Deploying Avaya Aura® Communication Manager Messaging

Release 7.0
Issue 1
September 2015

© 2014-2015, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

“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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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 one 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 products, 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 7
Purpose 7
Intended audience 7
Related resources 7
Documentation 7
Training 8
Viewing Avaya Mentor videos 9
Support 10
Chapter 2: Architecture overview 11
Appliance Virtualization Platform overview 11
Avaya Aura® Virtualized Environment overview 13
Topology 14
Components 15
Avaya components 15
VMware components 17
Third-party components 17
Deployment guidelines 17
Chapter 3: Deployment process 19
Chapter 4: Planning and configuration 20
Planning checklist 20
Server hardware and resources 20
Configuration tools and utilities 20
SAL Gateway 21
Software requirements 21
Transferring files using WinSCP 22
Communication Manager Messaging virtual machine resource requirements 23
Recommended setting to run Communication Manager Messaging at full capacity 24
Key customer configuration information 25
Downloading the Communication Manager Messaging OVA 26
Registering for PLDS 26
Downloading software from PLDS 26
Chapter 5: Deploying Communication Manager Messaging on the Avaya-provided server using Solution Deployment Manager 28
Checklist for deploying Communication Manager Messaging on Avaya-provided server 28
Installing the Solution Deployment Manager client on your computer 29
Deploying the Communication Manager Messaging OVA using Solution Deployment Manager 32
Chapter 6: Deploying Communication Manager Messaging on VMware using vSphere 35

Software installation checklist 35
Deploying the Communication Manager Messaging OVA using the vSphere Web client 35
Deploying the Communication Manager Messaging OVA using the vSphere client 39
Starting the Communication Manager Messaging virtual machine 43
Administering network parameters 43
Chapter 7: Configuration 45
Configuration checklist 45
Configuring the virtual machine automatic startup settings 45
IPv6 configuration 46
IPv6 46
Enabling IPv6 47
Disabling IPv6 48
Configuring the Communication Manager Messaging network 48
Network Configuration field descriptions 49
Setting the time zone 51
Setting up the network time protocol 51
Service pack installation 52
Communication Manager Messaging service packs 52
Downloading service packs 53
Installing a service pack 53
Removing a service pack 55
Chapter 8: Initial administration 58
License Management 58
License file for Communication Manager Messaging 58
Configuring the WebLM server 58
Authentication file management 59
Authentication file installation 59
Starting the AFS application 60
Creating an authentication file for a new system 60
Installing the authentication file 61
Obtaining the AFID 62
Chapter 9: Routine maintenance 63
Stopping Communication Manager Messaging 63
Backup and restore 63
Backing up the messaging application and the server data 63
Backup Now field descriptions 65
Restoring the messaging application and the server data 66
Starting Communication Manager Messaging 67
Shutting down the server 68
Appendix A: Upgrading and Migrating Communication Manager Messaging to Release 7.0 69
Overview 69
Migration roadmap and limitations 69

Checklist for upgrade or migration..... 71
Upgrading and migrating Communication Manager Messaging to Release 7.0 on Virtualized Environment..... 72
Appendix B: Best Practices for VMware performance and features..... 74
Best Practices for VMware performance and features..... 74
BIOS..... 74
VMware Tools..... 75
Timekeeping..... 76
Configuring the NTP time..... 77
VMware networking best practices..... 77
Storage..... 80
Thin vs. thick deployments..... 81
Best Practices for VMware features..... 81
Glossary..... 84

Chapter 1: Introduction

Purpose

This document provides procedures for deploying Avaya Aura® Communication Manager Messaging on:

- Avaya-provided server using Solution Deployment Manager
- VMware using the vSphere client or the vSphere Web client

This document includes installation, configuration, initial administration, 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 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			

Table continues…

	Title	Description	Audience
	Implementing Avaya Aura® Communication Manager Messaging	This document describes the implementation process of Communication Manager Messaging.	Service technicians Customers
Deployment and Upgrades			
	Deploying Avaya Aura® applications from Avaya Aura® System Manager	This document describes the deployment process of Avaya Aura® applications using Solution Deployment Manager.	Service technicians Customers
	Upgrading and Migrating Avaya Aura® applications from Avaya Aura® System Manager	This document describes the upgrade and migration process of Avaya Aura®applications using Solution Deployment Manager.	Service technicians Customers

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Training

The following courses are available on the Avaya Learning website at 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
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
2007V	What is New in Avaya Aura® 7.0
2009V	What is New in Avaya Aura® Communication Manager 7.0
2011V	What is New in Avaya Aura® System Manager & Avaya Aura® Session Manager 7.0
2009T	What is New in Avaya Aura® Communication Manager 7.0 Online Test
2013V	Avaya Aura® 7.0 Solution Management
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
2012V	Migrating and Upgrading to Avaya Aura® 7.0
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Chapter 2: Architecture overview

Appliance Virtualization Platform overview

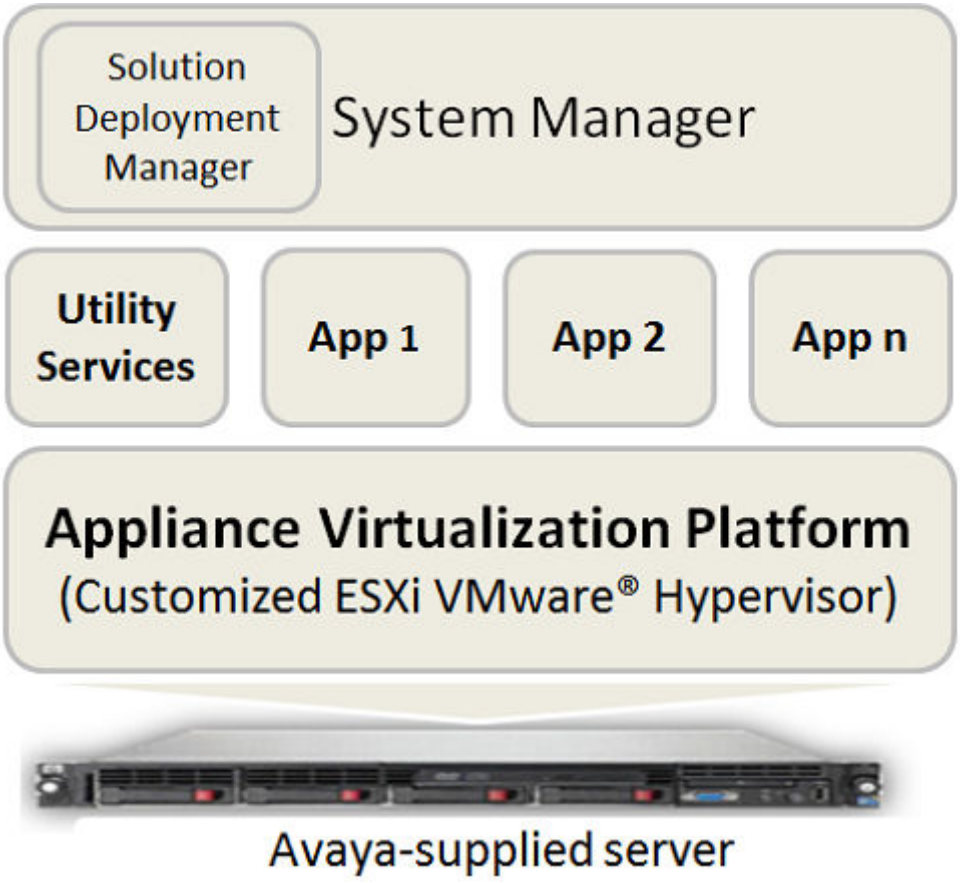
From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer.

Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, and HP ProLiant DL360p G8
- S8300D and S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.

Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.



In Release 7.0, Appliance Virtualization Platform replaces System Platform.

Avaya Aura® Release 7.0 supports the following applications on Appliance Virtualization Platform:

- Utility Services 7.0
- System Manager 7.0
- Session Manager 7.0
- Branch Session Manager 7.0
- Communication Manager 7.0
- Application Enablement Services 7.0
- WebLM 7.0
- Engagement Development Platform 3.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7

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.

Note:

The following terms are often used interchangeably in the document:

- Server and host
- Reservations and configuration values

Customer deployment

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.

