

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>.

Chapter 3: Planning and configuration

Planning checklist

Complete the following actions before deploying the virtual appliance.

#	Action	Notes	✓
1	Assess and verify the vSphere infrastructure resource requirements with the customer. The key factors are: <ul style="list-style-type: none">• CPU Utilization• Memory Usage• Storage Requirements• Network Utilization• Supported capacity	Capacity limits on page 17.	
2	If you are deploying the Session Manager OVA using vCenter, enter the required information in the Customer Configuration Data worksheet.	Customer configuration data on page 19.	
3	Verify the customer has all of the required hardware at the customer site.		
4	Licenses: <ol style="list-style-type: none">1. Verify the customer has all of the required licenses.2. 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.3. Verify that the licenses are accessible.		
5	Verify you have the necessary resources for the SAL Gateway.	SAL Gateway on page 20.	
6	Plan staging and verification activities, and assign resources to those activities.		

Capacity limits

Session Manager Device Footprints	Up to 1K Devices	2.4K Devices	3.5K Devices	4.5K Devices	7K Devices	10K Devices	21.5K Devices
vCPUs	2	3	4	5	8	12	20
Minimum vCPU Resources	4,600 MHz (2 x 2300 MHz)	6,900 MHz (3 x 2300 MHz)	9,200 MHz (4 x 2300 MHz)	11,500 MHz (5 x 2300 MHz)	18,400 MHz (8 x 2300 MHz)	27,600 MHz (12 x 2300 MHz)	46,000 MHz (20 x 2300 MHz)
Memory	4 GB	5 GB	6 GB	7 GB	10 GB	12 GB	20 GB
Storage Reservation	150 GB						
Operating System	RHEL 6.2 – reusing Session Manager kick start, 64-bit						
Shared NICs	Four virtual NICs @ 1000 Mbps, used for: <ul style="list-style-type: none"> • Management (eth0) • Services port (eth1) • ASSET (eth2) • NIC bonding (eth3) 						
SIP Devices (Normal/Failure)	1K/1.2K	2.4K/3K	3.5K/4K	4.5K/5K	7K/8K	10K/12K	21.5K/ 25K
	NOTE: Assigning a SIP profile to an H.323 endpoint reduces the total SIP capacity by that many endpoints. See Alternative H.323 Endpoint administration considerations and impacts on page 18.						
CC Agents (Normal/Failure)	833/1K	2K/2.5K	2.9K/3333	3.75K/ 4166	5.8K/6666	8333/10K	18K/21K
Presence Users (Normal/Failure)	1K/1.2K	2.4K/3K	3.5K/4K	4.5K/5K	7K/8K	10K/12K	18K/21K
Sessions (Sec/ Hour/Max)	10/36K/ 15K	24/86K/ 22.5K	35/126K/3 0K	45/162K/ 37.5K	70/256K/6 0K	100/ 360K/ 90K	150/ 540K/ 160K
Database Capacities	Supported database capacities for users, routing data, and so on are described in the <i>Avaya Aura® Session Manager Overview and Specification</i> document. Note that the capacities are based on large scale solutions of 100K users or more. Smaller footprint Session Managers are not intended for use in large scale solutions and the database capacities are scaled accordingly.						

Session Manager capacities and the associated resources are determined with the assumption that hyperthreading is active. The vCPUs are based on the number of available logical processors of a virtual host. The minimum MHz resources do not necessarily reflect the actual available MHz of the host, and a Session Manager deployment is not required to reserve the minimum MHz since hyperthreading is active. A recommendation is to reserve at least half of the minimum MHz resources to guarantee that the Session Manager has the necessary resources to achieve the

stated capacities. Another recommendation is to reserve all the stated memory to guarantee the associated capacities. Resource reservations are not necessary if the host resources are known (guaranteed) to never be oversubscribed. Oversubscribing resources of a virtual host can cause Session Manager call failures and/or prevent achieving the stated capacities.

Session Managers operate as redundant, homogeneous servers to provide high reliability if a Session Manager failure or a network component failure occurs. Each Session Manager has similar system resources and a balanced number of devices. The Session Managers must be similarly sized in both processing power and available memory.

Do not couple a smaller VMware Session Manager with a larger Session Manager. The smaller VMware-based offerings are a migration path for customers. Customer can increase the number of Session Managers or the Session Manager footprint as the number of supported devices increase.

You can implement a system that consists of a mixture of Session Managers hosted on *VMware* platforms as well as Session Managers hosted on the existing *non-VMware* platforms. Session Managers running under *VMware* and the *non-VMware* Session Managers can successfully interoperate with System Managers running on both System Platform and VMware.

 Note:

You must configure the VMware-based Session Managers to be similar to the non-VMware-based Session Managers across the enterprise. Similar configurations ensure the best use of system resources and handling failover scenarios.

 Caution:

Be careful when configuring the system where a large *non-VMware* Session Manager can failover to a Session Manager running in a *VMware* environment. You must ensure that the target Session Manager can handle the total capacities.

Alternative H.323 Endpoint administration considerations and impacts

The current method for administering H.323 endpoints is to use either of the following:

- System Manager to create an H.323 endpoint without a SIP profile.
- The Communication Manager SAT.

You must configure Session Manager to route calls to the correct Communication Manager.

Alternative method for administering H.323 endpoints

An alternative method for administering H.323 endpoints is to use System Manager to create a SIP profile for an H.323 endpoint. URE routing will automatically route calls to the correct Communication Manager.

The alternative method:

- Simplifies Session Manager routing configuration.
- Provides Dual Registration (H.323 and SIP endpoints on the same extension) with no further System Manager configuration.

- Provides an easy migration to a SIP endpoint by changing the endpoint type and removing the H.323 station.

Use Case

A customer has H.323 endpoints with DID numbers scattered randomly among different Communication Manager servers. This arrangement makes it cumbersome to configure Session Manager routing to send calls for H.323 endpoints to correct Communication Manager.

The Customer uses the new technique to take advantage of URE routing in place of manually administering Session Manager routing policies.

Impact on capacities

Important:

This method assigns a SIP profile to an H.323 endpoint. Using this method reduces the total SIP endpoint capacity by the number of H.323 endpoints assigned a SIP profile.

For example, if you configure 200 H.323 stations using the alternative method, you reduce the maximum number of SIP devices by 200.

Customer configuration data

The following table identifies the required customer configuration information for the deployment and configuration process for Session Manager.

Required Data	Value for System	Example Value
Session Manager server host name (short name)		example-sm-1
Session Manager IP address (Mgmt) - Eth 0 IP address (management interface for Session Manager on the customer network)		10.1.1.20
Netmask (Network Mask Eth0)		255.255.255.0
Gateway IP address (for Eth0)		10.1.1.254
Network Domain		MyCompany.com
Primary DNS server IP address		10.1.0.2
Secondary DNS (if applicable)		10.1.0.3
Tertiary DNS (if applicable)		
Local time zone		
NTP server		time-server.example.com
Secondary NTP server (if applicable)		
Tertiary NTP server (if applicable)		
Primary System Manager IP		10.1.1.100
Primary System Manager FQDN		smgr.example.com

Required Data	Value for System	Example Value
Secondary System Manager IP		
Secondary System Manager FQDN		
Virtual System Manager FQDN		
Enrollment Password: Set up in the Security section of System Manager.  Note: Verify the enrollment password is active.		Enroll01!

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>.

Chapter 4: Deploying the Session Manager OVA

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.

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.

Session Manager Deployment checklist

The Session Manager OVA is packaged as a virtual appliance that you can deploy using VMware vSphere Client or VMware vCenter.

