Deploying Communication Manager Messaging using VMware® in the Virtualized Environment

Release 6.3
Issue 1
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.

“Hosted Service” means a hosted service subscription that you acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If you purchase a Hosted Service subscription, the foregoing limited warranty may not apply but you may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

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").

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

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

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® Communication Manager Messaging using VMware 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 Communication Manager Messaging in a VMware® vSphere™ virtualization environment at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

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

Related resources

Documentation

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

	Title	Description	Audience
Implementation			
	Implementing Avaya Aura Communication Manager Messaging	This document describes the implementation process of Communication Manager Messaging 6.3.	Service technicians Customers

	Title	Description	Audience
	Implementing Avaya Aura Communication Manager Messaging Federal	This document describes the implementation process of Communication Manager Messaging Federal 6.3.	Service technicians Customers
Administration			
	Avaya Aura Communication Manager Messaging Documentation Library	This document contains the administration process of Communication Manager Messaging 6.3.	Service technicians Customers

Training

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

Course code	Course title	Duration	Delivery Mode
4U00030E	Avaya Aura® Communication Manager and Communication Manager Messaging Embedded Implementation This is a 54-hour course and consists of the following components: • 4U00030E_TH – 18 hours – self-directed theory • 4U00030E_INTRO – 4 hours – instructor-facilitated overview of content • 4U00030E_LAB – 32 hours – instructor-facilitated hands-on lab exercises using remote equipment	54 hours	Self-directed and Instructor-facilitated
5U00060E	Avaya Aura® Communication Manager and Communication Manager Messaging Support This is a 37-hour course and consists of the following components: • 5U00060E_TH – 17 hours – self-directed theory • 5U00060E_INTRO – 4 hours – instructor-facilitated overview of content • 5U00060E_LAB – 16 hours – instructor-facilitated hands-on lab exercises using remote equipment	37 hours	Self-directed and Instructor-facilitated

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support 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.

Chapter 2: Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with the virtualized server architecture of VMware. 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 cooling requirements, which reduces power consumption.
- Enables cost savings on capital equipment.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Enables deployment of Avaya products in a virtualized environment on customer-specified servers and hardware.
- Accommodates business scalability and rapid response to changing business needs.

For customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to deploy Communication Manager Messaging using their own VMware infrastructure.

The Virtualized Environment capability is only for VMware and is not intended to include any other industry hypervisor.

Note:

The following terms are often used interchangeably in the document:

- Server and host
- Reservations and configuration values

Customer deployment

vCenter Server and vSphere Client manage the deployment into the blade, cluster, and server.

The customer must provide the servers and the VMware infrastructure including the VMware licenses.

Software delivery

The software is delivered as prepackaged Open Virtualization Appliance (OVA) file with the following components:

- The application software and operating system
- Preinstalled VMware tools
- Preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Patches and updates

A minimum patch level is required for each supported application. For more information, 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 file is built with configuration values that optimize performance and follow recommended best practices. You must change the preconfigured settings in the OVA.

For more information about supported resource requirements, see Communication Manager Messaging virtual machine resource requirements on page 20.

Best Practices for VMware performance and features

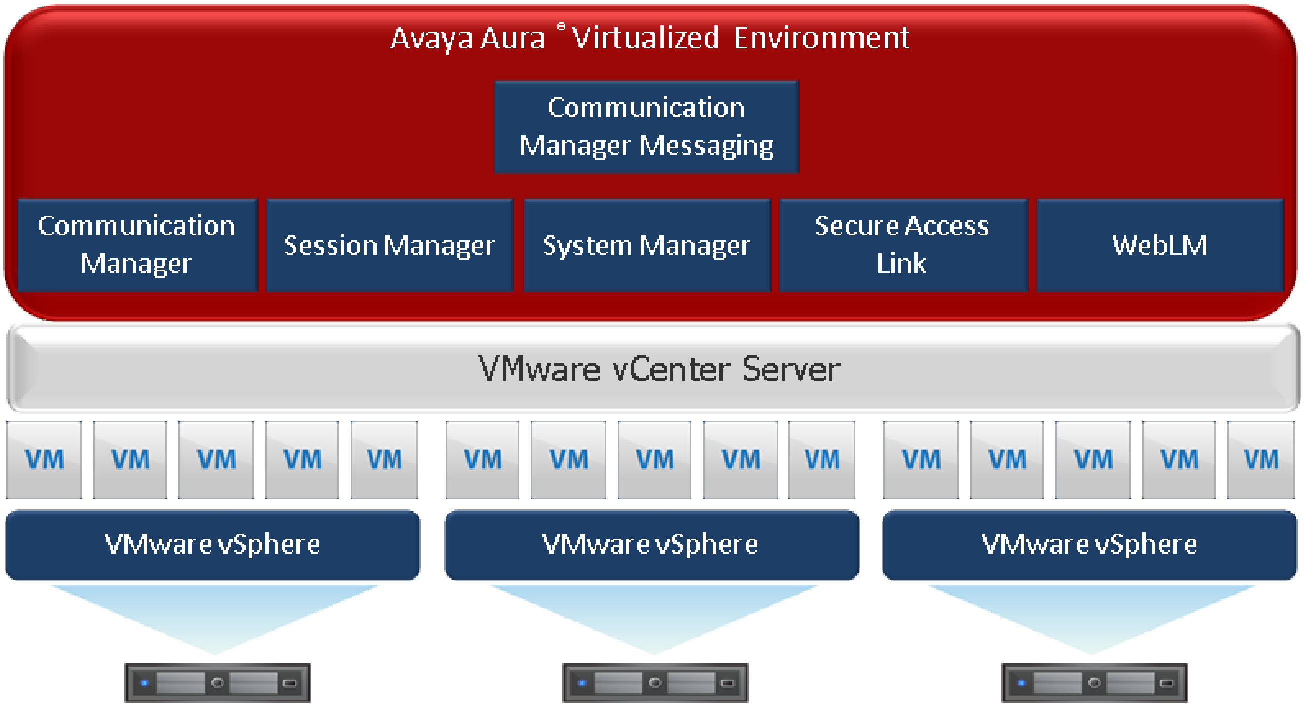
For more information about Avaya Aura® Virtualized Environment, see *Avaya Aura® Virtualized Environment Solution Description*.

Important:

Do not use VMware Snapshots because Snapshot operations can adversely affect Communication Manager Messaging service.

Topology

The following diagram shows the high-level topology for deploying Communication Manager Messaging in Virtualized Environment.



The VMware virtualization platform, VMware vSphere, supports the virtual machines. Each Avaya Aura® application, including Communication Manager Messaging, is installed as a separate virtual machine. Communication Manager Messaging OVA is built to support maximum capacity, so only one instance of this VM is needed. The VMware vCenter Server management system manages the applications as virtual machines and provides management and implementation features in addition to the standard System Manager features.

Components

Avaya components

Component	Version	Platform	Description
Avaya Aura® components			
Avaya Aura® Communication Manager	6.3 6.3.2	Virtualized Environment	The IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises.
Avaya Aura® Communication Manager Messaging	6.3	Virtualized Environment	A part of the Avaya Aura® architecture, but Communication Manager Messaging can also be used in other environments
Avaya Aura® Session Manager	6.3.2	Virtualized Environment	A SIP routing and integration tool that integrates SIP entities across the enterprise network. You can view

Component	Version	Platform	Description
	6.3.4		and manage each location, branch, and application in totality, not as separate units within the enterprise.
Avaya Aura® System Manager	6.3.2 6.3.4 6.3.8	Virtualized Environment	A product that takes a solution-level approach to network administration. System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager provides a common management framework that reduces the complexity of operations for distributed multisite networks with multiple control points inherent in SIP.
Other Avaya components			
Avaya WebLM	-	Virtualized Environment	A web-based license manager that manages licenses of one or more Avaya software products.
Message Networking	5.2	Avaya server with Red Hat Enterprise Linux	A component that supports interoperability with legacy voice mail products.
Avaya service components			
Secure Access Link	2.1	-	A component that remotely manages Messaging and sends alarms to Avaya Services.

