Deploying Avaya Aura® Utility Services on VMware® in Virtualized Environment

Release 6.3
Issue 4
June 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- 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.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.
- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

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

Purpose

This document provides installation, configuration, initial administration, and basic maintenance checklists and procedures.

Intended audience

This document is intended for people who install and configure a verified reference configuration at a customer site.

Document changes since last issue

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

- Updated the topic Software requirements on page 20 to include VMware vSphere ESXi 5.5 and VMware vCenter Server 5.5.
- Updated the topic VMware software requirements on page 20 to include VMware vSphere ESXi 5.5 and VMware vCenter Server 5.5.

Related resources

Documentation

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

Title	Description	Audience
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.	Sales Engineers
Administration		
Accessing and Managing Avaya Aura® Utility Services, 03-603628	Describes procedures for managing the features that are part of Utility Services. Features include IP phone settings, ADVD Settings, IP phone firmware management, log viewer, CDR tools, and Enhanced System Directory	Sales Engineers, Solution Architects, Implementation Engineers, 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
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
Docu00158	Whats New in Avaya Aura® Release 6.2 Feature Pack 2
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs

Course code	Course title
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
4U00115I, 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

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

About this task

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

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

Note:

Videos are not available for all products.

Support

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 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 Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. 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
Avaya Collaboration Pod for Enterprise Communications – Technical Solutions Guide	Provides an overview of the solution, specifications, and components that Avaya Collaboration Pod for Enterprise Communications integrates.
Avaya Collaboration Pod for Enterprise Communications – Pod Orchestration Suite User Guide	Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Collaboration Pod. This guide explains how to access and use the applications in the POS management suite.
Avaya Collaboration Pod for Enterprise Communications – Locating the latest product documentation	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.
Avaya Collaboration Pod for Enterprise Communications – Release Notes	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.

Deployment guidelines

The high-level deployment steps are:

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

The deployment guidelines for the virtual appliances are:

- Deploy as many virtual appliances on the same host as possible.
- Deploy the virtual appliances on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as Avaya Aura® applications, from other virtual machines.
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.

- Do not oversubscribe resources. Oversubscribing affects performance.
- Monitor the server, host, and virtual appliance performance.

Important:

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

Chapter 3: Planning and configuration

Planning

You must ensure that the customer has completed the following steps before deploying the virtual appliance:

#	Action	Notes	✔
1	No license is required for Utility Services. However, the Remote Feature Activation (RFA) authentication file must be downloaded from AFS system and stored at a location from where a computer running the vSphere client can access the file.		
2	Minimum of one ESXi host release 5.0 or later is required. The host must have at least one GB of RAM and 20 GB of storage.		
3	The Utility Services OVA file must be downloaded from http://plds.avaya.com and stored at a location from where a computer running the vSphere client can gain access to the file.	For information about downloading the ova file, see Downloading software from PLDS on page 18.	
4	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation. Make sure the license file copies are accessible.		

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.

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.

Utility Services virtual machine resource requirements

The following resources must be available on the ESXi host before deploying the Utility Services virtual machine:

VMware resource	Value
CPU core	1
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHZ
CPU Reservation	n/a
Memory	1 GB
Memory reservation	n/a
Storage reservation	20 GB
Shared NICs	One @ 1000 Mbps
Network Utilization	5 Mbps
IOPS	60

Note:

In the customer environment, performance of Utility Services might vary from the average results.

Software requirements

Utility Services Release 6.2 and later can be deployed on VMware vSphere Release 5.0, VMware vSphere Release 5.1, or VMware vSphere Release 5.5. VMware vSphere Release 4.1 does not support Utility Services. The Utility Services VMware virtualization environment is packaged as a virtual appliance ready for deployment on the VMware-certified hardware. The following table lists the software requirements:

Equipment	Software Release
VMware vCenter Server	5.0, 455964 or 5.1, 799730 or 5.5, 1623101
VMware vSphere Client	5.0, 469512 or 5.1, 786111 or 5.5, 1623387
VMware ESXi Host	5.0, 469512 or 5.1, 799733 or 5.5, 1623387
VMware Studio	2.6.0.0, 631426
VMware Tools	9.0.0.15210, 782409
Avaya Aura® Utility Services	6.3.0.0

VMware software requirements

Avaya Aura® Utility Services in a 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.

