Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide

Release 6.2
Issue 2
February 2013

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 its hardware and Software (“Product(s)”). 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. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. “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.

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.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation 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.

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). 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. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 5
- Purpose 5
- Intended audience 5
- Related resources 5
  - Documentation 5
  - Training 7
  - Avaya Mentor videos 7
- Support 7

Chapter 2: Architecture overview 9
- Avaya Aura® Virtualized Environment overview 9
- VMware components 11

Chapter 3: Planning and configuration 13
- Planning 13
- Server hardware and resources 14
- Customer configuration data 14
- Capacity limits 15
- Session Manager virtual machine resource requirements 15
- Software requirements 17
- VMware supported versions 17

Chapter 4: VMware best practices for performance 19
- BIOS 19
  - Intel Virtualization Technology support 19
  - Dell PowerEdge Servers — BIOS settings 20
  - HP ProLiant Servers — BIOS settings 20
- Time keeping 20
- VMware Tools 22
- VMware networking best practices 22
  - Using multiple vSwitches to separate Session Manager management and Security Module traffic 26
- Storage 27
- Thin vs. thick deployments 27
- Best Practices for VMware features 28
  - VMware High Availability 28
  - VMware vMotion 28
  - VMware Snapshots 29

Chapter 5: Deploying the Session Manager OVA 31
- Deployment checklist 31
- Deploying Session Manager OVA 32
- Powering On Session Manager 33
- Configuring the virtual machine automatic start and stop settings 34

Chapter 6: Session Manager Configuration 37
- Configuration Prerequisites 37
- Configuring Session Manager 37

Chapter 7: Post-installation verification 39
- Checks and verifications 39

Verifying the connections 39
Chapter 8: Maintenance Operations 41
Upgrading Session Manager 41
Upgrading Session Manager VMware Tools 42
Session Manager Service Pack and patch updates 42
Session Manager Backup and Restore 43
Migrating Session Manager 43
Appendix A: PCN and PSN notifications 45
PCN and PSN notifications 45
Viewing PCNs and PSNs 45
Signing up for PCNs and PSNs 46
Glossary 47
Index 49

Chapter 1: Introduction

Purpose

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

Intended audience

The primary audience for this document is anyone who is involved with installing, configuring, and verifying Session Manager on a VMware® vSphere ™ 5.0 virtualization environment at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers themselves.

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

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Understanding		
Avaya Aura® Session Manager Overview	Provides overview information on Session Manager and its various components and features.	Sales, Marketing, System Designer, Installer, Configurer, Integrator, Support Engineer, Developer,

Title	Description	Audience
		Professional Services Engineer, Supervisor, Agent, Administrator (All)
Implementation		
Implementing Avaya Aura® Session Manager	Provides the installation and initial administration information for Avaya Aura® Session Manager.	System Designer, Installer, Configurer, Integrator, Support Engineers
Upgrading Avaya Aura® Session Manager	Describes how to upgrade Session Manager to a new software release.	Customer IT organization, project deployment team, sales If Avaya Upgrade: BPs, integrators, Support Engineers, Installers, Configurers
Installing Service Packs For Avaya Aura® Session Manager	Describes how to install service packs on Session Manager.	Customer IT organization, project deployment team, sales If Avaya Upgrade: BPs, integrators, Support Engineers, Installers, Configurers
Administration		
Administering Avaya Aura® Session Manager	Describes how to administer Session Manager using System Manager.	System administrators, Call Center supervisors, BPs, Implementation engineers (for set-up and initial administration and configuration)
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Contains information for troubleshooting Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	System Designer, Installer, Configurer, Integrator, Support Engineers, Administrator, Supervisor, end-user

Training

Refer to the courses available at http://www.avaya-learning.com. To search for the course, log in to the Avaya Learning Center, enter the course code in the **Search** field, and click **Go**.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit the Avaya Mentor Videos website at http://www.youtube.com/AvayaMentor and enter **virtual appliance** in the **Search channel** field to view the list of available videos.

You can also enter the application product name to view videos that are available for a particular product.

Support

Visit 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 notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to get answers to questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment overview

Traditionally, Avaya Aura® has been sold and installed as an individual appliance within customer networks to offer collaboration capabilities and business advantages. The Avaya Aura® Virtualized Environment program integrates real-time Avaya Aura® applications with VMware® virtualized server architecture. The benefits of Virtualized Environment:

- leverages existing VMware IT infrastructure at customer sites for both equipment and ease of management.
- 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.
- satisfies customer demand for Avaya Products in a virtualized environment on customer specified servers and hardware.

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 to 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

Virtualized Environment applications

The Virtualized Environment supports the following Avaya products:

- Avaya Aura® Communication Manager Release 6.2 (Simplex & Duplex)
- Avaya Agile Communication Environment™ Release 6.2 (ACE)
- Avaya Aura® Application Enablement Services Release 6.2 (AES)
- WebLM Standalone Release 6.2 (WebLM)
- Secure Access Link Release 2.2 (SAL)
- Avaya Aura® System Manager Release 6.2 (SMGR)
- Avaya Aura® Presence Services Release 6.1 (PS)
- Avaya Aura® Session Manager Release 6.2 (SM)
- Avaya Aura® Utility Services Release 6.2 (US)

Customer deployment

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

The customer provides the servers, the virtual appliances, the hardware, and the VMware infrastructure including the VMware Licenses.

Software delivery

The software is delivered as a pre-packaged Open Virtualization Application (OVA) file posted on the Avaya Product Licensing and Download System (PLDS). The OVA contains the following components:

- the application software and operating system.
- pre-installed VMware tools for deployment on VMware ESXi 5.0.
- preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - NIC
  - other settings

Patches and upgrades

A minimum patch level may be required for each supported application. See the Compatibility Matrix at http://support.avaya.com/CompatibilityMatrix/Index.aspx for the application service pack information.

⚠ Caution:

Do not update the VMware tools software which 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 an Avaya Application issue occurs and the reservations have been modified by the customer. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

VMware components

The following table contains a list of the VMware components.