For Avaya Aura® Release 6.2 Feature Pack 4, you install the Session Manager OVA on ESXi 5.5, then install Avaya Aura® Release 6.2 Feature Pack 4.

Important:

You cannot administer a core Session Manager OVA as a Branch Session Manager (remote survivable server). Deploy the Session Manager OVA as a core Session Manager OVA only.

Perform the following actions to deploy the Session Manager Open Virtual Application:

#	Action	Reference	✓
1	Verify System Manager and Session Manager are configured.	Verifying configuration for deployment on page 23.	
2	Download the Session Manager OVA from PLDS.	Downloading software from PLDS on page 46.	
3	Deploy the Session Manager OVA. <i>Do not power up the Virtual Machine at this time.</i>	Methods for deploying the Session Manager OVA on page 23.	
4	Based on the user footprint requirement, reconfigure the hardware resources for the Session Manager virtual machine.	Reconfiguring hardware resources for user footprint on page 26.	
5	Configure the Session Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 27.	
6	Power on the Session Manager server.	Powering On Session Manager on page 47.	
7	Configure Session Manager.	Configuring Session Manager on page 28.	
8	Verify the installation.	Post-installation checklist on page 30.	

Verifying configuration for deployment

Both System Manager and Session Manager require network connectivity during the Session Manager OVA installation.

Procedure

1. Verify the System Manager is running the same or later Service Pack level as the Session Manager you will be installing.
2. On System Manager, create the Session Manager instance using the **Session Manager Administration** page.
3. Add the Session Manager as a SIP entity using the **Routing** page.
4. Define an Enrollment Password.
5. Define FQDNs for both System Manager and Session Manager. You can either configure the FQDNs in the referenced DNS servers or add the FQDN of Session Manager to the hosts file of the System Manager .

Methods for deploying the Session Manager OVA

Deploy the Session Manager OVA by using one of the following methods:

- [Deploying using vSphere Client connected to vCenter](#) on page 23.
- [Deploying using vSphere Client connected directly to VMware host](#) on page 24.

Deploying using vSphere Client connected to vCenter

When deploying using vCenter, the system prompts you during boot-up to enter the configuration information. Make sure you have a copy of the **Customer Configuration Data** worksheet available before you begin this procedure.

Before you begin

The vCenter must have access to the VMware host on which the Session Manager will be deployed.

- Install the vSphere client.
- Install the vCenter server.
- Add the VMware host to the vCenter.

Note:

If you use vSphere Client 5.5 to connect to vCenter Server 5.5, a warning displays asking you to use vSphere Web Client because of limitations with vSphere Client 5.5.

Procedure

1. Start the vSphere client.

2. Enter the IP address and the user credentials for the vCenter server. Ignore any security warnings that the system displays.
3. On the vSphere client, click **File > Deploy OVF Template**.
4. In the **Deploy OVF Template** dialog box, do one of the following:
 - In the **Deploy from a file or URL** field, enter the path to the Session Manager .ova file.
 - Click **Browse** and navigate to the Session Manager .ova file from the local computer, network share, CD-ROM, or DVD.
5. Verify the details of the OVF template, then 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 appropriate 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 space available.
14. On the **Network Mapping** page, for each network that you specified in the **OVA Template Details** page:
 - a. Click the **Destination Network** column.
 - b. Select a host network from the drop-down menu.
 - c. Click **Next**.
15. On the **Properties** page, enter the configuration data from the Customer Configuration Data worksheet, then click **Next**.
16. Verify the deployment settings, then click **Finish**.
17. Check the **Status** in the **Recent Tasks** window and wait for the **Deploy OVF template** task to display **Completed**.

Deploying using vSphere Client connected directly to VMware host

Procedure

1. Start the vSphere Client.

2. Enter the IP address and the user credentials for the ESXi host. Ignore any security warnings that the system displays.
3. Click **File > Deploy OVF Template**.
4. In the Deploy OVF Template dialog box, do one of the following:
 - In the **Deploy from a file or URL** field, enter the path to the Session Manager .ova file.
 - Click **Browse** and navigate to the Session Manager .ova file from the local computer, network share, CD-ROM, or DVD.
5. Verify the details of the template, then click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. On the **Name and Location** page, in the **Name** field, enter the name for the virtual machine, then click **Next**.
9. On the **Storage** page, select a destination storage for the virtual machine files, then click **Next**.

*** Note:**

The datastore can be local to the host or a mounted shared storage such as NFS or SAN. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

10. On the **Disk Format** page, select **Thick Provision Lazy Zeroed**, then click **Next**.
The system displays the data store that you selected and the available space.
11. On the **Network Mapping** page, for each network that you specified in the **OVA Template Details** page:
 - a. Click the **Destination Networks** column.
 - b. Select a host network from the drop-down menu.

Administer host networks for source networks as follows:

Source Networks	SM NICs	Destination Networks
Session ManagerManagement	Eth0	VM Network2
Session Manager Services	Eth1	VM Network2
Session Manager Security Module	Eth2, Eth3	VMs Network

*** Note:**

- Source Networks are defined in the OVA template. Source networks may contain zero or more Network Interface Cards from the actual virtual machine. You must map networks defined by the OVA template to networks defined on the host where the virtual machine has been deployed. This procedure assigns virtual

machine NICs to host networks. You can change these associations at a later time.

- The Session Manager Services source network contains the Session Manager services port. Map the Session Manager Services source network to the same destination network as Session Manager Management.
- The Session Manager Security Module must be on its own network link. Eth2 and Eth3 can be bonded. The Eth2 and Eth3 ports carry SIP TLS traffic. Depending on the size of the system, the amount of data could be significant.

 Important:

Do not mix the SIP TLS traffic with the administration traffic on the Eth0 port.

c. Click **Next**.

12. Verify the deployment settings, then click **Finish**.

13. Check the **Status** in the **Recent Tasks** window, and wait for the **Deploy OVF template** task to display **Completed**.

Reconfiguring hardware resources for flexible footprint

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

For information related to the different capacity limits and requirements, see [Capacity limits](#) on page 17.

Procedure

1. Connect to the host or cluster using the VMware vSphere client.
2. Log in as an administrator
3. Right-click on the virtual machine name and select **Edit Settings**.
4. Click the **Hardware** tab.
5. Click **Memory** and change the **Memory Size** to the appropriate limit.
6. Click the **Resources** tab.
7. Select **Memory** and verify the **Reservation** is set correctly.
8. If you want to limit the Session Manager memory use, clear the **unlimited** check box and verify the **Limit** slide is set to the same value as the **Reservation**.
9. Click the **Hardware** tab.
10. Select **CPUs** and change the **Number of sockets** according to the limit requirement.
11. Click the **Resources** tab.

12. Select **CPUs** and verify the **Reservation** is set correctly. The **Reservation** value must be at least half of the stated minimum MHz requirement because Session Manager capacities assume hyperthreading is active.
13. If you want to limit the Session Manager CPU use:
 - a. Clear the **unlimited** check box.
 - b. Verify the **Limit** slide is set to the *full* value of the stated minimum MHz requirement.
14. Click **OK** and wait until the virtual machine finishes the reconfiguration procedure.