Chapter 4: Deploying and configuring Utility Services Open Virtual Application

You must use one of the following methods to deploy and configure Utility Services Open Virtual Application (OVA):

- Direct deployment on the ESXi host through the vSphere client
- Deployment on vCenter through the vSphere client

Deployment of cloned and copied OVAs

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

Deployment and configuration on the ESXi host through the vSphere client

Deploying the Utility Services OVA

Procedure

1. Open the vSphere client.
2. In the vSphere client, enter the IP address of the vCenter server and the login credentials.
3. On the **File** menu, select **Deploy OVF Template**.
4. To select the file for deployment, use one of the following methods:

- If the OVA file is downloaded at a location accessible from your computer, click **Browse** and select the file. Click **Next**.
- If the OVA file is located on an HTTP server, enter the URL in the **Deploy from a file or URL** field. Click **Next**.

5. Verify the template details, and click **Next**.
6. Accept the End User License Agreement (EULA). Click **Next**.
7. In the **Name** field, assign a name of maximum 80 characters to the new virtual machine. Click **Next**.
8. Select the location to store the virtual machine files. Click **Next**.
9. Select **Thick Provision Lazy Zeroed** as the virtual disk format. Click **Next**.
   For more information about virtual disks, see Thin vs. thick deployments.
10. Verify the deployment settings and click **Finish**.

Related topics:

Thin vs. thick deployments on page 49

Configuring the Utility Services OVA

Procedure

1. In the vSphere Client, select the Utility Services virtual machine.
2. Click the **Getting Started** tab.
3. Click **Power on the virtual machine**.
4. Click the **Console** tab.
5. Log in to an account with administrative privileges.
6. Run the **`/opt/vsp/VMware_conf.sh`** command.
7. When the system prompts to continue, enter `y`.
8. Enter the values for the following network entities:
   a. Default Gateway
   b. Hostname
   c. DNS
   d. IP address allocation for eth0

   For more information about the fields, see *Properties field descriptions*.
9. To configure the timezone settings, select the region and the local area.

10. Enter the IP address of Communication Manager used for the Utility Services virtual machine.
11. Enter the IP address of the primary NTP server to be used for the Utility Services virtual machine.
12. The system installs the default authentication file. You must replace the file with the authentication file that you downloaded from RFA. For more information, see Installation of the RFA Authentication file on Utility Services.

Related topics:

Properties field descriptions on page 23
Installation of the RFA Authentication file on Utility Services on page 27

Properties field descriptions

Name	Description
Default Gateway	The IP address of the default gateway.
Hostname	The Linux hostname for the Utility Services virtual machine.
DNS	The IP address of the Domain Name System (DNS) server.
IP address allocation for eth0	The IP address of Utility Services.

Deployment and configuration on vCenter through the vSphere client

Deploying the Utility Services OVA

Procedure

1. Open the vSphere client.
2. In the vSphere client, enter the IP address of the host ESXi server and the login credentials.
3. On the **File** menu, select **Deploy OVF Template**.

4. To select the file to be deployed, use one of the following methods:
   - If the OVA file is downloaded at a location accessible from your computer, click **Browse** and select the file. Click **Next**.
   - If the OVA file is located on an HTTP server, enter the URL in the **Deploy from a file or URL** field. Click **Next**.
5. On the OVF Template Details screen, verify the template details, and click **Next**.
6. On the End User License Agreement screen, accept the End User License Agreement (EULA). Click **Next**.
7. On the Name and Location screen, in the **Name** field, assign a name of maximum 80 characters to the deployed template. Click **Next**.
8. Select the location to store the virtual machine files. Click **Next**.
9. On the Disk Format screen, select **Thick Provision Lazy Zeroed** as the virtual disk format. Click **Next**.

   For more information about virtual disks, see *Thin vs. thick deployments*.
10. On the Network Mapping screen, verify the network interface that the OVF template uses and click **Next**.
11. On the IP Address Allocation screen, select an allocation scheme to allocate IP addresses. You must select **Fixed**.

    Note:

    DHCP is not supported for Virtual Environment installation.
12. Select the IP Protocol, and click **Next**.
13. On the Properties screen, complete the following fields:
    a. In the Application section, complete the following fields:
       - **Communication Manager IP**
       - **Hostname**
       - **Timezone**
       - **NTP Server IP**

    b. In the Networking section, complete the following fields:
       - **Default Gateway**
       - **DNS**
       - **Network 1 IP Address**
       - **Network 1 Netmask**

    For more information about the fields, see *Properties field descriptions*.