VMware components

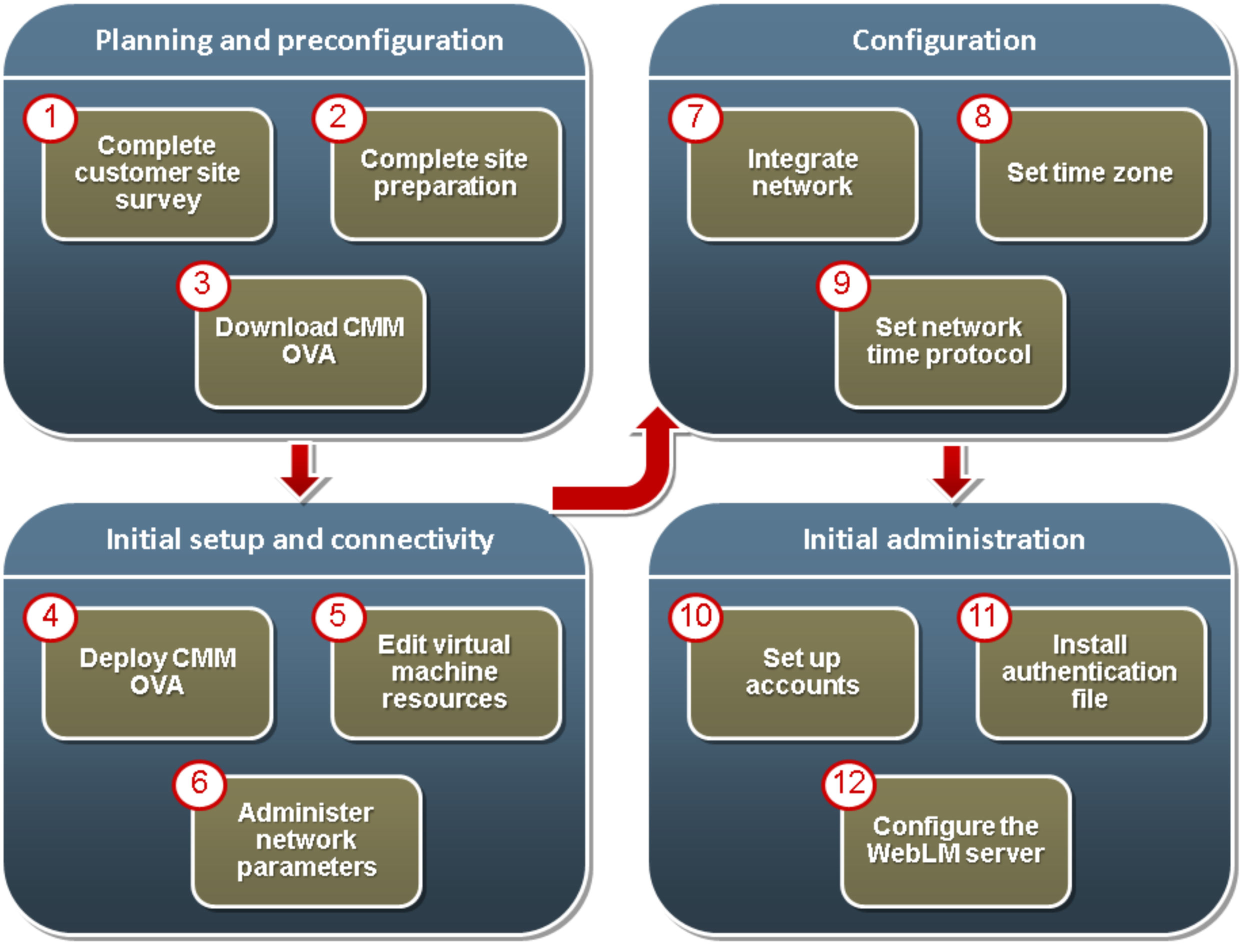
Component	Version	Description
ESXi Host	5.1 and 5.5	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	5.1 and 5.5	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	5.1 and 5.5	vSphere Client is an application that installs and 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. **Note:** You must access the ESXi host or the vCenter server by using the vSphere client from a computer running Windows Vista or a later version.
vCenter Server	5.1 and 5.5	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.

Third-party components

Component	Description
Storage Area Network	SAN is a high-speed network of storage devices that also connects those storage devices with servers.

Chapter 3: Deployment process

The following image shows the high-level tasks for deploying Communication Manager Messaging in a Virtualized Environment configuration.


Planning and preconfiguration
1
Complete customer site survey
2
Complete site preparation
3
Download CMM OVA
Configuration
7
Integrate network
8
Set time zone
9
Set network time protocol
Initial setup and connectivity
4
Deploy CMM OVA
5
Edit virtual machine resources
6
Administer network parameters
Initial administration
10
Set up accounts
11
Install authentication file
12
Configure the WebLM server

Chapter 4: Planning and configuration

Planning checklist

No.	Task	References	Notes	✔
1	Download the required documentation.	See Documentation on page 6.	—	
2	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 19.	—	
3	Plan the staging and verification activities and assign the resources.	See Communication Manager Messaging virtual machine resource requirements on page 20.	—	
4	Download Communication Manager Messaging OVA.	See Downloading software from PLDS on page 18.	—	

Software requirements

The following table lists the required software and the supported versions for Communication Manager Messaging in the Virtualized Environment:

Table 1: VMware software requirement

Equipment	Software versions
VMware vSphere ESXi	5.1 and 5.5
VMware vCenter Server	5.1 and 5.5 ✱ **Note:** VMware requires the version of vCenter be the same or greater than the version running on the hosts that it manages.

Table 2: Communication Manager Messaging software requirement

Software	Software versions
Communication Manager Messaging	6.3

Table 3: Service pack requirement

Software	Software versions
VMware tools	See *Avaya Aura® Communication Manager Messaging Release Notes*.
Kernel	See *Avaya Aura® Communication Manager Messaging Release Notes*.
Security	See *Avaya Aura® Communication Manager Messaging Release Notes*.
Communication Manager	See *Avaya Aura® Communication Manager Messaging Release Notes*.
Communication Manager Messaging	See *Avaya Aura® Communication Manager Messaging Release Notes*.

Key customer configuration information

The following table identifies the customer configuration information that you must enter during the deployment and configuration processes:

Required data	Value for the system
IPv4 IP address	
IPv4 subnet mask	
IPv4 Default Gateway address	
IPv6 IP address (optional)	
IPv6 subnet mask (optional)	
IPv6 Default Gateway address (optional)	

Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring Communication Manager Messaging open virtual application (OVA):

- A remote computer running the VMware vSphere Client

- A browser for accessing the Communication Manager Messaging System Management Interface pages
- An sftp client for Windows, for example WinSCP
- An ssh client, for example, PuTTy

SAL Gateway

A Secure Access Link (SAL) Gateway is required for remote access and alarming.

Through SAL, support personnel or tools can gain remote access to managed devices to troubleshoot and debug problems.

A SAL Gateway:

1. Receives alarms from Avaya products in the customer network.
2. Reformats the alarms.
3. Forwards the alarms to the Avaya support center or a customer-managed Network Management System.

You can deploy the SAL Gateway OVA using vCenter through a vSphere client. You can also deploy the SAL Gateway OVA directly to the ESXi server through a vSphere client.

For more information about the SAL Gateway, see the Secure Access Link documentation on the Avaya Support website at http://support.avaya.com .

Downloading the Communication Manager Messaging OVA

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.

2. Log in to SSO with your SSO ID and password.

   The PLDS registration page is displayed.

3. If you are registering:

   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an email to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To

  - Ship-To number
  - License authorization code (LAC)

4. Click **Submit**.

   Avaya will send you the PLDS access confirmation within one business day.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
   - By download name
   - By selecting an application type from the drop-down list
   - By download type
   - By clicking **Search Downloads**
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Chapter 5: Initial setup and connectivity

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.
- 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.