Starting with Communication Manager Messaging Release 7.0, you can deploy Communication Manager Messaging on Virtual Environment in the following ways:

Deployment client	Client connection
vSphere Web Client	vCenter Server
vSphere Client	vCenter Server
vSphere Client	ESXi Host

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.

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 23.

Security

You can use the Out Of Band Management (OOBM) feature for secure management and administration of Avaya products. Out Of Band Management physically and logically separates each network connection to a customer's private IT management network from the other.

You can use **System Management Interface** to configure the system and restrict management traffic to the administered out-of-band interface.

You can configure Out Of Band Management after the OVA deployment, using **System Management Interface** > **Server Configuration** > **Network Configuration**.

Best Practices for VMware performance and features

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

Important:

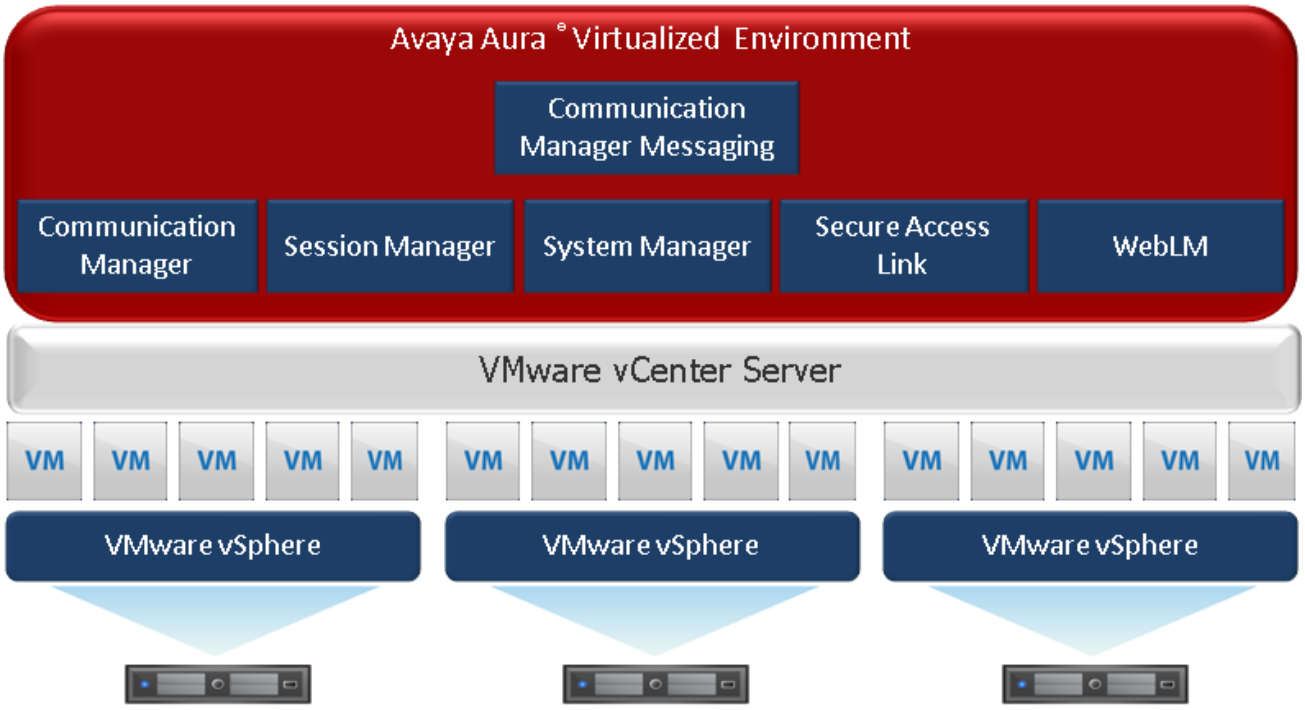
Do not use VMware Snapshots because Snapshot operations can adversely affect Communication Manager Messaging service.

Related links

Topology on page 14

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 minimum capacity. 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.

Note:

You can integrate Communication Manager Messaging with a Communication Manager simplex or duplex configuration.

Related links

Avaya Aura Virtualized Environment overview on page 13

Components

Avaya components

Component	Version	Platform	Description
Avaya Aura® components			

Table continues…

Component	Version	Platform	Description
Avaya Aura® Communication Manager	7.0 6.3.100 6.3.6 6.3.4 6.3.2 6.3	Virtualized Environment	The IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises.
Avaya Aura® Communication Manager Messaging	7.0 6.3.3	Virtualized Environment	A part of the Avaya Aura® architecture, but Communication Manager Messaging can also be used in other environments
Avaya Aura® Session Manager	7.0 6.3.9 6.3.8 6.3.4 6.3.2	Virtualized Environment	A SIP routing and integration tool that integrates SIP entities across the enterprise network. You can view and manage each location, branch, and application in totality, not as separate units within the enterprise.
Avaya Aura® System Manager	7.0 6.3.9 through 6.3.15 6.3.8 6.3.4 6.3.2	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	7.0 6.3.8 6.3.4 6.3.2	Virtualized Environment	A web-based license manager that manages licenses of one or more Avaya software products.
Message Networking	6.3 5.2	Avaya server with Linux® Operating System	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	5.0, 5.1, and 5.5	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	5.0, 5.1, and 5.5	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	5.0, 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	5.0, 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.

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.

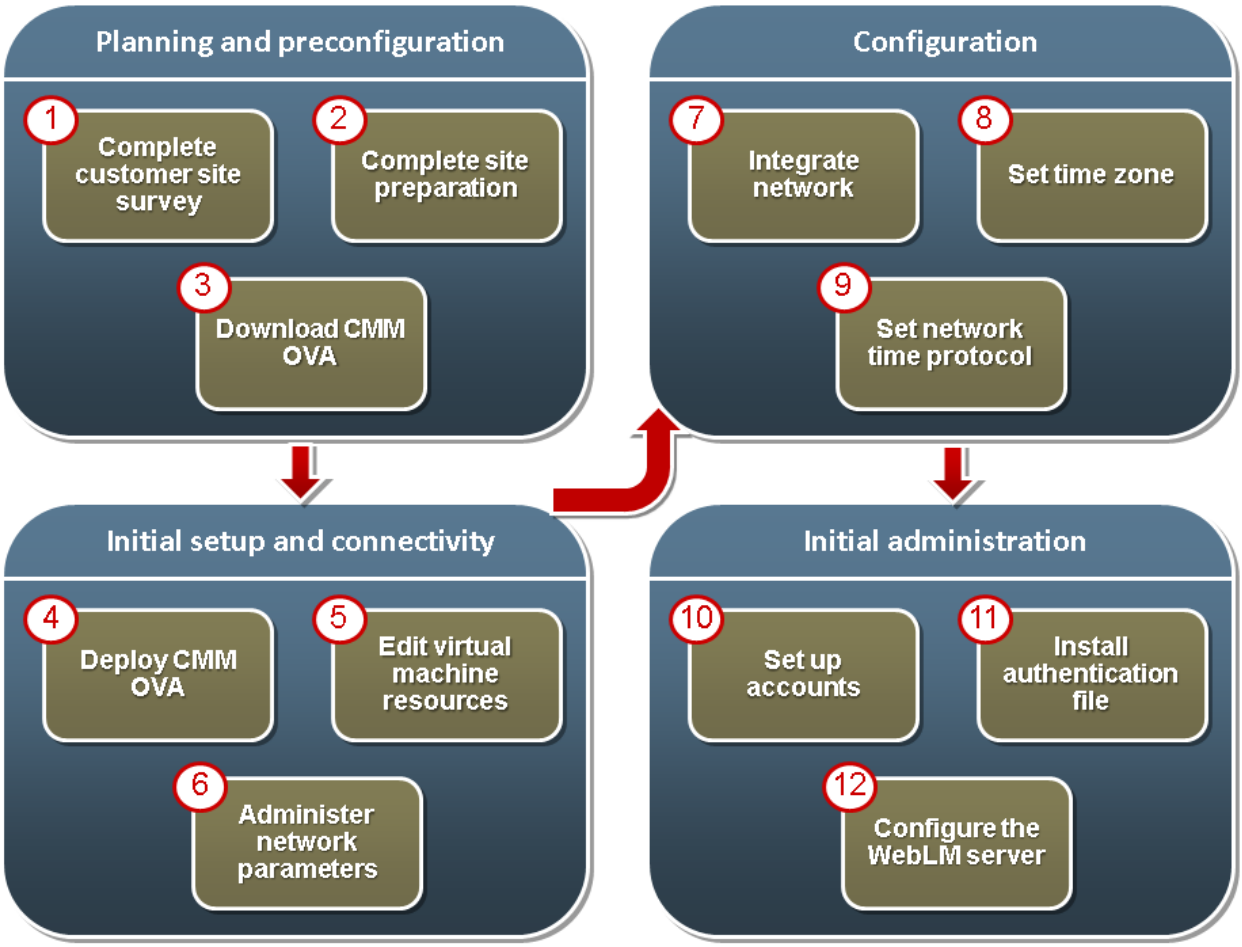
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not oversubscribe resources. Oversubscribing affects performance.
- Monitor the server, host, and virtual appliance performance.