14. On the Ready to Complete screen, verify the deployment settings and click **Finish**.

Related topics:

Viewing the status of the NTP server on page 28
Thin vs. thick deployments on page 49

Configuring the Utility Services OVA

Procedure

1. In the vSphere Client, select the Utility Services virtual machine.
2. Click the **Getting Started** tab.
3. Click **Power on the virtual machine**.
4. Click **Edit Virtual Machine Settings**. The system displays a new window containing the details of the Utility Services virtual machine.
5. Click the **Options** tab.
6. Click **Properties**.
7. On the Properties screen, complete the following fields:
   a. In the Application section, complete the following fields:
      - **Communication Manager IP**
      - **Hostname**
      - **Timezone**
      - **NTP Server IP**
   b. In the Networking section, complete the following fields:
      - **Default Gateway**
      - **DNS**
      - **Network 1 IP Address**
      - **Network 1 Netmask**

   For more information about the fields, see *Properties field descriptions*.
8. Click **OK**.
9. The system installs the default authentication file. You must replace the default authentication file with the authentication file that you have downloaded from RFA.

For more information, see Installation of the RFA Authentication file on Utility Services.

Related topics:

Properties field descriptions on page 26
Installation of the RFA Authentication file on Utility Services on page 27
Viewing the status of the NTP server on page 28

Properties field descriptions

Name	Description
Communication Manager IP	The IP address of Communication Manager used for CDR collection, MyPhone, and Phone Firmware Manager.
Hostname	The Linux hostname.
Timezone	The Linux standard timezone to be applied to the Utility Services virtual machine.
NTP Server IP	The IP Address of the primary Network Time Protocol (NTP) server for the Utility Services virtual machine.
Default Gateway	The IP address of the default gateway.
DNS	The IP address of the Domain Name System (DNS) server.
Network 1 IP Address	The IP Address of the Utility Services virtual machine.
Network 1 Netmask	The IP address of the subnet mask.

Related topics:

Viewing the status of the NTP server on page 28

Installation of the RFA Authentication file on Utility Services

You must use one of the following methods to install the RFA Authentication file:

- Through the vSphere client
- Through the Utility Services webpage

Installing the RFA Authentication file through the vSphere client

Procedure

1. In the vSphere Client, select the Utility Services virtual machine.
2. Click the **Getting Start** tab.
3. Click **Power on the virtual machine**.
4. Click the **console** tab.
5. Log in with administrative privileges.
6. Rename the authentication file to *asg_auth_file.xml* using the `mv source destination` command, where *source* is the authentication file name.
7. Use **scp** or **WinSCP** to transfer files. For more information about transferring files using **WinSCP**, see *Transferring files using WinSCP*.

   You can use the **scp** command to copy the authentication file to the Utility Services virtual machine. You must download the following programs to enable **scp**:

   - Pscp.exe
   - WinSCP
8. Depending on the privilege of the account, move the authentication file that is currently in the default home directory to either the **/tmp** directory or **/opt/vsp** directory. Type the `mv source destination` command and press enter.
9. Type**/opt/vsp/vami_set_asg** and press enter.
10. The system installs the file immediately. You do not need to reboot the system.

Related topics:

Transferring files using WinSCP on page 40

Installing the RFA Authentication file through the Utility Services Web page

Procedure

1. Use an account with the administrator privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) Web page.
2. Click **Utilities** > **Utility Admin**.
3. In the navigation pane, in the **Miscellaneous** section, click **Upload Files**.
4. Click **Browse**, and select the RFA Authentication file.

   The name of the file must be **asg_auth_file.xml**.
5. Click **Upload File**.
6. In the navigation pane, in the **Miscellaneous** section, click **RFA License Activation**.

   The **A Valid Authentication File is currently** field must show Available. If the file is missing or has an incorrect name, the **A Valid Authentication File is currently** field shows Not Available.
7. Click **Activate the Authentication File**.

   The activation is immediate and applies to all the future login attempts.

Viewing the status of the NTP server

Procedure

1. Use an account with administrator-level privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) Web page.
2. Click **Utility Services** > **Utility Admin**.
3. In the navigation pane, in the **Miscellaneous** section, click **NTP Status**.

   On the NTP Synchronization Status page, the system displays:

   - The status of the NTP server.
   - The estimated accuracy of the clock.
   - An indication of the delay to the next polling interval.