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

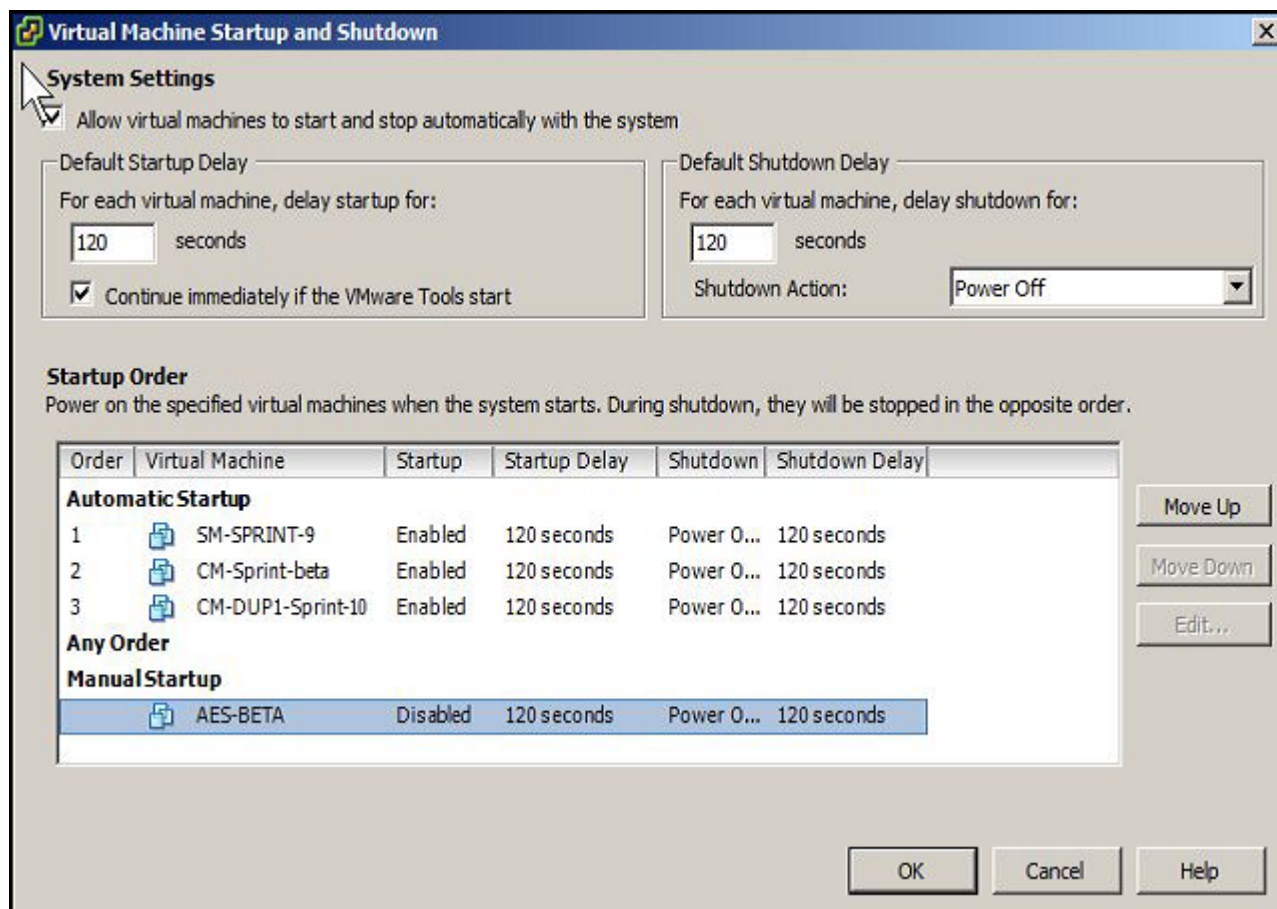
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

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.



Configuring Session Manager

If you deployed the Session Manager OVA through vCenter, only perform Step 1 and skip the rest of the procedure.

Perform this entire procedure *only* if you deployed the Session Manager OVA using vSphere Client connected directly to the VMware host. The Session Manager is not yet configured. **SMnetSetup** requires the information entered on the Customer Configuration Data worksheet. Make sure you have the worksheet available before you begin this procedure.

Procedure

1. Verify System Manager is configured and operational for the deployed Session Manager.
2. If you deployed the Session Manager OVA through vCenter, skip the rest of this procedure.
3. Right-click the Session Manager virtual machine and select **Open Console**.
4. Log in using the customer account.

5. Configure Session Manager:

- a. Enter **SMnetSetup**.
- b. At each prompt, enter the appropriate information from the Customer Configuration Data worksheet.
- c. Press **Enter** when the prompt appears.
- d. When prompted, enter the Primary System Manager IP Address.

SMnetSetup automatically configures the configuration information related to the System Manager.

- e. Verify your settings.
- f. Enter the enrollment password.

The system starts the configuration process. The process takes approximately 15 minutes to complete.

Chapter 5: Post-installation verification

Post-installation checklist

Perform the following steps to verify the Session Manager OVA installation.

#	Action	Link	✓
1	Verify the Session Manager server resources.	Using the hardware_info command on page 30.	
2	Verify the Session Manager VMware administration.	Verifying the Session Manager as a VMware instance on page 31.	
3	Verify the connections of the deployed Session Manager.	Verifying the connections on page 31.	
4	Upgrade Session Manager to the latest release.	Service Pack and patch updates on page 49.	
5	Run the maintenance tests on the deployed Session Manager.	Running Session Manager maintenance tests on page 48.	
6	Verify data replication.	Verifying Data Replication on page 51.	
7	Upgrade the Session Manager VMware tools.	Upgrading VMware Tools on page 36.	

Using the hardware_info command

The `hardware_info` command displays detailed information about a server.

The output of the command is the same when run on VMware and non-VMware core Session Manager servers with the following exceptions:

- The **System Information** field displays as **VMware Virtual Platform**.
- The **Raid Information** field displays as **N/A**.
- The **Disk Information** field contains the linux path to the disk drive and the allocated size of the disk in GB.

Procedure

1. Log in to the core Session Manager server.

2. Enter the command `hardware_info`.
3. Verify the hardware information.

Verifying the Session Manager as a VMware instance

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Click **Session Manager Administration**.
3. Under the Session Manager Instances section, select the appropriate Session Manager instance from the **Session Manager Instances** list.
4. Click **View**.
5. In the General section, verify the **VMware Virtual Machine** check box is selected. If the check box is not selected:
 - a. Click **Return**.
 - b. Select the Session Manager instance from the **Session Manager Instances** list and click **Edit**.
 - c. Select the **VMware Virtual Machine** check box.
 - d. Click **Commit**.

Verifying the connections

Verify the connections of the deployed Session Manager.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. On the **Dashboard** page, verify the Service State of the Session Manager instance is **Accept New Service**. If the service state is not **Accept New Service**:
 - a. Select the Session Manager instance.
 - b. Click **Service State > Accept New Service**.
3. Verify the **Security Module state** is **Up**.

Chapter 6: Upgrading Session Manager on VMware

Upgrade checklist



Warning:

All existing logs, other than the installation log, are lost as part of the upgrade process. To save the logs, you must manually copy the logs to an external server. For information on managing logs, see *Administering Avaya Aura® Session Manager*.

Upgrade Procedure

You can upgrade Session Manager on VMware using vSphere or vCenter.



Note:

Before upgrading Session Manager, ensure that you upgrade System Manager to the required release.

#	Action	Link/Notes	✓
1	(Optional) Copy the logs to an external server.	See <i>Administering Avaya Aura® Session Manager</i> .	
2	Verify System Manager is running the correct release.		
3	Download the standard kickstart upgrade ISO image. Either burn the ISO image to a DVD or place the ISO image on a network share connected to vCenter or vSphere.	Downloading software from PLDS on page 46.	
4	Verify the Enrollment Password is not expired.	Verifying Enrollment Password status on page 34.	
5	Change the state of the Session Manager to Deny New Service .	Denying new service on page 44.	
6	Verify the Active Call Count field is zero.	Verifying Active Call Count on page 51.	
7	View the Entity Links and note any links that are down.	Viewing Session Manager Entity Link Connection Status on page 53.	

