Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment

Release 6.3
Issue 5
June 2015

© 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.

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”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel

Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the 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.

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.

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.

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 and Avaya Aura® are registered trademarks 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.

Contents

Chapter 1: Introduction ... 7
Purpose ... 7
Intended audience ... 7
Document changes since last issue ... 7
Related resources ... 8
Documentation ... 8
Training ... 9
Viewing Avaya Mentor videos ... 10
Support ... 10
Chapter 2: Architecture overview ... 11
Avaya Aura® Virtualized Environment Overview ... 11
Avaya Collaboration Pod for Enterprise Communications ... 12
VMware components ... 13
S8300E server ... 13
Deployment guidelines ... 14
Chapter 3: Planning and configuration ... 15
Planning ... 15
Downloading software from PLDS ... 15
Server hardware and resources ... 16
Configuration tools and utilities ... 17
Migration data ... 17
Migrating from Communication Manager Release 5.2.1 to Release 6.3 ... 18
Migrating from Communication Manager Release 6.2 to Release 6.3 ... 18
Certificates ... 19
LDAP and AAA authentication ... 20
Communication Manager virtual machine resource requirements ... 21
Correcting the CPU resources ... 23
VMware software requirements ... 23
Software requirements ... 24
Communication Manager virtual appliance licensing on VMware ... 24
Centralized Licensing ... 25
SAL Gateway ... 25
Chapter 4: Communication Manager OVA deployment ... 27
Deploying Communication Manager Open Virtual Application ... 27
Deployment of cloned and copied OVAs ... 28
Duplex OVA deployment ... 29
Changing the virtual machine settings ... 29
Reducing CPU reservations on the duplex Communication Manager server ... 30
Chapter 5: Configuration ... 31

Configuration and administration checklist.... 31
Starting the Communication Manager virtual machine.... 31
Configuring the virtual machine automatic startup settings.... 32
Administering network parameters.... 33
Applying the Communication Manager patch.... 34
Setting the time zone.... 34
Setting up the network time protocol.... 35
Configuring the WebLM server.... 35
Installing the authentication file.... 36
Authentication files for Communication Manager.... 36
Starting the AFS application.... 36
Creating an authentication file for a new system.... 38
Adding an administrator account.... 39
Installing an authentication file.... 40
Obtaining the AFID from Communication Manager SMI.... 41
IPv6 configuration.... 41
Enabling IPv6.... 41
Disabling IPv6.... 42
Network port considerations.... 42
Communication Manager virtual machine configuration.... 43
Server role configuration.... 44
Configuring Server Role.... 45
Server Role field descriptions.... 45
Network.... 47
Network configuration.... 47
Configuring the Communication Manager network.... 48
Network Configuration field descriptions.... 48
Duplication parameters configuration.... 50
Duplication parameters.... 50
Configuring duplication parameters.... 50
Duplication Parameters field descriptions.... 51
Chapter 6: Postinstallation verification and testing.... 54
Installation tests.... 54
Verifying the license status.... 55
Accessing Communication Manager System Management Interface.... 55
Viewing the license status.... 56
License Status field descriptions.... 56
Verifying the software version.... 57
Verifying the survivable virtual machine registration.... 58
Verifying the virtual machine mode.... 58
Appendix A: Troubleshooting Communication Manager custom kernel VMware vSphere tools.... 59
Identifying corrupted Communication Manager VMware vSphere Tools.... 59

Repairing Communication Manager VMware vSphere tools.... 60
Appendix B: Communication Manager debugging.... 61
Communication Manager processes.... 61
Creating Communication Manager virtual machine core images.... 61
VMware generated core images on Communication Manager virtual machine images.... 62
Appendix C: Communication Manager software duplication with VMware high availability.... 63
Software duplication enhancement.... 64
Appendix D: Upgrading Communication Manager Open Virtual Application.... 65
Upgrading Communication Manager using full backup.... 65
Creating a backup.... 66
Upgrading Communication Manager virtual machine and restoring the translations.... 66
Communication Manager patches.... 67
Connection preservation upgrade on Communication Manager Duplex OVA.... 68
Communication Manager Duplex OVA upgrade.... 68
Presite upgrade checklist.... 68
Preupgrade tasks on the active server.... 69
Preupgrade tasks on the standby server.... 71
Upgrade tasks on the standby server that was active before the interchange.... 74
Postupgrade tasks on the active server running Release 6.3.... 74
Postupgrade tasks on the standby server running Release 6.3.... 75
Appendix E: Migrating Communication Manager to the VMware Virtualized Environment.... 76
Appendix F: VMware best practices for performance.... 80
BIOS.... 80
Intel Virtualization Technology.... 80
Dell PowerEdge Server 81
HP ProLiant Servers.... 81
VMware Tools.... 82
Timekeeping.... 82
VMware networking best practices.... 83
Thin vs. thick deployments.... 87
Storage.... 88
Best Practices for VMware features.... 88
VMware snapshots.... 88
High availability.... 90
VMware vMotion.... 91
Appendix G: PCN and PSN notifications.... 92
PCN and PSN notifications.... 92
Viewing PCNs and PSNs.... 92
Signing up for PCNs and PSNs.... 93
Glossary.... 94

Chapter 1: Introduction

Purpose

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

Intended audience

The primary audience for this document is anyone who is involved with installing, configuring, and verifying Avaya Aura® Communication Manager on a VMware vSphere™ 5.0, 5.1, and 5.5 virtualization environment at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers themselves.

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

Document changes since last issue

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

- In the *VMware software requirements* section, added support for VMware vSphere ESXi 5.5.
- Added the *IPv6 configuration* section.
- Added the *Software duplication enhancement* section.
- Added the *Storage* section.
- Updated the *Software requirements* section.
- Updated the *Configuring the Communication Manager network* section.
- Updated the *Network Configuration field descriptions* section.
- Updated the *Configuring duplication parameters* section.
- Updated the *Duplication Parameters field descriptions* section.

Related resources

Documentation

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

Title	Description	Audience
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.	Sales Engineers
Implementation		
Deploying Avaya Aura® Communication Manager on System Platform	Describes the instructions for deploying Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Deploying Avaya Aura® Utility Services on VMware® in Virtualized Environment	Describes the instructions for deploying Utility Services.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Deploying Avaya Aura® System Manager on VMware in Virtualized Environment	Describes the instructions for deploying System Platform.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Deploying Avaya WebLM on VMware® in Virtualized Environment	Describes the instructions for deploying WebLM.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300431	Describes the commands for Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		

Table continues…

Title	Description	Audience
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel

Training

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

Course code	Course title
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
Docu00158	Whats New in Avaya Aura® Release 6.2 Feature Pack 2
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
4U00115I, 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration

Table continues…

Course code	Course title
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.

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment Overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture. Virtualized Environment provides the following benefits:

- simplifies IT management using common software administration and maintenance.
- requires fewer servers and racks which reduces the footprint.
- lowers power consumption and cooling requirements.
- enables capital equipment cost savings.
- lowers operational expenses.
- uses standard operating procedures for both Avaya and non-Avaya products.
- customers can deploy Avaya products in a virtualized environment on customer-specified servers and hardware.
- business can scale rapidly to accommodate growth and to respond to changing business requirements.

For existing customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

The Virtualized Environment project is only for VMware and is not intended to include any other industry hypervisor. Virtualized Environment is inclusive of the Avaya Aura® portfolio.

Note:

This document uses the following terms, and at times, uses the terms interchangeably.

- server and host
- reservations and configuration values

Customer deployment

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

The customer provides the servers and the VMware infrastructure including the VMware licenses.

Software delivery

The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS) and the Avaya support site. Each OVA contains the following components:

- the application software and operating system.
- pre-installed VMware tools.
- preset configuration details for
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Patches and upgrades

A minimum patch level can be required for each supported application. For more information regarding the application patch requirements, see the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Important:

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

Performance and capacities

The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

Modifying these values can have a direct impact on the performance, capacity, and stability of the virtual machine. It is the responsibility of the customer to understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) may not be able to assist in fully resolving a problem if the virtual hardware or resource allocation has been changed to unsupported values for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

Avaya Collaboration Pod for Enterprise Communications

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

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

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

Documentation

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

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

VMware components

VMware software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.

S8300E server

The S8300E server is based on a 2.0 GHz, dual core Intel Ivy Bridge processor. The S8300E server is supported in the G430 Branch Gateway and G450 Media Gateway. The S8300E server supports System Platform Release 6.3.7, and Communication Manager Release 6.3.8 and later. The S8300E server is certified by VMware as VMware Ready.

Deployment guidelines

The high-level deployment steps are:

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

The deployment guidelines for the virtual appliances are:

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

Important:

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

Chapter 3: Planning and configuration

Planning

Ensure that the customer completes the following before deploying the Communication Manager open virtual application (OVA):

#	Task	Description	✔
1	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See *Server hardware and resources*.	
2	Plan the staging and verification activities and assign the resources.	See *Communication Manager virtual machine resource requirements*.	
3	Purchase the required licenses. Register for PLDS and perform the following: • Obtain the license file. • Activate license entitlements in PLDS.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4	Download the required Communication Manager OVA.	See *Downloading software from PLDS*. See *Configuration tools and utilities*.	
5	If applicable, migrate from Communication Manager 5.2.1 or Communication Manager 6.2 to Communication Manager 6.3.	See *Migration data*.	

Downloading software from PLDS

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

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

Note:

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

Procedure

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

    Note:

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

Server hardware and resources

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

Configuration tools and utilities

To deploy and configure the Communication Manager open virtual application (OVA), you need the following tools and utilities:

- Duplex OVA
- Simplex OVA
- Communication Manager service packs
- A remote computer running the vSphere client
- A browser for accessing the Communication Manager System Management Interface pages

  Communication Manager SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
- PuTTy, WinSCP, and WinZip

For information about tools and utilities, see *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394.

Migration data

Migration from Communication Manager Release 5.2.1 to Release 6.3

To migrate from a standard Communication Manager Release 5.2.1 installation to Communication Manager 6.3 OVA on VMware, see *Migrating from Communication Manager Release 5.2.1 to Release 6.3*.

Migration from Communication Manager Release 6.2 to Release 6.3

To migrate from a standard Communication Manager Release 6.2 installation to Communication Manager Release 6.3 OVA on VMware, see *Migrating from Communication Manager Release 6.2 to Release 6.3*.

To record the required information for the migration, go to the Avaya Support website at http://support.avaya.com. See *Migrating from Avaya Aura® Communication Manager 6.x to VMware Workbook* and *Migrating from Avaya Aura® Communication Manager 5.2.1 to VMware Workbook*. When you open the spreadsheet, click **Enable Macros** on the dialog box.

After recording the Communication Manager migration information in the appropriate workbook, perform the next steps. See Migrating Communication Manager to the VMware Virtualized Environment on page 76.

Related Links

Migrating from Communication Manager Release 5.2.1 to Release 6.3 on page 18

Migrating from Communication Manager Release 5.2.1 to Release 6.3

Use this procedure to migrate from the standard Communication Manager Release 5.2.1 installation to Communication Manager 6.3 virtual open application deployment on VMware.

Procedure

1. Install the migration patch on the Communication Manager 5.2.1 server.
2. Back up data from the Communication Manager 5.2.1 System Management Interface page.
3. Restore the data on the Communication Manager 6.3 VMware platform.