Hardware requirements

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.

Communication Manager Messaging virtual machine resource requirements

The Communication Manager Messaging OVA is built with configuration values that optimize performance and follow recommended best practices. After installing the OVA, adjust resource settings as needed to meet the guidelines set forth in the following table.

The following set of resources must be available on the ESXi host for deploying the Communication Manager Messaging virtual machines.

Note:

The following resource requirements are recommended for both commercial customers and U.S. DoD and approved Federal Government customers.

Resource Requirements	Small System	Large System
	Heavy traffic[1]	**Heavy traffic**[2]
Mailboxes	1000	15000
Ports	24	210
Virtual machine	1	1
Virtual CPUs	1	2
Minimum CPU speed	2 GHz	2 GHz
Virtual CPU reservations	2 GHz	4 GHz
Virtual memory	2 GB	2 GB
Virtual memory reservations	2 GB	2 GB
Virtual storage	230 GB	230 GB
Average I/OPS	27	123
Shared Network Interface Cards	One @ 1000 Mbps	One @ 1000 Mbps
Average network usage	527 KBps	4162 KBps

For Communication Manager Messaging to run at full capacity, ensure that the recommended resource requirements are met.

- The default values for the Communication Manager Messaging OVA are 4 vCPU, 4 GB memory, and 230 GB (thick provisioned) hard disk.
- Use the recommended CPU and memory reservations to meet the acceptable performance level. You can check the CPU requirements in the **Summary** tab of the virtual machine.
- Communication Manager Messaging might not perform adequately if the cumulative CPU or memory resources of the virtual machines co-located on the same physical ESXi host as the Communication Manager Messaging virtual machine exceeds 70% of the physical hardware of server. The customer assumes all risk if this threshold is exceeded.

[1] **CMM is expecting to serve a new call every four seconds. On an average, each user receives thirteen voice messages every 24 hours.**

[2] **CMM is expecting to serve two calls per second. On an average, each user receives seven voice messages every 24 hours.**

- The recommended resource requirements are based on the following hardware configurations:
  - iSCSI SAN storage: One Dell Equallogic PS6100XV array of 24 terabytes.
  - ESXi 5.1 hosts: Six Dell R720 servers. Each server with two quad-core Xeon 2620 CPU and 2 GHz, HyperThreaded. Each host server with 32 logical vCPUand each vCPU core provides 2 GHz.
  - VCenter server and Dell SAN Headquarter: One Dell R320 server running Windows 2008R2, with a single quad-core Xeon CPU and 500 GB RAID-1 hard disk drive array.
  - LAN: A stacked pair of Avaya ERS4850GTS, dedicated and configured for each Dell Equallogic SAN requirements. Each ESXi host server has four connections to the SAN switch to take advantage of the Dell Equallogic Multi-I/O for max storage I/O performance. A fifth SAN connection is dedicated for vMotion traffic.

Note:

- Avaya does not provide support for performance issues due to variance in the recommended settings.
- If a problem occurs with the virtual machine, Avaya Global Support Services (GSS) might not be able to assist in resolving the problem. Reset the values to the required values before starting to investigate the problem.

Software installation checklist

No.	Task	References	Notes	✔
1	Deploy the Communication Manager Messaging OVA.	See Deploying the Communication Manager Messaging OVA on page 21.	—	
2	Edit the virtual machine resources.	See Editing the virtual machine resources on page 23.	—	
3	Administer network parameters.	See Administering network parameters on page 24.	—	

Deploying the Communication Manager Messaging OVA

About this task

Use this procedure to deploy the Communication Manager Messaging OVA to the ESXi server through a vSphere client.

Procedure

1. Log in to the vCenter or the ESXi server using the vSphere Client.

2. Select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the OVA file:
    - If the OVA file is downloaded to a location accessible from your computer, click **Browse** to select the location.
    - If the OVA file is located on an http server, enter the full URL in the **Deploy from a file or URL** field.
4. Click **Next**.
5. In the OVF Template Details window, verify the details of the Communication Manager Messaging OVA template and click **Next**.
6. In the End User License Agreement window, read the license agreement, click **Accept**, and click **Next**.
7. In the Name and Location window, in the **Name** field, type a unique name for the new virtual machine, and select the inventory location to deploy the virtual machine and click **Next**.
8. Select the host or cluster and click **Next**.

    If you did not select a host before deploying the template, the wizard prompts you to select now. If you selected a host or cluster while deploying the OVF template, the wizard processes the request to install the virtual machine on that host.
9. In the Storage window, select the data store location to store the virtual machine files, and click **Next**.

    The data store can be local to the host or a mounted shared storage, such as SAN. The virtual machine configuration file and virtual disk files are stored on the data store. Select a data store large enough to accommodate the virtual machine and all its virtual disk files.
10. In the Disk Format window, accept the default disk format, **Thick Provision Lazy Zeroed**, and click **Next**.

    The default disk format allocates the required 230-GB disk space for the Communication Manager Messaging virtual machine.

    For more information about the virtual disk, see Thin vs. thick deployments on page 53.
11. If there are multiple virtual machine networks configured on the host where you are deploying the Communication Manager Messaging OVA, the wizard prompts you to associate networks specified in the OVA with networks available on the host.
    - For a single **source network**, choose a host network by clicking the **Destination Network** column. Click the entry in the drop-down menu, for example, VM Network 2. Click **Next**.
    - If there is only a single virtual machine network on the host you are deploying the Communication Manager Messaging OVA, the wizard will not prompt you.
12. In the Ready to Complete window, verify the deployment settings, and click **Finish**.

    The progress of the tasks displays in a **vSphere Client Status** panel.

    The deployment process takes about 10 to 12 minutes to complete. If the OVA file location is an http server, the deployment process might take more time.

Next steps

Edit the virtual machine resources.

Editing the virtual machine resources

About this task

The OVA file is built with configuration values that optimize performance and follow recommended best practices.

After installing the OVA, use this procedure to adjust the virtual machine resources as needed to meet the guidelines set forth in CMM virtual machine resource requirements on page 20.

Procedure

1. Right-click the virtual machine, and click **Edit Settings**.
2. On the Virtual Machine Properties window, click the **Hardware** tab.
    a. CPU: In the left pane, click **CPUs**. Select a value from the **Number of virtual sockets** and the **Number of cores per socket** fields.

       To determine the total number of cores, multiply the number of cores per socket by the number of virtual sockets. The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

    b. Memory: In the left pane, click **Memory**. Adjust the memory configuration slider to an appropriate number. Alternatively, in the **Memory Size** field, enter the exact number.
3. On the Virtual Machine Properties window, click the **Resources** tab.
    a. CPU limitations: In the left pane, click **CPU**. Adjust the CPU reservation to an appropriate number. Alternatively, in the **Reservations** field, enter the exact CPU reservation number.

    b. Memory: In the left pane, click **Memory**. Adjust the memory reservation to an appropriate number. Alternatively, in the **Reservations** field, enter the exact memory reservation number.
4. Click **OK**.

Next steps

If you did not select the option to start the virtual machine automatically, start the virtual machine manually.

Start the Communication Manager Messaging virtual machine console, and configure the Communication Manager Messaging parameters.

Starting the Communication Manager Messaging virtual machine

Procedure

1. In the vSphere client, right-click the Communication Manager Messaging virtual machine, and click **Power** > **Power On**.
2. In the Recent Tasks window, wait until the status of the **Power on virtual machine** shows **Completed**.
3. Right-click the Communication Manager Messaging virtual machine, and select **Open Console**.

   The console displays the system startup messages. The system starts the system services and the Communication Manager Messaging services. After the startup process is complete, the system displays a message to log in to the virtual machine.

Next steps

Administer network parameters.

Administering network parameters

Procedure

1. In the vSphere client console window, log in as `craft`.

   Note:

   If you need any assistance for log in to the system, go to the Avaya Support website at http://support.avaya.com to open a service request.