#	Action	Link/Notes	✓
	 Important: Make sure that entity links for this Session Manager are UP .		
8	Take a snapshot of Session Manager.	Creating a snapshot on page 44.	
9	Upgrade the operating system.  Note: This step is only required if you are upgrading from Release 6.2.3.	Upgrading the operating system on page 34.	
10	Upgrade the Session Manager software.  Warning: The Session Manager upgrade process might cause errors with the VMware tools. If you lose network connectivity, upgrade the VMware Tools. See Upgrading VMware Tools on page 36.	If upgrading using a DVD, see Using a DVD on page 35. If upgrading using the Session Manager iso image, see Using Network transfer on page 36.	
11	After the Session Manager server reboots, log in to the server.	After the Session Manager upgrade, the craft login will be ASG-challenged and available only to Avaya Services.	
12	Using the <code>wversion</code> command, verify the upgrade completed successfully. If the upgrade is not successful, contact Avaya Global Services.	The Release must start with 6.3.	
13	Test the Test the Session Manager.	Running Session Manager maintenance tests on page 48.	
14	Create and install an authentication file.  Note: This step is not required when upgrading from Session Manager 6.2.	<ul style="list-style-type: none"> • Creating an authentication file for a Session Manager on page 38. • Installing an authentication file on page 39. 	
15	Verify data replication between System Manager and Session Manager. Data takes about 10-15 minutes to synchronize.	Verifying Data Replication on page 51.	
16	Verify the Security Module is active for Session Manager.	Viewing Security Module status on page 52.	
17	If SIP monitoring is provisioned for the Session Manager, verify the links are active for that Session Manager. The system takes about 15 minutes to update the data. Refresh the screen as necessary.	Viewing the SIP Monitoring Status Summary page on page 53.	

#	Action	Link/Notes	✓
18	Change the state to Accept New Service for the upgraded Session Manager server.	Accepting new service on page 43.	
19	Make test calls to verify Session Manager is processing calls properly.		
20	Delete the VMware snapshot.	Deleting a snapshot on page 45 .	

Verifying the Enrollment Password status

Session Manager requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and the Session Manager. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, or if you do not know the password, do one of the following:

- Ask the customer for a password.
- Make up a password.

Procedure

1. On the home page of the System Manager web console, under **Services**, select **Security > Certificates > Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, you need to reset the password:
 - a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
 - b. Enter a password in the **Password** field.
 - c. Re-enter the password in the **Confirm Password** field.
 - d. Make a note of the password for future reference.
 - e. Click **Commit**.

The system updates the **Time remaining** field.

Upgrading the operating system

Upgrade the operating system of the Session Manager virtual machine.

* Note:

Perform this procedure *only* if you are upgrading from Release 6.2.3.

VMware provides several DVD sourcing options, including using:

- the media tray of the vSphere Client
- the media tray of the VMware host
- a virtual image of the DVD located in the datastore.

After the upgrade, the virtual machine will be running RHEL 6.2.

Procedure

1. Open the virtual console to the Session Manager.
2. From vSphere or vCenter, click **VM > Edit Settings**.
3. On the **Hardware** tab, click **CD/DVD drive 1** to see the DVD sourcing options.
4. Select the appropriate **Device Type** for the DVD source.
5. Select **Connect at power on**.
6. Click the **Options** tab and select **Boot Options**.
7. In the **Power on Boot Delay** field, enter the time as **10,000** ms.
8. Select **Force BIOS Setup**.
9. Click **OK**.
10. Verify that the DVD source is available at the location you specified earlier.
11. Reboot the virtual machine.
12. After the BIOS screen displays, set the boot order to boot from CD/DVD first.
13. From vSphere or vCenter, click **VM > Edit Settings**.
14. On the **Hardware** screen, clear **Connect at power on**.
15. Click **OK**.

Upgrading Session Manager using a DVD

Procedure

1. From vSphere or vCenter, click **VM > Edit Settings**.
2. On the **Hardware** tab, click **CD/DVD drive 1** to see the DVD sourcing options.
3. Select the appropriate **Device Type** for the location of the Session Manager installer DVD.
4. Select the **Connect at power on** check box.
5. Log in using the customer account.
6. Verify the DVD is available at the location you specified earlier.
7. Enter the command `$HOME/upgradeSM` to start the upgrade script.

8. If prompted, enter the Enrollment Password. The script takes about 20 minutes to complete. After the script installs the software, the virtual machine reboots.

Using Network transfer

Transfer the downloaded Session Manager ISO image to the Session Manager server and run the upgrade script.

Procedure

1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for remote login.

 Note:

You can connect your laptop directly to the service port of the server.

2. Enter `rm -f $HOME/asm*installer.iso`
3. Enter `echo $HOME`
4. Transfer the ISO file to the directory represented by `$HOME` in the Session Manager server.

 Note:

You can transfer the files over the network using WinSCP or another file transfer application.

5. Enter `cd $HOME`
6. Enter `upgradeSM asm*installer.iso` to mount the ISO image and run the upgrade script.
7. If prompted, accept the EULA.
8. If prompted, enter the Enrollment password. The script takes about 20 minutes to complete.

 Note:

The upgrade process does not prompt for the Enrollment Password when upgrading from Session Manager 6.3 to Session Manager 6.3.8 and later.

Upgrading Session Manager VMware Tools

Installing Session Manager service packs might cause loss of network connectivity due to incorrect drivers.

The guest operating system checks the version of VMware Tools when you power on a virtual machine. The status bar of the virtual machine displays a message regarding the availability of a new version.

 Caution:

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.

Procedure

1. Right-click the target Session Manager virtual machine.
2. On the **Guest** menu, click **Install/Upgrade VMware Tools**.
3. Select **Automatic Tools Upgrade** in the pop-up window.
4. Click **OK**.
5. In the Recent Tasks window, check the status of the **Initiated VMware Tools install or upgrade** task. Wait until the status displays **Completed**.
6. Reboot the Session Manager virtual machine.

When the reboot completes, network connectivity is restored.

Authentication files for Session Manager

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for Session Manager. With the ASG keys, Avaya Services can securely gain access to the customer system.

A default authentication file is installed with Session Manager. You must replace the default file using the Authentication File System (AFS) to create a unique authentication file. AFS is an online application available at [RFA](#).

Each authentication file contains an authentication file ID (AFID) to identify the file. You use the AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

 Note:

Installation of the the unique authentication file is essential. Failure to install the unique authentication file results in receiving an alarm that retransmits daily until you install the authentication file.

Creating an authentication file for a Session Manager

AFS is available only to Avaya service personnel and Avaya Partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

To acquire an authentication file, use one of the following options:

- Download the authentication file directly from AFS.
- Receive the authentication file in an email.

After AFS creates the authentication file, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

Procedure

1. Enter <http://rfa.avaya.com> in your browser and log in.
2. Click **Start the AFS Application**, then click **I agree**.
3. In the **Product** field, select **SM Session Manager**.
4. In the **Release** field, select the software release number, then click **Next**.
5. If you are installing a new Session Manager instance (not upgrading), select **New System**, then click **Next**.
6. If you want to download the authentication file directly from AFS to your computer:
 - a. Click **Download file to my PC**.
 - b. Click **Save** in the File Download dialog box.
 - c. Select the location where you want to save the authentication file, then click **Save**.
 - d. Click **Close** in the **Download complete** dialog box to complete the download.
7. To receive the authentication file in an email message:
 - a. Enter the email address of the recipient in the **Email Address** field.
 - b. Click **Download file via email**.