Related Links

Migration data on page 17

Migrating from Communication Manager Release 6.2 to Release 6.3

Use this procedure to migrate from the standard Communication Manager Release 6.2 installation to Communication Manager 6.3 virtual open application deployment on VMware.

Procedure

1. Install the latest patch on the standard Communication Manager Release 6.2 system.
2. **(Optional)** Create a Privileged Administrator account, if you do not have this account.
3. Run the **`save translation`** command to save the translation.
4. On the Communication Manager command line interface, type the command `sudo backup -b d /var/home/ftp/pub -- verbose -- migration-60` to take a full backup of Communication Manager Release 6.2.
5. Verify that the `tar.gz` file is in the `/var/home/ftp/pub` directory and that the file has a timestamp.
6. To retain the same IP address for Communication Manager, move the migration backup (`tar.gz`) file from `/var/home/ftp/pub` to other remote machine.
7. Shutdown the standard Communication Manager Release 6.2 system.
8. Deploy the Communication Manager 6.3 OVA, and apply the latest patch.
9. Copy the `tar.gz` file from `/var/home/ftp/pub` or from the remote machine to the Communication Manager Release 6.3 virtual machine.

   For example, you can copy the `tar.gz` file to the `/var/home/craft` location.
10. Log in to SMI of the Communication Manager Release 6.3 virtual machine.

11. Restore the backup on the Communication Manager Release 6.3 virtual machine.

Restoring backup

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Data Backup/Restore** > **View/Restore Data**.

   The system displays the View/Restore Data page.
4. In the **Network Device** section, perform the following to restore the data:
   a. Select the method to restore the data.
   b. In the **User Name** field, enter the user name.
   c. In the **Password** field, enter the password
   d. In the **Host Name** field, enter the host name.
   e. In the **Directory** field, enter the path for the directory.
5. Click **View**.

   The system displays the View/Restore Data Results page.
6. Click the `tar.gz` file.
7. Select **Force restore if server name mismatch**.
8. Click **Restore**.

   On the View/Restore Data Results page, the system displays the message `Restore Successfully Completed`.

Certificates

Certificates provide identity to the virtual machine. When you install a license file or authentication file on Communication Manager, the system installs the required certificates on Communication Manager. These certificates are secure and work fine for most customers. Some customers generate and install custom certificates.

If you do not have custom certificates installed, you can skip the following description.

If you have installed the custom certificates, you must generate new certificates for your new Communication Manager VMware virtual machine. Certificates link to virtual machine by a fully qualified domain name (FQDN) or IP address. If you change the FQDN or IP address, you must install the new certificates on the VMware instance. If you are using the custom certificates, Avaya recommends that you generate new certificates for the VMware virtual machine. If you have custom certificates on your old machine and you want to use the same certificates, go to the Avaya Support website at https://support.avaya.com/.

LDAP and AAA authentication

LDAP provides a directory server that allows users to login to multiple machines using the same credentials. The administrator does not need to perform any specific user account maintenance on each machine. Instead, the administrator can just setup the LDAP server contact information one time, and all authorized LDAP users can then login to the machine. Communication Manager virtual machines have the capability to use LDAP and other AAA services for authentication. However, this is a rare configuration. In both Communication Manager 5.2.1 and 6.x, you must have root access to set up the authentication or had Avaya setup LDAP or AAA for them. For more information about setting up LDAP or AAA authentication, go to the Avaya Support website at https://support.avaya.com/.

If you have LDAP setup on your original Communication Manager, you can capture a few files to reconfigure the LDAP authentication on your new VMware Communication Manager virtual machine. Use the steps below to gather the files you need to setup LDAP and AAA on a new virtual machine.

A full explanation of LDAP configuration is outside the scope of this document; however, many of the settings in these files will likely translate directly from one virtual machine to the other virtual machine. The notable exception is the `/etc/pam.d` directory and its included files. These files should be handled carefully by a knowledgeable administrator to prevent system lockouts or security holes.

Note:

You must have root access to set up the LDAP and AAA authentication. For more information about setting up LDAP or AAA authentication, go to the Avaya Support website at https://support.avaya.com/

1. Log in to the old Communication Manager system to gather the necessary information.
2. Log in as root user.
3. Execute the **`cd /var/home/ftp/pub`** command to go to the correct directory.
4. Execute the following command to gather the necessary information.

   ```
   tar -czf old_auth.tgz /etc/pam.d /etc/ldap.conf /etc/openldap/
   ldap.conf /etc/raddb /etc/nsswitch.conf /etc/security
   ```

5. Use the Linux **`scp`** command to copy the files to a remote server while accessing the Communication Manager virtual machine.

   ```
   scp old_auth.tgz <user>@<ip_address>:<location>
   ```

   For example: scp old_auth.tgz bob@192.168.1.1:/home/bob

   If you are copying the files from a remote system, for example:

   - Linux: Use the **`scp`** command to copy the files back to the system the user is running on.

     ```
     scp user@CM_VM _Ipor_name:/directory/filename
     to_remote_system_location
     ```

- Windows PC: Use the **WinSCP** utility to copy the files back to the system the user is running on.

6. Your data will be backed up on the remote server in the directory you specified. If you need to examine that data, you can execute the **tar -xzf old_auth.tgz** command to extract the data.

   Use the **tar -xzf old_auth.tgz** command to extract all the files with their full path names into the current directory. You should execute this command from a private directory, for example,/home/bob, to avoid accidental breakage from overwriting other files.

   Note:

   For Windows PC, use the WinZip option to extract the data.

For more information about LDAP or AAA logins, go to the Avaya Support website at https://support.avaya.com/.

Transferring files using WinSCP utility

Use the following instructions to transfer the files from a remote system to the Communication Manager virtual machine using the WinSCP utility.

Procedure

1. Use WinSCP or a similar file transfer utility to connect to the Communication Manager virtual machine.
2. Enter the credentials to gain access to SCP.
3. Click **OK** or **Continue** as necessary in the warning dialog boxes.
4. Change the file transfer protocol from SFTP to **SCP**.
5. Click **Browse** to locate and select the file.
6. In the WinSCP destination machine window, browse to **/home/**.
7. Select **/home/<customerloginname>** as the destination location for the file transfer.
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 transfer the file.
10. When the copy completes, close the WinSCP window (**x** icon) and click **OK**.

Communication Manager virtual machine resource requirements

The Communication Manager virtual machine requires the following set of resources to be available on the ESXi host before deployment. Communication Manager OVA specifies the required resources.

VMware resource	Simplex values	Duplex values
CPU core	1	3
CPU reservation	2400 MHz	• 8700 MHz to support up to 36,000 users • 7200 MHz to support up to 30,000 users **Note:** To reduce reservation on Communication Manager duplex server, see Reducing reservation on CM Duplex server on page 30.
Minimum CPU speed based on Xeon E5620 or equivalent processor	2400 MHz	• 2900 MHz to support up to 36,000 users • 2400 MHz to support up to 30,000 users
Memory reservation	4.0 GB	5.0 GB
Storage reservation	30 GB	30 GB
Shared NICs	One vmxnet3 @ 1000 Mbps	Two vmxnet3 @ 1000 Mbps
IOPS	4	4
Average Network usage	3500 Kbps	3500 Kbps **Note:** Communication Manager duplication bandwidth requires 1Gbps for Communication Manager duplication link bursts. For more information about Communication Manager duplication bandwidth, see PSN003556u.

Note:

You can deploy the Communication Manager OVA on a host that does not have the resources to allocate to the virtual machine. But the host must have the required resources to start the virtual machine. When you start the virtual machine with limited CPU resources, the system displays the `Insufficient capacity on each physical CPU` pop-up message. You can use the OVA file to assign the CPU reservations to the virtual machine to adjust a specific server speed. For information about adjusting the CPU resources, see *Correcting the CPU resources*.

Related Links

Correcting the CPU resources on page 23

Correcting the CPU resources

Procedure

1. Select and right-click the virtual machine.
2. Click **Edit Settings**.

   The system displays the Virtual Machine Properties window.
3. Click the **Resources** tab to display the virtual machine resources, such as CPU, Memory, Disk, Advanced CPU, and Advanced Memory.
4. In the *Resource Allocation* section, adjust the CPU reservation and click **OK**.
5. Check the CPU requirements in the **Summary** tab of the virtual machine.
   - Duplex: 3* the CPU speed noted under the host's **Summary** tab
   - Simplex: 1* the CPU speed noted under the host's **Summary** tab

   Sometimes adjusting the CPU reservations might not correct the problem for starting the virtual machine. To start the virtual machine adjust the CPU speed more. Also, you can follow the same procedure to adjust the other virtual machine resources.

   Important:

   Do not change any other resource settings, for example, removing resources completely. Modifying these allocated resources can have a direct impact on the performance and capacity of the Communication Manager virtual machine. Virtual machine must meet the resource size requirements so that Communication Manager can run at full capacity. Removing or greatly downsizing resource reservations can put this requirement at risk. You are responsible for making any modifications to the resource reservation settings.

   Warning:

   If a virtual machine problem occurs, Avaya Global Support Services (GSS) might not be able to assist in fully resolving a problem. Avaya GSS can help you to reset the values to the optimized values before starting to investigate the problem.

Related Links

Communication Manager virtual machine resource requirements on page 21

VMware software requirements

The following VMware software versions are supported:

- VMware vSphere ESXi 5.0
- VMware vSphere ESXi 5.1

- VMware vSphere ESXi 5.5
- VMware vCenter Server 5.0
- VMware vCenter Server 5.1
- VMware vCenter Server 5.5

ESXi 5.0 can be added under vCenter Server 5.0 and vCenter Server 5.1. However, ESXi 5.1 can be added only under vCenter Server 5.1 and ESXi 5.5 under vCenter Server 5.5. To view compatibility with other solution releases, see *VMware Product Interoperability Matrices* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

Note:

ESXi 4.1 is not supported.

Software requirements

You can deploy the Communication Manager OVA Release 6.3 using VMware vSphere 5.0, VMware vSphere 5.1 or VMware vSphere 5.5. You cannot deploy the Communication Manager OVA using VMware vSphere 4.1. The Communication Manager VMware virtualization environment is a virtual appliance that you can deploy on VMware certified hardware.

Communication Manager virtual appliance licensing on VMware

You can deploy the Communication Manager OVA on VMware either as a simplex or as a duplicated Communication Manager software-duplication pair. In both cases, use only a single instance of WebLM license server to host the Communication Manager license file. To host the license file you must use the WebLM instance that is within System Manager.

If the customers do not want to deploy System Manager, the customers can use the standalone WebLM virtual appliance to host the Communication Manager license file.

In a network of multiple Communication Manager systems, each Communication Manager server or Communication Manager software-duplication pair requires a separate license file. Using the Centralized Licensing feature, install the Communication Manager or Communication Manager software-duplication pair license files on System Manager WebLM. You can also install the Communication Manager license files on the standalone WebLM virtual appliance for each Communication Manager or Communication Manager software-duplication pair.

For information about centralized licensing and license utilization, see *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394 and *Administering Avaya Aura® System Manager*.