- The status of the NTP Peer servers.

Chapter 5: Configuration

Configuring the virtual machine automatic startup settings

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

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

Before you begin

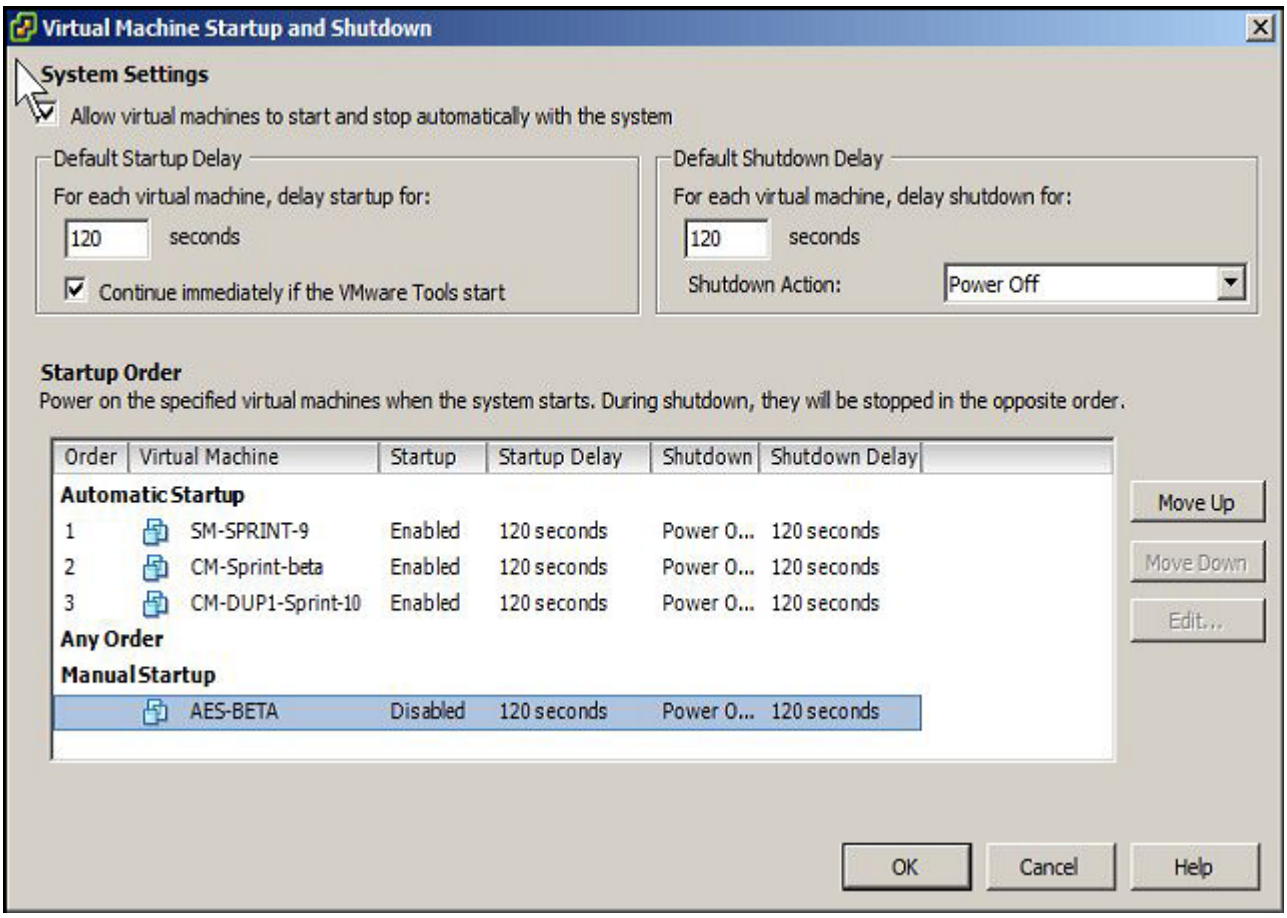
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

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

Example

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



Post deployment reconfiguration

With the post deployment reconfiguration, you can modify the parameters of the Utility Services OVA after initial deployment. You can modify the network parameters such as, IP address, Hostname, and DNS, and application parameters such as, Communication Manager IP Address.