AFS sends the email message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
 - c. Save the authentication file to a location on the computer of the email recipient.
8. To view the header information in the authentication file:
 - a. Locate the saved file.
 - b. Open the file with WordPad.

The header includes the AFID, product name and release number, and the date and time that AFS generated the authentication file.

Installing an authentication file

Procedure

1. Log in using the customer login to the Session Manager server using an SSH tool such as PuTTY.
2. Enter the command `echo $HOME`.
3. Using WinSCP or some other file transfer program, transfer the authentication file to the Session Manager server into the directory represented by `$HOME`.
4. Load the authentication file manually using the `loadpwd` command. For example:

```
loadpwd -l <path to the auth file>.
```
5. Enter the `displaypwd` command to display information about the currently loaded authentication file.

Chapter 7: Migrating Session Manager

This chapter provides the procedures for migrating a bare-metal instance of a Session Manager to a VMware-based Session Manager. The Session Manager virtual machine reuses the IP addresses and hostname of the hardware Session Manager.

Warning:

Capacities for the hardware-based Session Manager differ from the VMware-based Session Manager. Before attempting a migration, verify the load capacity of the VMware Session Manager is compatible with the hardware-based Session Manager. For information about the VMware configuration requirements, see [Capacity limits](#) on page 17.

Migration checklist

#	Action	Reference	✓
1	Plan the migration activities using the planning checklist.	Planning checklist on page 16	
2	Verify System Manager is configured properly.	Verifying configuration for deployment on page 23.	
3	Download the Session Manager OVA from PLDS.	Downloading software from PLDS on page 46.	
4	Deploy the Session Manager OVA. <i>Do not power up the virtual machine.</i>	Methods for deploying the Session Manager OVA on page 23.	
5	Based on the user footprint requirement, reconfigure the hardware resources for the Session Manager virtual machine. <i>Do not power up the virtual machine.</i>	Reconfiguring hardware resources for user footprint on page 26.	
6	Verify the Enrollment Password.	Verifying Enrollment Password status on page 34.	
7	Deny new service for the Session Manager	Denying new service on page 44.	
8	Shut down the Session Manager.	<ul style="list-style-type: none">• Using the CLI to shut down or reboot the server on page 42	

#	Action	Reference	✓
		<ul style="list-style-type: none"> • Using the GUI to shut down or reboot the server on page 41 	
9	Disconnect the Session Manager from the power source and the network.	You do not want the old Session Manager to return to service and interfere with the new Session Manager.	
10	Configure the Session Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 27.	
11	Power on the Session Manager virtual machine.	Powering On Session Manager on page 47.	
12	Configure the new Session Manager.	Configuring Session Manager on page 28.	
13	Verify the Session Manager is configured as a VMware instance.	Verifying the Session Manager as a VMware instance on page 31.	
14	Upgrade the Session Manager to the appropriate version depending on the version of the Session Manager at the time of migration.	<p>For example, the Session Manager OVA deployment is 6.2.2, and you want to be running Session Manager 6.3.8. You need to upgrade the Session Manager virtual machine to Session Manager 6.3.8.</p> <p>See Upgrading Session Manager on VMware on page 32.</p>	
15	Manage the serviceability agent. Redeploying Session Manager requires a cleanup of the existing serviceability agent data.	This procedure requires root access. Contact Avaya Global Services	
16	Verify the migration.	Continue with the Post-installation checklist on page 30.	

Using the GUI to shut down or reboot the server

Procedure

1. On System Manager Web Console, select **Elements > Session Manager**.
2. Select the Session Manager server that you want to shut down or reboot.

 Note:

You can shut down or reboot only one Session Manager at a time.

3. Click **Service State**.
4. Select **Deny New Service**.

5. Wait for all active calls on the Session Manager to end before shutting down or rebooting the server.
6. Click **Shutdown System** .
7. Select **Shutdown** or **Reboot** from the drop-down menu.

The system displays a confirmation screen. If the Session Manager is not in the **Deny New Service** state, the system displays an additional screen with the recommended action.

Using the CLI to shut down or reboot the server

About this task

If you experience problems accessing System Manager, use the CLI to shut down or reboot that particular Session Manager using the following procedure:

Procedure

1. Log in to the Session Manager using the **cust** login.
2. Enter one of the following commands:
 - **shutdownSM** (to shut down the server)
 - **rebootSM** (to reboot the server)
3. If Session Manager is shut down, the confirmation screen warns that onsite personnel must restart the system.

Chapter 8: Maintenance and administration procedures

Adding Session Manager as a SIP entity

Procedure

1. On the System Manager web console home page, under **Elements**, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter the name of the Session Manager.
4. In the **FQDN or IP Address** field, enter the IP address of the Session Manager Security Module. This IP address is *not* the management IP address.
5. In the **Type** field, set the type to Session Manager.
6. In the **Port** section of the screen, click **Add**.
7. Add the port, protocol, and default domain entries for each port and protocol on which the Session Manager listens for SIP traffic. Add failover ports if the SIP entity is a failover group member. For more information about Failover Groups, see *Administering Avaya Aura® Session Manager*.
8. Click **Commit**.

Accepting new service

Note:

Even though the Security Module displays the status as **Up**, the security module might take 5 to 10 minutes before the security module can begin routing calls.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager in the **Session Manager Instances** table.

3. Click **Service State**.
4. Select **Accept New Service** from the drop-down menu.
5. Click **Confirm**.

Denying new service

When you change the state of the selected Session Manager to **Deny New Service**, the system denies any new call attempts and service requests. Existing calls remain in effect until the users terminate the calls.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager check box in the **Session Manager Instances** table.
3. Click **Service State**.
4. From the drop-down list box, select **Deny New Service**.
5. On the confirmation page, click **Confirm**.

Creating a snapshot



Caution:

Do not perform any activity on the virtual application until the snapshot backup is complete. Snapshot operations can adversely affect service.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Create snapshot** is available on the virtual machine.



Note:

Differences exist between the vSphere Web Client versions. You might need to modify the following steps accordingly.

Procedure

1. Select a virtual machine.
 - If you are using the vSphere Web Client:
 - a. Search for a virtual machine and select it from the search results list.

- b. Stop the application that is running on the virtual machine or set to out-of-service.
 - c. Right-click the virtual machine and select **Snapshot > Take Snapshot**.
- If you are using the vSphere Client:
 - a. Stop the application that is running on the virtual machine or set to out-of-service.
 - b. Click **Inventory > Virtual Machine > Snapshot > Take Snapshot**.
- 2. In the **Name** field, enter a name for the snapshot.
- 3. In the **Description** field, enter a description for the snapshot.
- 4. Disable **Snapshot the virtual machine's memory**.
- 5. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
- 6. Click **OK**.

The system displays `Completed` to indicate that the snapshot backup is complete.

Deleting a snapshot

Note:

Differences exist between the vSphere Web Client versions. Modify the steps accordingly.

Before you begin

Verify the required privilege **Virtual machine.State.Remove snapshot** is available on the virtual machine.

Procedure

1. Open the **Snapshot Manger**.
 - If you are using the vSphere Web Client:
 - a. Search for a virtual machine and select it from the search results list.
 - b. Right-click the virtual machine and select **Snapshot > Snapshot Manager**.
 - If you are using the vSphere Client:
 - a. Select **Inventory > Virtual Machine > Snapshot > Snapshot Manager**.
2. In the **Snapshot Manager**, click a snapshot to select it.
3. Select **Delete from Disk** to delete the single snapshot from the Snapshot Manager and the virtual machine.
4. Click **Yes** in the confirmation dialog box.
5. If you are using the vSphere Web Client, click **Close** to close the Snapshot Manager.