Centralized Licensing

System Manager WebLM Release 6.3.4 supports the Centralized Licensing feature in System Platform and VMware Enablement environments. The Centralized Licensing feature is available only for Avaya Aura® Communication Manager. Using the Centralized Licensing feature, you can install up to 600 license files for Communication Manager on a single System Manager WebLM server. After installing a license file for a Communication Manager main server (simplex or duplex pair), you must link the Communication Manager main server to the license file in WebLM.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Communication Manager main server.
- Eliminates the need to log in to each WebLM server to manage licenses for each Communication Manager main server.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Communication Manager.

Note:

- The standalone (non-System Manager) WebLM server does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Communication Manager server.

For System Manager and Communication Manager centralized licensing backward compatibility, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

SAL Gateway

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

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

A SAL Gateway:

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

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

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

Chapter 4: Communication Manager OVA deployment

Deploying Communication Manager Open Virtual Application

Procedure

1. In the vSphere client, select the host ESX server for deploying the Communication Manager OVA.
2. Select **File** > **Deploy OVF Template**.

   The system displays the Deploy OVF Template window.
3. You can use one of the following options to deploy the Communication Manager OVF package (CM-6.03.0.124.0-e51-1.ova):
   - Click **Browse** and provide the Communication Manager OVA file location.
   - If the OVA file is on an http server, enter the URL in the **Deploy from a file or URL** field to deploy the Communication Manager OVA.
4. Click **Next**.

   The system displays the OVF Template Details window.
5. Verify the details of the installed OVA template and click **Next**.

   The system displays the End User License Agreement window.
6. Read the license agreement and click **Accept** to accept the license agreement.
7. Click **Next**.

   The system displays the Name and Location window.
8. In the **Name** field, enter the name of the new virtual machine and select the **inventory location** to deploy the virtual machine.

   If you have not selected a host when you choose to **Deploy OVF Template**, the wizard prompts you to select the host or cluster to deploy the virtual appliance. Select the host or cluster to deploy the virtual appliance.

   If you have selected a host or cluster when you choose to **Deploy OVF Template**, the system deploys the virtual appliance on that host.

9. Click **Next**.

   The system displays the Storage window.

10. Select the data store location to store the virtual machine files and click **Next**.

    The system displays the Disk Format window.

11. Accept the default disk format to store the virtual machine and virtual disks for the Communication Manager OVA and click **Next**.

    For information about virtual disks, see Thin vs. thick deployments on page 87.

12. If you have configured multiple virtual machine networks on the host where you are deploying the Communication Manager OVA, the wizard prompts you to associate networks specified in the OVA with networks available on the host. For the single **source network**, choose a host network by clicking the **Destination Network** column, and click the entry in the drop-down menu, for example, VM Network 2. Click **Next**.

    If you have only a single virtual machine network on the host you are deploying the Communication Manager OVA, the wizard does not prompt to map the network.

    Note:

    During deployment of the Communication Manager duplex OVA, on the Network Mapping screen, the second vNIC labeled *Asset* is the Communication Manager duplication link. You must appropriately link the Communication Manager duplication link to the customers network. After the duplex OVA deployment the duplication link displays as *Network Adapter 2* on the Virtual Machine Properties window and then you can edit the duplication link.

    The system displays the Ready to Complete window.

13. Verify the deployment settings and click **Finish**.

    The system displays the progress of the tasks in a **vSphere Client Status** panel. For more information about deploying templates in VMware, see VMware documentation on deploying an OVF template.

Deployment of cloned and copied OVAs

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

Duplex OVA deployment

To deploy the Duplex OVA, install the Duplex OVA on two different hosts. Ensure that the hosts reside on two different clusters. Similar to the Simplex OVA, the Duplex OVA has one network interface configured in the OVA. The system automatically assigns the Duplex OVAs first NIC and second NIC to the one network. An example host configuration for the Duplex OVA can be setup to include two virtual machine network connection type vSwitches, For example,

- *VM Network* to use with the Communication Manager NIC 0 administration/call_processing traffic – connected to say vmnic 0
- *CM_duplication_link* to use with the Communication Manager NIC 1 duplication link traffic – connected to say vmnic 2

Before you start the virtual machine, you must change the Communication Manager virtual machine settings to configure the second NIC. For information about changing the virtual machine settings, see *Changing the virtual machine settings*.

Note:

For the Communication Manager Duplex virtual appliance:

- If you are using a 2900 MHz (2.9GHZ) processor, the Communication Manager virtual appliance supports the 36000 endpoints.
- If you are using a 2400 MHz (2.4GHZ) processor, the Communication Manager virtual appliance supports the 30000 endpoints.

Related Links

Changing the virtual machine settings on page 29

Changing the virtual machine settings

To configure the second NIC, you must change the virtual machine settings.

Procedure

1. Right-click the OVA and select **Edit Settings**.

   The system displays the Virtual Machine Properties window.

2. In the **Hardware** tab, select the Network adapter 1 to assign to the *VM Network* under *Network Connection*.
3. Select the Network adapter 2 and then select the *CM_duplication_link* network name from the **Network label** drop-down list under *Network Connection*.

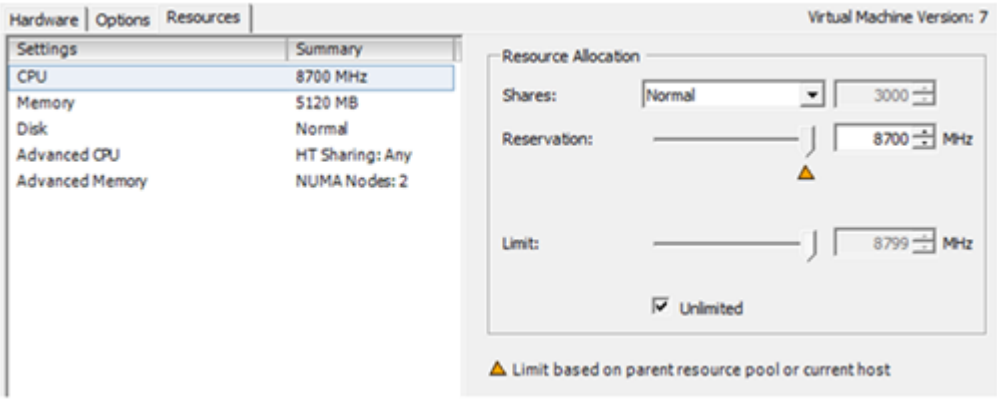
Related Links

Duplex OVA deployment on page 29

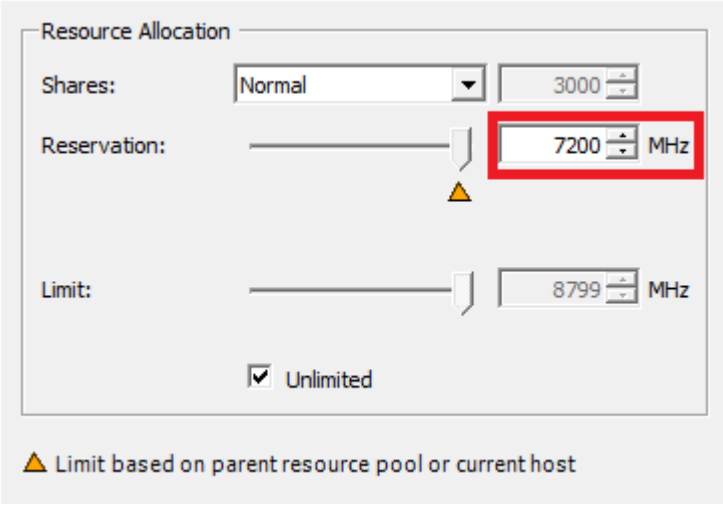
Reducing CPU reservations on the duplex Communication Manager server

Procedure

1. Deploy the Communication Manager OVA.
2. Reduce reservations before the virtual machine starts booting.
   a. Right-click the Communication Manager virtual machine and select **Edit Settings**.
   b. On the **Settings** window, select the **Resources** tab.



   c. In the left pane, under **Settings**, select **CPU**.
   d. In the right pane, adjust the MHz values in the **Reservation** line.
   e. Change the value from **8700** to **7200** MHz.



   f. Click **OK** to exit the window.
3. Boot the Communication Manager virtual machine.

Chapter 5: Configuration

Configuration and administration checklist

Use the following checklist to configure the Communication Manager virtual appliance.

#	Action	Link	✔
1	Start the Communication Manager virtual machine.	Starting the Communication Manager virtual machine on page 31	
2	Configure the Communication Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic startup settings on page 32	
3	Set up network configuration.	Administering network parameters on page 33	
4	Apply the latest Communication Manager Release 6.2 and later patch.	Applying the Communication Manager patch on page 34	
5	Configure the time zone	Setting the time zone on page 34	
6	Set up the network time protocol.	Setting up the network time protocol on page 35	
7	Direct Communication Manager to the WebLM server.	Configuring WebLM Server on page 35	
8	Create an suser account.	Adding an administrator account login on page 39	
9	Load the authentication files.	Installing an authentication file on page 40	

Starting the Communication Manager virtual machine

Procedure

In the vSphere client, select the host server, right-click the virtual machine, highlight the **Power**, and click **Power On**.

Communication Manager takes some time to start. If Communication Manager does not start, you must wait for Communication Manager to boot before log in.

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.

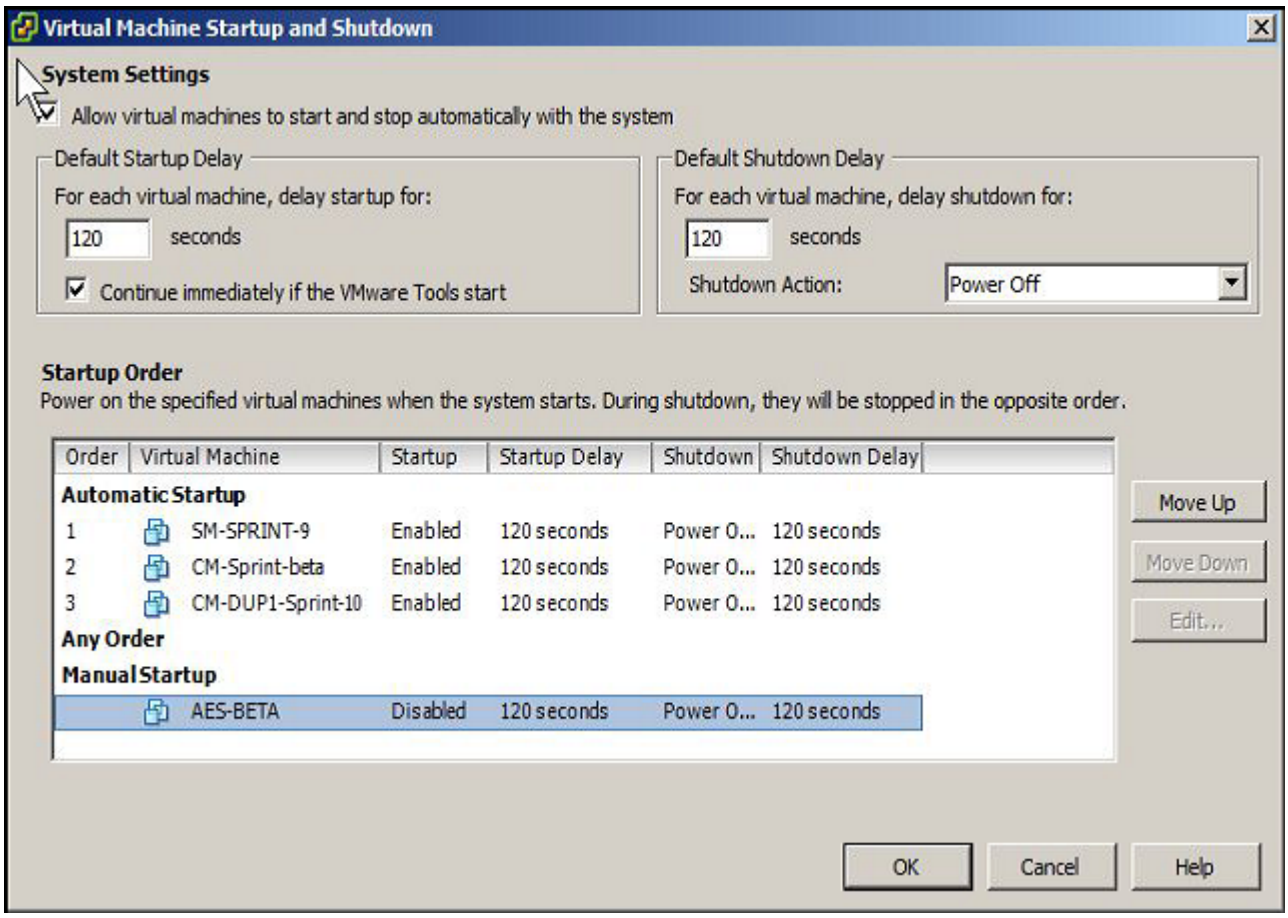
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