VMware 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	The client application that is installed on a personal computer or accessible through a Web interface. The ESXi Hypervisor connects to a vCenter server or directly to an ESXi server in the case where vCenter is not used. Enables the installation and management of Virtual Machines.
vCenter	vCenter provides centralized control and visibility at every level of the virtual infrastructure. Virtual machines are managed through vSphere client software which provides alarming and performance monitoring of ESXi hosts and Virtual Machines.

Chapter 3: Planning and configuration

Planning

Ensure that the customer has completed the following before deploying the vAppliance:

#	Action	Notes	✔
1	Assessment of vSphere Infrastructure resource requirement. The key factors are: • CPU Utilization • Memory Usage • Storage Requirements • Network Utilization • Supported capacity		
2	All required hardware has been purchased and delivered.		
3	All required license have been purchased and are accessible.		
4	Staging and verification activities have been planned and resources assigned.		

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:

For the current release, the *VMware* based Session Managers must be sized and configured similar to the *non-VMware* based Session Managers across the enterprise in order to ensure the best utilization of system resources and to handle the failover scenarios. See the topic Capacity limits on page 15 for understanding the supported limits.

Warning:

When configuring the system in a manner where a large *non-VMware* Session Manager may failover to a Session Manager running in a *VMware* environment, ensure that overall capacities can be handled by the target Session Manager. In other words, do not over subscribe a Session Manager capacity as defined in the topic Capacity limits on page 15.

Server hardware and resources

The server must be listed in the VMware Hardware Compatibility List. Go to http://www.vmware.com/resources/guides.html to see the list of certified servers.

Virtualized Environment requires VMware-certified servers to be running ESXi 5.0. Releases prior to 5.0 are not supported.

Customer configuration data

The following table identifies the key customer configuration information that will be required throughout 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 (that is., MyCompany.com)		example.com
Primary DNS server IP address		10.1.0.2
Secondary DNS (if applicable)		10.1.0.3
Tertiary DNS (if applicable)		
DNS Search Domains (separated with a space)		example.com
Local time zone		
NTP server		time-server.example.com

Required Data	Value for System	Example Value
Secondary NTP server (if applicable)		
Tertiary NTP server (if applicable)		
System Manager IP		10.1.1.100
System Manager FQDN		smgr.example.com
Enrollment Password: Set up in the Security section of System Manager. **Note:** Ensure that the enrollment password is active.		Enroll01!

Capacity limits

Session Manager on VMware is capable of supporting the following capacities:

- Up to 6000 users under normal condition
- Up to 7000 users under failure condition
- 45000 simultaneous sessions

Also see the book *Avaya Aura® Session Manager Overview and Specification* for the capacities table.

Session Manager virtual machine resource requirements

The Session Manager virtual machine requires the following set of resources to be available on the ESXi host before deployment.

VMware Resource	*Value*
vCPUs	Eight
CPU reservation	19200MHz = 8x2400MHz **Note:** The functionality and capacity of Session Manager Virtual Machine has been tested and verified using both of the following configurations: • 8x2400MHz • 10x1995MHz

	If it becomes necessary to have more than 8 vCPUs on a Session Manager virtual machine, the virtual hardware must first be upgraded.
Minimum CPU Speed	1.995 GHz
Assumed CPU Speed	2400MHz
Memory	12GB
Memory reservation	12GB
Virtual Disk Size	150GB
Virtual NIC(s)	Four virtual NICs @ 1000 Mbps, used for management and asset.

The Session Manager OVA is built to the specifications as described above. It is possible that the ESXi host, that the Session Manager virtual machine is deployed on, will not be able to meet the required CPU reservation with 8 vCPUs. It may also be possible to meet the reservation with greater or fewer than 8 vCPUs. In either case, a user is allowed to add or remove CPUs as necessary to meet the required CPU reservation. The table below prescribes the minimum specification to which the Session Manager virtual machine may be configured.

VMware Resource	*Value*
vCPUs	Varies **Note:** A Session Manager can be configured with a larger or smaller number of vCPUs. In this way, you can match the performance of the hardware platform with the required CPU reservation. The Session Manager virtual machine must meet the minimum CPU reservation as specified below.
CPU reservation	19200MHz
Minimum CPU speed	1995Mhz Xeon E7540 or equivalent
Memory	12GB
Memory reservation	12GB
Storage reservation	150GB
Shared NIC(s)	One @ 1000 Mbps

Session Manager may be deployed on a host that does not have the resources to allocate to the VM for power up. There are CPU reservations assigned to the virtual appliance, built into the OVA, that are specified for a specific server speed.

In the case of CPU resource limitations, system displays appropriate message. In such cases, you can adjust the VM properties as follows:

1. Right click on the VM and click **Edit Settings**. System displays **Virtual Machine Properties** window.
2. Click the **Resources** tab which displays the VM resources, such as, CPU, Memory, Disk and Advanced CPU.
3. For CPU limitations, click **CPU** from the left-hand pane and adjust the slider to the appropriate number for starting the VM. Alternatively, type the exact number into the **Reservations** field.

In some cases the noted CPU adjustments may not correct the power up conditions and the CPU speed may need to be further lowered. This same procedure can be followed to also lower other VM resources if necessary.

Note:

Any modification to the resource settings, such as, removal of resources all together, is not recommended. Modifying these allocated resources could have a direct impact on the performance and capacity of the Session Manager virtual machine. To run at full capacity, the specified resource size requirements must be met. Removing or greatly downsizing reservations could put this resource requirement at risk. Avaya is not liable for any losses on account of any deviations from the specified limits.

Warning:

Session Manager has been tested at a high capacity. On average, Session Manager at a high capacity averages 3400 Kilobits per second in total network utilization and 7 disk I/O operations per second in total disk utilization. Your experience may differ from these results.