Restoring a snapshot

Use this procedure to return the memory, settings, and state of the virtual machines to the state when you took the snapshot. The power and data states of the virtual machines return to the state when you took the parent snapshot.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

 Important:

Do not perform any activity on the virtual application until the snapshot restoration is complete.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Revert to snapshot** is available on the virtual machine.

 Note:

Differences exist between the vSphere Web Client versions. You might need to modify the steps accordingly.

Procedure

1. Click **Inventory > Virtual Machine**.
2. Right-click the virtual machine name on which you want to restore the snapshot, and click **Snapshot**.
3. Open **Snapshot Manager**.
4. Select the snapshot version that you want to restore.
5. Click **Go to**.
6. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task.

Wait until the message `Completed` displays.

Downloading software from PLDS

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from <http://support.avaya.com> using the **Downloads and Documents** tab at the top of the page.

 Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. Enter <http://plds.avaya.com> in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Select **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

 Note:

- The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. (Internet Explorer only) If you receive an error message, click on the **install ActiveX** message at the top of the page and continue with the download.
 14. Select a location where you want to save the file and click **Save**.
 15. If you used the Download Manager, click **Details** to view the download progress.

Powering On Session Manager

Procedure

1. Start the vSphere Client.
2. Select the deployed Session Manager virtual machine from the list of virtual machines for the target host.
3. Do one of the following:
 - On the **Summary** page, click **Power On**
 - Right-click the virtual machine and click **Power** > **Power On**.

4. Right-click the virtual machine, highlight the **Power**, and click **Power On**.
5. In the Recent Tasks window, check the Status of the **Power On virtual machine** task and wait until the **Completed** message displays.
6. Right-click the Session Manager virtual machine and select **Open Console**.
Wait for the Session Manager virtual machine to finish the initialization process.
7. If the Session Manager virtual machine does not power on, see [Troubleshooting a Session Manager virtual machine that is unable to power on](#) on page 48.

Troubleshooting a Session Manager virtual machine that is unable to power on

The system displays appropriate messages for CPU or memory resource limitations. The Session Manager might be deployed on a host that does not have the necessary resources allocated for power up. A power up failure indicates the newly deployed OVA must be resized or resources are being oversubscribed. The recommendation is to *not* oversubscribe resources.

Default CPU and memory reservations are built into the Session Manager OVA. The reservations must be adjusted to match the desired configuration. To adjust the virtual machine resources, see [Reconfiguring hardware resources for flexible footprint](#) on page 26. If adjusting the reservations does not correct the power up failure, it is likely that the available host resources are not adequate for this Session Manager deployment. You must select a different, more available, host.

Running maintenance tests

Run the maintenance tests on the current System Manager or any configured Session Manager.

Procedure

1. On the System ManagerWeb Console, under **Elements**, select **Session Manager > System Tools > Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager** or a Session Manager instance from the drop-down menu.
3. To run all of the tests, select **Execute All Tests**.
4. To run only certain tests:
 - a. Select the test to run from the test list.
 - b. Click **Execute Selected Tests**.
5. Verify the tests pass.

Session Manager Service Pack and patch updates

For the procedures to apply service pack and patch updates to Session Manager, see *Installing Service Packs for Avaya Aura® Session Manager* on the Avaya support website <http://support.avaya.com>.

Before you apply service pack or patch updates to Session Manager, take a snapshot of Session Manager. Delete the snapshot after you successfully apply the service pack or patch to increase available space.

*** Note:**

Applying service pack or patch updates to Session Manager might require you to update the version of VMware tools. For more information about how to update the version of VMware tools, see [Upgrading VMware Tools](#) on page 36.

Session Manager Backup and Restore

Use the native System Manager backup and restore function for the long-term backup and recovery of the Session Manager virtual machine data when running on VMware.

For more information about Session Manager backup and restore, see *Administering Avaya Aura Session Manager* on the Avaya support website at <http://support.avaya.com>.

During the data restore operation on the virtual machine, verify that the maximum load capacity does not exceed the load as defined in [Capacity limits](#) on page 17.

*** Note:**

This procedure only backs up administration data.

Accessing the Backup and Restore service

Procedure

On System Manager Web Console, click **Services > Backup and Restore**.

*** Note:**

The secondary System Manager that is in the standby mode does not display the **Backup and Restore** link on the web console.

Result

The system displays the Backup and Restore page.

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: <ul style="list-style-type: none"> • Backup • Restore
File Name	<ul style="list-style-type: none"> • 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.
Path	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Verifying the Active Call Count

The **Active Call Count** value indicates the number of active calls on the Session Manager instance. Active calls are calls that were already active before the Session Manager was placed in the denial state. Changing the state to **Deny New Service** does not drop calls that are currently processed.

To prevent any impact on calls that are active, the **Active Call Count** must be zero before proceeding with the Session Manager upgrade. If the administrator decides to continue the upgrade if the active call count is not zero, the active calls are dropped.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Wait until **Active Call Count** is zero. Refresh the screen to update the count.

Verifying data replication

Procedure

1. On the System Manager web console home page, under **Services**, click **Replication**.
2. Select the Session Manager instance and click **View Replica Nodes**.
3. Confirm that the target Session Manager is **Synchronized** (green).
4. If the Session Manager is not **Synchronized**:
 - a. Select the Session Manager instance.
 - b. Click **Repair**.

Troubleshooting Data Replication

Procedure

1. On the home page of the System Manager Web console, under **Services**, click **Replication**.
2. If the status for the replica group is not **Synchronized**:
 - a. Select the check box in front of the affected replica group.
 - b. Click **View Replica Nodes**.
 - c. Verify that an entry for the upgraded Session Manager exists.
 - d. Select the check box next to the upgraded Session Manager.
 - e. Click **View Details**.
 - f. Under the **Synchronization Statistics** section, wait until the **Pending Batches** number is zero. Refresh the page as necessary.

3. If the **Pending Batches** number does not change to zero, perform the following steps:
 - a. Click **Done**.
 - b. On the **Replica Nodes** page, click **Repair**.
 - c. Click **OK** in the dialog box.
4. Wait until the status of the Session Manager is **Synchronized**. Refresh the page as necessary.

Viewing Security Module status

Procedure

1. On the System Manager Web Console, select **Elements > Session Manager**.
The **Session Manager Dashboard** page displays the details and Security Module status for all the administered Session Manager servers and Survivable Remote Session Manager servers (BSM).
2. If the Security Module state of a particular Session Manager is not displayed as **Up**, see [Troubleshooting Security Module Sanity failure](#) on page 52.

Troubleshooting Security Module Sanity failure

Procedure

1. On the System Manager Web Console, select **Elements > Session Manager > System Status > Security Module Status**.
2. Select **Refresh** to display the current status.
3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.
5. If the status is selected as **Down**, reset the security module:
 - a. Select the appropriate Session Manager instance from the table.
 - b. Click **Reset**.

 Warning:

Session Manager cannot process calls while the system resets the security module.

6. Select **Refresh** to display the current status.

Viewing the Session Manager Entity Link Connection Status

An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all the connections are up, then the Entity Link status is **up**. If one or more connections are down but at least one connection is up, the link status is **partially down**. If all the connections are down, the Entity Link status is **down**.

On the Session Manager dashboard page, the number of down links and total links are shown in the **Entity Monitoring** column. The values have the format **# of Down links / # of Total links**.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Red link values indicate that at least one entity link is down. Click the link to display the Session Manager Entity Link Connection Status page.

The Session Manager Entity Link Connection Status page displays the details for each link. If a link is down, the page displays a reason code.

3. To view the SIP Entity Link Monitoring Status Summary page, click **Summary View**.

Viewing the SIP Monitoring Status Summary page

About this task

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all the administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager server and a SIP entity.