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.

Chapter 3: Deployment process

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



Chapter 4: Planning and configuration

Planning checklist

No.	Task	References	Notes	✔
1	Download the required documentation.	See Documentation on page 7.	—	
2	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 20.	—	
3	Plan the staging and verification activities and assign the resources.	See Communication Manager Messaging virtual machine resource requirements on page 23.	—	
4	Download Communication Manager Messaging OVA.	See Downloading software from PLDS on page 26.	—	

Server hardware and resources

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see http://www.vmware.com/resources/guides.html.

Configuration tools and utilities

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 and vSphere web client
- Solution Deployment Manager 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

Related links

SAL Gateway on page 21

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 .

Related links

Configuration tools and utilities on page 20

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	5.0, 5.1, and 5.5
VMware vCenter Server	5.0, 5.1, and 5.5 **Note:** VMware requires the version of vCenter to be the same or greater than the version running on the hosts that it manages.

Table 2: Appliance Virtualization Platform software requirement

Equipment	Software versions
Appliance Virtualization Platform ESXi	5.5

Table 3: Communication Manager Messaging software requirement

Software	Software versions
Communication Manager Messaging	7.0

Table 4: 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*.

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**.

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.

Resource Requirements	Small System	Medium System	Medium System	Large System
	Heavy traffic[1]	Heavy traffic[2]	Heavy traffic[3]	Heavy traffic[4]
Mailboxes	1,000	2,400	6,000	15,000
Ports	24	40	210	210
Virtual machine	1	1	1	1
Virtual CPUs	1	1	1	2
Minimum CPU speed	2 GHz	2 GHz	2 GHz	4 GHz
Virtual CPU reservations	2 GHz	2 GHz	2 GHz	4 GHz
Virtual memory	2 GB	2 GB	2 GB	2 GB
Virtual memory reservations	2 GB	2 GB	2 GB	2 GB
Media (Hard disk 3) disk space	25 GB	60 GB	150 GB	375 GB
Total VM disk space	90 GB	125 GB	215 GB	440 GB
Average I/OPS	27	57	121	118
Shared Network Interface Cards	One @ 1000 Mbps	One @ 1000 Mbps	One @ 1000 Mbps	One @ 1000 Mbps
Average network usage	552 KBps	785 KBps	3956 KBps	4259 KBps

Note:

1. Heavy Traffic: CMM to serve a new call every 4 seconds. On an average, each user receives twelve voice messages every 24 hours.

2. CMM to serve a new call every 3 seconds. On an average, each user receives nine voice messages every 24 hours.
3. CMM to serve two calls every second. On an average, each user receives eighteen voice messages every 24 hours.
4. CMM to serve two calls every second. On an average, each user receives seven voice messages every 24 hours.

Recommended setting to run Communication Manager Messaging at full capacity

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 1 vCPU, 2 GB memory, and 90 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.
- 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.

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
VM Name	
Number of subscriber mailboxes	
Messaging IPv4 Address	
Messaging IPv4 Netmask	
Messaging IPv4 Gateway	
Out of Band Management IPv4 Address (optional)	
Out of Band Management IPv4 Netmask (optional)	
Messaging Hostname	
NTP Server(s) (optional)	
DNS Server(s) (optional)	
Search Domain List (optional)	
WebLM Server IPv4 Address	
Messaging Privileged Administrator User Login	
Messaging Privileged Administrator User Password	
IPv6 IP address (optional)	
IPv6 subnet mask (optional)	
IPv6 Default Gateway address (optional)	

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 by using one of the following:
   - Select an application type from the list and the version number.

- By download name

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: Deploying Communication Manager Messaging on the Avaya-provided server using Solution Deployment Manager

Checklist for deploying Communication Manager Messaging on Avaya-provided server

Use the checklist to deploy Communication Manager Messaging by using the Solution Deployment Manager client or from System Manager Solution Deployment Manager.

#	Action	Link/Notes	✔
1	Download the `Avaya_SDMClient_win64_7.0.0.1.17824_7.zip` file from the Avaya Support website at http://support.avaya.com.	Perform the task if System Manager is unavailable.	
2	From the Avaya Support website at http://support.avaya.com, download the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and the `.ova` files for Communication Manager Messaging.	-	
3	Upload the software for deployment and upgrade operations to the local or remote software library of System Manager. For example, OVA, firmware, software patches, service packs, and images.	For more information see *Administering Avaya Aura® System Manager*.	
4	For Communication Manager Messaging deployment, install the S8300D or S8300E server.		
5	Install Appliance Virtualization Platform on the server.	For more information, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.	

Table continues…

#	Action	Link/Notes	✔
6	Install the `Avaya_SDMClient_win64_7.0.0.1.17824_7.exe` file.	For more information, see Installing the Solution Deployment Manager client on your computer on page 29.	
7	Ensure that network configuration data such as naming conventions, IP address, netmask, and gateway, is accessible.	-	
8	Add a location.	For more information, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.	
9	Add an Appliance Virtualization Platform host as 192.168.13.6.		
10	Create the virtual machine, deploy Utility Services, and complete the required configuration.	For more information, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.	
11	Close the Solution Deployment Manager client.		
12	Set the following parameters on the computer on which the Solution Deployment Manager client is installed: • IP address: 192.11.13.5 • Netmask: 255.255.255.252 • Gateway: 192.11.13.6	See Key customer configuration information on page 25.	
13	Start the Solution Deployment Manager client with the new IP address.		
14	Deploy Communication Manager and then Communication Manager Messaging.	For more information, see Deploying CMM through Solution Deployment Manager on page 32.	
15	Verify that the deployment of Communication Manager Messaging is successful.	-	

Installing the Solution Deployment Manager client on your computer

About this task

In Avaya-appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches and hypervisor patches.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

Important:

For deployments through service port by using the Solution Deployment Manager client, get the Solution Deployment Manager client software from the Avaya support site. The Solution Deployment Manager client software version available in the media does not support the service port deployment.

Before you begin

1. Ensure that Windows 7.0 or 8.1 operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

2. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

   Tip:

   In the explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space available.

3. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.

4. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
5. Ensure that 443 and 1527 ports are available.
6. Close all applications that are running on your computer.
7. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

   Tip:

   On **Computer**, right-click properties, and perform the following:

   a. In the left navigation pane, click **Advanced system settings**.

   b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.

   c. Verify the system variables.

8. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Any operation that you perform might fail if the computer is not connected to the network.

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.0.1.17824_7.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

On the Avaya PLDS website, you can provide the application name as **System Manager**, and version as **7.0**.

2. Copy the zip file, and extract to a location on your computer by using the WinZip application.
3. Using the **Run as administrator** option, run the `Avaya_SDMClient_win64_7.0.0.1.17824_7.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
4. On the Welcome page, click **Next**.
5. On the License Agreement page, click **I accept the terms of the license agreement** and click **Next**.
6. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.
7. Click **Next**.
8. On the Preinstallation Summary page, review the information, and click **Next**.
9. On the Summary and Validation page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

      The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.
   c. Verify the product information and the system requirements.

      The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.

      Important:

      If port 443 is unavailable, verify if the Skype application is running on the computer, and quit the application. If you close Skype, the application continues to run in the background. For more information, see “Solution Deployment Manager client installation fails” in *Troubleshooting Avaya Aura® System Manager*.
10. Click **Install**.
11. To exit the installer, on the Install Complete page, click **Delete**.