Use one of the following methods to reconfigure Utility Services OVA:

- Through the ESXi host
- Through vCenter

Related topics:

Reconfiguring the Utility Services OVA through the ESXi host on page 33
Reconfiguring the Utility Services OVA through vCenter on page 34

Reconfiguring the Utility Services OVA through the ESXi host

About this task

The reconfiguration can be carried out at any time and the changes takes effect immediately.

Procedure

1. In the vSphere Client, select the Utility Services virtual machine.
2. Click the **Getting Started** tab.
3. Click **Power on the virtual machine**.
4. Click the **Console** tab.
5. Log in to an account with administrative privileges.
6. Run the **`/opt/vsp/VMware_conf.sh`** command.
7. When the system prompts to continue, enter `y`.
8. Enter the values for the following network entities:
   a. Default Gateway
   b. Hostname
   c. DNS
   d. IP address allocation for eth0

   For more information about the fields, see *Properties field descriptions*.
9. To configure the timezone settings, select the region and the local area.
10. Enter the IP address of Communication Manager used for the Utility Services virtual machine.
11. Enter the IP address of the primary NTP server to be used for the Utility Services virtual machine.
12. The system installs the default authentication file. You must replace the file with the authentication file that you downloaded from RFA. For more information, see Installation of the RFA Authentication file on Utility Services.

Related topics:

Properties field descriptions on page 23
Installation of the RFA Authentication file on Utility Services on page 27

Reconfiguring the Utility Services OVA through vCenter

About this task

When the virtual machine is running, the system displays the properties as read-only. Therefore, you must stop the virtual machine to make any changes. The changes take effect on starting the virtual machine.

Procedure

1. In the vSphere Client, select the Utility Services virtual machine.
2. Click the **Getting Started** tab.
3. Click **Power on the virtual machine**.
4. Click **Edit Virtual Machine Settings**. The system displays a new window containing the details of the Utility Services virtual machine.
5. Click the **Options** tab.
6. Click **Properties**.
7. On the Properties screen, complete the following fields:
   a. In the Application section, complete the following fields:
      - **Communication Manager IP**
      - **Hostname**
      - **Timezone**
      - **NTP Server IP**
   b. In the Networking section, complete the following fields:
      - **Default Gateway**
      - **DNS**
      - **Network 1 IP Address**
      - **Network 1 Netmask**

   For more information about the fields, see *Properties field descriptions*.
8. Click **OK**.
9. The system installs the default authentication file. You must replace the default authentication file with the authentication file that you have downloaded from RFA. For more information, see Installation of the RFA Authentication file on Utility Services.

Related topics:

Properties field descriptions on page 26
Installation of the RFA Authentication file on Utility Services on page 27

Chapter 6: Maintenance

Upgrading the Utility Services virtual machine

Procedure

1. Create a backup including the IP firmware of the existing Utility Services virtual machine on your local machine. For more information about creating a backup, see *Creating a backup of Utility Services*.

   Note:

   For a Utility Services Release 6.3 upgrade, while creating a backup of the previous release, you must exclude the IP phone firmware.

2. Stop the old Utility Services virtual machine.
3. Deploy and configure the new Utility Services virtual machine. For more information about deploying and configuring, see *Deploying and configuring Utility Services Open Virtual Application*.
4. Start the new Utility Services virtual machine.
5. Log in to the new Utility Services virtual machine.
6. Restore the local backup on the new Utility Services virtual machine. For more information on restoring a backup, see *Restoring a backup of Utility Services*.

Related topics:

Deploying and configuring Utility Services Open Virtual Application on page 21
Creating a backup of Utility Services on page 39
Restoring a backup of Utility Services on page 39

Updating patches and service packs

Procedure

1. Use an account with administrator-level privileges to log in to the Utility Services command-line interface.
2. Copy the patch or service pack to the **/tmp** directory. **scp** is the preferred method. However, some errors might occur because System Domain (Domain-0) and Console Domain support only **scp** and most laptops do not support **scp**.

   To enable **scp**, you must download the following programs :

   - Pscp.exe
   - WinSCP
3. Use the **/opt/vsp/update** command to update the patch. You can enter the following arguments with this command. If you do not enter any arguments, the system displays a usage list.
   - -i : to install a patch or a service pack. The patch or service pack must be in /tmp directory.
   - -r <patchnumber>: to remove a patch or service pack.
   - -l: to list all installed patches and service packs.
   - -q <patchnumber>: to view the contents of the specified patch or service pack.