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

Example

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



Administering network parameters

Procedure

1. In the vSphere client, start the Communication Manager virtual machine console and log in as `craft`.

2. On first attempt log in as `craft`, you must type the following details according to the prompts:

   a. In the **IPv4 IP address** field, type the IP address.

   b. In the **IPv4 subnet mask** field, type the network mask IP address.

   c. In the **IPv4 Default Gateway address** field, type the default gateway IP address.

3. In the **Are these correct** field, verify the IP address details and type `y` to confirm the IP address details.

4. To configure the additional network settings, log in to Communication Manager System Management Interface as *craft* and navigate to **Administration** > **Server (Maintenance)** > **Network Configuration**.

   Note:

   If the system interrupts the initial network prompt or you provide the incorrect data, run the **`/opt/ecs/bin/serverInitialNetworkConfig`** command to retype the data.

Applying the Communication Manager patch

You must apply the latest patch on the Communication Manager virtual machine to set the time zone, to set up the network time protocol, to load the authentication file, or to configure the WebLM server. Using the Communication Manager System Management Interface, you can install and apply the Communication Manager Release 6.2 and later patch.

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Upgrades** > **Manage Updates** .

   The system displays the Manage Updates page.
4. Select the update ID to activate or deactivate the updates.

Setting the time zone

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Time Zone Configuration** .
4. On the Time Zone Configuration page, select the time zone, and click **Apply**.

   Note:

   After changing the time zone settings, you must restart the virtual machine to ensure that the system processes use the new time zone.

Setting up the network time protocol

Procedure

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

   The system displays the Network Time Protocol (NTP) Configuration page.
4. Enable or disable the NTP mode.
5. In NTP Servers, type the primary server, secondary server (Optional), and tertiary server (Optional) details.
6. Click **Apply**.

Configuring the WebLM server

Note:

To perform the administration tasks, you must first install the license file on the Communication Manager virtual machine.

Procedure

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

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

   Note:

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

Installing the authentication file

Authentication files for Communication Manager

You must have a new authentication file that contains Access Security Gateway (ASG) keys and the server certificate for Communication Manager. With the ASG keys, Avaya Services can securely gain access to the customer system.

Note:

Before installing the authentication file, you must create a *privileged administrator* account to prevent a *lock out* situation after loading the new authentication file. For adding an administrator account, see Adding an administrator account login on page 39.

The Authentication File System (AFS) creates unique authentication files. You can start the AFS application from http://rfa.avaya.com and download the file. Use the *SP System Platform/VE VMware* product type for creating the authentication file. After you create and download the authentication file, use the Communication Manager System Management Interface to install the file.

Tip:

You can also send the file to your email ID.

Every time you upgrade Communication Manager to a new major release, you must create and install a new authentication file.

Authentication files for duplicated OVAs and survivable OVAs

Each survivable OVA must have a unique authentication file.

For duplicated pair configurations, you must install the same authentication file on both the active virtual machine and the standby virtual machine. The system does not automatically synchronize the authentication file on the active virtual machine with the standby virtual machine.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies the file. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the virtual machine.

Starting the AFS application

You must have a login ID and password to log in to the AFS application. You can register for a login at http://rfa.avaya.com.

AFS is available only to Avaya service personnel and Avaya partners.

If you are performing the installation as a customer, Avaya provides a default authentication file to secure your system. To download the default authentication file directly from the Avaya PLDS website, see the *Downloading the default authentication file* section.

Note:

You need the authorization file only for Communication Manager 6.x Simplex or Duplex virtual appliance VMware deployments.

Procedure

1. In your web browser, type `http://rfa.avaya.com`.
2. Enter the credentials, 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.

Downloading the default authentication file

Use this procedure to download the default authentication file directly from the Avaya PLDS website.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. At the top of the Avaya Support homepage, click the **Downloads & Documents** tab.
3. In the **Enter Your Product Here** field, type Communication Manager. Once you start typing the product name, the website displays the results matching to the entered text. You can select the complete product name from the displayed list.
4. In the **Choose Release** field, select the product release, 6.3.x.
5. In the **Select a content type** section, select Downloads.
6. Click **Enter**.

   The website displays a list of downloads for the selected product and release.
7. Click the *Avaya Aura® Communication Manager 6.3 Software and Communication Manager Pre-upgrade Software* link.

   The system display the **Downloads & Documents** page.
8. At the bottom of the page, click the `asg_auth_file_6.xml , 6.3.x` link.

   The system displays the Avaya PLDS page.
9. Enter the user name and password.

   The system displays the link to download the default authentication file in **Search by Download**.
10. Click on the *Download* link.

The system displays the Download Manager page.

11. Download the `asg_auth_file_6.xml file` on your system.

Creating an authentication file for a new system

You can download the authentication file directly from AFS to your computer, or you can have the authentication file sent in an email message.

Procedure

1. Start AFS and log in.

   For more information, see Starting the AFS application on page 36.

2. In the **Product** field, click SP System Platform/VE VMware.
3. In the **Release** field, click the release number of the software, and then click **Next**.
4. On the Authentication File Delivery page, select **New System**, and then click **Next**.
5. Type the fully qualified domain name (FQDN) of the Communication Manager system. For duplicated Communication Manager virtual machines, type the alias FQDN.
6. Type the FQDN of Utility Services.

   Note:

   The **Utility Services FQDN** field is not applicable for the Communication Manager AFS.

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 system type, product type, release, and authentication file ID (AFID). You must note the AFID for upgrading the system and for creating the authentication files.

8. To send the authentication file in an email message:
   a. In the **Email Address** field, enter the email address.
   b. Click **Download file via email**.

      AFS sends the authentication file to the specified email address. The email contains the AFID, system type, and release in the message text.

   c. Save the authentication file to a location on the computer of the email recipient.

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

9. 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.

Adding an administrator account

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Administrator Accounts**.
4. Select **Add Login**.
5. Select the **Privileged Administrator** login for a member of the SUSERS group.

   You can also add the following types of login:

   - **Unprivileged Administrator**: This login is for a member of the USERS group.
   - **SAT Access Only**: This login has access only to the Communication Manager System Administration Terminal (SAT) interface.
   - **Web Access Only**: This login has access only to the server webpage.
   - **CDR Access Only**: This login has access only to the survivable CDR feature.
   - **Business Partner Login (dadmin)**: This login is for primary business partners.
   - **Business Partner Craft Login**: This login is for profile 3 users.
   - **Custom Login**: This login is for administrators with login parameters that you can customize. You can create a new user profile and later add users with this new profile.
6. Click **Submit**.

   The system displays the Administrator Login - Add Login screen.
7. In the **Login name** field, enter the administrator login name.

   The login name:

   - Can have alphabetic characters.
   - Can have numbers.
   - Can have an underscore (_).
   - Cannot have more than 31 characters.
8. In the **Primary group** field, enter **susers** for a privileged login.
9. In the **Additional group (profile)** field, add an access profile.

   The system automatically populates the values in the **Linux shell** and the **Home directory** fields.

10. To set lock parameters for the login, select the **Lock this account** check box.

    Note:

    If you set the lock parameters, the user cannot log in to the system.

11. In the **SAT Limit** field, enter the limit for the concurrent SAT sessions.

    Note:

    You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

12. To assign an expiry date to the login, in the **Date on which account is disabled** field, enter the date in the yyyy-mm-dd format.
13. In the **Select type of authentication** field, select one of the following types of authentication:
    - Password
    - ASG: enter key
    - ASG: auto-generate key
14. In the **Enter password or key** field, enter the password for the login.
15. In the **Re-enter password or key** field, reenter the same password.
16. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select yes.
17. Click **Submit**.

Installing an authentication file

You must create and download the authentication file from AFS.

To install the authentication file on Communication Manager, you must create an *administrator* account using Communication Manager System Management Interface. You must install the authentication file on Communication Manager to log in to Communication Manager.

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Security** > **Load Authentication File**.
3. In the **Select the Authentication File** field, click **Browse**.
4. In the Choose File to Upload dialog box, find and select the authentication file, and then click **Open**.

Note:

To override the validation of the AFID and the date and time, select **Force load of new file** on the Authentication File page. Select this option in one of the following situations:

- You must install an authentication file that has a different unique AFID than the file that you installed on Communication Manager.
- You have already installed a new authentication file, but must reinstall the original file.

Do not select this option if you are replacing the default authentication file with a unique authentication file.

Caution:

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

5. Click **Install**.

   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.

6. To confirm that you installed the authentication file on Communication Manager, log in to Communication Manager System Management Interface and check the Authentication File page.

Obtaining the AFID from Communication Manager SMI

Use this procedure when the installer must redeploy the authentication file and needs to obtain the AFID.

Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Authentication File**.

   The system displays the AFID in the **AFID** field.

IPv6 configuration

Enabling IPv6

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

Procedure

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

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

Disabling IPv6

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

Procedure

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

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

Network port considerations

The main virtual machine, survivable remote virtual machines, and survivable core virtual machines use a specific port across a customer network for registration and translation distribution. Use the **`firewall`** command with *suser* level access, to change the firewall settings from the command line.

Note:

Use ports 80 and 443 to gain access to System Management Interface. Use port 5022 for a secured System Access Terminal (SAT).

Use the information in the following table to determine the ports that must be open in the customer network in a survivable core virtual machine environment.