2. Provide information in the following fields:
   a. **IPv4 IP address** : Enter the IP address.
   b. **IPv4 subnet mask**: Enter the network mask IP address.
   c. **IPv4 Default Gateway address**: Enter the default gateway IP address.
3. In the **Are these correct** field, verify the IP address details and enter `y` to confirm.

   Important:

   You might have to reenter the data in the following conditions:

   - The initial network prompt for entering the IP address, Subnet mask, and Default gateway address is interrupted.
   - Incorrect data is specified.

   To reenter data, run the following on the command line:

   ```
   /opt/ecs/bin/serverInitialNetworkConfig
   ```

4. Configure additional network settings.

For more information, see Configuring the network on page 28.

WebLM

Avaya provides a web-based license manager (WebLM) to manage licenses of one or more Avaya software products.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

The license file is in XML format and contains information about the product such as the licensed capacities of each feature that you purchase. You activate the license file in PLDS and install the license file on the WebLM server.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration, see *Administering Avaya Aura® System Manager*.

Chapter 6: Configuration

Configuration checklist

No.	Tasks	References	Notes	✔
1	Configure the virtual machine automatic startup settings.	See Configuring the virtual machine automatic startup settings on page 26.	—	
2	Configure the network settings.	See Configuring the network on page 28.	—	
3	Set the time zone.	See Setting the time zone on page 29.	—	
4	Set up the network time protocol.	See Setting up the network time protocol on page 29.	—	
5	Install service packs.	See Communication Manager Messaging service packs on page 30.	—	

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**.

IPv6 configuration

Enabling IPv6

Before you begin

You must apply the Communication Manager Release 6.3.6 patch on the Communication Manager Messaging virtual machine.

Procedure

1. Log in to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. From the **IPv6 is currently** drop-down list, select enabled.
5. Click **Change** to enable the IPv6 fields.

Disabling IPv6

Before you begin

You must apply the Communication Manager Release 6.3.6 patch on the Communication Manager Messaging virtual machine.

Procedure

1. Log in to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.

4. From the **IPv6 is currently** drop-down list, select disabled.
5. Click **Change** to disable the IPv6 fields.

Configuring the Communication Manager Messaging network

Procedure

1. Log in to Communication Manager Messaging System Management Interface on the virtual machine on which you want to configure the network.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. Type the values in the fields.

   If IPv6 is not enabled, you cannot configure the IPv6 fields.

   For field descriptions, see the *Network Configuration field descriptions* section.
5. Click **Change** to save the network configuration.

Network Configuration field descriptions

Name	Description
Host Name	The Communication Manager Messaging system host name. The host name must be unique.
DNS Domain	The DNS domain name of the server. For example, company.com.
Search Domain List	The DNS search list. If there is more than one entry, use a comma (,) to separate each entry.
Primary DNS	The Primary DNS IP address.
Secondary DNS	The Secondary DNS IP address.
Tertiary DNS	The Tertiary DNS IP address.
Server ID	The unique server ID (SVID) of the server.
Default Gateway IPV4	The default gateway address of IP version 4.
Default Gateway IPV6	The default gateway address of IP version 6.

Name	Description
IP Configuration	The set of parameters to configure an Ethernet port. The parameters are: • **IPv4 Address** • **Subnet Mask** • **IPv6 Address** • **Prefix**
Mask	The number for the mask. If you are assigning an IPv4 address, you must set this field to the subnet mask that is required for this network setup. The system supports short version and long version of the mask. If you are using the short version, enter a numeric number from 1 to 32.
Functional Assignment	The indication on how to use the interface.

Setting the time zone

Procedure

1. Log on to the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Time Zone Configuration**.
3. On the Time Zone Configuration page, select the time zone and click **Apply**.

   Note:

   After changing the time zone settings, some features of the system use the new time zone only after you reboot the virtual machine. However, you can defer the reboot until you install the service packs.

Setting up the network time protocol

Procedure

1. Log on to the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **NTP Configuration**.
3. Enable or disable the NTP mode.

4. In NTP Servers, enter the primary server, secondary server (Optional), and tertiary Server (Optional) details.
5. Click **Apply**.

Service pack installation

Communication Manager Messaging service packs

A service pack provides product updates and bug fixes. When a service pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the service pack. Even if the system does not have problems, install the service packs to keep the systems up-to-date and minimize the likelihood of future issues.

You must install, download, and manage the service packs from Communication Manager Messaging System Management Interface.

For each type of service pack, when the latest version is available, you must install the service packs in the following order:

- VMware Tools
- Kernel
- Security
- Communication Manager
- Communication Manager Messaging

For Communication Manager Messaging kernel service packs, additional caution is required:

- To install a kernel service pack, unpack, activate, and commit the service pack.
- To remove a kernel service pack, deactivate, commit, and remove the service pack.

Important:

- To install the latest version of any service pack, you must remove the earlier installed version.
- You cannot install or remove a service pack if any other service pack is being installed or removed.

For each applicable service pack, repeat the procedures in Downloading service packs on page 31 and Installing service pack on page 31.

Downloading service packs

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Miscellaneous** > **Download Files**.
2. To download files from your system to the Avaya server, select **File(s) to download from the machine I'm using to connect to the server** and then:
   a. Click **Choose File** or enter the path to the file that resides on your system. You can specify up to four files to download.
   b. Click **Open**.
3. To download files from a Web server to the Avaya server, select **File(s) to download from the LAN using URL** and then:
   a. Specify the complete URL of up to four files.
   b. If you require a proxy server for an external Web server that is not on the corporate network, you must enter the details in the `server:port` format.
      - Enter the name of the proxy server such as network.proxy or IP address.
      - If the proxy server requires a port number, add a colon (:).
   c. Click **Download**.

Installing a service pack

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. Click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

   The Manage Updates page displays the list of uploaded service packs.
3. Select a service pack from the list.
   a. Click **Unpack**.
   b. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **unpacked**.
4. Select the same service pack from the list.
   a. Click **Activate**.

      If the service pack installation process affects the availability of the Communication Manager Messaging service, the system prompts you to confirm the action.
   b. **(Optional)** Click **Yes** to confirm the action.
   c. Click **Continue** to return to the Manage Updates page.

The status of the selected service pack changes to **activated**. If the selected service pack is a kernel service pack, the status stays in the **activating** state until about one minute after the system reboots. Then the status changes to **pending_commit**.

Note:

The service pack installation process takes approximately 10 minutes for a kernel or security service pack.

5. Click **Messaging** > **Server Information** > **System Status** to verify that the Communication Manager Messaging system is functional.

   The System Status webpage displays the status of the following modules.

   - VM - Voice Messaging
   - ela - Enhanced List Administration
   - iim - Internet Messaging
   - ldap - Lightweight Directory Access Protocol
   - mtce - Maintenance
   - vs - Voice System

   Tip:

   Click the **Refresh** button of your browser periodically until all entries in the Module List have a status of `IN SERVICE`, `RUNNING`, or `UP`.

   Note:

   The system reboots for a kernel or security service pack installation. During the system reboot, the System Status webpage remains inaccessible.

6. Verify that the status of the installed service pack shows **activated** on the Manage Updates page.

   If the status shows **pending_commit**, proceed to Step 7.

7. **(Optional)** Select the service pack from the list if the update that you want to activate shows **pending_commit** in the **Status** column.

   a. Click **Commit**.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to the Manage Updates page.

Removing a service pack

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. Click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

The Manage Updates page displays the list of uploaded service packs.

3. Select a service pack from the list.
    a. Click **Deactivate**.

        If the service pack installation process affects the availability of the Communication Manager Messaging service, the system prompts you to confirm the action.
    b. Click **Yes** to confirm the action.
    c. Click **Continue** to return to the Manage Updates page.

    The status of the selected service pack changes to **unpacked**. If the selected service pack is a kernel service pack, the status stays in **deactivating** state until about one minute after the system reboot and then changes to **pending_deactivate**.

    Note:

    The service pack deactivation process takes approximately 10 minutes for a kernel or security service pack.
4. Click **Messaging** > **Server Information** > **System Status** to verify that the Communication Manager Messaging system is functional.