Backup and restore

Use the local backup and restore function of Utility Services for the long-term backup and recovery of the Utility Services data when running on VMware. You must schedule the backup and restore function to run periodically.

Include/Exclude IP Firmware option

You can choose to include or exclude the IP Firmware option while creating backups. By default, the IP Firmware option is included for backups. If you exclude the IP Firmware option, the backup process is much quicker and generates a smaller backup file. However, for any disaster recover procedures, you must have at least one backup with IP Firmware included.

Disaster Recovery

If the Utility Services virtual machine fails completely, you can redeploy the OVA with the same settings used originally and restore a full backup to regain full functionality.

Creating a backup of Utility Services

Procedure

1. Use an account with administrator-level privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) webpage.
2. Click **Utility Services** > **Utility Admin**.
3. In the navigation pane on the left side of the page, click **Miscellaneous** > **Utility Services Backup and Restore**.
4. Use one of the following methods to create a backup:
   - To include the IP firmware in backup, click **Include Firmware in Backup**.
   - To exclude the IP firmware in backup, click **Exclude Firmware in Backup**.
5. Click **Create Backup**.
   The system creates a backup file.
6. The system displays the name and the location of the backup file.
7. Click **Download the newly created Utility Services Backup File** to save the backup file to the local machine.
8. Click **Continue**.

Restoring a backup of Utility Services

Procedure

1. Use an account with administrator-level privileges to log on to the Avaya Aura® Utility Services System Management Interface (SMI) webpage.
2. Click **Utility Services** > **Utility Admin**.
3. In the navigation pane on the left side of the page, click **Miscellaneous** > **Utility Services Backup and Restore**.

4. Click **Browse** and select the backup file that you want to restore from the local machine.
5. Click **Upload Backup**.

   The system restores the backup file.
6. Click **Continue**.

Transferring files using WinSCP

Transfer files using the WinSCP utility from a remote system to the virtual machine. WinSCP is a SFTP client and FTP client for Windows. The main function of WinSCP is to securely transfer files between a local and a remote computer. WinSCP uses Secure Shell (SSH) and supports Secure FTP and legacy SCP protocol.

Before you begin

Ensure that WinSCP is installed on your computer. WinSCP is available as a download from the Internet.

Procedure

1. Use WinSCP to connect to the virtual machine.
2. Enter the credentials for SCP access.
3. Click OK or Continue as necessary in the warning dialogue boxes.
4. Change the file transfer protocol from SFTP to SCP.
5. Click Browse to locate and select the file.
6. In the WinSCP destination machine window, browse to /home/.
7. Select **/home/customerloginname** as the destination location for the file transfer. This is likely to be the first destination when WinSCP opens.
8. Click and drag the file from the WinSCP source window to **/home/customerloginname** in the WinSCP destination window.
9. Click the WinSCP Copy button to start the file transfer.
10. When the copy completes, close the WinSCP window and click OK.

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

Related topics:

Intel Virtualization Technology on page 41
Dell PowerEdge Server on page 42
HP ProLiant Servers on page 42

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

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

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings

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

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

Dell PowerEdge Server

When the Dell server starts, press F2 to display the system setup options.