Software requirements

The Session Manager uses the current release 6.2 Service Pack 3 of software as its standard release on VMware vSphere 5.0. VMware vSphere 4.1 is not currently supported. The Session Manager VMware virtualization environment is packaged as an virtual application ready for deployment on VMware certified hardware. The Session Manager includes VMware tools 5.0 or any of its updates and enables VMware host features to utilize VMware hardware version 7. The Session Manager also supports the update of VMware tools from the vSphere Client, vCenter and others, to enable VMware host features.

VMware supported versions

The supported version of VMware is ESXi 5.0 (including latest updates).

Chapter 4: VMware best practices for performance

The following sections describe the best practices for VMware performance and features.

BIOS

For details on BIOS settings to improve the environment for latency-sensitive workloads for an application, see the *Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs* technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following are examples of the best performance BIOS settings for a few specific servers. Similar changes are needed to the BIOS settings of your server to enhance performance. Please consult the manufacturer technical data for your particular server.

Intel Virtualization Technology support

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 feature:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature may be called VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked (either on or off) at boot time. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The host server will reboot, and the BIOS changes will take effect.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs also offer two power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- 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 make and models may have other terminology but equivalent BIOS controls.

Dell PowerEdge Servers — BIOS settings

When the Dell server starts, you select F2 to display the system setup options. The following are the recommended BIOS settings for the Dell PowerEdge servers.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- Under Processor Settings, set **Turbo Mode** to **enable**.
- Under Processor Settings, set **C States** to **disabled**.

HP ProLiant Servers — BIOS settings

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**.

Time keeping

Linux guests should use the Network Time Protocol (NTP) as a time source rather than the ESXi hypervisor for accurate time keeping.

The NTP servers can be local to the LAN or over the Internet. If the NTP servers are on the Internet, then the corporate firewall must open the UDP port 123 so that NTP service can communicate with the external NTP servers.

VMware tools time synchronization 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 VMware Tools Timesync is **disabled**, run the command **/usr/bin/vmware-toolbox-cmd timesync status**.

In special situations, such as powering up the virtual machine, after vMotion, and after resuming a suspended virtual machine, the ESXi hypervisor will push an updated view of its clock into a virtual machine. If this view is very different from that received over the network (over 1000 seconds), the NTP service might not adjust to the network time and shutdown. In this situation, the guest 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. The VMware recommendation is to add **tinker panic 0** as the first line in 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 in setting the NTP configuration, you must configure the Domain Name Service in the guest before administering the NTP service. Otherwise, the NTP service will not be able to locate the time servers. If the NTP service is administered 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 to verify the NTP service is getting time from a network time source. The results indicate which network time source is being used, how close the guest is to the network time, and how often the guest checks the time. The guest polls the time source between every 65 and 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 seems to be consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when it loses synchronization with a network time source.

For more information, see the *Timekeeping best practices for Linux guests* article at http://kb.vwmare.com/kb/1006427. The article presents best practices for Linux timekeeping. These recommendations include specifics on the particular kernel command line options to use for the Linux operating system of interest. There is also a description of the recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration to achieve best timekeeping results.

VMware Tools

VMware Tools are included as part of the application OVA. The tools are a suite of utilities that enhances the performance of the guest operating system on the virtual machine and improves the management of the virtual machine.

The tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing
- Startup/Shutdown scripts

For more information, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

Caution:

Do not update the VMware tools software which 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 information in this section provides a few of the VMware networking possibilities. These examples are not the only supported networking configurations, and implement several best practices and recommendations from Avaya's perspective.

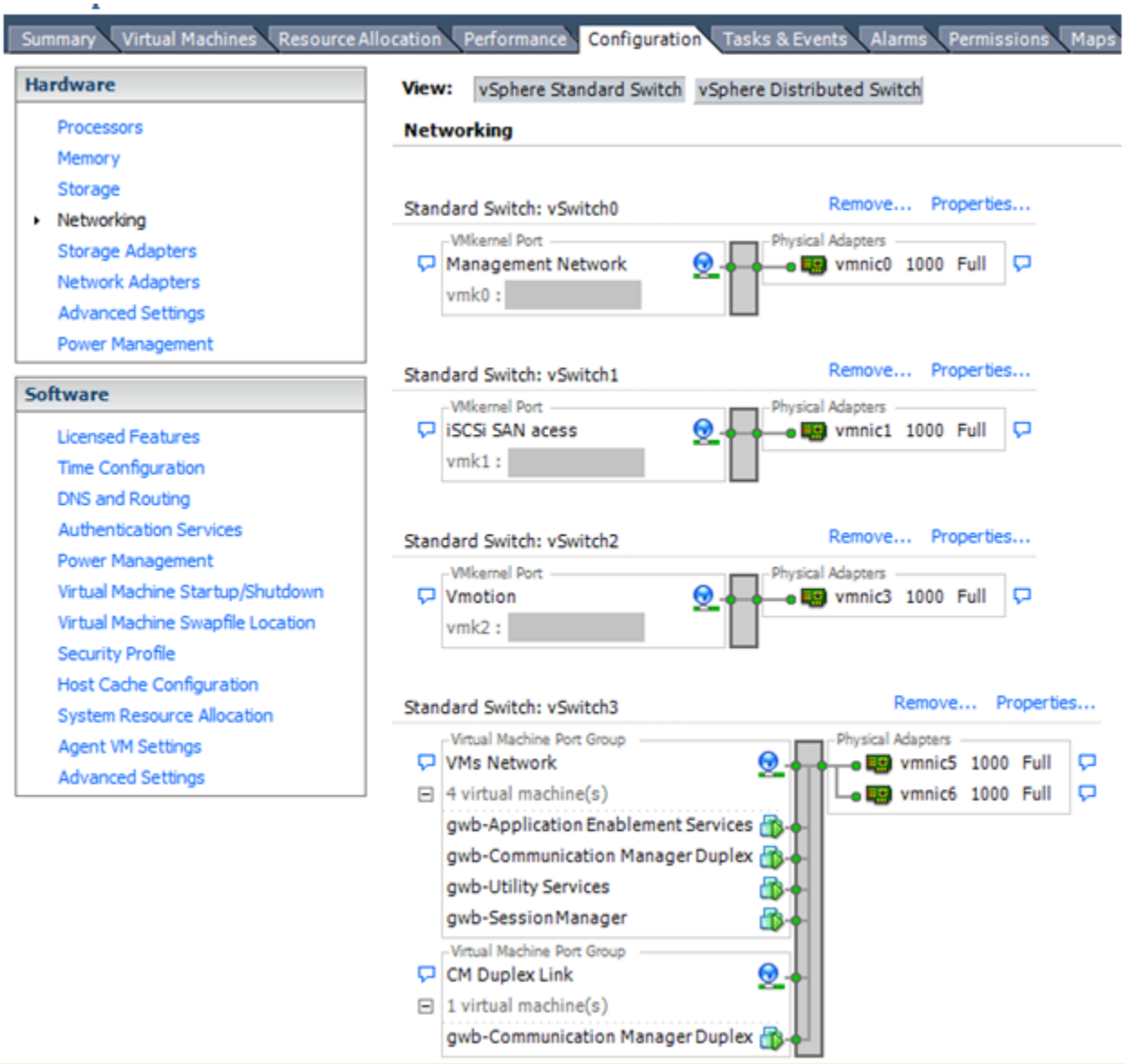
This section is not a substitute for the actual VMware documentation. If you do not have experience networking with VMware, you must review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network supporting applications deployed on VMware Hosts.