    The installer creates a shortcut on the desktop.
12. To start the client, click 

.

Next steps

To enable the Solution Deployment Manager client to communicate with the services port of Appliance Virtualization Platform, set the following on the technician computer:

- IP address: 192.168.13.5
- Netmask: 255.255.248
- Gateway: 192.168.13.1

Deploying the Communication Manager Messaging OVA using Solution Deployment Manager

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy Communication Manager Messaging OVA on the Avaya-provided server.

To deploy Communication Manager Messaging, you can use the System Manager Solution Deployment Manager or the Solution Deployment Manager client, if System Manager is unavailable.

Before you begin

- Ensure that you complete the deployment checklist

  For more information, see Checklist for deploying Communication Manager Messaging using SDM on page 28.
- Add a location.
- Add Appliance Virtualization Platform to a location.
- Download the required OVA files to System Manager.

  For information, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (), and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, perform the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.

c. In **VM Name**, type the virtual machine name.

5. In the Select Resource Pool and Datastore section, select a data store.
6. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      If you are deploying the OVA by using the Solution Deployment Manager client, you can use the default software library that is set during the client installation.

   b. In **Select OVAs**, select the Communication Manager Messaging OVA file that you want to deploy.
   c. In **Select Flexi Footprint**, select a subscriber configuration based on the system capacity needs:

Number of subscribers	Media (Hard disk 3) disk space in GB	Total VM disk space in GB
1,000	25	90
2,400	60	125
6,000	150	215
15,000	375	440

      In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to Communication Manager Messaging.

7. In the Network Parameters section, configure the following parameters:
   a. In the **Messaging IPv4 Address** field, type the address.
   b. In the **Messaging IPv4 Netmask** field, type the network mask address.
   c. In the **Messaging IPv4 Gateway** field, type the gateway address.
   d. **(Optional)** In the **Out of Band Management IPv4 Address** field, type the OOBM address.
   e. **(Optional)** In the **Out of Band Management IPv4 Netmask** field, type the OOBM network mask address.
   f. In the **Messaging Hostname** field, type the **Fully Qualified Domain Name (FQDN)** for the host.
   g. **(Optional)** In the **NTP Server(s)** field, type the NTP server names.
   h. **(Optional)** In the **DNS Server(s)** field, type the name of the DNS server.
   i. **(Optional)** In the **Search Domain List** field, type the domain search list.
   j. In the **WebLM Server IPv4 Address** field, type the address for the webLM server.
   k. In the **Messaging Privileged Administrator User Login** field, type the user name.
   l. In the **Messaging Privileged Administrator User Password** section, in the **Enter password** field, type the password. In the **Confirm password** field, retype the password.

8. In the Configuration Parameters section, complete the fields.

   For more information, see Configuring the network on page 48.

9. Click **Deploy**.
10. Click **Accept the license terms**.

    In the Host for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Host <host name> page.

    Note:

    The Manage Elements page in the inventory does not display the user credentials. You must manually update the user credentials.

11. To view details, click the **Status Details** link.

    For information about VM Management field descriptions, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

Chapter 6: Deploying Communication Manager Messaging on VMware using vSphere

Software installation checklist

No.	Task	References	Notes	✔
1	Deploy the Communication Manager Messaging OVA.	• To deploy Communication Manager Messaging using the vSphere web client, see Deploying CMM OVA on vCenter with vSphere web client on page 35. • To deploy Communication Manager Messaging using the vSphere client, see Deploying CMM using vSphere client on page 39.	—	
2	Administer network parameters.	See Administering network parameters on page 43.	—	

Deploying the Communication Manager Messaging OVA using the vSphere Web client

About this task

Use this procedure to deploy the Communication Manager Messaging OVA on a host managed by vCenter using the vSphere Web client.

Note:

You cannot deploy the Communication Manager Messaging OVA to a host not managed by vCenter using the vSphere Web client.

Procedure

1. Log in to the vCenter using the vSphere Web client.

2. Click **Hosts and Clusters**.

   The system displays the list of available hosts and clusters.

3. Click the host where you want to deploy the Communication Manager Messaging OVA.
4. Click **Actions** > **Deploy OVF Template**.
5. In the Select source window, select the OVA file and click **Next**. Perform one of the following to select the OVA file:
   - If the OVA file is located on an http server, enter the full URL in the **URL** field.
   - If the OVA file is downloaded to a location accessible from your computer, click **Browse** to select the location.
6. In the Review details window, verify the details of the Communication Manager Messaging OVA template and click **Next**.
7. In the Accept License Agreements window, read the license agreement, click **Accept**, and click **Next**.
8. In the Select name and folder window, do the following:
   a. In the **Name** field, type a unique name for the new virtual machine.
   b. In the **Select a folder or datacenter** field, select a folder or a datacenter location to store the virtual machine.
   c. Click **Next**.
9. In the Select configuration window, select a subscriber configuration based on the system capacity needs as shown in the table below:

Number of subscribers	Media (Hard disk 3) disk space (GB)	Total VM disk space (GB)
1,000	25	90
2,400	60	125
6,000	150	215
15,000	375	440

   Though you select the subscriber configuration in this step, you must allocate the required resources after you complete the deployment procedure. For more information, see step 16 of this procedure.

10. In the Select storage window, select a data store large enough to accommodate the virtual machine and all its virtual disk files.

    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.

    a. In the **Select virtual disk format** field, accept the default disk format, **Thick Provision Lazy Zeroed**
    b. In the **VM Storage Policy** field, select an appropriate option to choose VM storage policies for the host that you have selected.

To use this option, you must define VM storage policies for the host that you have selected.

c. In the datastore table, select a datastore that accommodates your subscriber configuration selected in step 9.

d. Click **Next**.

11. In the Network Mapping window, use **Out of Band Management** (OOBM) to separate the management traffic from the rest of the network traffic.

    Out of Band Management helps you to separate the management traffic by associating the network defined in the Communication Manager Messaging VM with the network defined on the host. If there are multiple virtual machine networks configured on the host, you can choose a different **Destination Network** for each of the **Source Network**.

    a. In the **Source Network** column, for both the **Public** and **Out of Band Management** entries, click the default entry under the **Destination Network** column.

    Note:

    You may need to click on the default entry multiple times to make the drop-down menu appear.

    The system displays a drop-down menu.

    b. Click on a host network in the **Destination Network** drop-down menu to associate with an entry in the **Source Network** column.

12. Click **Next**.

13. If you are deploying the Communication Manager Messaging OVA file using the vSphere Web client through vCenter, you must configure some of the application settings using the Customize template window.

    a. In the **Messaging IPv4 Address** field, type the address.

    b. In the **Messaging IPv4 Netmask** field, type the network mask address.

    c. In the **Messaging IPv4 Gateway** field, type the gateway address.

    d. **(Optional)** In the **Out of Band Management IPv4 Address** field, type the OOBM address.

    e. **(Optional)** In the **Out of Band Management IPv4 Netmask** field, type the OOBM network mask address.

    f. In the **Messaging Hostname** field, type the **Fully Qualified Domain Name (FQDN)** for the host.

    g. **(Optional)** In the **NTP Server(s)** field, type the NTP server names.

    h. **(Optional)** In the **DNS Server(s)** field, type the name of the DNS server.

    i. **(Optional)** In the **Search Domain List** field, type the domain search list.

    j. In the **WebLM Server IPv4 Address** field, type the address for the webLM server.

    k. In the **Messaging Privileged Administrator User Login** field, type the user name.

l. In the **Messaging Privileged Administrator User Password** section, in the **Enter password** field, type the password. In the **Confirm password** field, retype the password.

m. Click **Next**.

14. In the Ready to Complete window, verify the deployment settings.

a. Do not select the **Power on after deployment** check box.

b. Click **Finish**.

The system displays the progress of the task in the **vSphere Client Status** panel.

The deployment process takes about 15 minutes to complete, based on the network speed. If the OVA file location is an http server, the deployment process might take more time.

15. Right-click the virtual machine, and click **Edit Settings**.

If you have set the subscriber configuration properly during the deployment of the OVA file, the CPU and memory values are automatically configured by the system. However you must set the disk size accordingly. If you are deploying Communication Manager Messaging through the vSphere client directly connected to a host, you must set the CPU, memory, and disk space.