Port	Used by	Description
20	ftp data	-

Table continues…

Port	Used by	Description
21	ftp	-
22	ssh/sftp	-
23	telnet server	-
68	DHCP	-
514	Communication Manager 1.3 to download the translations.	-
1719 (UDP port)	The survivable core virtual machine to register to the main virtual machine.	This a survivable core virtual machine registers with the main virtual machine using port 1719. For more information about survivable core virtual machine registration, see *Avaya Aura® Communication Manager Survivability Options*, 03-603633.
1024 and later	Processor Ethernet	TCP outgoing
1956	Command server - IPSI	-
2312	Telnet firmware monitor	-
5000 to 9999	Processor Ethernet	TCP incoming
5010	IPSI/Virtual machine control channel	-
5011	IPSI/Server IPSI version channel	-
5012	IPSI/Virtual machine serial number channel	-
21874 (TCP port)	The main virtual machine that downloads translations to the survivable core virtual machine.	The main virtual machine uses port 21874 to download translations to the survivable core virtual machine and the survivable remote virtual machines.

Communication Manager virtual machine configuration

To complete the configuration tasks, use Communication Manager System Management Interface to configure the following:

- Server Role: Indicate the type of virtual machine: main, survivable core, or survivable remote.
- Network configuration: Use to configure the IP-related settings for the virtual machine. On the Network Configuration page, the fields are prepopulated with data generated during the OVA template installation.
- Duplication parameters: Use to configure the duplication settings if you installed the Duplex Main or the Survivable Core OVA or both.

Related Links

Server role configuration on page 44
Configuring Server Role on page 45
Server Role field descriptions on page 45

Server role configuration

A telephony system consists of several virtual machines. Each virtual machine has a certain role, such as main or primary virtual machine, a second redundant virtual machine, Survivable Remote virtual machine, or Survivable Core virtual machine. Use Communication Manager System Management Interface to configure the virtual machine roles, and then configure at least two of the following fields.

- Virtual machine settings
- Survivable data
- Memory

OVA type and virtual machine role

The Communication Manager OVA type determines the virtual machine role.

Note:

- The Communication Manager Simplex and Duplex OVAs support Avaya Aura® Call Center Elite.
- The Communication Manager Simplex and Duplex OVAs do not support Avaya Aura® Communication Manager Messaging.

You can configure the Communication Manager Duplex OVA as one of the following:

- Main server
- Survivable core server

Note:

For a Communication Manager duplicated pair configuration, deploy the Communication Manager duplicated servers either on the VMware platform or on the non-VMware hardware. However, you can mix and match the deployment of the survivable core server, the survivable remote server, or the main server in a configuration. For example, the main servers can be a CM-duplicated pair on VMware, and the survivable core server can be on an Avaya hardware, such as System Platform.

You can configure the Communication Manager Simplex OVA as one of the following:

- Main server
- Survivable core server (formerly called Enterprise Survivable Server [ESS])
- Survivable remote server (formerly called Local Survivable Processor [LSP])

Important:

You can deploy the Communication Manager Simplex OVA and then administer the Communication Manager Simplex OVA as a survivable remote server. However, you cannot administer a core Session Manager OVA as a Branch Session Manager or a remote survivable server. Deploy the Session Manager OVA as a core Session Manager OVA only.

Related Links

Communication Manager virtual machine configuration on page 43

Configuring Server Role

Procedure

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

   The system displays the Server Role page.
4. In the **Server Settings**, **Configure Survivable Data** , and **Configure Memory** sections, enter the required information.

   Note:

   If you are configuring a role for the main virtual machine, the system does not display **Configure Survivable Data**.
5. Click **Change** to apply the virtual machine role configuration.

Related Links

Communication Manager virtual machine configuration on page 43

Server Role field descriptions

Server Settings field descriptions

Name	Description
This Server is	Specifies the role of the server. Select from the following roles: • **a main server:** For a primary virtual machine. • **an enterprise survivable server (ESS):** For a survivable core virtual machine. • **a local survivable server (LSP):** For a survivable remote virtual machine.

Table continues…

Name	Description
SID	Specifies the system ID. This ID must be the same for the main server and each survivable server. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.
MID	Specifies the module ID. The main server module ID must be 1 and the ID of the other server must be unique and 2 or more. For a survivable remote server, the MID must match the Cluster ID or MID for that server.

Configure Survivable Data field descriptions

Name	Description
Registration address at the main server (C-LAN or PE address)	Specifies the IP addresses of the Control LAN (C-LAN) or the Processor Ethernet (PE). You must register the main server to this address.
File Synchronization address at the main cluster (PE address)	Specifies the IP addresses of the NICs of the main server and the second redundant server connected to a LAN to which you also connected the Survivable Remote server or the Survivable Core server. **Note:** If a second server is not in use, keep this field blank. The Survivable Remote or the Survivable Core server must be able to ping these addresses. Avaya recommends use of the enterprise LAN for file synchronization.
File Synchronization address at the alternate main cluster (PE address)	Specifies the IP address of the interface that you can use as an alternate file synchronization interface.

Configure Memory field descriptions

Name	Description
This Server's Memory Setting	Specifies the servers memory settings of the server. The options are: small, medium, and large.
Main Server's Memory Setting	Specifies the main servers memory settings of the server.

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

Related Links

Communication Manager virtual machine configuration on page 43

Network

Network configuration

Use the Network Configuration page to configure the IP-related settings for the virtual machine.

Note:

Some changes made on the Network Configuration page can affect the settings on other pages under the **Server Configuration** page. Ensure that all the pages under **Server Configuration** have the appropriate configuration information.

Using the Network Configuration page, you can configure or view the settings of the hostname, alias host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

If the configuration setting for a field is blank, you can configure that setting on the Network Configuration page.

The virtual machine uses virtual NICs on virtual switches internal to the hypervisor. The system uses eth0 in most cases except for duplication traffic. Use eth1 for the duplication IP address.

The Network Configuration page displays the network interfaces that Communication Manager uses. The setting is eth0 for all Communication Manager OVAs except CM_Duplex. For CM_Duplex, the network interfaces are eth0 and eth1.

To activate the new settings on the virtual machine, you must restart Communication Manager after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Configuring the Communication Manager network

Procedure

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

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

   For configuring the Communication Manager Duplex Survivable Core OVA, the system displays additional fields. You can use the same values to duplicate the data on the second Communication Manager virtual machine.

   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.
6. Click **Restart CM**.

   Note:

   To configure for duplication, restart Communication Manager only after you configure the duplication parameters.

   The system takes about 2 minutes to start and stabilize the Communication Manager processes. Depending on your enterprise configuration, the system might require additional time to start the port networks, the gateway, and the telephones.

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.
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.

Table continues…

Name	Description
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.
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. The parameters are: • **IPv4 Address** • **Subnet Mask** • **IPv6 Address** • **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	The options are: • Corporate LAN/Processor Ethernet/Control Network • Corporate LAN/Control Network • Duplication Link

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. **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.

Duplication parameters configuration

Duplication parameters

The system displays the Duplication Parameters page if you install the Duplex OVA. Configuring duplication parameters ensures that the telephony applications run without interruption even when the primary virtual machine is not functional. Communication Manager supports two types of virtual machine duplication: software-based duplication and encrypted software-based duplication.

The duplication type setting must be the same on both the virtual machines. If you are changing the duplication parameters settings, ensure that you make the changes in the following order:

1. Busy out the standby virtual machine, and then change the settings on the standby virtual machine.
2. Change the settings on the active virtual machine. This causes a service outage.
3. Release the standby virtual machine.

Important:

If you change the duplication parameters settings on the active virtual machine, the standby virtual machine becomes the active virtual machine. The new active virtual machine is unavailable for call processing.

Configuring duplication parameters

Procedure

1. Log in to Communication Manager System Management Interface.

2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Duplication Parameters**.

   The system displays the Duplication Parameters page.
4. Type the values in the fields.

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

   For field descriptions, see the *Duplication Parameters field descriptions* section.
5. Click **Change**.
6. Click **Restart CM**.

   In the pop-up confirmation page, you click **Restart Now** to restart the virtual machine immediately or click **Restart Later**, to restart the virtual machine later.

Duplication Parameters field descriptions

Name	Description
Select Server Duplication	Specifies the duplication method. The choices are: • **This is a duplicated server using software-based duplication**: Software-based duplication provides memory synchronization between an active and a standby virtual machine by using a TCP/IP link. • **This is a duplicated server using encrypted software-based duplication**: Encrypted software-based duplication provides memory synchronization between an active and a standby virtual machine by using AES 128 encryption.
Hostname	The host name of the other virtual machine.
Server ID	The unique virtual machine ID of the other virtual machine, which must be an integer from 1 through 256.
Corporate LAN/PE IP	• **IPv4**: The IP address of the Corporate LAN or Processor Ethernet interface for the other virtual machine. • **IPv6**: The IPv6-compliant IP address of the Corporate LAN or Processor Ethernet interface for the other virtual machine.
Duplication IP	• **IPv4**: The IP address of the duplication interface of the other virtual machine. You can assign the IP addresses according to the network configuration.

Table continues…

Name	Description
	• **IPv6**: The IPv6-compliant IP address of the duplication interface of the other virtual machine. You can assign the IP addresses according to the network configuration.
PE Interchange Priority	A relative priority as compared to IPSIs in configurations that use both Processor Ethernet and IPSIs. Select one of the following priority levels: • **HIGH:** Favors the virtual machine with the best PE state of health (SOH) when PE SOH is different between virtual machines. • **EQUAL:** Counts the Processor Ethernet interface as an IPSI and favors the virtual machine with the best connectivity count. • **LOW:** Favors the virtual machine with the best IPSI connectivity when IPSI SOH is different between virtual machines. • **IGNORE:** Does not includes the Processor Ethernet in virtual machine interchange decisions.
IP address for PE Health Check	• **IPv4**: The IP address that enables the virtual machine to determine whether the PE interface is working. **Note:** The network gateway router is the default address. However, use the IP address of any other device on the network that responds. • **IPv6**: The IPv6-compliant IP address that enables the virtual machine to determine whether the PE interface is working.

Button descriptions

Name	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes. The system displays a dialog box with three buttons: **Restart Now**, **Restart Later**, and **Cancel**. **Note:** Click **Restart Now** only after configuring the complete settings of the virtual machine. Too many restarts can escalate to a full Communication Manager reboot.

Table continues…

Name	Description
Restart CM	Updates the system configuration files with the current values on the page. **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.

Chapter 6: Postinstallation verification and testing

Installation tests

You must perform many post installation administration, verification, and testing tasks to ensure that you have installed and configured the system components as part of the Communication Manager installation.

This section provides a list of tasks for testing the OVA, virtual machine, and system component installation and configuration. You cannot perform certain tests until you install and configure the complete solution, including port networks.

Note:

To perform the following tests, you must configure the Communication Manager translation and IPSIs.

You must first perform the following post installation administration and verification tasks:

- Verifying the translations
- Clearing and resolving alarms
- Backing up the files

You can perform the following tests only after you install and configure the port networks and UPS.

- Testing the IPSI circuit pack
- Testing the IPSI LEDs

For the server-specific post installation administration and verification tasks, see the relevant server installation documents.

For information about the LEDs state, see *LED Descriptions for Avaya Aura® Communication Manager Hardware Components*.

Verifying the license status

Accessing Communication Manager System Management Interface

You can gain access to Communication Manager System Management Interface (SMI) remotely through the corporate LAN connection. You must connect the virtual machine to the network.

Procedure

1. Open a compatible web browser.

   SMI supports Internet Explorer 7.0 and Mozilla Firefox 3.6 and later.