    The System Status webpage displays the status of the following modules.
    - VM - Voice Messaging
    - ela - Enhanced List Administration
    - iim - Internet Messaging
    - ldap - Lightweight Directory Access Protocol
    - mtce - Maintenance
    - vs - Voice System

    Tip:

    Click the **Refresh** button of your browser periodically until all entries in the Module List have a status of `IN SERVICE`, `RUNNING`, or `UP`.

    Note:

    The system reboots for a kernel or security service pack installation. During the system reboot, the System Status webpage remains inaccessible.
5. Verify that the status of the installed service pack shows **deactivated** on the Manage Updates page.

    If the status shows **pending_deactivate**, proceed to Step 6.
6. **(Optional)** Select the same service pack from the list if the update that you want to deactivate shows **pending_deactivate** in the **Status** column.
    a. Click **Commit**.
    b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **deactivated**.

7. **(Optional)** Select the same service pack from the list to remove the deactivated service packs and reclaim the server space.

   a. Click **Remove**.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to Manage Updates page.

   The status of the selected service pack changes to **packed**.

8. **(Optional)** Select the same service pack from the list to clean up the hard disk drive by deleting the installation file of an uninstalled service pack.

   a. Click **Remove**.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to Manage Updates page.

   The list does not display the removed service pack. Repeat Step 8 if the service pack continues to display in the list.

Chapter 7: Initial administration

Initial administration checklist

No.	Tasks	References	Notes	✔
1	Add the privileged administrator login.	See Adding a privileged administrator login on page 35.	—	
2	Download and install the authentication file.	See Authentication file installation on page 37.	—	
3	Install the license file.	See License file for Communication Manager Messaging on page 40.	—	
4	Reboot the server.	See Shutting down the server on page 46.	—	

Account management

Adding a privileged administrator login

About this task

You must add a privileged administrator login that is a member of the SUSERS group. This login provides the highest level of access with the maximum permissions. A user with the privileged administrator login can gain access to all the System management Interface pages and Command Line Interface after you install the authentication file.

Procedure

1. Log on to the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. In the **Select Action** area, select **Add Login**.
4. Select **Business Partner Login (dadmin)**.

   This login provides the highest level of access with the maximum permissions to a user. A user can gain access to all the SMI pages and CLI. You can add this login only once.

5. Click **Submit**.

   The system displays the Administrator Accounts -- Add Login: Privileged Administrator Web page.

6. Enter information in the following fields:

   - **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field
   - **Enter password or key**
   - **Re-enter password or key**

7. Click **Submit**.
8. Click **Continue** to go back to the Administrator Accounts Web page.

Administrator Accounts field descriptions

Field	Description
Select Action	
Add Login	Select this option and select the type of login to add. The options are: • **Privileged Administrator**: Provides the highest level of access with the maximum permissions. A user can gain access to all the SMI pages and CLI. • **Unprivileged Administrator**: Provides restricted access. A user can gain access to the SMI pages that are for querying the Communication Manager Messaging status and backing up data and CLI. • **Web Access Only**: Provides access only to the SMI pages. A user can administer the SMI pages that the user can gain access to in the **Web Access Mask** settings of the profile of the user. • **CDR Access Only**: Not applicable. • **Business Partner Login (dadmin)**: Provides the highest level of access with the maximum permissions to a user and is similar to **Privileged Administrator**. A user can gain access to all the SMI pages and CLI. You can add this login only once. • **Business Partner Craft Login**: Provides the highest level of access with the maximum permissions and is similar to **Business Partner Login (dadmin)**. A user can gain access to all the SMI pages and CLI. With this login, the user can suppress alarms from the server when logging in to SMI.

Field	Description
	• **Custom Login**: Provides customized access. You can select the level of access to the user.
Change Login	Select this option and select a login from the drop-down list.
Remove Login	Select this option and select a login from the drop-down list.
Lock/Unlock Login	Select this option and select a login from the drop-down list.
Add Group	Select this option to add a group.
Remove Group	Select this option and select a group from the drop-down list.

Authentication file management

Authentication file installation

To grant Avaya service personnel and Avaya partners access to the customer system, you need a new authentication file with Access Security Gateway (ASG) keys and the server certificate for Communication Manager Messaging. Authentication file ensures system security and prevents unauthorized access to your Communication Manager Messaging system.

Authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate. To change the authentication information, replace the entire file. If the authentication file is missing or corrupted, the system denies all logins to the Avaya server. The Communication Manager Messaging system continues to run, but the system blocks further administration until you install a new authentication file.

Note:

If the authentication file is not installed, the system displays an error message that the system cannot display the authentication file information.

Starting the AFS application

Before you begin

Authentication File System (AFS) is available only to Avaya service personnel and Avaya partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

To start the AFS application, you must have a login ID and password. Sign up for a login ID at http://rfa.avaya.com.

Procedure

1. Type `http://rfa.avaya.com` in your web browser.
2. Enter your login information and click **Submit**.

3. Click **Start the AFS Application**.

   The system displays a security message.

4. Click **I agree**.

   The system starts the AFS application.

Next steps

Create an authentication file.

Creating an authentication file for a new system

Procedure

1. Log in to the AFS application.
2. In the **Product** field, click **SP System Platform/VE VMware**.
3. In the **Release** field, click the release number of the software, and then click **Next**.
4. On the Authentication File Delivery page, select **New System**, and then click **Next**.
5. In the **Communication Manager 6.x** field, type the fully qualified domain name (FQDN) of the host system where Communication Manager Messaging is installed.
6. To download the authentication file directly from AFS to your computer:

   a. Click **Download file to my PC**.

   b. In the File Download dialog box, click **Save**.

   c. Select the location to save the authentication file, and then click **Save**.

   d. In the Download complete dialog box, click **Close**.

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

7. To send the authentication file in an email message:

   a. In the **Email Address** field, enter the email address.

   b. Click **Download file via email**.

   AFS sends the email message that contains:

   - The system AFID, system type, and system release in the message text.
   - The authentication file as an attachment.

8. To view the header information in the authentication file, open the file in WordPad.

   The header includes the following information:

   - AFID
   - Product name
   - Release number
   - Date and time

Next steps

Install the authentication file.

Installing the authentication file

Procedure

1. Log on to the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Load Authentication File**.
3. In the **Select the Authentication File** field, click **Browse**.
4. In the **Choose File to Upload** dialog box, click the authentication file, and then click **Open**.

   Note:

   To override the validation of the AFID and the date and time, select **Force load of new file**. Select this option if you:

   - Must install an authentication file with a different AFID than the installed file.
   - Must reinstall the original file after installing a new authentication file.

   Do not select this option to replace the default authentication file, AFID 7100000000, with a unique authentication file.

   Caution:

   Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, you might encounter certificate errors and login issues.
5. Click **Install**.

   The system uploads the selected authentication file and validates the file before installing it.

Obtaining the AFID

If you want to redeploy the authentication file, use this procedure to obtain the AFID.

Procedure

1. Log on to the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Authentication File**.

   The system displays the AFID in the AFID field.

License management

License file for Communication Manager Messaging

The license file is an Extensible Markup Language (XML) file with information about the product, the major release, and the license features and capacities. Avaya provides a web-based license manager (WebLM) to easily manage licenses of one or more Avaya software products.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration. see *Administering Avaya Aura® System Manager*.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager Messaging. The Avaya PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Communication Manager Messaging, the license entitlements on the order are automatically created in PLDS. After these license entitlements are created, you receive an email notification from PLDS with a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Configuring the WebLM server

Procedure

1. Log in to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Licensing**.
3. In the left navigation pane, click **WebLM Configuration**.

   The system displays the WebLM Configuration page.
4. In the **WebLM Server Address** field, type the WebLM server IP address to fetch the license file.

   Note:

   You can specify the IP address of the WebLM server within System Manager or of the standalone WebLM virtual appliance.
5. Click **Submit**.