Number of subscribers	Virtual CPUs	Virtual CPU reservations (GHz)	Virtual memory (GB)	Virtual memory reservations (GB)	Media (Hard disk 3) disk space (GB)
1,000	1	2	2	2	25
2,400	1	2	2	2	60
6,000	1	2	2	2	150
15,000	2	4	2	2	375

16. To edit the hardware settings, on the Virtual Machine Properties window, click the **Hardware** tab, perform the following:

a. CPU: In the left pane, click CPU. 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.

Note:

The system automatically performs the steps a and b mentioned above .

c. Hard disk: In the left pane, click **Hard disk 3**.

In the **Disk provision** area, in **Provisioned size** field, enter the value for disk space. Ensure that you allocate the size based on the subscribers that you have configured.

17. To edit resource settings, on the Virtual Machine Properties window, click the **Resources** tab, perform the following:
    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 by selecting a value. CPU reservation defines guaranteed CPU allocation for a virtual machine.
    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, by selecting a value. Select whether the memory is specified in MB or GB.
18. Click **OK**.

Deploying the Communication Manager Messaging OVA using the vSphere client

About this task

Use this procedure to deploy the Communication Manager Messaging OVA to the ESXi host using the vSphere client. The vSphere client can be directly connected to the ESXi host or connected through vCenter.

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, select the OVA file, and click **Next**. 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. In the OVF Template Details window, verify the details of the Communication Manager Messaging OVA template and click **Next**.
5. In the End User License Agreement window, read the license agreement, click **Accept**, and click **Next**.
6. In the Name and Location window, do the following:
    a. In the **Name** field, type a unique name for the new virtual machine.
    b. Select the inventory location to deploy the virtual machine.
    c. Click **Next**.

Note:

You are not prompted for the inventory location if you are deploying through the vSphere client directly connected to the ESXi host.

7. In the Deployment Configuration window, select a subscriber configuration based on the system capacity needs as shown in the table below:

Number of subscribers	Media (Hard disk 3) disk space (GB)	Total VM disk space (GB)
1,000	25	90
2,400	60	125
6,000	150	215
15,000	375	440

Though you select the subscriber configuration in this step, you must allocate the required resources after you complete the deployment procedure. For more information, see step 16 of this procedure.

8. In the Host/Cluster window, select a host or cluster, and click **Next**.

Note:

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**.

Note:

The system does not display the Storage window if you are deploying through the vSphere client directly connected to the ESXi host. In that case the only storage choice is that of the hard disk on the host.

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 that accommodates your subscriber configuration selected in step 7.

10. In the Disk Format window, accept the default disk format, **Thick Provision Lazy Zeroed**, and click **Next**.

For more information about the virtual disk, see Thin vs. thick deployments on page 81.

11. In the Network Mapping window, use **Out of Band Management** (OOBM) to separate the management traffic from the rest of the network traffic.

Out of Band Management helps you to separate the management traffic by associating the network defined in the Communication Manager Messaging VM with the network defined on

the host. If there are multiple virtual machine networks configured on the host, you can choose a different **Destination Network** for each of the **Source Network**.

a. In the **Source Network** column, for both the **Public** and **Out of Band Management** entries, click the default entry under the **Destination Network** column.

Note:

You may need to click on the default entry multiple times to make the drop-down menu appear.

The system displays a drop-down menu.

b. Click on a host network in the **Destination Network** drop-down menu to associate with an entry in the **Source Network** column.

12. Click **Next**.
13. If you are deploying the Communication Manager Messaging OVA file using the vSphere client through vCenter, you must configure some of the application settings using the Properties window.
    a. In the **Messaging IPv4 Address** field, type the address.
    b. In the **Messaging IPv4 Netmask** field, type the network mask address.
    c. In the **Messaging IPv4 Gateway** field, type the gateway address.
    d. **(Optional)** In the **Out of Band Management IPv4 Address** field, type the OOBM address.
    e. **(Optional)** In the **Out of Band Management IPv4 Netmask** field, type the OOBM network mask address.
    f. In the **Messaging Hostname** field, type the **Fully Qualified Domain Name (FQDN)** for the host.
    g. **(Optional)** In the **NTP Server(s)** field, type the NTP server names.
    h. **(Optional)** In the **DNS Server(s)** field, type the name of the DNS server.
    i. **(Optional)** In the **Search Domain List** field, type the domain search list.
    j. In the **WebLM Server IPv4 Address** field, type the address for the webLM server.
    k. In the **Messaging Privileged Administrator User Login** field, type the user name.
    l. In the **Messaging Privileged Administrator User Password** section, in the **Enter password** field, type the password. In the **Confirm password** field, retype the password.

    If the vSphere client is directly connected to the ESXi host, you need to manually configure the network parameters after deployment. For more information, see *Configuring the Communication Manager Messaging network*.

    m. Click **Next**.
14. In the Ready to Complete window, verify the deployment settings.
    a. Do not select the **Power on after deployment** check box.

b. Click **Finish**.

The system displays the progress of the task in the **vSphere Client Status** panel.

The deployment process takes about 15 minutes to complete, based on the network speed. If the OVA file location is an http server, the deployment process might take more time.

15. Right-click the virtual machine, and click **Edit Settings**.

If you have set the subscriber configuration properly during the deployment of the OVA file, the CPU and memory values are automatically configured by the system. However you must set the disk size accordingly. If you are deploying Communication Manager Messaging through the vSphere client directly connected to a host, you must set the CPU, memory, and disk space.

Number of subscribers	Virtual CPUs	Virtual CPU reservations (GHz)	Virtual memory (GB)	Virtual memory reservations (GB)	Media (Hard disk 3) disk space (GB)
1,000	1	2	2	2	25
2,400	1	2	2	2	60
6,000	1	2	2	2	150
15,000	2	4	2	2	375

16. To edit hardware settings, on the Virtual Machine Properties window, click the **Hardware** tab, perform the following:

a. CPU: In the left pane, click CPU. 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.

c. Hard disk: In the left pane, click **Hard disk 3**.

In the **Disk provision** area, in **Provisioned size** field, enter the value for disk space. Ensure that you allocate the size based on the subscribers that you have configured.

17. To edit resource settings, on the Virtual Machine Properties window, click the **Resources** tab, perform the following:

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 by selecting a value. CPU reservation defines guaranteed CPU allocation for a virtual machine.

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, by selecting a value. Select whether the memory is specified in MB or GB.

18. Click **OK**.

Starting the Communication Manager Messaging virtual machine

Procedure

1. In the vSphere client or vSphere web 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

About this task

You must perform the following procedure only if you are deploying the Communication Manager Messaging OVA using the vSphere client that is directly connected to the ESXi host.

Procedure

1. In the vSphere client console window, log in as `craft` and type `craft01` as the password.

   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. In the **Enter Login Name** field, type the login name for the Customer Privileged Administrator account. For example, `dadmin`
5. In the **New password** field, type the new password.
6. In the **Retype new password** field, reenter the password.
7. Configure additional network settings.

   For more information, see Configuring the network on page 48.

Chapter 7: 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 45.	—	
2	Configure the network settings.	See Configuring the network on page 48.	—	
3	Set the time zone.	See Setting the time zone on page 51.	—	
4	Set up the network time protocol.	See Setting up the network time protocol on page 51.	—	
5	Install service packs.	See Communication Manager Messaging service packs on page 52.	—	

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

IPv6

Internet Protocol version 6 (IPv6) is the successor to IPv4. IPv6 supports 128–bit addresses and satisfies the rapidly growing demand for IP addresses. In contrast, IPv4 supported 32–bit. IPv6 also improves security, ease of configuration, and routing performance. IPv6 can coexist with IPv4 networks, easing the transition process.

The IETF (Internet Engineering Task Force) published RFC 2460, the internet standard specification that defines IPv6, in December 1998.

Addressing

By using 128-bit addresses, IPv6 has about $3.4x10^{38}$ unique IP addresses, more than enough for every network device. This eliminates the IPv4 mechanisms, such as NAT (network address transitions), that are used to relieve IP address exhaustion. IPv6 addresses are normally written as hexadecimal digits with colon separators, for example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents a string of zeroes, according to RFC4291.