- Separate network services to achieve greater security and performance. Create a vSphere standard or distributed switch with dedicated NICs for each service to achieve greater security and performance. If separate switches are not possible, consider port groups with different VLAN IDs.
- The vMotion connection must be located on a separate network that is devoted to vMotion

- To protect sensitive VMs, deploy firewalls in the VM that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks to physical networks.
- Specify VM NIC hardware type **vmxnet3** for best performance. Avaya .ova files are built using **vmxnet3** by default.
- All physical NICs that are connected to the same vSphere standard or distributed switch must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).

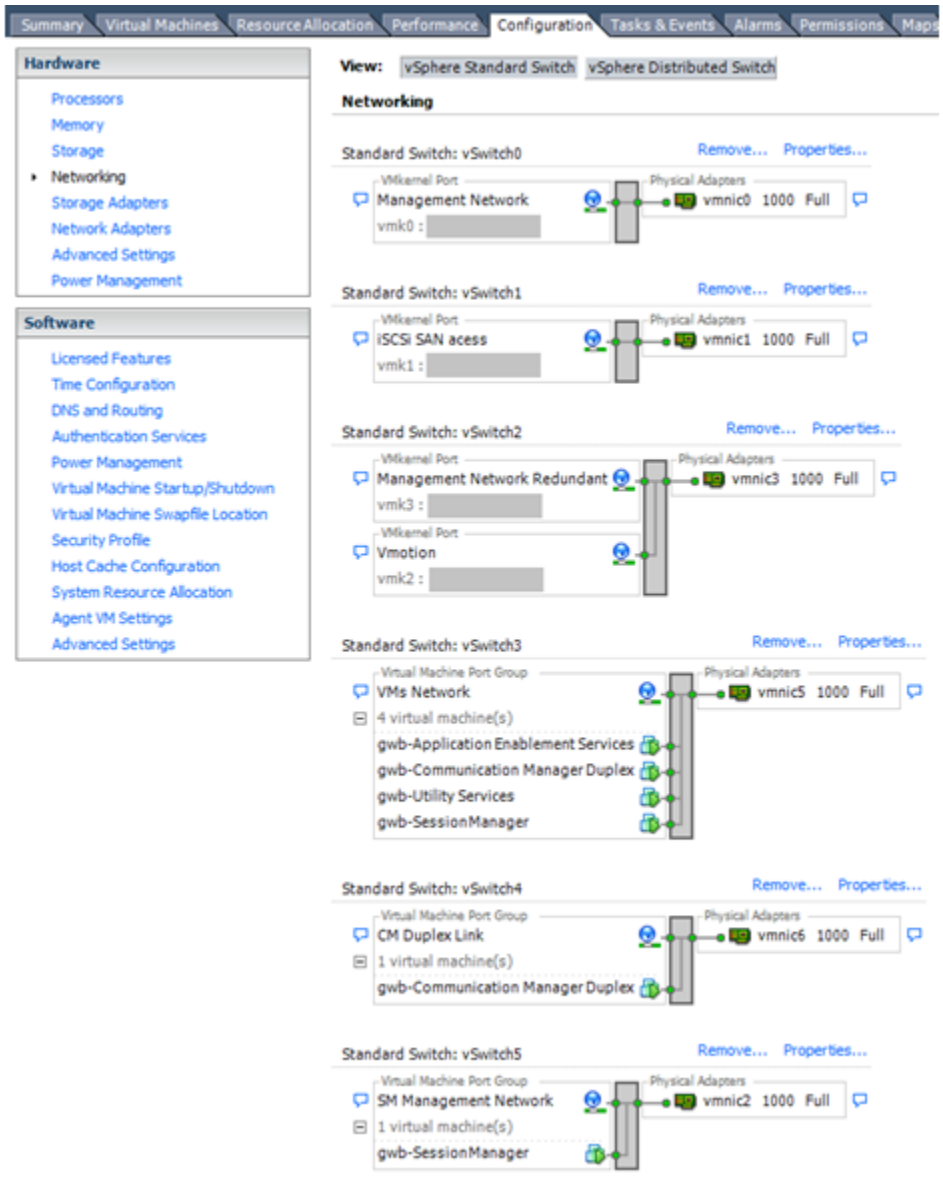
Networking Avaya applications on VMware ESXi — Example 1