Routine maintenance

Backup and restore

Backing up the system

About this task

Communication Manager Messaging uses LAN to back up the Communication Manager Messaging data to an external server. The Communication Manager Messaging application data and the server data can be backed up simultaneously or independently. During a system failure, Communication Manager Messaging uses the information stored on the external server to restore the system.

Communication Manager Messaging supports the following backup methods:

- FTP
- SFTP
- SCP

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The system delays the shutdown for three minutes after which the system ends all active calls.

   The Stop Messaging Software webpage refreshes periodically during the shutdown routine. After the Communication Manager Messaging software stops, the system displays the `Stop of Messaging completed` message.
4. Click **OK**.
5. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.
6. On the Backup Now webpage, in the **Data Sets** area, click **Specify Data Sets**. Click the following fields:
   a. **Server and System Files**
   b. **Security File**
   c. **Messaging**
7. In the **Messaging** area, click **Messaging Translations, Names, and Messages**.
8. In the **Backup Method** area, click **Network Device** and then complete the following fields:
   a. **Method**
   b. **User Name**

   c. **Password**
   d. **Host Name**
   e. **Directory**
9. If you want to encrypt the backup data, select **Encrypt backup using pass phrase** and enter a pass phrase using an arbitrary string of 15 to 256 characters.
10. Click **Start Backup**.

    For more information, see Backup Now field descriptions on page 42.
11. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

    The Start Messaging Software webpage refreshes periodically during the startup process and displays a status message after displaying the **Start Messaging information** message.

    After the Communication Manager Messaging software starts successfully, the system displays the `Start of Messaging completed` message.
12. Click **OK**.

Backup Now field descriptions

Settings	Description
Specify Data Sets	The data sets that you want to back up. The available options are: • **Server and System Files**: Back up the variable information to configure the server for a particular installation. • **Security File**: Back up the variable information to maintain security of the server. • **Messaging**: Back up one of the following options: - **Messaging Announcements** - **Messaging Translations and Messages** - **Messaging Translations, Names, and Messages** - **Messaging Translations and Names** - **Messaging Translations**
Full Backup	A full backup includes security data sets and files that configure both the Linux operating system and the applications. A **Full Backup** does not include any of the data sets.
Backup Method	
Method	The following methods are available for backup: • **SCP**: A means of securely transferring computer files between a local and a remote host, or

Settings	Description
	between two remote hosts, using the Secure Shell (SSH) protocol. • **FTP**: When you choose this option, you must enter the user name, the password, the host name or the IP address, and the directory. The default directory for backup data on the FTP server is `/var/home/ftp`. If you want to use the default directory, enter a forward slash (/) in the directory field. You must start the FTP server before backing up data. • **SFTP**: A network protocol that provides file transfers over data streams. The system adds the SFTP client to all Linux platforms.
User Name	The user name for storing the backup.
Password	The password for storing the backup.
Host Name	The host name.
Directory	The backup is stored on this network directory.
Encryption	
Encrypt backup using pass phrase	Defines if you want to encrypt the backup data. The pass phrase can be an arbitrary string of 15 to 256 characters. The pass phrase can contain any characters except the following: single quote ('), ampersand (&), back slash (\), single back quote (`), quote ("), and percent sign (%).

Restoring the system

About this task

You will need to stop Communication Manager Messaging before you restore the system.

The time required to restore the database depends on the amount of data in the backup and the LAN speed. Perform the following procedure for attended and unattended backups.

Procedure

1. Stop Communication Manager Messaging.

   For more information see, *Stopping Communication Manager Messaging.*

2. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.

   The system displays the View/Restore Data Web page.

3. In the **View current backup contents in** area, select **Network Device** or **Local Directory**. Use the same information that you used when you backed up the data to complete the following fields in case you selected **Network Device**:

   a. **Method**

   b. **User Name**
   c. **Password**
   d. **Host Name**
   e. **Directory**

4. Click **View**.

   The View/Restore Data Results Web page lists the backup images stored in the location that you specified. The system lists the most recent backups at the bottom of the list.

   You must select a backup image before you click **View**, or the system displays an error message. To clear the error message, click **Back** on the browser and then select a backup image.

5. To select the backup image you want to view or restore, click the corresponding option.

6. Click one of the following:

   - Preview. Use **Preview** if you are unsure that you have selected the correct backup image. When you click **Preview**:
     - A **View/Restore Data Results** screen displays a brief description of the data associated with the backup image.
     - Communication Manager Messaging data has one of the following names attached to the backup file name:
       - os-*
       - security-*
       - audix-tr-msg for translations and messages
       - audix-tr-name-msg for translations, names, and messages
       - audix-tr-name for translations and names
       - audix-tr for translations only
     - Click **Restore** on the second screen to begin the restore process.
   - Restore. When you click **Restore**, the system displays the View/Restore Data Results Web page which displays whether the restore procedure was successful.

7. Do one of the following:

   - If you do not have any remote networked machines, continue with Step 8.
   - If you have remote networked machines, do the following:

   a. Log off the Communication Manager Messaging server.
   b. Log in to the Communication Manager Messaging Web page.
   c. Run a manual update to and from all remote networked machines to correct any database inconsistencies.
   d. Continue with Step 8.

8. Restart Communication Manager Messaging.

   For more information, see *Stopping Communication Manager Messaging* and *Starting Communication Manager Messaging*..

Stopping Communication Manager Messaging

Use the Stop Messaging Software Web page to stop the Communication Manager Messaging software.

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.

   The system displays the Stop Messaging Software Web page.
3. To initiate a shutdown, click **Stop**.

   The system delays the shutdown process until all calls are completed. However, after three minutes the system ends all calls that remain active.

   The Stop Messaging Software Web page refreshes periodically during the shutdown process and displays a status message following the **Stop Messaging info** text.

   After the Communication Manager Messaging software stops completely, the system displays the *Stop of Messaging completed* message.
4. Click **OK**.

Starting Communication Manager Messaging

Use the Start Messaging Software Web page to start the Communication Manager Messaging software.

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

   The system displays the Start Messaging Software Web page.

   The Start Messaging Software Web page refreshes periodically during the startup process and displays a status message following the **Start Messaging information** text.

   After the Communication Manager Messaging software starts successfully, the system displays the *Start of Messaging completed* message.
3. Click **OK**.

Shutting down the server

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
3. On the Shutdown Server Web page, select from the following options:
   - **Delayed Shutdown**
   - **Immediate Shutdown**
4. (Optional) Select the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The system displays the confirmation screen.
6. Click **Ok** to continue.

Transferring files using WinSCP

Use the WinSCP utility to securely transfer files from a remote system to the virtual machine. WinSCP uses Secure Shell (SSH) and supports Secure FTP and legacy SCP protocols.

Before you begin

Ensure you have WinSCP on your computer. If not, download WinSCP from the Internet.

Procedure

1. Use WinSCP to connect to the virtual machine
2. Enter the credentials for SCP access.
3. In the warning dialogue boxes, click **OK** or **Continue** as necessary.
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 transfer is complete, close the WinSCP window and click **OK**.

Chapter 8: Optimization and scalibility

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers
- HP ProLiant Servers

Intel Virtualization Technology

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

All Intel Xeon processors include:

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

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

Note:

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

Other suggested BIOS settings

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

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

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

Dell PowerEdge Server

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

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

HP ProLiant Servers

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

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

VMware Tools

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

VMware tools provide:

- VMware Network acceleration

- Host to Guest time synchronization
- Disk sizing

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

❗ **Important:**

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

Timekeeping

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

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

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

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

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.