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

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

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

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

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

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest

operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

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

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

VMware networking best practices

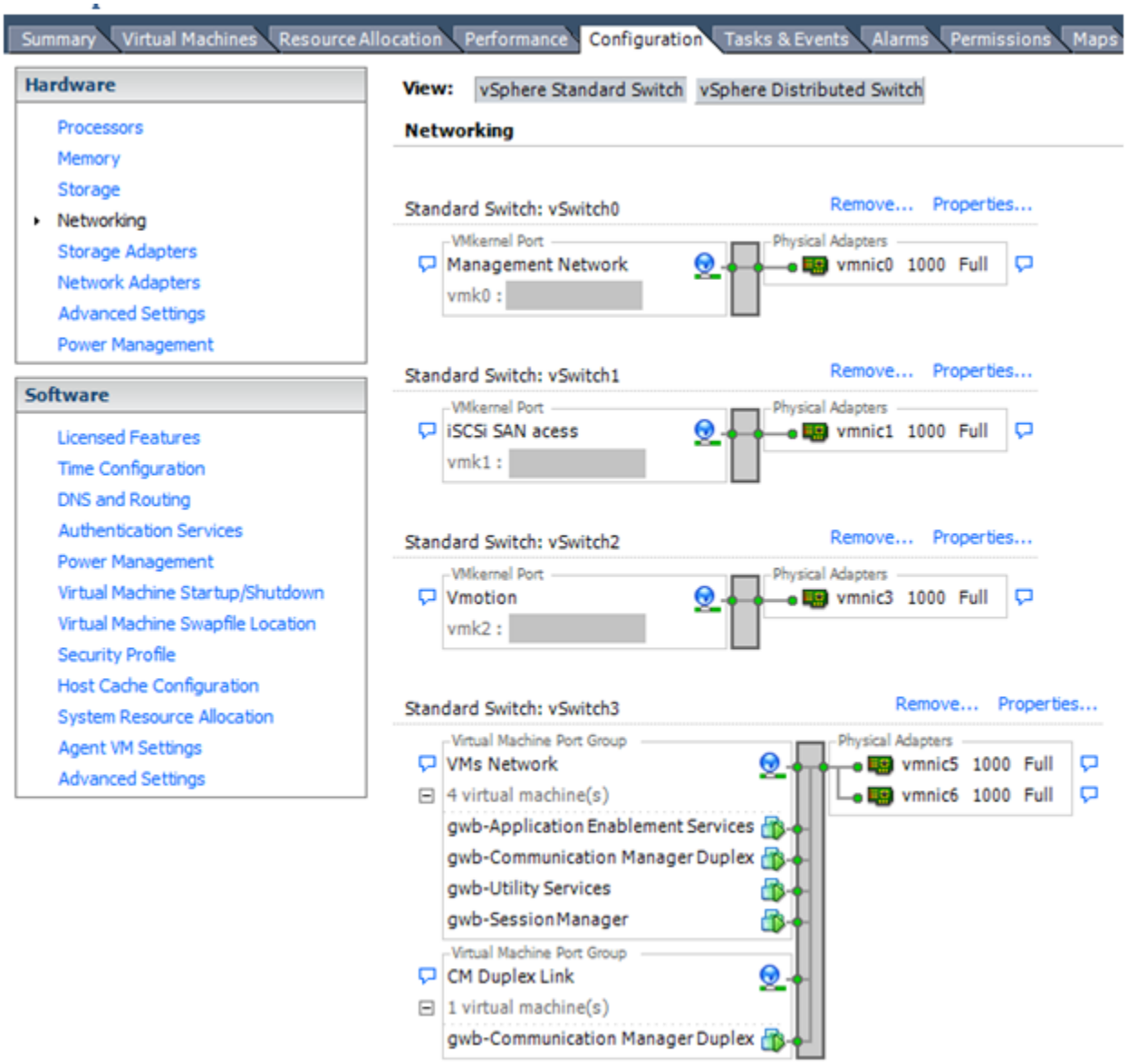
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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