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 VM 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 VMs Network. Load balancing provides additional bandwidth for the VMs 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. There are several methods of doing this, but Example 1 displays separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements, detailed in Avaya PSN003556u at https://downloads.avaya.com/css/P8/documents/100154621. Communication Manager software duplex connectivity minimum requirements are defined as:
  - 1 Gbps total capacity, or greater, with 50 Mbps of reserved bandwidth for duplication data
  - 8 ms round-trip delay, or less
  - 0.1% round-trip packet loss, or less
  - Both servers duplication ports are on the same IP subnet
  - Duplication link encryption must be disabled for busy-hour call rates that result in greater than 40% CPU occupancy (“list measurements occupancy”, Static + CP occupancy)
  - CPU occupancy on the active server (Static + CP) must be maintained at less than 65% to provide memory refresh from the active to standby server.
- Session Manager vNIC mapping: The Session Manager OVA defines four separate virtual NICs within the VM. However, this example shows all of those 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, it is possible to create a VLAN for the appropriate network.
- Virtual networking: Virtual machines which connect to the same vSwitch, as is the case in VMs Network of vSwitch 3, can communicate without ever entering the physical network. In other words, the network connectivity between these VMs is purely virtual. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi — Example 2



This configuration shows a more complicated situation, where more physical network interface cards are available for use. Highlights which differ from Example 1 include:

- VMware Management Network redundancy: In this example, a second VMkernel Port has been added to 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 VMs Network: This example removes the teamed physical NICs on vSwitch3, which was providing more bandwidth and tolerance of a single NIC failure in favor of reallocating this NIC to other workloads.

- Communication Manager Duplex Link: vSwitch4 has been dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network, which still follows the requirements described in PSN003556u.
- Session Manager Management Network: This example also shows the Session Manager Management network separated onto its own vSwitch, including a dedicated physical NIC which 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	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf
VMware vSphere Basics	http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.introduction.doc_50%2FGUID-F7A7E6C0-FA25-4806-8921-0438F1B2AEAE.html

Using multiple vSwitches to separate 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 VM or Hypervisor level. The result is like a Session Manager VM 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 solution, follow the below mentioned procedures:

Procedure

1. Create a vSwitch for dedicated Session Manager Security Module traffic.
2. From vSphere client inventory view, right-click the Session Manager VM 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

The general recommendation is to deploy thick disks which are *lazy-zeroed*. A lazy-zeroed thick disk has all space allocated at the time of creation, but each block is zeroed only on first write. The result is a shorter creation time but reduced performance the first time a block is written.

Some configurations require *eager-zeroed* thick disks, for example, Fault Tolerance (FT). An eager-zeroed thick disk

- has all space allocated and zeroed out at the time of creation.
- increases the time it takes to create the disk.
- results in the best performance, even on the first write to each block.

Thin provisioned disks:

- can grow to the full size specified at the time of the virtual disk creation but do not shrink. The blocks cannot be unallocated after the blocks have been allocated.
- 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, thin disks are a viable option. Otherwise, the general recommendation is to deploy thick disks.

Best Practices for VMware features

VMware High Availability

VMware High Availability is a viable option for Session Manager recovery in the VMware environment. When VMware HA has been configured on the ESXi host with Session Manager VM installed, failure of this ESXi host results in Session Manager being moved to a standby host. Once the cold boot of Session Manager on the standby host has completed, the host then continues to execute new call processing requests.

Note:

The following should be noted when configuring VMware HA:

- All VMs and their configuration files need to be on shared storage, e.g. Fibre Channel SAN, iSCSI SAN, or SAN iSCI NAS.
- The console network should have redundant network paths in order to have reliable failure detection for HA clusters. This is because 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 vMotion

VMware uses the vMotion technology to migrate a running Virtual Machine from one ESX host to another without incurring downtime. This process, known as a **hot-migration**, enables the live migration of running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

When you the use VMware vMotion, note the following:

- Ensure that each host that migrates VMs to or from the host uses a licensed vMotion and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure identical Port Groups 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. The snapshots are useful for short-term point-in-time copies of the running system before major upgrades or before patching the system.

Snapshots can:

- consume large amounts of data resources.
- cause increased CPU loads on the host.
- affect performance.
- affect service.

Due to these adverse behaviors, consider the following recommendations when using the snapshot feature.

- Snapshot operations can adversely affect service. The application that is running on the VM should be stopped or set to out-of-service before performing a snapshot operation. When the snapshot operation has completed, the application can then be restarted or brought back into service.
- 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.** Use no single snapshot for more than 24-72 hours. The recommended actions are to take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot as soon as the proper working state of the virtual machine is verified. Following the recommended actions prevents 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 length of time the host takes to write the memory onto the disk is relative to the amount of memory the virtual machine is configured to use and can add several minutes to the time it takes to complete the operation. If the snapshot is activated, saving memory will make calls appear to be active or in progress and can cause confusion to the user. When creating a snapshot, make sure that you
  - uncheck the **Snapshot the virtual machine's memory** check box in the **Take Virtual Machine Snapshot** window.
  - select the **Quiesce guest file system (Needs VMware Tools installed)** check box to make sure all writes to the disks have completed. It gives a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots over a long period of time, you must consolidate the snapshot files on a regular basis to improve performance and reduce disk usage. Before you can merge the snapshot delta disks back into the base disk of the VM, you must first delete stored snapshots.

Note:

In the event of a consolidate failure, 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 VM, a warning is presented in the UI.

Related resources

See the following resources for more information regarding snapshots:

Title	Web page
Best practices for virtual machine snapshots in the VMware environment	http://kb.vmware.com/kb/1025279
Understanding virtual machine snapshots in VMware ESXi and ESX	http://kb.vmware.com/kb/1015180
Working with snapshots	http://kb.vmware.com/kb/1009402
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	http://kb.vmware.com/kb/1018029
Consolidating snapshots in vSphere 5.x	http://kb.vmware.com/kb/2003638

Chapter 5: Deploying the Session Manager OVA

Deployment checklist

The Session Manager for VMware is packaged as a vAppliance that is ready for deployment using VMware vSphere Client or VMware vCenter. The following table lists the procedures required to deploy the Session Manager Open Virtual Application (OVA):