VMware networking best practices

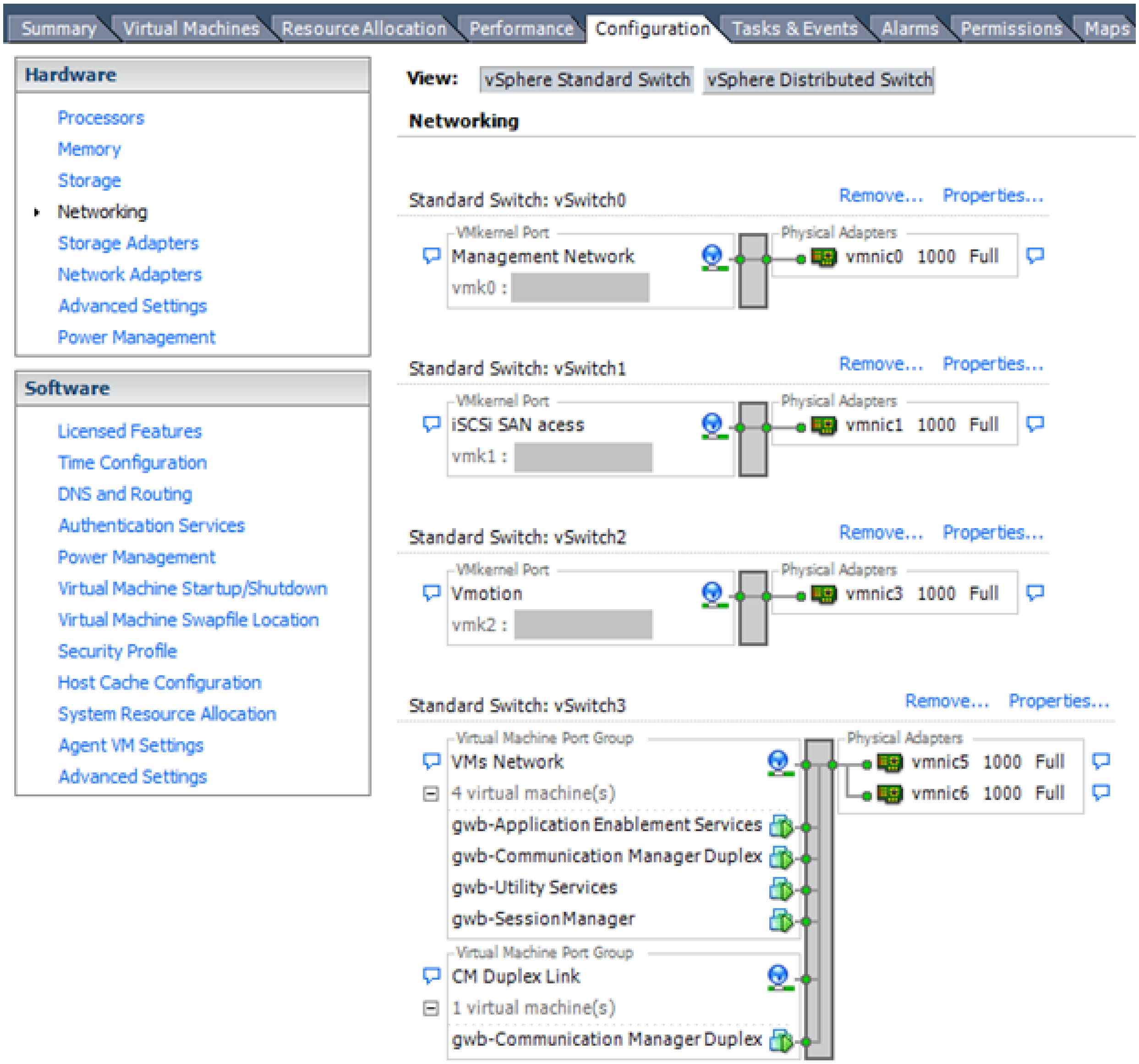
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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



Standard Switch: vSwitch0

VMkernel Port: Management Network, vmk0 : [redacted]

Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1

VMkernel Port: iSCSi SAN acess, vmk1 : [redacted]

Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2

VMkernel Port: Vmotion, vmk2 : [redacted]

Physical Adapters: vmnic3 1000 Full

Standard Switch: vSwitch3

Virtual Machine Port Group: VMs Network, 4 virtual machine(s)

- gwb-Application Enablement Services
- gwb-Communication Manager Duplex
- gwb-Utility Services
- gwb-SessionManager

Virtual Machine Port Group: CM Duplex Link, 1 virtual machine(s)

- gwb-Communication Manager Duplex

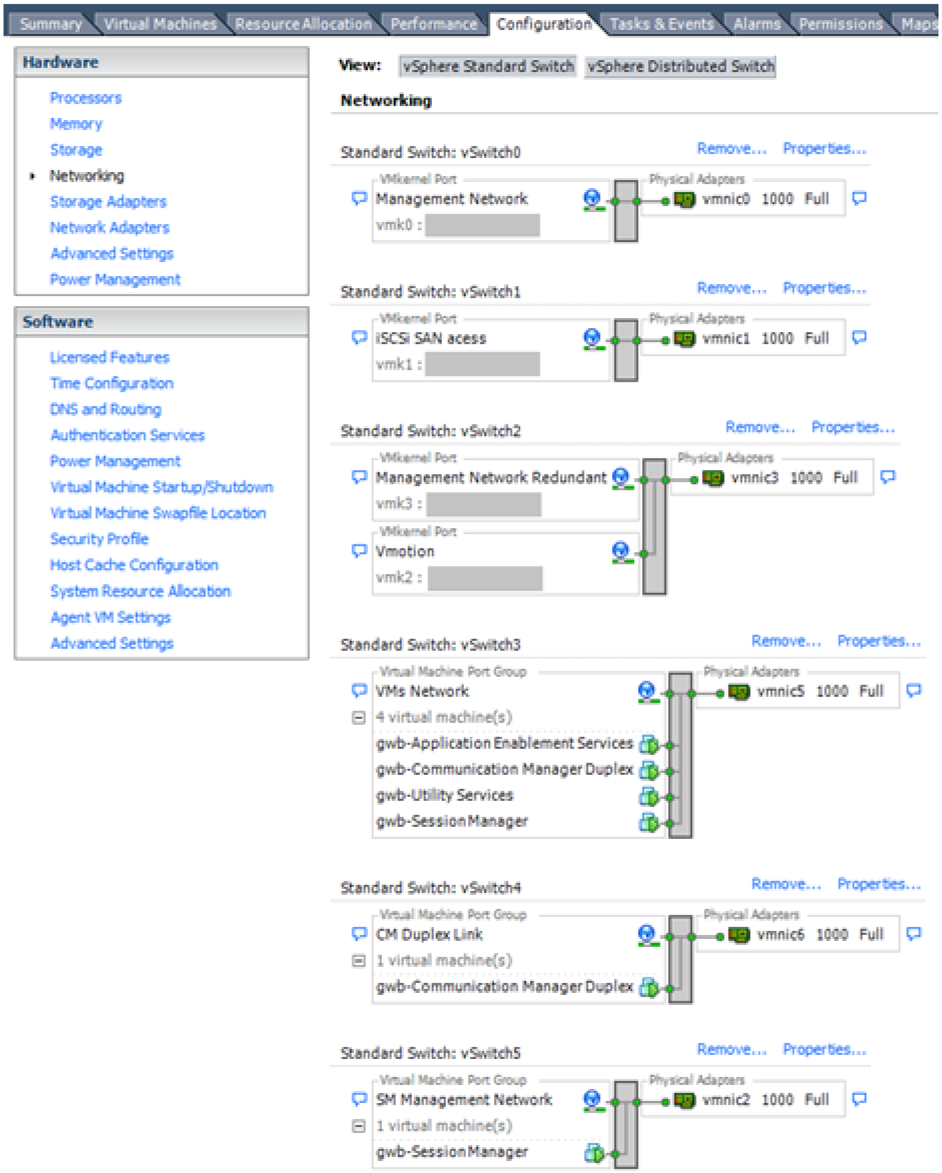
Physical Adapters: vmnic5 1000 Full; vmnic6 1000 Full

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.
- 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



Networking

Standard Switch: vSwitch0
- VMkernel Port: Management Network, vmk0 : [redacted]
- Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1
- VMkernel Port: iSCSI SAN acess, vmk1 : [redacted]
- Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2
- VMkernel Port: Management Network Redundant, vmk3 : [redacted]
- VMkernel Port: Vmotion, vmk2 : [redacted]
- Physical Adapters: vmnic3 1000 Full

Standard Switch: vSwitch3
- Virtual Machine Port Group: VMs Network
  - 4 virtual machine(s)
  - gwb-Application Enablement Services
  - gwb-Communication Manager Duplex
  - gwb-Utility Services
  - gwb-Session Manager
- Physical Adapters: vmnic5 1000 Full

Standard Switch: vSwitch4
- Virtual Machine Port Group: CM Duplex Link
  - 1 virtual machine(s)
  - gwb-Communication Manager Duplex
- Physical Adapters: vmnic6 1000 Full

Standard Switch: vSwitch5
- Virtual Machine Port Group: SM Management Network
  - 1 virtual machine(s)
  - gwb-Session Manager
- Physical Adapters: vmnic2 1000 Full

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.