Simplicity

IPv6 simplifies the routing process by changing the packet header and packet forwarding:

- Simplified packet header, despite enhanced functionality.
- IPv6 routers do not perform fragmentation. This is carried out by IPv6 hosts.
- IPv6 routers do not need to recompute a checksum when header fields change.
- Routers no longer need to calculate the time a packet spent in a queue.
- IPv6 supports stateless address configuration, so IPv6 hosts can be configured automatically when connected to a routed IPv6 network through ICMPv6. Stateful configuration using DHCPv6 and static configuration are also available.

Deployment and transition

There are several mechanisms that ease the deployment of IPv6 running alongside IPv4. The key to the transition is dual-stack hosts. Dual-stack hosts refers to the presence of two IP software implementations in one operating system, one for IPv4 and one for IPv6. These dual-stack hosts can run the protocols independently or as a Hybrid. The Hybrid is the common form on recent server operating systems and computers.

When an IPv6 host or network must use the existing IPv4 infrastructure to carry IPv6 packets, *Tunneling* provides the solution. Tunneling encapsulates IPv6 packets within IPv4. Tunneling can be either *automatic* or *configured*, the latter being more suitable for large, well-administered networks.

Key differences between IPv4 and IPv6

	IPv4	IPv6
Address space	32-bit, about $4.3x10^9$	128-bit, about $3.4x10^{38}$
Security	IPSec support is optional.	IPSec support is required.
Configuration	Requires DHCP or manual configuration.	Stateless auto-configuration. Does not require DHCP or manual configuration.
Address format	Decimal digits with colon separators, for example: 192.168.1.1	Hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents four zeros "0000"
Broadcast and Multicast support	Yes	No Broadcast. Various forms of Multicast — better network bandwidth efficiency
QoS support	ToS using DIFFServ	Flow labels and flow classes, more granular approach.

Feature Support in Avaya Branch Gateways

Certain Branch Gateway features are not supported in IPv6.

Enabling IPv6

Procedure

1. Log on to Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43

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

Procedure

1. Log on to Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43

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

About this task

You must perform the following procedure only if you are deploying the Communication Manager Messaging OVA using the vSphere client that is directly connected to the ESXi host.

Procedure

1. Log on to Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43

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 host name of the virtual machine. You can align the host name with the DNS name of the virtual machine. Do not type underscore (_) in the **Host Name** field.
Alias Host Name	The alias host name for duplicated virtual machines only. When a duplicated virtual machine runs in survivable mode, ensure that the system displays the **Alias Host Name** field.
DNS Domain	The domain name server (DNS) domain of the virtual machine.
Search Domain List	The DNS domain name of the search list. If there are more than one search list names, separate each name with commas.
Primary DNS	The primary DNS IP address.
Secondary DNS	The secondary DNS IP address. This field is optional.
Tertiary DNS	The tertiary DNS IP address. This field is optional.
Server ID	The unique server ID, which is a number between 1 and 256. On a duplicated virtual machine or survivable virtual machine, the number cannot be 1.
IPv6 is currently	Specifies the status of IPv6. The options are: enabled and disabled.
Default Gateway IPv4	The default gateway IP address.
Default Gateway IPv6	The IPv6-compliant IP address of the default gateway.
IP Configuration	The set of parameters to configure an Ethernet port, such as, eth0, eth1, or eth2. The parameters are: • **IPv4 Address** • **Subnet Mask** • **IPv6 Address**

Table continues…

Name	Description
	• **Prefix** • **Alias IP Address: IPv4 Address** (for duplicated virtual machines only) • **Alias IP Address: IPv6 Address** (for duplicated virtual machines only) **Note:** You can configure as many Ethernet ports as available on the NICs of your virtual machine.
Functional Assignment	Based on the system configuration, the system displays the following options. • Corporate LAN/Processor Ethernet/Control Network • Corporate LAN/Control Network • Duplication Link • Services Port • Out-of-Band Management **Note:** When you select the Out-of-Band Management option, the system displays the **Restrict Management traffic to Out-Of-Band interface is currently** field.
Restrict Management traffic to Out-Of-Band interface is currently	The possible values are: • enabled: restricts the management traffic to Out-Of-Band interface. • disabled: allows the management traffic to Out-Of-Band interface. By default the value of this field is set to disabled.

Button descriptions

Name	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes.
Restart CM	Updates the system configuration files with the current values on the page.

Table continues…

Name	Description
	Note: Click **Restart CM** only after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Setting the time zone

Procedure

1. Log on to the Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43

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

About this task

You must perform the following procedure only if you are deploying the Communication Manager Messaging OVA using the vSphere client that is directly connected to the ESXi host.

Procedure

1. Log on to the Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

Note:

The system creates the user and password when you perform any of the following tasks:

- Deploying CMM OVA on vCenter with vSphere web client on page 35
- Deploying CMM using vSphere client on page 39
- Administering network parameters on page 43

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 53 and Installing service pack on page 53.

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, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39

- Administering network parameters on page 43

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, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43

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 8: Initial administration

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. You can access the PLDS at https://plds.avaya.com. 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 and install on the webLM server.

To track and manage licenses in an organization, WebLM requires a license file from Avaya PLDS website.

Configuring the WebLM server

About this task

You must perform the following procedure only if you are deploying the Communication Manager Messaging OVA using the vSphere client that is directly connected to the ESXi host.

Procedure

1. Log in to Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user and password created earlier.

Note:

The system creates the user and password when you perform any of the following tasks:

- Deploying CMM OVA on vCenter with vSphere web client on page 35
- Deploying CMM using vSphere client on page 39
- Administering network parameters on page 43

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.

   If you change the **WebLM Server Address**, then you must restart Messaging.
5. Click **Submit**.

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.

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

About this task

You can download the authentication file directly from the AFS application to your computer.

Procedure

1. Start AFS and log in.

   For more information, see Starting the AFS application on page 60.
2. From the **Product** drop-down list, select Avaya Aura Communication Manager Messaging.

   Note:

   You can also select SP System Platform/VE VMware with 7.x release to generate valid authentication for Release 7.x system.
3. From the **Release** drop-down list, select 7.x.
4. Click **Next**.
5. On the Authentication File Delivery page, select **New System**, and then click **Next**.
6. Type the fully qualified domain name (FQDN) of the Communication Manager Messaging 7.x system.

7. To download the authentication file directly from AFS to your computer:
   a. Click **Download file to my PC**.
   b. Click **Save** in the File Download dialog box.
   c. Select the location to save the authentication file, and then click **Save**.
   d. Click **Close** in the Download complete dialog box to complete the download.

   When the system creates the authentication file, AFS displays a confirmation message that contains the product name, release, and authentication file ID (AFID). You must note the AFID for upgrading the system and for creating the authentication files.

   Note:

   On the confirmation message, the AFS application still displays Product Name as SP System Platform.
8. To view the header information in the authentication file, go to the location where you saved the file and use WordPad to open the file.

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

   Note:

   In the created and generated authentication file, the system displays Product Name as SP System Platform.

Installing the authentication file

Procedure

1. Log on to the Communication Manager Messaging **System Management Interface**, with the Customer Privileged Administrator account user and password created earlier.

   Note:

   The system creates the user and password when you perform any of the following tasks:

   - Deploying CMM OVA on vCenter with vSphere web client on page 35
   - Deploying CMM using vSphere client on page 39
   - Administering network parameters on page 43
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**.
5. To override the validation of the AFID and the date and time, select **Force load of new file**.
6. 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.

Chapter 9: Routine maintenance

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**.

Backup and restore

Backing up the messaging application and the server data

Before you begin

Stop Communication Manager Messaging. For more information, see Stopping Messaging on page 63.

About this task

Communication Manager Messaging uses the network to back up the Communication Manager Messaging data to an external server. 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 **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.
3. On the Backup Now webpage, in the **Data Sets** area, choose one of the following, based on which type of backup is being performed:
   a. Click **Full Backup**.
   b. Click **Specify Data Sets**, click **Messaging** and click **Messaging Application, Translations, Names, and Messages**.
4. 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**
5. 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.
6. Click **Start Backup**.

   For more information, see Backup now field descriptions on page 65.
7. Start Communication Manager Messaging.

   Note:

   Do not perform this step during migration or upgrade. For more information, see Starting the messaging virtual machine on page 43.