If all connections are up, then the entity link status is **up**. If one or more connections are down but there is at least one connection up, the link status is **partially down**. If all of the connections are down, the entity link status is **down**. If the connection denies any new service, the entity link status is **deny new service**.

Procedure

1. On System Manager Web Console, click **Elements > Session Manager**.
2. In the left navigation pane, click **System Status > SIP Entity Monitoring**

The **SIP Entity Link Monitoring Status Summary** page displays the SIP Entity Link monitoring status for all Session Manager instances.

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**.

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.

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.

VMware networking best practices

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

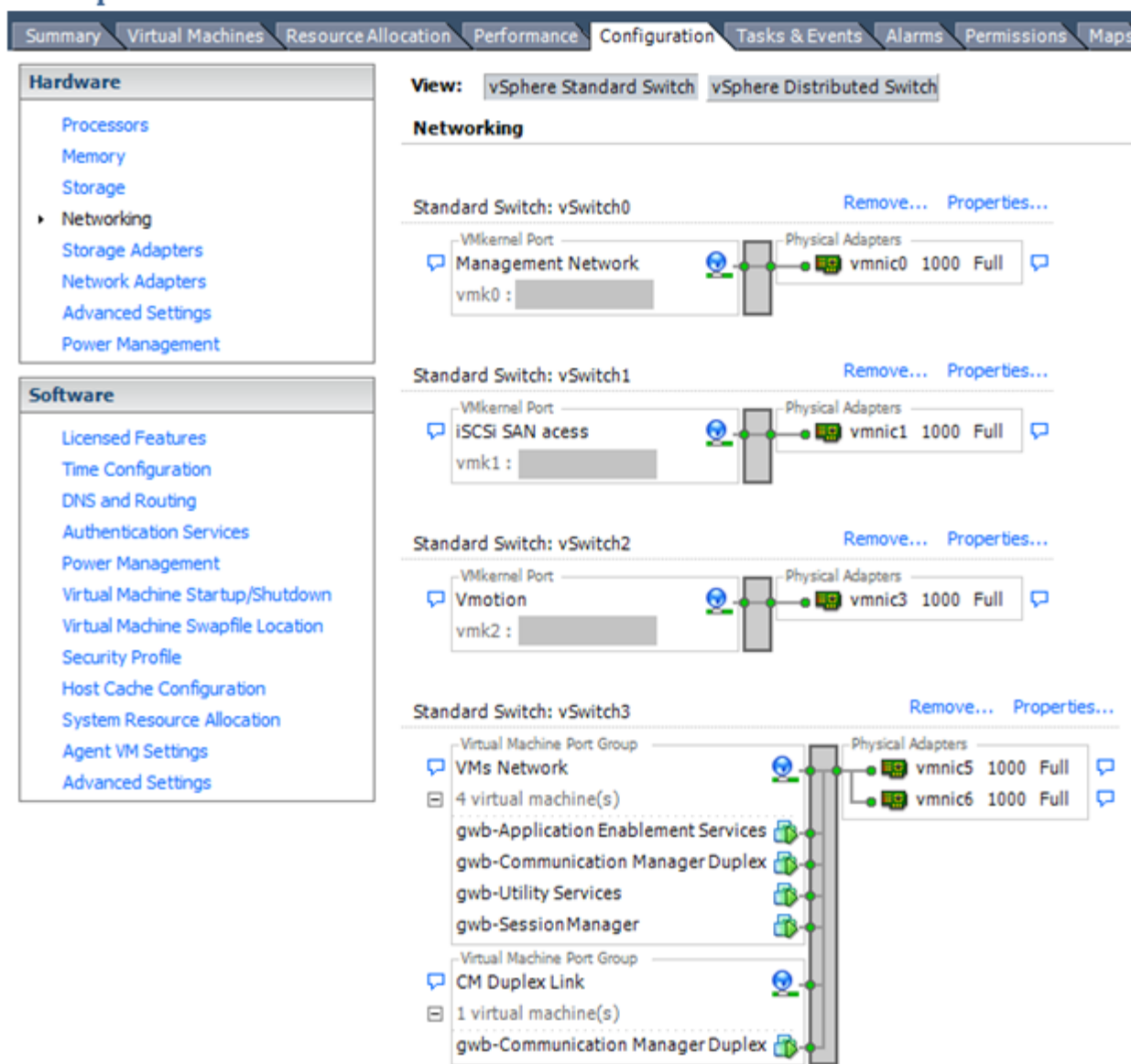
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.

- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

Networking Avaya applications on VMware ESXi – Example 1

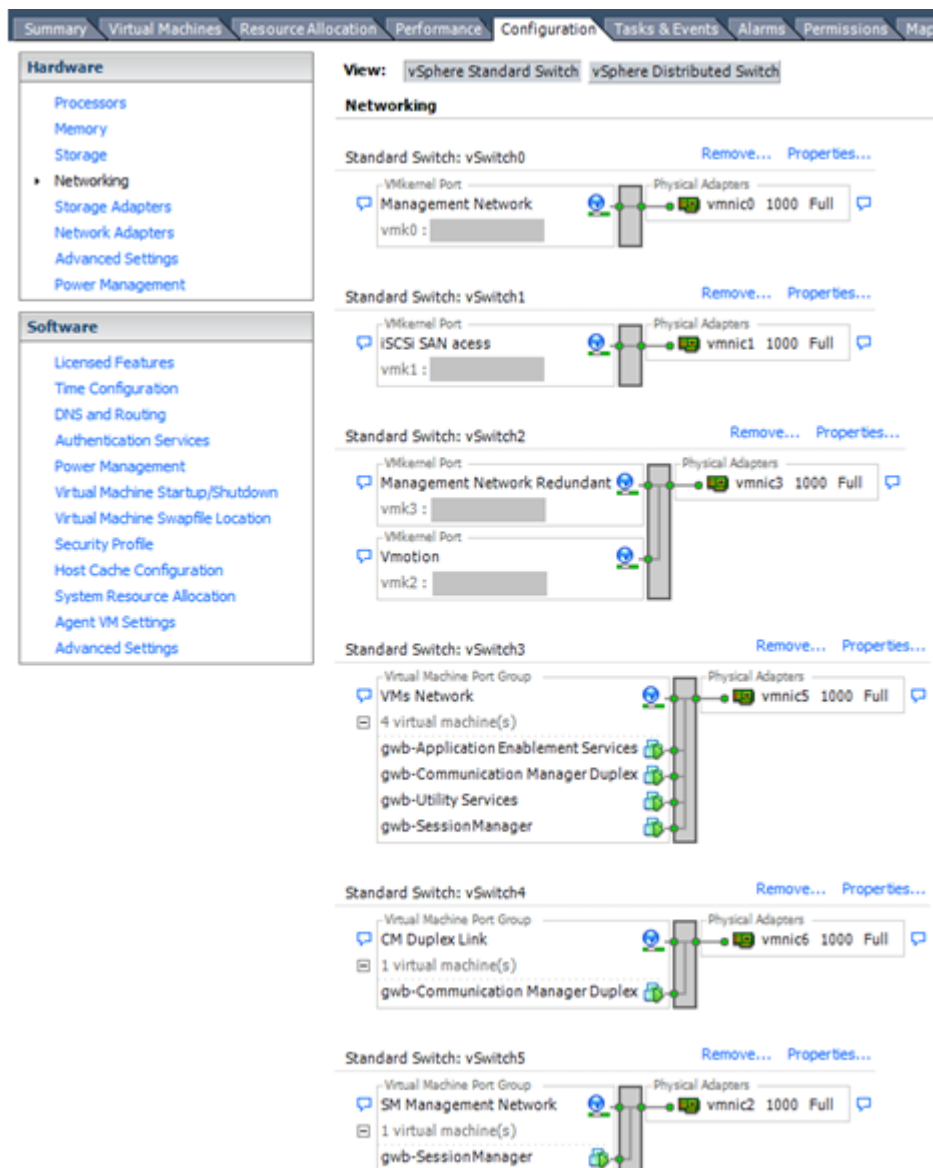


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

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

- **Communication Manager Duplex link:** Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements. for more information, see Avaya PSN003556u at [PSN003556u](#). The following are the minimum requirements of the Communication Manager software duplex connectivity:
 - The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
 - The round-trip delay must be 8 ms or less.
 - The round-trip packet loss must be 0.1% or less.
 - Both servers duplication ports must be on the same IP subnet.
 - You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
 - The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.
- **Session Manager vNIC mapping:** Session Manager OVA defines four separate virtual NICs within the VM. However, Example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- **Virtual networking:** The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



This configuration shows a complex situation using multiple physical network interface cards. The key differences between Example 1 and Example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at [PSN003556u](#).

- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere™ 5.0	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/

Separating Session Manager management and Security Module traffic

About this task

As a best practice, Session Manager management and Security Module related traffic should be separate. There are many ways in which to separate Session Manager including VLANs, VMware port groups, and VMware virtual switches connected to different physical network interface cards.

Using a VLAN to separate management and Security Module related traffic must be done from a customer's switch, as VLAN configuration cannot be accomplished from a virtual machine or Hypervisor level. The result is a Session Manager virtual machine with all of its NICs connected to the same vSwitch.

If the defaults are selected during deployment, management and Security Module traffic are placed on the same vSwitch. As a best practice, separate Session Manager management and Security Module traffic using the following procedure.

Procedure

1. Create a vSwitch for dedicated Session Manager Security Module traffic.
2. From the vSphere client inventory view, right-click the Session Manager virtual machine and select **Edit Settings**.
3. The **Hardware** tab is selected by default. Select the proper Network adapter from the hardware list on the left-side.
4. On the right side, under the **Network label** list, select a separate vSwitch for this NIC.
5. Click **OK** to complete configuration.

Storage

There is no stipulation on the underlying storage vendor type and storage technology used. Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

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 High Availability

VMware High Availability (HA) provides automatic detection of hardware failures, server failures, and operating system failures. In the event of a physical server failure, VMware HA automatically restarts the affected virtual machine on other production servers that have spare capacity. In the event of an operating system failure, VMware HA restarts the affected virtual machine on the same server.

VMware HA ensures that capacity is available to restart all virtual machines that are affected by a service failure. HA continuously monitors capacity utilization and reserves spare capacity to restart virtual machines.

VMware HA helps users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions along with suggested remediation steps.

For more information, see the VMware website at <http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf>.

 Note:

- All virtual machines and their configuration files must be on shared storage, e.g. Fibre Channel SAN, iSCSI SAN, or SAN iSCSI NAS.
- The console network must have redundant network paths to have reliable failure detection for HA clusters. VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses virtual machine priority to decide order of restart.
- VMware HA only works across a LAN. VMware HA does not work across a WAN.

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 under-performing 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 the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

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

Appendix B: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at <http://support.avaya.com>.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

 Note:

You can select multiple filters to search for different types of documents at one time.

7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at <http://support.avaya.com>.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **Hi, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
 - a. Click **Add More Products**.
 - b. Select the appropriate product.
7. In the Product box that appears on your screen:
 - a. Select the appropriate release or releases for which you want to receive notifications.
 - b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
 - c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

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 <i>bare-metal hypervisor</i> . 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

accepting new service	43
accessing the Backup and Restore service	49
Active Call Count	
verifying	51
adding SIP Entity	
Session Manager	43
authentication file	
installing	39
Authentication File	
creating	38
automatic restart	
virtual machine	27
Avaya Learning	9

B

Backup and Restore page	50
backup and restore service; access	49
best practices	
performance and features	54
VMware networking	57
BIOS	54
BIOS for HP servers	55
BIOS settings	
for Dell servers	55

C

capacity limits	17
change service state	
deny new service	44
checklist	
deployment procedures	22
migration procedures	40
planning procedures	16
post-installation procedures	30
clones	
deployment	21
Collaboration Pod	13
components	14
VMware	14
configuration data	
customer	19
configuration verification	23
configuring	
Session Manager	28
virtual machine automatic restart	27
connections	
verifying	31
courses	9
creating a snapshot	44

creating Authentication File	38
customer configuration data	19

D

data replication	51
verifying	51
deleting a snapshot	45
deny new service	44
deploying	
using vSphere connected directly	24
deploying copies	21
deploying Session Manager OVA	
using vCenter	23
deployment	
thick	62
thin	62
deployment configuration verification	23
deployment guidelines	21
deployment procedures	
checklist	22
documentation	
related	8
document changes	7
downloading software	
using PLDS	46

E

Enrollment Password status	34
Entity Link Connection Status	53

F

features best practices	54
flexible footprint	
reconfiguring hardware resources	26

G

guidelines	
deployment	21

H

H.323 endpoint considerations	18
hardware_info	
verification check	30
hardware resources	
reconfiguring for flexible footprint	26

I	
installing	
authentication file	39
Intel Virtualization Technology	54
L	
legal notice	
M	
maintenance tests	48
migrating Session Manager	40
migration procedures	
checklist	40
multiple vSwitches	61
N	
Network transfer	36
new service	
changing state to accept	43
notifications	66
NTP time source	56
O	
overview	12
P	
PCNs	
viewing	66
PCN updates	66
performance best practices	54
planning procedures	
checklist	16
PLDS	
downloading software	46
post-installation	
checklist	30
product notification enrollment	67
product notifications	
e-notifications	67
PSNs	
viewing	66
PSN updates	66
R	
related documentation	8
requirements	
virtual machine resources	17
resource requirements	17
resources	
server	15
restoring a snapshot	46
running	
maintenance tests	48
S	
SAL Gateway	20
Security Module sanity failure	
troubleshooting	52
server hardware and resources	15
service packs and patches	49
Session Manager	
backup	49
configuring	28
does not power up	48
power on the virtual machine	47
restore	49
Session Manager OVA	
deployment using vCenter	23
Session Manager updates	49
shutdown or reboot the server	
using the CLI	42
SIP monitoring	
viewing the SIP Monitoring Status Summary page	53
snapshot	
creating	44
deleting	45
restoring	46
snapshots	64
status	
Enrollment Password	34
storage	62
support	11
supported versions	
VMware	14
T	
thick deployment	62
thin deployment	62
timekeeping	56
training	9
troubleshooting	51
power on problem	48
Security Module sanity failure Alarms	52
U	
upgrade checklist	32
upgrading	
operating system	34
VMware tools	36
upgrading Session Manager	
using a DVD	35
using	

Index

using (<i>continued</i>)	
CLI to shut down or reboot the server	42
using, shutdown using GUI	
GUI to shut down or reboot the server	41
reboot using GUI	41

V

verifying	
Active Call Count	51
connections	31
data replication	51
Session Manager VMware administration	31
videos	10
viewing	
Entity Link Connection Status	53
PCNs	66
PSNs	66
SIP Monitoring Status Summary page	53
viewing security module status	52
virtual machine	
automatic restart configuration	27
vMotion	63
VMware High Availability	63
VMware networking	
best practices	57
VMware software	
supported	14
VMware tools	
upgrading	36
VMware Tools	57
vSphere	
deployment	24
VT support	54

W

warranty	11
----------------	--------------------