Communication Manager Messaging only supports thick provisioning.

Appendix A: Migration

Overview

You can migrate a Communication Manager Messaging 6.x system running on System Platform or a Communication Manager Messaging 5.x system to a Virtualized Environment using VMware®.

The migration process consists of two phases:

1. Backing up data from the old system on page 55.
2. Restoring data on the new system on page 58.

Supported migration paths are based on the Communication Manager platform on which Communication Manager Messaging is installed.

If the installed Communication Manager Messaging system does not match the software release and patches required to start the migration, first upgrade your Communication Manager Messaging system. For more information, see Migration roadmap and limitations on page 54.

Migration roadmap and limitations

Roadmap

The minimal software required to migrate from Communication Manager Messaging 6.x running on System Platform is:

System Platform	VMware
Communication Manager Messaging 6.2 with Communication Manager Service Pack 7.01 and Communication Manager Messaging Service Pack 4.	Communication Manager Messaging 6.3 with Communication Manager Service Pack 6.3.6.0 and Communication Manager Messaging Service Pack 3.
Communication Manager Messaging 6.3 with Communication Manager Service Pack 6.3.1 and Communication Manager Messaging Service Pack 0.	Communication Manager Messaging 6.3 with Communication Manager Service Pack 6.3.6.0 and Communication Manager Messaging Service Pack 3.

The minimal software required to migrate from Communication Manager Messaging 5.x is:

Communication Manager Messaging 5.x	VMware
Communication Manager Messaging 5.2.1 with Communication Manager Patch 20790 and Communication Manager Messaging RFUs C1317rf +i.rpm and A9021rf+i.rpm	Communication Manager Messaging 6.3 with Communication Manager Service Pack 6.3.6.0 and Communication Manager Messaging Service Pack 3.

Supported data types

The system migrates the following types of data:

- Users, passwords, and profiles for System Management Interface and ssh access to Communication Manager Messaging virtual machine
- System password policies
- Backup schedules configured on System Management Interface
- Alarming and SNMP configuration
- System configuration, users, names, greetings, and messages

Limitations

The system does not migrate the following types of data. You must reconfigure the following data on VMware:

- Network configuration
- Time zone
- Network time protocol
- Authentication file
- Licensing configuration

Migrating Communication Manager Messaging to Virtualized Environment

Backing up data from the old system

Procedure

1. Upgrade the Communication Manager Messaging system to the minimal required software version. For more information about minimal required software, see Migration roadmap and limitations on page 54.
2. Stop Communication Manager Messaging.

   For more information, see Stopping Communication Manager Messaging on page 45.

3. Back up data.
   - If migrating from 6.x to VMware, the backups needs to be done from command line.
     - Migration data on the Communication Manager Messaging virtual machine by running `sudo /opt/ecs/sbin/backup -b -d ftp|scp|sftp://<user>:<passwd>@<hostname></full-path-directory> --verbose --migration-60` command.
     - Communication Manager Messaging application data by running `sudo /opt/ecs/sbin/backup -b -d ftp|scp|sftp://<user>:<passwd>@<hostname></full-path-directory> --verbose -- audix-tr-name-msg` command.

   Note:

   Only privileged users, dadmin, craft, init, and sroot can perform the migration backup. Administrative users admin and cust cannot perform migration backups.

   - If migrating from 5.2.1 to VMware, then the backups are to be done from SMI/web. Two backups are needed.
     - Migrating the Communication Manager Messaging system data. For more information, see Migrating the Communication Manager Messaging system data from 5.2.1 on page 56.
     - Backing up the Communication Manager Messaging application data. For more information, see Backing up the Communication Manager Messaging application data from 5.2.1 on page 57.
4. Shut down the Communication Manager Messaging system. For more information, see Shutting down the server on page 46.

Next steps

Restore data on the new system.

Migrating the Communication Manager Messaging system data from 5.2.1

Before you begin

Log on to System Management Interface.

To view the **Linux Migration to CM 6.0** option in System Management Interface, install the pre-migration patch. For more information, see *Migration roadmap and limitations*.

About this task

Perform this procedure to generate a backup file that you later restore on the VMware system.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)**.
2. In the navigation pane, click **Data Backup/Restore** > **Linux Migration to CM 6.0**.
3. On the Linux Migration to CM 6.0 - Backup Initiate page, complete the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.

- **User Name**
- **Password**
- **Host Name**. The hostname or IP address.
- **Directory**. The complete directory path where the backup is stored.

4. Click **Submit**.

   The system displays the Linux Migration - Backup Results dialog box.

5. To view the backup history, click **Status**.

   The system displays the Backup History page and a list of recent backups.

6. Select the backup file from the list and click **Check Status**.

   When the backup is complete, the system displays the message `Backup successful`.

   ⚠ **Caution:**

   Check the text to verify that there are no backup failure messages. If you ignore the backup failure, the restore operation might fail.

Backing up the Communication Manager Messaging application data from 5.2.1

Before you begin

Connect to the server where you want to back up the data.

Procedure

1. Log on to the System Management Interface page.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Data Backup/Restore** > **Backup Now**.
4. Select **Specify Data Sets**.
5. Clear the **Avaya Call Processing (ACP) Translations** check box.
6. Select the **Communication Manager Messaging** check box.

   The system displays the check box only if Communication Manager Messaging is installed on Communication Manager.

7. Select **Translations, Names, and Messages**.
8. Select the **Network Device** radio button.
9. Fill in the following fields:
   - **Method**. Select **scp**, **ftp**, or **sftp**.
   - **User Name**
   - **Password**
   - **Host Name**. The hostname or IP address.

- **Directory**. The complete directory path where the backup is stored.

10. To limit the size of a transferable file over the network for successful backup of the Communication Manager Messaging data, in the **Download size for the data being transferred** field, type a value from `1` through `200`.

    The value must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises one or more files that do not exceed the specified size. For example, if you set the download size to 5, the size of the data is 500 MB.

11. Click **Start Backup**.

    Communication Manager Messaging downloads and processes each backup file sequentially before downloading the next backup file in the data set.

    ❗ **Important:**

    The backup data set can contain multiple backup tar files. However, the system displays only the meta tar backup file on the View / Restore Data page.

Restoring data on the new system

Procedure

1. Deploy the Communication Manager Messaging OVA.

   For more information, see Deploying the Communication Manager Messaging OVA on page 21.

2. Administer network parameters. For more information, see Administering network parameters on page 24.

3. Configure the network settings.

   For more information, see Configuring the network on page 28.

4. Install the minimal required Communication Manager Messaging service packs.

   For more information, see *Avaya Aura® Communication Manager Messaging Release Notes*.

5. Stop Communication Manager Messaging.

   For more information, see Stopping Communication Manager Messaging on page 45.

6. Restore the following data using the *craft* user login:

   a. Migration data

   b. Communication Manager Messaging application data

   For more information, see Performing a restore on page 43.

7. Start Communication Manager Messaging.

   For more information, see Starting Communication Manager Messaging on page 45.

8. Configure the Communication Manager Messaging system. For more information, see Initial administration checklist on page 35.
9. Reconfigure the password for the scheduled backup.
10. Reboot Communication Manager Messaging.

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