#	Action	Reference	✔
1	Ensure that the configuration prerequisites to deploy the Session Manager OVA are fulfilled.	Configuration Prerequisites on page 37	
2	Deploy the Session Manager OVA.	Deploying OVA on page 32	
3	Configure the Session Manager VM to start automatically after a power failure.	Configuring the virtual machine automatic start and stop settings on page 34	
4	Power On Session Manager.	Powering On on page 33	
5	Configure Session Manager	See *Chapter 6: Session Manager Configuration*.	
6	Perform checks to verify the deployment of the Session Manager OVA.	Checks and verifications on page 39	
7	Upgrade Session Manager to the latest service packs.	Upgrading on page 41	
8	Upgrade Session Manager VMware tools.	Upgrading VMware Tools on page 42	

Deploying Session Manager OVA

Procedure

1. To deploy the Session Manager OVA, in the vSphere client, select the host ESX server.
2. Click **File** > **Deploy OVF Template**.
   The vSphere client displays the Deploy OVF Template window.
3. To deploy the Session Manager OVF package, use one of the following options:
   - Click **Browse**, and provide the Session Manager OVA file location.
   - Enter the URL of the HTTP server where the Session Manager OVA file is located in the **Deploy from a file or URL** field.
4. Click **Next**.
   The OVF Template Details window displays.
5. Verify the details of the installed OVA template, and click **Next**.
   The End User License Agreement window displays.
6. To accept the license agreement, read the license agreement, and click **Accept**.
7. Click **Next**.
   The Name and Location window displays.
8. In the **Name** field, enter the name of the new virtual machine (VM).
9. Select the **Inventory Location** where you would like to have this VM reside by selecting the location from the inventory location tree.
10. If you do not have a host selected when you choose to **Deploy OVF Template**, the wizard prompts you for the host or cluster name to deploy the virtual appliance. Select the host or cluster to deploy the VM.
11. Click **Next**.
    The Storage window displays.
12. Select a destination storage for the virtual machine files and click **Next**. The datastore can be local to the host or a mounted shared storage, such as NFS or SAN. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.
    The Disk Format window displays.
13. Select **Thick Provision Lazy Zeroed**, and click **Next**.

    For more information about virtual disks, see Thin vs. thick deployments on page 27.

14. Session Manager contains three virtual network interface cards (SM NICs). The installation wizard prompts you to associate networks specified in the OVA with host networks. To choose a host network for each source network, perform the following steps:

    a. Click the **Destination Network** column.
    b. Click an entry in the drop-down menu.
    c. Click **Next**.

    For more information on how to administer host networks for source networks, see the following table:

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

    Note:

    - Source Networks are those networks defined in the OVF template. Source networks may contain 0 or more Network Interface Cards from the actual virtual machine. You must map networks defined by the OVF template to networks defined on the host, where virtual machine has been deployed. This assigns VM NICs to host networks. However, you can change these associations later.
    - Session Manager Services source network contains the Session Manager services port. It is generally recommended to map Session Manager Services source network to the same destination network as Session Manager Management.

15. Verify the deployment settings, and click **Finish**.
16. Check **Status** in the **Recent Tasks** window, and wait for the **Deploy OVF template** task, to show **Completed**.

Powering On Session Manager

About this task

Using the vSphere Client, perform the following steps:

Procedure

1. Select the deployed Session Manager VM from the list of VMs for the target host.
2. Click **Power On**.
3. Check in the Recent Tasks window for the Status of the **Power On virtual machine** task and, wait until this shows **Completed**.
4. Right-click the Session Manager virtual machine, and select **Open Console**. Wait for the Session Manager VM to finish booting up.

Configuring the virtual machine automatic start and stop settings

Configure the virtual machine to start automatically after a power failure or a restart of the hypervisor. The default is set to **no**.

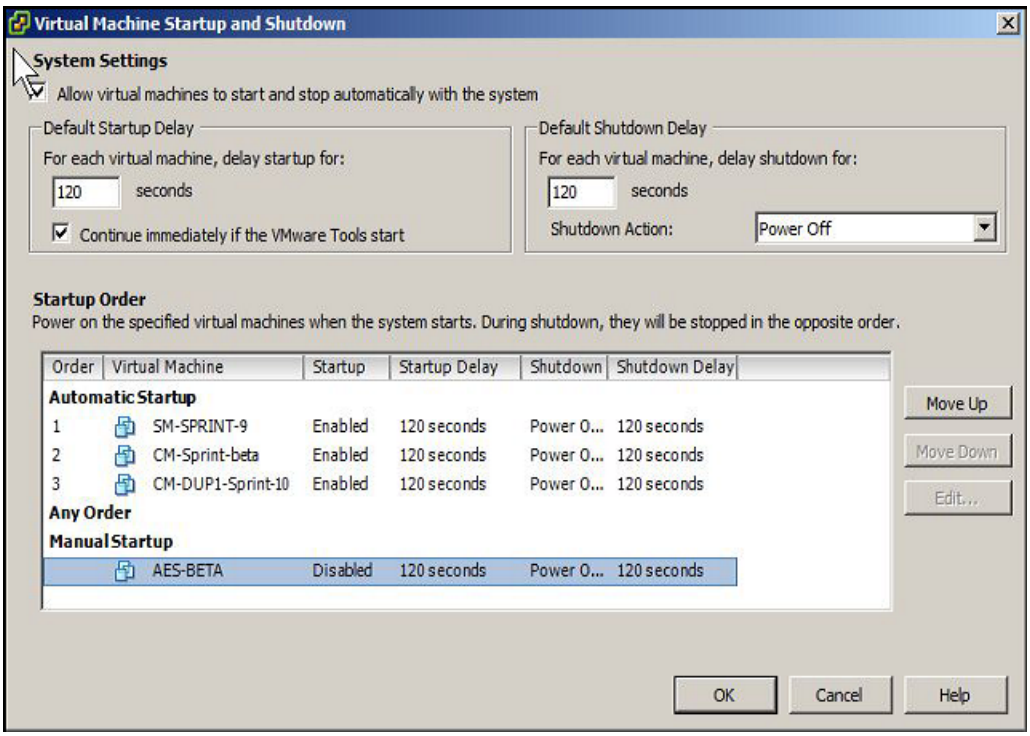
In high availability (HA) clusters, the VMware HA software ignores the Startup selections.