2. In the browser, choose one of the following options depending on the virtual machine configuration:

   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the Communication Manager virtual machine in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

3. Press `Enter`.

   Note:

   If the browser does not have a valid security certificate, the system displays a warning with instructions to load the security certificate. If your connection is secure, accept the virtual machine security certificate to access the Logon screen. If you plan to use this computer and browser to access this virtual machine or other Communication Manager virtual machine again, click **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type the user name.

   Note:

   If you use an Avaya services login that Access Security Gateway (ASG) protects, you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the

Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type the password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Viewing the license status

Use this procedure to view the Communication Manager license status.

Procedure

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

   The License Status page displays the license mode, error information, System ID, and Module ID.

   The license status can be one of the following:

   - Successfully installed and valid
   - Unlicensed and within the 30-day grace period
   - Unlicensed and the 30-day grace period has expired

License Status field descriptions

Name	Description
CommunicaMgr License Mode	Specifies the license status. • Normal: The Communication Manager license mode is normal and the system has no license errors. • Error: The Communication Manager license has an error and the 30-day grace period is active. • No License: The Communication Manager license has an error and the 30-day grace period has expired. The Communication Manager software is running, but blocks normal call processing. The switch administration software remains active so

Table continues…

Name	Description
	that you can correct license errors, for example, reducing the number of stations.
checking application CommunicaMgr version	Specifies the version of Communication Manager. For example, R016x.00.0.340.0.
WebLM server used for License	Displays the WebLM server URL used for the license. For example, `https://10.18.2.8:52233/WebLM/LicenseServer`.
Module ID	The Communication Manager main virtual machine has a default module ID of 1. You can configure the module ID on the Server Role page. Each survivable virtual machine has a unique module ID of 2 or more. The module ID must be unique for the main virtual machine and all survivable virtual machines.
System ID	Communication Manager has a default system ID of 1. You can configure the system ID on the Server Role page. The system ID is common across the main virtual machine and all survivable virtual machines. Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.

Verifying the software version

When the system is on a new software release, you must log in with the super user login that you configured before installing the AFS file. For information about adding an administrator account, see Adding an administrator account login on page 39.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server** > **Software Version**.
4. Verify that the **CM Reports as:** field shows the correct software load.
5. On the menu bar, click **Log Off**.

Verifying the survivable virtual machine registration

If you configured a Survivable Core or Survivable Remote virtual machine, verify that the virtual machine is registered with the main virtual machine. This task can take several minutes to complete.

Procedure

1. On the SAT screen, type **`list survivable-processor`**.

   The system displays the Survivable Processor screen.

2. Verify that the **Reg** field is set to **y**.

   This setting indicates that the survivable virtual machine is registered with the main virtual machine.

3. Verify that the **Translations Updated** field shows the current time and date.

   This setting indicates that the system has scheduled the translations for the survivable virtual machine.

Verifying the virtual machine mode

Use this procedure to verify the virtual machine mode, process status, and operations.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server** > **Status Summary**.
4. Verify the **Mode** field.
   - `Active` on an active virtual machine.
   - `StandBy` on a standby virtual machine.
   - `BUSY OUT` on a busy out virtual machine.
5. To verify the process status, click **Server** > **Process Status**.
6. In the **Frequency** section , select **Display When**.
7. Click **View**.

   The system displays the Process Status Results page.

8. Verify that all operations are:
   - `Down` for dupmanager
   - `UP` all other operations

Appendix A: Troubleshooting Communication Manager custom kernel VMware vSphere tools

Identifying corrupted Communication Manager VMware vSphere Tools

It is possible to have the VMware vSphere Tools tailored for the Communication Manager custom kernel to become corrupted by having the standard VMware vSphere Tools installed over the Communication Manager VMware vSphere Tools. There is no visual indication in either the vSphere Client connected to the ESXi host or the vCenter server. There may be indications manifesting in impaired performance. To identify corrupted Communication Manager VMware vSphere tool:

Procedure

1. Log on to the Communication Manager virtual machine and run command **`/sbin/lsmod | grep v`**

   If you do not see the following drivers the tool is corrupted.

   - vmxnet or vmxnet3
   - vmci
   - vmmemctl
   - pvscsi
   - vsock

2. Execute the command **`/usr/bin/vmware-toolbox-cmd –v`** to verify the installed version of VMware Tools.

   For example,

```
root@cm-rr0> /usr/bin/ vmware-toolbox-cmd -v
8.6.5.11214 (build-621624)
```

Repairing Communication Manager VMware vSphere tools

Communication Manager custom kernel version of VMware vSphere Tools is deployed as an RPM. For example, for VMware vSphere 4.1 and Communication Manager Release 6.2 and later the RPM is *VMware Tools-8.3.2_257589.2-2.6.18_238.AV02PAE.i386.rpm*. RPM elements are:

- *VMware Tools-8.3.2_257589* specifies the VMware version of the tools.
- *2.6.18_238.AV02PAE* specifies the Communication Manager kernel for which the VMware Tools are compiled
- *i386.rpm* is the VMware version string (RPM build number).

The RPMs are located in the `/var/disk/rpms` directory. To restore the Communication Manager custom kernel version of VMware vSphere tool:

Procedure

1. Log on to the Communication Manager virtual machine console as *root*.

   You might have only one VMware Tools RPM now.

2. Run the command **`cd /var/disk/rpms`** and verify that the VMwaretools RPM is available. For example, *ls VMwaretools**.
3. Run command **`rpm -U --force Vmwaretools-*********.i386.rpm`**.
4. Run command **`lsmod | grep v`** and verify the correct drivers.

Appendix B: Communication Manager debugging

Communication Manager processes

Using the *gdb* debugger, you can analyze the Communication Manager processes core files. For example, by segmentation faults that generate core files that are written into the `/var/crash` directory.

Creating Communication Manager virtual machine core images

Currently, the creation and debugging of Communication Manager virtual machine core images created by the VM kernel is not supported. If you have to create a Communication Manager virtual machine core images to debug, for example, a reproducible problem, use the following steps.

Procedure

1. Install the kexec-tools rpm that provides the functionality to generate core files, for example, on kernel panics. You can install the Virtual Machine kernel dump service from the Virtual Machine kernel dump service documentation Web link. You can follow the CLI instructions for easier navigation. You must note the following points:
   a. The Virtual Machine kernel dump service documentation Web link describes changes to the GRUB tool, which for Communication Manager is lilo, that is `/etc/lilo.conf`. It states to add `crashkernel=128M` on the kernel entry line but actually the string to add is `crashkernel=128M@16M`. Execute the **`lilo`** command and reboot the virtual machine.
   b. Execute the **`service kdump status`** command to ensure that the *kdump rc* script is setup and running.
2. Execute the following to ensure that a virtual machine kernel core can be created

```
echo 1 > /proc/sys/kernel/sysrq
echo c > /proc/sysrq-trigger
```

3. After the Communication Manager virtual machine is rebooted ensure the core image is written to the virtual machine disk space in the `/var/crash/_date_/vmcore` directory.

Use the RedHat Crash Utility to debug the core images in the `/var/crash/_date_/vmcore` directory. See VMware generated core images on Communication Manager virtual machine images on page 62.

VMware generated core images on Communication Manager virtual machine images

VMware provides technical assistance for debugging virtual machine issues, for example, VM kernel panics and virtual machines that hang. When you log a service request, you must send the performance snapshots to troubleshoot the issue. You can execute the **`vm-support`** command to collect the virtual machine logs. The **`vm-support`** command also creates a *.tar* file for sending the logs to VMware. The core image can be debugged using the RedHat Crash Utility as described in Collecting performance snapshots using vm-support.

VMware also provides a utility to help you to take an initial look at virtual machine issues, for example, VM kernel panics, a virtual machine with very slow response times, or for a virtual machine that hangs. The utility is called vmss2core. The vmss2core is a command line tool for creating virtual machine core file that you can use with the RedHat crash utility. For the vmss2core command, see VMware Knowledge Base, which includes the vmss2core technical link. The vmss2core tool generates a `vmcore` core file, using the virtual machine's `.vmsn` file from a snapshot, or `.vmss` file from a suspended virtual machine. For the RedHat crash utility, see White paper: RedHat Crash Utility.

Appendix C: Communication Manager software duplication with VMware high availability

This Appendix shows an illustration of Communication Manager software duplication with four ESXi Hosts configured in two data clusters with VMware high availability (HA).

- In the Figure 1: VMware cluster configuration with four ESXi hosts on page 64, Communication Manager software duplication is established across two VMware Data Clusters. Each cluster is using the VMware HA. Communication Manager active and standby virtual machines are not supported within the same data cluster with VMware HA.
- To establish the connectivity the Software Duplication link must be tied together through a dedicated Ethernet IP private Switch or VLAN, Host to Host (Figure). Hosts 1 and 3 are on Data Cluster A and Hosts 2 and 4 are on Data Cluster B.
- The illustration has two Communication Manager virtual machines, CMVM_01 and CMVM_02 configured as an Active (ACT) and Standby (STB) pair using Communication Manager virtual machine software duplication link.
- CMVM_01 (ACT) Eth2 configuration virtual switch is tied to physical adapter VMnic2 on Host 1 and CMVM_02 (STB) Eth2 configuration virtual switch is tied to physical adapter VMnic2 on Host 4.
- Other virtual machines are not using the VMnic2.

Example: When Active virtual machine fails

In the Figure 1: VMware cluster configuration with four ESXi hosts on page 64:

- Host 1 (CMVM_01) is ACT with a duplication link communicating over VMnic2 through the network switch.
- Host 4 (CMVM_02) is STB with a duplication link communicating over VMnic2 through the network switch.
- If Host 1 fails, CMVM_02 becomes ACT.
- VMware HA starts CMVM_01 on Host 3.
- Host 3 (CMVM_01) starts communication over VMnic2.
- Host 1 is booting so no communication over VMnic2.

- Host 3 (CMVM_01) and Host 4 (CMVM_02) link up and communicate across the network switch over each VMnic2.