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

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

Networking Avaya applications on VMware ESXi – Example 1



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

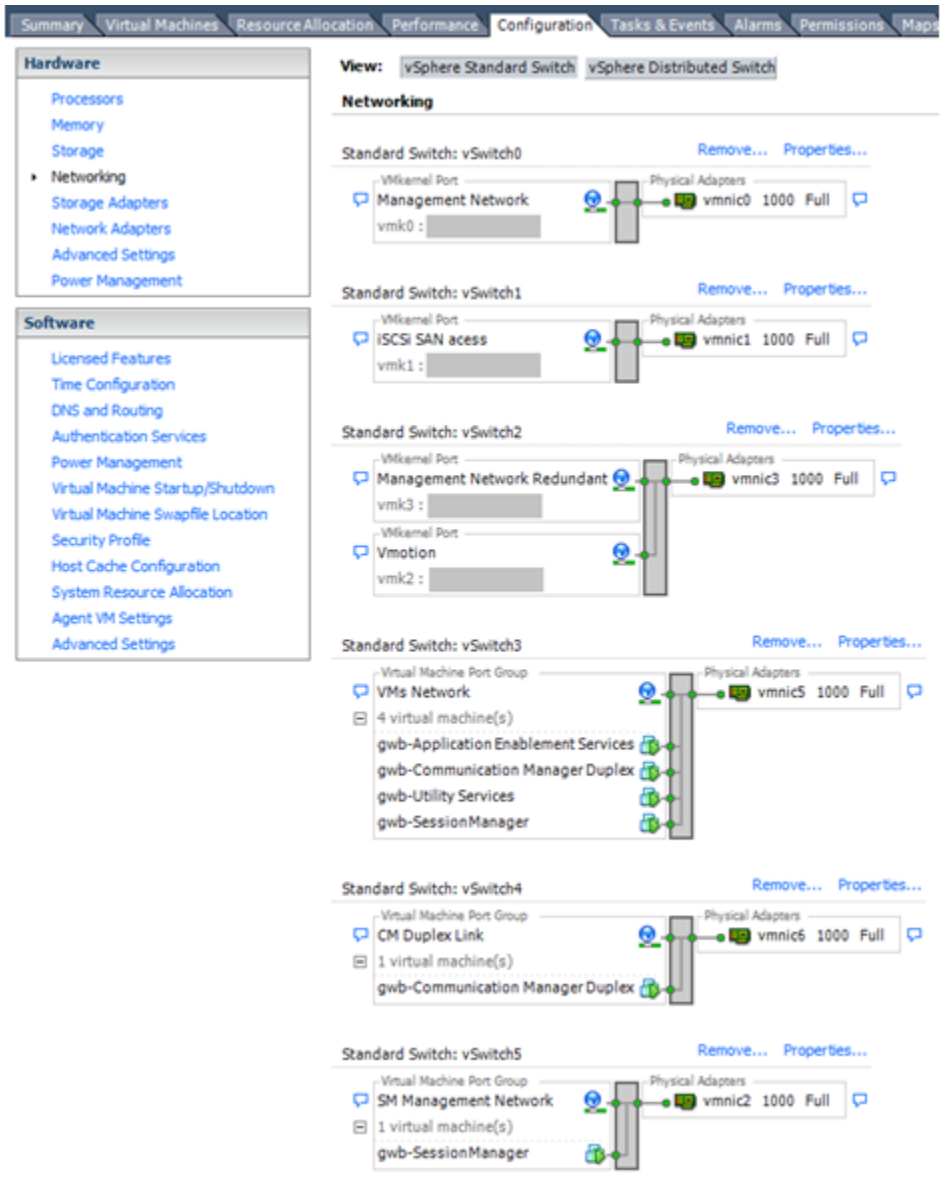
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network

requirements. for more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:

- The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
- The round-trip delay must be 8 ms or less.
- The round-trip packet loss must be 0.1% or less.
- Both servers duplication ports must be on the same IP subnet.
- You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
- The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.

- Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, Example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



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

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.
- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere™ 5.0	Performance Best Practices for VMware vSphere™ 5.0
Performance Best Practices for VMware vSphere™ 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
VMware vSphere 5.0 Basics	VMware vSphere Basics - ESXi 5.0
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Thin vs. thick deployments

When creating a virtual disk file, by default VMware ESXi uses a thick type of virtual disk. 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.

VMware Features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- *Do not* rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- *Do not run a virtual machine off of a snapshot.* Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, *do not* save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

Note:

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, a warning is displayed in the UI.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots

Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

VMware Cloning

Installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process. However, if making a clone of the Avaya Aura® Utility Services, do not perform any Guest Customization. Select Do not customize as this option is not currently supported.

VMware High Availability

VMware High Availability is a viable option for Avaya Aura® Utility Services recovery in the VMware environment. Where VMware HA has been configured on the ESXi host on which an Avaya Aura® Utility Services VM has been installed, failure of this ESXi host results in Avaya Aura® Utility Services being moved to a standby host. Once the cold boot of Avaya Aura® Utility Services on the standby host has completed, it will then continue to provide all of the usual features and services.

The following should be noted when configuring to use 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.
- To have reliable failure detection for HA clusters, the console network should have redundant network paths. 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 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 Storage vMotion

VMwares Storage vMotion technology is the process by which a running Virtual Machine is migrated from one storage medium to another without incurring downtime. This is known as a **hot-migration**. It enables the live migration of running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

The following should be noted when configuring to use VMware Storage vMotion:

- Ensure that each host that will have VMs migrated to or from it has VMware Storage vMotion licensed and enabled.
- Identical vSwitches are required. Storage vMotion needs to be enabled on these vSwitches.
- Storage vMotion requires identical Port Groups.
- In order to ensure the best performance, Storage vMotion requires a dedicated NIC.

Appendix B: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) 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 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 **DOCUMENTS**.
3. On the 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 the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs 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. The Avaya E-Notifications process manages this proactive notification system.

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.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Glossary

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Application	A software solution development by Avaya that includes a guest operating system.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also

	creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Client	The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

Index