Backup Now field descriptions

Name	Description
Specify Data Sets	The data sets that you want to back up. The **Full Backup** does not include any of the Messaging data sets. 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 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 of the backup server.
Directory	The backup is stored on this network directory.
Encryption	

Table continues…

Name	Description
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 messaging application and the server data

Before you begin

Stop Communication Manager Messaging. For more information, see Stopping Messaging on page 63.

About this task

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

Procedure

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

   The system displays the View/Restore Data webpage.
2. In the **View current backup contents in** area, select **Network Device**.
3. In the following fields, enter the same information that you used when you backed up the data:
   - **Method**
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   In **Host Name**, enter the IP address of the backup server.
4. Click **View**.
5. On the View/Restore Data Results webpage, select a backup image stored in the location that you specified.

   The system lists the most recent backups at the bottom of the list.
6. To select the backup image you want to view or restore, click the corresponding option.
7. Click **Preview** if you are unsure that you selected the correct backup image.
8. Click **Restore** on the second screen to begin the restore process.

   If the server name does not match, click **Force Restore if server name mismatch**.

When you click **Restore**, the system displays the View/Restore Data Results webpage with the status of the restore process.

Note:

For restoring data completely, do the following:

- Restore Full Backup that was backed up. For more information, see Backup now field descriptions on page 65.
  - Perform *Restoring data* procedure with full-* for server files, system files and security files.
- Restore Messaging data that was backed up. For more information, see Backup now field descriptions on page 65.
  - Perform *Restoring data* procedure with audix-ap-tr-name-msg-* for translations, names, messages, and Messaging application files.

9. Start Communication Manager Messaging.

   Note:

   Do not perform this step during migration or upgrade. For more information, see Starting Communication Manager Messaging on page 67.

10. If you have remote networked computers, perform the following:
    a. Log in to the Communication Manager Messaging webpage.
    b. Go to the **Administration** > **Messaging**.
    c. Select **Server Administration** > **Request Remote Update**.
    d. Run a manual update to and from all remote networked computers to correct any database inconsistencies.

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.

Appendix A: Upgrading and Migrating Communication Manager Messaging to Release 7.0

Overview

Communication Manager Messaging 5.2.1 or 6.x running on System Platform based Communication Manager with Avaya provided hardware can be migrated to 7.0 on Avaya provided hardware running the Appliance Virtualization Platform by Solution Deployment Manager. To perform the migration to Release 7.0, follow the procedure as documented in *Upgrading and Migrating Avaya Aura® applications from Avaya Aura® System Manager*.

Communication Manager Messaging 5.2.1 or 6.x running on System Platform based Communication Manager with Avaya provided hardware can be migrated to the 7.0 Virtualized Environment on customer provided hardware using the procedures in this appendix. Also Communication Manager Messaging 6.3 or 6.3.100 running on the Virtualized Environment can be upgraded to 7.0 on the Virtualized Environment using the procedures in this appendix.

Migration roadmap and limitations

Upgrade

The minimal software required to upgrade from Communication Manager Messaging 6.3.x running on VMware is:

VMware	VMware
Communication Manager Messaging 6.3.100 Communication Manager Service Pack 6.3.111 Communication Manager Messaging 6.3.100 Service Pack 5	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1
Communication Manager Messaging 6.3 Communication Manager Service Pack 6.3.1 Communication Manager Messaging 6.3 Service Pack 4	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1

Migration

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

System Platform	VMware
Communication Manager Messaging 6.3.100 Communication Manager Service Pack 6.3.111 Communication Manager Messaging 6.3.100 Service Pack 5	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1
Communication Manager Messaging 6.3 Communication Manager Service Pack 6.3.11 Communication Manager Messaging 6.3 Service Pack 4	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1
Communication Manager Messaging 6.2 Communication Manager 6.2 Service Pack 8 Communication Manager Messaging 6.2 Service Pack 3	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1
Communication Manager Messaging 6.0.1 Communication Manager 6.0.1 Service Pack 11.01 Communication Manager Messaging 6.0.1 Service Pack 5	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1

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 Messaging RFUs C1317rf+i & A9021rf+k	Communication Manager Messaging 7.0 Communication Manager Service Pack 7.0.0.1

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
- Time zone
- 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
- Network time protocol
- Authentication file

- Licensing configuration
- Backup schedules configured on System Management Interface
- Alarming and SNMP configuration

Checklist for upgrade or migration

The upgrade or migration process consists of the following steps:

No.	Task	Description	✔
1	Backup the messaging application data and server data.	For more details, see Backing up the messaging application and the server data on page 63.	
2	Deploy the Communication Manager Messaging OVA	Perform one of the following: • Deploying the Communication Manager Messaging OVA using the vSphere client on page 39 • Deploying the Communication Manager Messaging OVA using the vSphere Web client on page 35	
3	Restore the messaging application data and server data.	For more details, see Restoring the messaging application and the server data on page 66.	

Note:

- Supported migration and upgrade 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 or upgrade, first upgrade your Communication Manager Messaging system. For more information, see Migration roadmap and limitations on page 69.

Upgrading and migrating Communication Manager Messaging to Release 7.0 on Virtualized Environment

Procedure

1. Backup the following data from the System Management Interface of the old virtual machine using the Customer Privileged Administrator user login:
   - Full backup
   - Communication Manager Messaging application data

   For more information, see Backing up the messaging application and the server data on page 63.
2. Shutdown the old Virtual Machine.

   For more information, see Shutting down the server on page 68.
3. Deploy the new Communication Manager Messaging Virtual Machine.
   - Deploying the Communication Manager Messaging OVA using the vSphere client on page 39
   - Deploying the Communication Manager Messaging OVA using the vSphere Web client on page 35
4. Start the new Virtual Machine.

   For more information, see Starting the Communication Manager Messaging virtual machine on page 43.
5. Administer initial network parameters if deploy was through vSphere client directly connected to the host.

   For more information, see Administering network parameters on page 43.
6. Configure the remaining network settings if deploy was through vSphere client directly connected to the host.

   For more information, see Configuring the Communication Manager Messaging network on page 48.
7. Set up the network time protocol.

   For more information, see Setting up the network time protocol on page 51.
8. Install the minimal required Communication Manager Messaging service packs.

   For more information, see Communication Manager Messaging service packs on page 52.
9. Install the license file.

   For more information see, License file for Communication Manager Messaging on page 58.
10. Download and install the authentication file.

    For more information, see Installing the authentication file on page 61.

11. Stop **Messaging**.

    For more information, see Stopping Communication Manager Messaging on page 63.

12. Restore the following data from the System Management Interface using the Customer Privileged Administrator user login:

    - Full backup
    - Communication Manager Messaging application data

    For more information, see Restoring the messaging application and the server data on page 66.

13. Restart the Communication Manager Messaging server. Select the **Restart server after shutdown** check box.

    For more information, see Shutting down the server on page 68.

Appendix B: Best Practices for VMware performance and features

Best Practices for VMware performance and features

BIOS

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

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

The following sections describe the recommended BIOS settings for:

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

Intel Virtualization Technology

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

All Intel Xeon processors include:

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

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

Note:

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

Other suggested BIOS settings

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

- 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.

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.

Configuring the NTP time

Procedure

1. Select the ESXi server and click the **Configuration** tab.
2. In the left navigation pane, click **Software** > **Time Configuration**.
3. At the upper-right side of the Time Configuration page, click **Properties...**.
4. On the Time Configuration dialog box, in the NTP Configuration area, perform the following:
   a. Select the **NTP Client Enabled** check box.
   b. Click **Options**.
5. On the NTP Daemon (ntpd) Options dialog box, perform the following:
   a. In the left navigation pane, click **NTP Settings**.
   b. Click **Add**.
   c. On the Add NTP Server dialog box, in the **NTP Server** area, enter the IP address of the NTP server.
   d. Click **OK**.

   The date and time of the System Manager virtual machine synchronizes with the NTP server.
6. Select the **Restart NTP service to apply changes** check box.
7. Click **OK**.

   The Time Configuration page displays the date and time, NTP Servers, and the status of the NTP client.