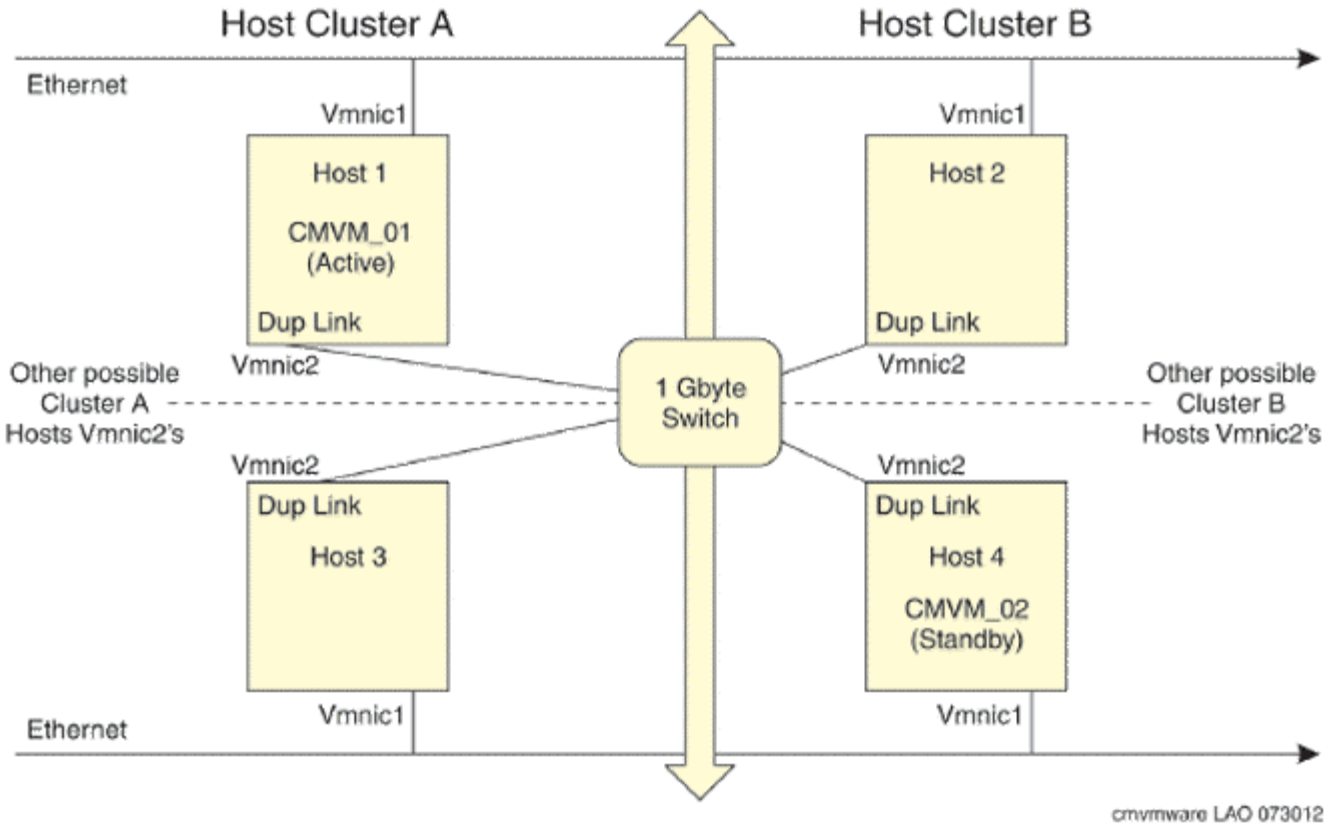


Figure 1: VMware cluster configuration with four ESXi hosts

Software duplication enhancement

With Communication Manager Release 6.3.6, you can configure both active and standby servers in the same data cluster. For more information about duplicated server configuration, see *Duplicated Avaya Aura® Communication Manager on VMware* on the Avaya Support website at https://support.avaya.com/.

Appendix D: Upgrading Communication Manager Open Virtual Application

Upgrading Communication Manager using full backup

Note:

Save the translations before taking the full backup.

Use the following procedure to upgrade the new Communication Manager VMware virtual machine by taking a full backup of an existing Communication Manager VMware virtual machine.

Procedure

1. Take a full backup of the existing Communication Manager virtual machine.
2. Deploy the new Communication Manager virtual machine on a host server.
3. Start the new Communication Manager virtual machine.
4. Log in to the new Communication Manager virtual machine console with the *craft* login.
5. Shut down the existing Communication Manager virtual machine.

   Note:

   The existing Communication Manager virtual machine will be out of service.
6. On the new Communication Manager virtual machine, administer the network parameters, such as IP address, network net mask, and router gateway.
7. Log in to Communication Manager System Management Interface with the *craft* login.
8. Use the View/Restore Data page to restore the full backup on the new Communication Manager virtual machine, and reboot Communication Manager.

   You can now use the new Communication Manager virtual machine.

Related Links

Creating a backup on page 66

Creating a backup

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Data Backup/Restore** > **Backup Now**.

   The system displays the Backup Now page.
4. Click **Full Backup**.
5. In the **Network Device** section, select the backup method and type the user name, password, host name, and path of the directory in which you stored the data.
6. Click **Start Backup**.

   On the Backup Now Results page, the system displays the message `Backup Successfully Completed`.

Related Links

Upgrading Communication Manager using full backup on page 65

Upgrading Communication Manager virtual machine and restoring the translations

Use the following procedure to upgrade the new Communication Manager virtual machine by using the translations of an existing Communication Manager.

The following procedure requires an SMI webpage session for the existing Communication Manager virtual machine and the new Communication Manager virtual machine.

Procedure

1. Deploy the new Communication Manager virtual machine on a host server.
2. Start the new Communication Manager virtual machine.
3. Save the translations of the existing Communication Manager virtual machine.
4. Shutdown the existing Communication Manager virtual machine.
5. Log in to the new Communication Manager virtual machine console with the `craft` login.
6. Administer the new Communication Manager virtual machine:
   a. Administer the network parameters.
   b. Apply the Communication Manager patch.
   c. Set the time zone.

   d. Set the network time protocol.
   e. Add an suser account.
   f. Load an authentication file.
7. On the new Communication Manager virtual machine, log in to Communication Manager System Management Interface and set the host name and DNS information of the new Communication Manager in the same way as on the existing Communication Manager virtual machine.
8. Restore the translations on the new Communication Manager virtual machine.
9. Reboot the new Communication Manager virtual machine.
10. Log in to Communication Manager System Management Interface of the new Communication Manager virtual machine and configure the WebLM server.

Communication Manager patches

The Communication Manager Simplex and Duplex OVAs might not include the latest Communication Manager Service Pack. After deploying the OVA, you must check for the latest Communication Manager service pack on the Avaya Support website at http://support.avaya.com/ to install the latest service pack on the OVA.

Using Communication Manager System Management Interface, you can unpack, activate, validate, and apply the updates. On SMI, navigate to **Adminstration** > **Server(Maintenance)** > **Server Upgrades** > **Manage Updates** page.

For Communication Manager Kernel patching additional caution is required associated with the Communication Manager VMware Tools package, that is,

- When installing a new version of the VMware Tools RPM for the current Kernel, unpack and activate the new VMware Tools update, and manually reboot LINUX.
- When installing a new version of the VMware Tools for a new version of the Kernel, first unpack and activate the new VMware Tools update. The second step is to activate the new Kernel update and to automatically reboot LINUX.

You do not need to deactivate a currently active VMware Tools update (if there is one) before activating the new VMware Tools update. The new VMware Tools update replaces the current VMware Tools update (if present) and changes the VMware Tools update state to *unpacked* similar to that for Kernel updates.

The VMware Tools update goes directly to the activated and/or unpacked state. Kernel updates stay in activating and/or deactivating state until about one minute after the LINUX reboot and then switch to pending_commit and/or pending_deactivate. This is necessary to permit activation of the Kernel update if needed, since additional update operations are not allowed if there are any Kernel updates in the activating, deactivating, pending_commit, or pending_deactivate states.

Connection preservation upgrade on Communication Manager Duplex OVA

Communication Manager Duplex OVA upgrade

This section describes the procedure to upgrade Communication Manager from Release 6.2 to Release 6.3 on the duplex OVA. The upgrade procedure includes:

- Backing up translations, security, and system files.
- Upgrading the Communication Manager OVA.
- Performing the verification tasks.

The upgrade procedure preserves Communication Manager translations, administrator accounts, and the server configuration. You do not require the following files during the upgrade:

- A new or an updated license file
- An authentication file

Use this section to upgrade Communication Manager from Release 6.2 to Release 6.3 on:

- The main server
- The survivable server

Presite upgrade checklist

Before you go onsite, perform the following tasks:

#	Task	Description	✔
1	Redesign the voice network, dial plan, and E911 for remote locations.	Perform this task only if applicable.	
2	Verify that you have the required Communication Manager OVA.	-	
3	Ensure that the circuit packs are on the latest firmware.	For more information, see *Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates* on the Avaya Support website at http://support.avaya.com.	

Preupgrade tasks on the active server

Clearing alarms

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Alarms** > **Current Alarms**.
4. In the **Server Alarms** section, select the alarms.
5. Click **Clear** or **Clear All**.
6. Resolve any major alarms with SAT commands and a terminal emulation application, such as Native Configuration Manager.

Starting a SAT session

Procedure

1. To establish an SSH connection,
   a. In the **Host Name (or IP address)** field, type `192.152.254.201`.
   b. In the **Port** field, type `5022`.
2. To establish a Telnet connection,
   a. In the **Host Name (or IP address)** field, type `192.152.254.201`.
   b. In the **Port** field, type `5023`.
3. Log on to the server using an appropriate user ID.
4. Suppress alarm origination.

Recording the busyout equipment

Procedure

1. On the SAT screen, type the command **`display errors`** and press **Enter**.

   The system displays the Error Report screen.
2. In the **Error Type** field, type `18`.

   The system displays a list of busied out equipment.
3. Make a note of the busied out equipments.

Checking clock synchronization

Procedure

1. On the SAT screen, type the command **`status synchronization`** and press **Enter**.

The system displays the Synchronization Status screen.

2. In the **Switching Capabilities** field, ensure that the system displays `enabled`.

Disabling the scheduled maintenance

The scheduled daily maintenance might interfere with the server upgrade, so you must reschedule the daily maintenance activity.

Procedure

1. On the SAT screen, type the command **`change system-parameters maintenance`** and press **Enter**.

   The system displays the Maintenance-Related System Parameters screen.

2. Make a note of the settings in the **Stop Time** and **Start Time** fields.
3. Perform one of the following:
   - If scheduled maintenance is in progress, set the **Stop Time** field to 1 minute after the current time.
   - If scheduled maintenance is not in progress, set the **Start Time** field to a time after the system completes the server upgrade.

   For example, if you start the server upgrade at 8:00 p.m. and the upgrade takes 90 minutes, set the **Start Time** field to `21:30` p.m.

Saving translations

Perform the following procedure on the main server only.

Procedure

1. On the SAT screen, type the command **`save translation all`**.

   The system displays the `Command successfully completed` or the `all error messages are logged` message.

2. At the command prompt, type `filesync -Q all`.
3. Verify whether the system displays the filesync errors or not.

Backing up the system data on the active server

For information about creating backup, see Creating a backup on page 66.

Connection preservation during an upgrade

When upgrading within the same release, for example, Release 6.2 to Release 6.3, Communication Manager preserves the following connections:

- The audio portion of many stable telephone calls throughout the course of the upgrade.
- The data transmission between many stable fax, data, or multimedia endpoints.

Communication Manager does not preserve the following connections during an upgrade:

- H.323 IP trunks
- SIP trunks

  For example, trunks established for SIP endpoints that use Communication Manager and Session Manager for SIP connections.
- ISDN-BRI trunks or stations
- Unstable calls

  For example, calls that are in the ringing or dialing stage, calls that are on hold, or calls in any state that require control signaling. Unstable calls are dropped, regardless of whether they are carrying voice or data transmissions.
- SAT sessions
- Adjunct links

  For example, links to a CMS, ASAI, or CDR adjunct, a link to a system printer, or any other links configured using the IP Services screen.

Activating connection preservation during an upgrade

Preserve connections immediately after you perform all standard preupgrade tasks.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Upgrade** > **Pre Update/Upgrade Step**.
4. On the Pre Update/Upgrade Step screen, click **Continue** to start the preupgrade step.

   The system displays the status of the preupgrade step operations.