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 under **Automatic Startup**.
8. Click **OK**.

Example

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


Virtual Machine Startup and Shutdown
System Settings
Allow virtual machines to start and stop automatically with the system
Default Startup Delay
For each virtual machine, delay startup for:
120
seconds
Continue immediately if the VMware Tools start
Default Shutdown Delay
For each virtual machine, delay shutdown for:
120
seconds
Shutdown Action:
Power Off
Startup Order
Power on the specified virtual machines when the system starts. During shutdown, they will be stopped in the opposite order.
Order
Virtual Machine
Startup
Startup Delay
Shutdown
Shutdown Delay
Automatic Startup
1 SM-SPRINT-9 Enabled 120 seconds Power O... 120 seconds
2 CM-Sprint-beta Enabled 120 seconds Power O... 120 seconds
3 CM-DUP1-Sprint-10 Enabled 120 seconds Power O... 120 seconds
Any Order
Manual Startup
AES-BETA Disabled 120 seconds Power O... 120 seconds
Move Up
Move Down
Edit...
OK
Cancel
Help

Chapter 6: Session Manager Configuration

Configuration Prerequisites

Before configuring Session Manager, ensure that you configure System Manager. On System Manager, ensure that you:

- Configure the target Session Manager and create:
  - Session Manager instance in the **Session Manager Administration** module.
  - SIP entity in **Routing** module.
- Define Enrollment password.
- Define FQDNs for both System Manager and Session Manager , and configure either in the referenced DNS server(s) or add the FQDN for Session Manager to the hosts file of System Manager.

Configuring Session Manager

About this task

If you deployed Session Manager through vCenter, the installation wizard prompts you for the relevant configuration information during the deployment. This procedure enables you to reconfigure Session Manager, or to configure Session Manager without vCenter.

Using the vCenter vSphere Client or vSphere Client, configure Session Manager as follows:

Procedure

1. Right-click the Session Manager virtual machine, and select **Open Console**.
2. Login as **craft**.

   Note:

   If **SMnetSetup** is executed before, the craft login will be unavailable. Use the customer login instead.
3. Run the **SMnetSetup** script.

Note:

Ensure that, before you run the **SMnetSetup** script, you configure System Manager. For more information about how to configure System Manager and how to run the **SMnetSetup** script, see the book *Implementing Avaya Aura® Session Manager*, 03-603473, on the Avaya support website: http://support.avaya.com.

4. Ensure that System Manager is configured and available for the deployed Session Manager and then run the **SMnetSetup** script. See the book *Implementing Avaya Aura® Session Manager* for further details.
5. Enter the configuration data for the Session Manager.

Chapter 7: Post-installation verification

Checks and verifications

Perform the following checks and verifications after deployment:

1. On the System Manager console, view the Session Manager Administration page and verify if the field *SM on VMware* is selected. If the field is selected, then you can conclude that the Session Manager is running in a VMware environment, otherwise the Session Manager is running directly on a standard hardware based platform.
2. Execute the **`hardware_info`** command for a core Session Manager that is running on a VMware environment, and verify the hardware related details. This command provides the same status as when executed on an existing *non-VMware* core Session Manager with the following exceptions:
   - The **System Information** field shows as **VMware Virtual Platform**.
   - The **Raid Information** field shows as *N/A*.
   - The **Disk Information** field contains the linux path to the disk drive and the allocated size of the disk in GB.

   For more information about this command, see *Maintaining and troubleshooting Avaya Aura® Session Manager*.
3. Perform the following verifications:
   - Verify the connections of the deployed Session Manager.
   - Verify the data replication.

Related topics:

Verifying the connections on page 39

Verifying the connections

About this task

Using System Manager console, verify the connections of the deployed Session Manager:

Procedure

1. On the System Manager console, in the **Elements** section, click **Session Manager**.
2. In the left navigation pane, click **Dashboard** to open the Session Manager Dashboard page.
3. Verify that the Service State of the **Session Manager** instance is **Accept New Service**.
4. Else, select the **Session Manager** instance and click **Service State** > **Accept New Service**.
5. Verify that the **Security Module state** is **Up**.
6. Verify that the **Tests Pass** has a green tick.
   - On the System Manager console, in **Elements**, click **Session Manager**.
   - Click **System Tools** > **Maintenance Tests** to open the Maintenance Tests page.
   - Select the Session Manager instance and click **Execute All Tests**.

   Test Result for all tests should be Success.

Verifying Data Replication

Procedure

1. On the System Manager Web console, click **Services** > **Replication**.
2. Select the Session Manager instance and click **View Replica Nodes**.
3. Confirm that target Session Manager is **Synchronized** .

   Note:

   Synchronization Status should be green.

   - Else, select the Session Manager instance and click **Repair**.

Chapter 8: Maintenance Operations

Upgrading Session Manager

Before you begin

Before you use the newly deployed Session Manager VM, ensure that you:

- Take a snapshot of Session Manager.
- Upgrade the Session Manager software to the latest version.

For more information about how to take snapshots and how to upgrade the Session Manager software, see *Upgrading Avaya Aura Session Manager, 03-603518* at the Avaya support website: http://support.avaya.com. The high level steps for upgrading Session Manager are:

Procedure

1. Change the service state to **Deny New Service** for Session Manager.
   Wait for the Active Call Count to display zero.
2. Upgrade the operating system of Session Manager.
3. Upgrade the Session Manager software.
4. Install an **Authentication** file.
5. Verify that replication is working between System Manager and the Session Manager.
6. Test the Session Manager server.
7. Change the service state of the upgraded Session Manager to **Accept New Service**.

   ⚠ Warning:

   Session Manager might upgrade kernels during the upgrade process, which might cause errors with the VMware tools. If you lose network connectivity, then upgrade the VMware Tools as per the topic Upgrading VMware Tools on page 42.