VMware networking best practices

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

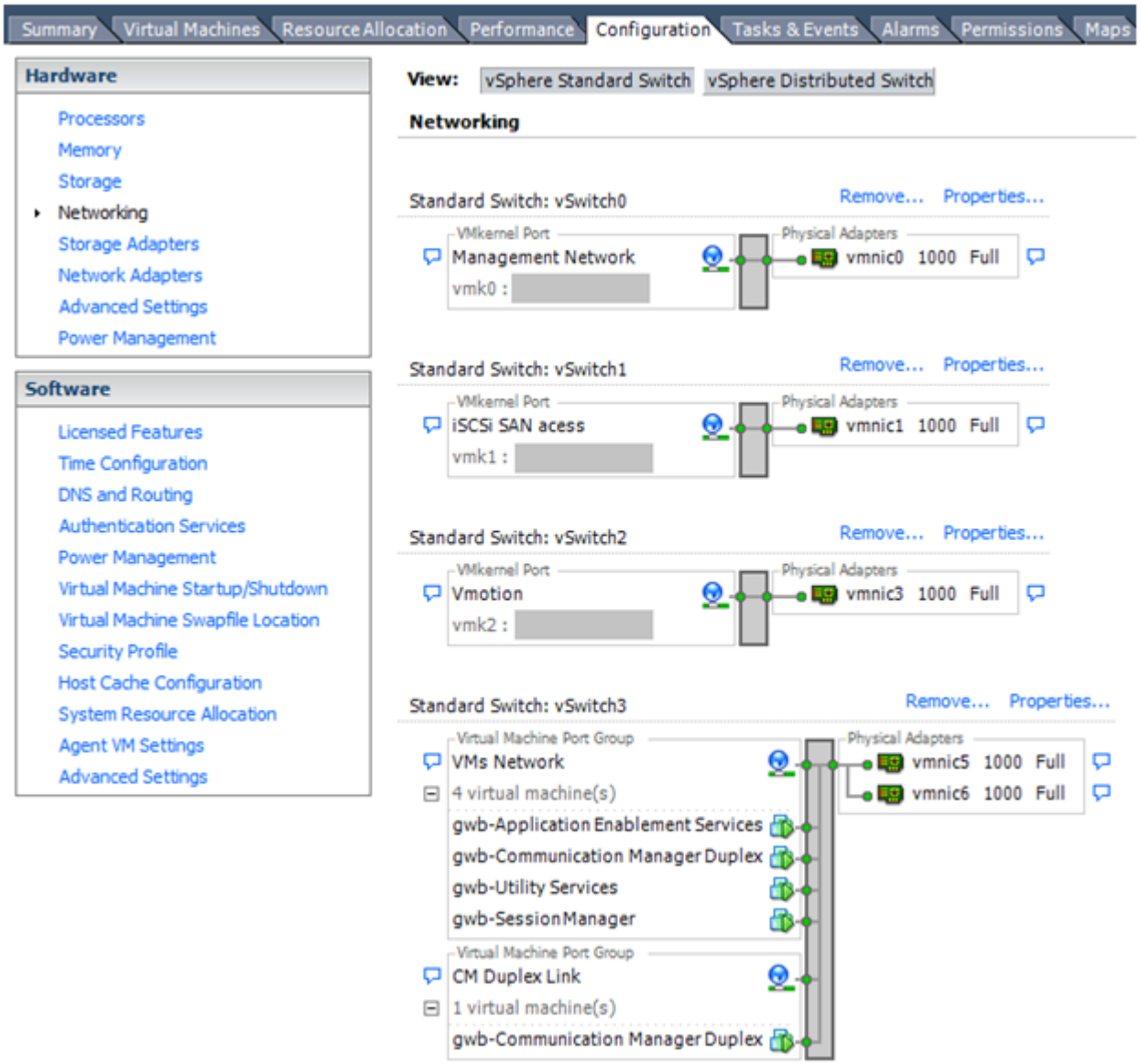
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

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

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

- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernal vNICs to be the same IP Maximum Transmission Unit (MTU).

Networking Avaya applications on VMware ESXi – Example 1



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

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.

- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



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

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

References

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

Storage

When you deploy Avaya Aura® System Manager in Virtualized Environment, observe the following set of storage recommendations:

- Always deploy System Manager with a thickly provisioned disk.
- For best performance, use System Manager only on disks local to the ESXi Host, or Storage Area Network (SAN) storage devices. Do not store System Manager on an NFS storage system.

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates all of the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all of the sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Communication Manager Messaging only supports thick provisioning.

Best Practices for VMware features

VMware Snapshots

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

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

Caution:

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

Snapshots can:

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

- Affect service.

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

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

  Note:

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

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

VMware Cloning

System Manager does not support VMware Cloning.

VMware High Availability

InVirtualized Environment, use the VMware High Availability (HA) method to recover System Manager in the event of ESXi Host failure. For more information, see the High Availability documentation for VMware.

When you use VMware HA with System Manager, the communication between System Manager and Avaya Aura® Communication Manager fails. The virtual machine then starts again on a standby server, and the system starts running.

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or underperforming servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Note:

If System Manager WebLM is being used as a master WebLM server in an enterprise licensing deployment for a product, after migration of virtual machine to another physical server by using vMotion, validate connectivity with added local WebLM servers. This is to ensure that the master WebLM server can communicate with local WebLM servers.

Glossary

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

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

Index

A

administering
network parameters 43
AFID
obtaining 62
AFS
starting 60
Appliance Virtualization Platform overview 11
attended backup 63
authentication file
creating for new system 60
installing 61
automatic restart
virtual machine 45
Avaya appliance offer 11
Avaya courses 8
Avaya virtualization platform 11

B

backing up
system 63
backup now 65
backup screen
field descriptions 65
best practices
performance and features 74
VMware networking 77
BIOS 74
BIOS for HP servers 75
BIOS settings
for Dell servers 75

C

checklist
configuration 45
deployment 28
planning 20
software installation 35
Cloning 83
cmm
migration 72
cmm deployment
using vSphere Web client 35
components
Avaya 15
third party 17
VMware 17
configuration data
customer 25
configuration tools 20
configure 77
configuring
network 48
virtual machine automatic restart 45
WebLM Server 58
customer configuration information 25

D

data
restoring 66
Deploying
using vSphere client 39
Deploying an OVA file
utility services 32
deployment
thick 81
thin 81
deployment guidelines 17
deployment process 19
disabling
IPv6 48
downloading
service packs 53
downloading software 26

E

enabling
IPv6 47

F

features best practices 74
field descriptions
backup screen 65
Network Configuration 49

G

guidelines
deployment 17

H

HA 83
High Availability 83

I

install

install *(continued)*
Application Enablement Services 29
Avaya Aura applications 29
Avaya Aura Media Server 29
Branch Session Manager 29
Communication Manager 29
Engagement Deployment Platform 29
SAL 29
SDM 29
Session Manager 29
Solution Deployment manager client 29
System Manager 29
WebLM 29
installing
authentication file 61
service packs 53
Intel Virtualization Technology 74
intended audience 7
IPv6 46

L

licensing 58

M

Messaging
migration roadmap 69
migration
checklist 71
roadmap 69
migration roadmap 69

N

Network Configuration
field descriptions 49
network time protocol
setting 51
NTP time 77
NTP time source 76

O

obtaining
AFID 62
overview 13

P

performance best practices 74
planning
checklist 20
PLDS 26
downloading software 26
purpose 7

R

recommended settings 24
registering 26
related documentation 7
removing
service packs 55
requirements
software 21
virtual machine resources 23
resource requirements 23
resources
server 20
restoring
data 66

S

SAL Gateway 21
SDM
installation 29
server hardware and resources 20
service pack 52
service packs
installing 53
removing 55
setting
network time protocol 51
time zone 51
shutting down
server 68
snapshots 81
software installation
checklist 35
software requirements 21
Solution Deployment Manager client
install 29
starting
virtual machine 43
start Messaging 67
stop Messaging 63
storage 80
support 10
system
backing up files 63
start 67
stop 63

T

thick deployment 81
thin deployment 81
third party
components
product 17
timekeeping 76
time zone

time zone *(continued)*
setting 51
topology 14
training 8

U

upgrading 69
utilities 20

V

videos 9
virtual machine
automatic restart configuration 45
starting 43
virtual machine resource requirements 23
vMotion 83
VMware
components 17
VMware Cloning 83
VMware High Availability 83
VMware networking
best practices 77
VMware Tools 75
VT support 74

W

WinSCP
using 22