Related topics:

Upgrading Session Manager VMware Tools on page 42

Upgrading Session Manager VMware Tools

About this task

Session Manager service packs might upgrade kernels along with the virtual machine during the upgrade process, which might cause loss of network connectivity due to incorrect drivers. This procedure provides information on how to upgrade the VMware tools using the vCenter vSphere client or the vSphere client.

Procedure

1. Right-click the target Session Manager VM.
2. On the **Guest** menu, click **Install/Upgrade VMware Tools**.
3. From the pop-up window, select **Automatic Tools Upgrade**.
4. Click **OK**.
5. Check in the Recent Tasks window for the status of the **Initiated VMware Tools install or upgrade** task, and wait until the status displays **Completed**.
6. To access the Session Manager virtual machine console, right-click the virtual machine, and click **Open Console**.
7. As root, run: **`service network restart`**.
   Once the command completes, network connectivity is restored.

Session Manager Service Pack and patch updates

For details about how to apply service pack and patch updates to Session Manager, see *Installing Service Packs for Avaya Aura® Session Manager*, at 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.

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 the topic *Session Manager VMware Tools upgrade*.

Session Manager Backup and Restore

The native System Manager backup and restore function should be used for the long-term backup and recovery of the Session Manager VM data when running on VMware.

For more information about Session Manager backup and restore, see the book *Administering Avaya Aura Session Manager, 03-603324* at the Avaya support website: http://support.avaya.com.

This activity should be scheduled to run periodically in the same way as would be done for a standard physical deployment.

Note:

This procedure only backs up administration data.

Migrating Session Manager

About this task

This procedure provides high level steps for migrating hardware Session Manager to VMware based Session Manager. VMware Session Manager copies the entire identity of the hardware Session Manager, including IP addresses, hostname, and other parameters.

Note:

Capacities for the hardware Session Manager differ from the VMware-based Session Manager. Before attempting a migration, verify that the load capacity of VMware Session Manager is compatible with the hardware based Session Manager.

See the book *Implementing Avaya Aura® Session Manager* for details regarding migration procedures.

The high level steps for migrating Session Manager are:

Procedure

1. Change the service state to **Deny New Service** for the active hardware instance of Session Manager.

   Wait for the Active Call Count to display zero.
2. Power down the active hardware instance of Session Manager.
3. Run **SMnetSetup** on the VMware instance of Session Manager.
4. Install an **Authentication** file.

5. Verify that replication is working between System Manager and the Session Manager.
6. Test the Session Manager server.
7. Change the service state of the upgraded Session Manager to **Accept New Service**.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

A product-change notice (PCN) is issued in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. A product-support notice (PSN) is issued when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both of these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, click **DOWNLOADS & DOCUMENTS**.
3. On the Downloads & Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select **Documents** as the content type.
6. Select the appropriate filters as per your search requirement. For example, selecting Product Support Notices will display only product support notices in the documents list.

Note:

You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. This proactive notification system is performed by the Avaya E-Notifications process.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications as per the steps indicated in the **How to set up your E-Notifications** procedure.

Glossary

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 many virtual machines, each with its virtualized applications. Some of the servers are staged with the OS and application software installed. Some of the servers are sold as just the server with DVD or software downloads.
Avaya Services VM	A virtual machine that supports Avaya services applications. Currently, the services virtual machine is part of System Platform which uses a non-VMware hypervisor.
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.
DRS	Distributed Resource Scheduler. A VMware feature that intelligently places workloads based on available virtual resources.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
FT	Fault Tolerance. A VMware feature that provides a call preserving failover when the primary computer resource fails.
HA	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.
Hypervisor	A hypervisor is also known as Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique that 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 Application. An OVA is the virtual machine description, disk images, and a manifest zipped into a single file. An OVA follows the Distributed Management Task Force (DMTF) specifications.
OVF	Open Virtualization Format. Similar to an OVA. An OVA contains a single virtual machine. An OVF can contain multiple virtual machines. An OVF contains the descriptions and disk images for each included virtual machine as well as the manifest.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
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	Capture a virtual applicance configuration in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
SRM	Site Recovery Manager. A VMware feature that provides a disaster recovery option to a secondary data center.
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	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.
vSphere	The hypervisor that VMware provides. Similar to an operating system.

Index

A

Avaya applications 22
networking 22
Avaya Mentor videos 7

B

best practices 19
performance 19
BIOS 19
BIOS for Dell servers 20
BIOS for HP servers 20

C

capacity limits 15
checklist 13, 31
deployment procedures 31
planning procedures 13
clock source 20
components 11
VMware 11
configuration data 14
customer 14
configuring Session Manager 37
courses 7
customer configuration data 14

D

Deploying 32
Open Virtual Application 32
OVA 32
deployment 27
thick 27
thin 27
deployment procedures 31
checklist 31
document purpose 5
documentation 5

I

Intel VT support 19
intended audience 5

L

legal notice .....

M

migrating Session Manager 43
multiple vSwitches 26

N

networking Avaya applications 22
networking best practices 22

O

overview 9

P

PCN 45
PCN notification 45
PCNs 45
performance best practices 19
planning procedures 13
checklist 13
Power On Session Manager 33
prerequisites 37
PSN 45
PSN notification 45
PSNs 45
purpose of document 5

R

related documentation 5
related resources 7
Avaya Mentor videos 7
requirements 15, 17
software 17
virtual machine resources 15
resource requirements 15
resources 14

server and hardware 14

S

server hardware and resources 14
Service Packs and Patches 42
Session Manager 43
backup 43
restore 43
Session Manager VM 42
signing up for PCNs and PSNs 46
snapshots 29
software requirements 17
storage 27
support 7
contact 7

T

thick deployment 27
thin deployment 27
time keeping 20
training 7

U

upgrading Session Manager 41
upgrading VMware Tools 42

V

version 17
VMware 17
videos 7
Avaya Mentor 7
virtual machine 34
shutdown setting 34
startup setting 34
virtual machine resource requirements 15
vMotion 28
VMware High Availability 28
VMware Tools 22
VMware version 17
supported 17
VT support 19