The system locks the translations on the active server. This allows the standby server to precisely synchronize translations and preserve connections during the interchange. When the upgrade is complete, the translations are unlocked and the normal synchronization process resumes.

Preupgrade tasks on the standby server

Clearing alarms on the standby server

For information about clearing alarms, see Clearing alarms on page 69.

Backing up the system data on the standby server

For information about creating backup, see Creating a backup on page 66.

Busying out the standby server

Procedure

1. Log in to Communication Manager System Management Interface of the standby server as `craft` or `dadmin`.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Click **Server** > **Busy-Out/Release Server**.
4. Click **Busy Out**.

Communication Manager upgrade

You must perform the upgrade of Communication Manager, and install the latest service packs or patches.

For more information about Communication Manager patches, see Communication Manager patches and Applying Communication Manager sections.

Reconfiguring the Communication Manager license server

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Licensing**.
3. In the navigation pane, click **weblm configuration**.
4. Enter the IP address of the WebLM server to fetch the license file.

Upgrading Communication Manager OVA

For information about full backup upgrade, see Upgrading using full backup on page 65

Verifying Communication Manager operation

Releasing the server

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Server** > **Busy-Out/Release Server**.
4. On the Busy-Out/Release Server page, click **Release**.

Performing an integrity check

Procedure

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

4. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
5. In the navigation pane, click **Server** > **Process Status**.
6. In the **Frequency** section, click **Display Once**.
7. Click **View**.
8. Verify that the status for all operations is `UP STANDBY`.
9. Ping the IP address of Communication Manager by using SSH or Telnet.

Server role interchange

When the standby server is ready, interchange the roles of the standby and active servers.

Interchanging the servers

Complete this procedure to verify if you can interchange the active and standby servers successfully.

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Click **Server** > **Interchange Servers**.
4. Click **Interchange**.

   The system changes the roles of the active and standby servers.

Performing an integrity check after server interchange

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the navigation pane, click **Server** > **Status Summary**.
4. Verify the following:
   - **Server Hardware**: okay
   - **Processes**: okay
5. In the navigation pane, click **Server** > **Process Status**.
6. In the **Frequency** section, click **Display Once**.
7. Click **View**.
8. Verify that the status for all operations is `UP`.
9. Ping the IP address of Communication Manager by using SSH or Telnet.

Upgrade tasks on the standby server that was active before the interchange

Tasks on the standby server

Perform the following procedures on the server that was formerly active and changed to the standby state after you have interchanged the server roles.

1. Busying out the standby server on page 71
2. Communication Manager upgrade on page 72
3. Reconfiguring the Communication Manager license server on page 72
4. Upgrading CM OVA on page 72
5. Releasing the server on page 72
6. Performing an integrity check on page 72

Postupgrade tasks on the active server running Release 6.3

Busying out previously busied out equipment

Procedure

If you recorded any equipment that was busied out before the upgrade on the main server only, busy it out after the upgrade.

Enabling scheduled maintenance

To schedule daily maintenance:

Procedure

Reset the settings that you recorded earlier in Disabling the scheduled maintenance on page 70.

Save translations

For information about saving translations, see Saving translations on page 70.

Resolving alarms

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. Click **Alarms** > **Current Alarms**.

   The system displays the Current Alarms page.
4. In the **Server Alarms** section, select the alarms you want to clear.

5. Click **Clear**.
6. To resolve new alarms after the server upgrade, use a SAT session.

   For information, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways, and Servers*, 03-300431 and *Avaya Aura® Communication Manager Server Alarms*, 03-602798.

Back up the system data

To back up the system data, see Creating a backup on page 66.

Logging off all administration applications

When you complete all the administration activities, log off from all the applications you used.

Postupgrade tasks on the standby server running Release 6.3

Resolve alarms

For information about resolving the alarms, see Resolving alarms on page 74.

Back up the system data

To back up the system data, see Creating a backup on page 66.

Logging off all administration applications

When you complete all the administration activities, log off from all the applications you used.

Appendix E: Migrating Communication Manager to the VMware Virtualized Environment

This procedure describes how to migrate Communication Manager from a non-VMware environment to the VMware Virtualized Environment. This procedure applies to both Communication Manager Simplex and Communication Manager Duplex.

This procedure requires certain steps to be performed in parallel between several different organizations (the customer, Avaya Professional Services, Avaya Technical Support, Avaya Registration Team). The customer does not have access to the registration forms. SAL Gateway testing and configuration must be in sync with the record updates/changes in Seibel.

Important:

Current users with embedded Communication Manager Messaging need to find another way to host messaging if they move Communication Manager to Virtualized Environmentsince Communication Manager Messaging has not been virtualized and is not supported in Virtualized Environment.

If existing IP addresses will be reused, the Communication Manager non-VMware environment and the Communication Manager Virtualized Environment *cannot* exist on the customer's network at the same time. If one server is turned on, the other server must be turned off.

Administrator accounts are not migrated and must be added back manually. If SNMP is implemented, the SNMP settings must be noted and re-entered.

VMware is not supported on S8300D Server. The System Platform-based implementation will be used. You must upgrade Survivable Remote servers to System Platform 6.2.1.0.9 or later before you can upgrade the Communication Manager template to the Survivable embedded remote template. Survivable servers must be the same version or higher than the main server.

Important:

Ensure any Survivable Remote server has the same version as the Communication Manager virtual application version. The survivable remote version must remain at 6.2. Use the 6.2 media if you must update the version.

Procedure

1. Download and save the migration workbooks from the Avaya Support website. In the **Security Warning** dialog box, click **Enable Macros**.
   - For Communication Manager 5.2.1, download the *Migrating from Avaya Aura® Communication Manager 5.2.1 to VMware® Workbook* at https://downloads.avaya.com/css/P8/documents/100167657.
   - For Communication Manager 6.x, download the *Migrating from Avaya Aura® Communication Manager 6.x to VMware® Workbook* at https://downloads.avaya.com/css/P8/documents/100167658.
2. Record the Communication Manager configuration data in the workbook.

   You will need this information when you restore migration backup.
3. Navigate to the Communication Manager SMI page of the existing main Communication Manager server.
4. Back up the data from the SMI page:
   - Communication Manager 5.2.1 or 6.x migration backup files
   - Utility Services migration backup files ((if applicable). This is available only in Release 6.2 and later. For information about creating backup file, see *Deploying Avaya Aura® Utility Services on VMware® in Virtualized Environment*.
5. If using Utility Services 6.1:
   a. Note the DHCP server settings if in use.
   b. Note any special firmware that has been loaded and ensure you have a copy of the firmware to be uploaded onto the new server. This includes Branch Gateway, ADVD, and IP phone firmware.
   c. Note the Communication Manager server IP address, login, and password so Utility Services can interrogate the system to understand the IP phone firmware.
6. Download and install the following virtual application OVA files but *do not* turn on the applications.
   - Communication Manager
   - Utility Services (if applicable)
   - WebLM (if applicable)
   - Secure Access Link (not needed if a Standalone SAL Gateway is in place)

   See the appropriate deployment guide for downloading and installing the virtual application OVA file.
7. If SAL is in use on System Platform:
   a. Log in to the SAL Gateway.
   b. Capture settings using screen capture.
8. Turn off the existing server.

9. If a Standalone SAL Gateway is *not* in place, turn on and configure the SAL virtual application. Reuse the details on the screen captures from the existing SAL Gateway.
10. Turn on the following virtual applications:
    - Communication Manager. Provision the initial IP address as required by the deployment guide.
    - Utility Services (if applicable)
    - WebLM (if applicable)
11. Download and activate the latest Communication Manager patch.
12. Navigate to the Communication Manager SMI page.
13. On the SMI page, do the following:
    a. Set the date and time.
    b. Set the NTP. Reboots are required to synchronize all processes to NTP.
    c. Add a superuser login.
    d. Restore existing Communication Manager migration backup file. Update and confirm your system configuration using the migration workbook worksheet. Re-enter SNMP data if needed.
    e. Retranslate the WebLM server destination, if applicable. Navigate to **Administration** > **Licensing** > **WebLM Configuration**.
14. Restore Utility Services (6.2 and later) or retranslate Utility Services , as applicable.
15. Retranslate the Utility Services server destination, if applicable.
16. Set up the System Manager or WebLM virtual appliance to provide licensing support for Communication Manager. Obtain a new PLDS. Do not use the MAC address from the previously used server. To obtain the MAC address information for WebLM, log in to WebLM and click **Properties**.
17. Complete the SAL registration spreadsheet in the migration workbook.
18. Reregister Communication Manager as a virtual application.
19. Remove records for Communication Manager as System Platform. This step must be performed by the Avaya Registration team.
20. Add records. This step must be performed by the Avaya Registration team.
21. Verify SAL connectivity after the new SAL Gateway is communicating to the data center.
22. Test an alarm and verify that alarming is working properly.
23. Verify survivability with existing LSP or ESS.

24. If there were multiple SAL Gateways in use on System Platform before the migration, and the SAL Gateways will be consolidated into a single SAL Gateway virtual application , do the following:
    a. Choose settings for one SAL Gateway virtual application that will carry forward. Make a screen capture of the administration settings and export managed elements for the primary SAL Gateway.
    b. Export managed elements for each existing System Platform-based SAL Gateway to the virtual application-based SAL Gateway.
    c. Update the virtual SEID and Product IDs for each System Platform-based SAL Gateway that is no longer used.
25. If IP addresses were reused, the pre-VMware Communication Manager environment cannot be running on the customer's network at the same time as the VMware-based Communication Manager. Remove the Ethernet cables from the decommissioned server as a network safety measure.
26. Determine the disposition of the server on which applications were previously running. The server cannot be reused for any other Avaya applications unless the server has the same comcode as the Communication Manager server. If the server will not be used, submit the appropriate forms to the Avaya Customer Care Center to remove the server from the installed base record.
    - For Avaya personnel, the forms can be found at Avaya Personnel Forms.
    - For Business Partners, the forms can be found at Business Partner Forms.
27. Remove the physical server from the maintenance contract if it is no longer utilized. The customer contacts the Avaya Customer Care Center and requests removal from the installed base record of the Functional Location (FL). The adjustment becomes effective with the next contract renewal or true-up because the contract is prepaid by the customer.

Appendix F: VMware best practices for performance

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

Related Links

VMware Tools on page 82
Timekeeping on page 82
VMware networking best practices on page 83
Thin vs. thick deployments on page 87
Storage on page 88

BIOS

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

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

The following sections describe the recommended BIOS settings for:

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

Intel Virtualization Technology

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

All Intel Xeon processors include:

- Intel Virtualization Technology

- Intel Extended Memory 64 Technology
- Execute Disable Bit

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

Note:

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

Other suggested BIOS settings

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

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

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

Dell PowerEdge Server

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

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

HP ProLiant Servers

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

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

VMware Tools

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

The tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing
- Startup/Shutdown scripts (with VMware Toolbox running as *root*)

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

The VMware Tools have been tailored to run with the Communication Manager virtual machine kernel. **You should not upgrade the VMware Tools**.

You can refer to the Identifying corrupted Communication Manager VMware vSphere Tools on page 59.

Related Links

VMware best practices for performance on page 80

Timekeeping

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

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

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

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

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

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

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

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

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

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

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

Related Links

VMware best practices for performance on page 80
Setting up the network time protocol on page 35

VMware networking best practices

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

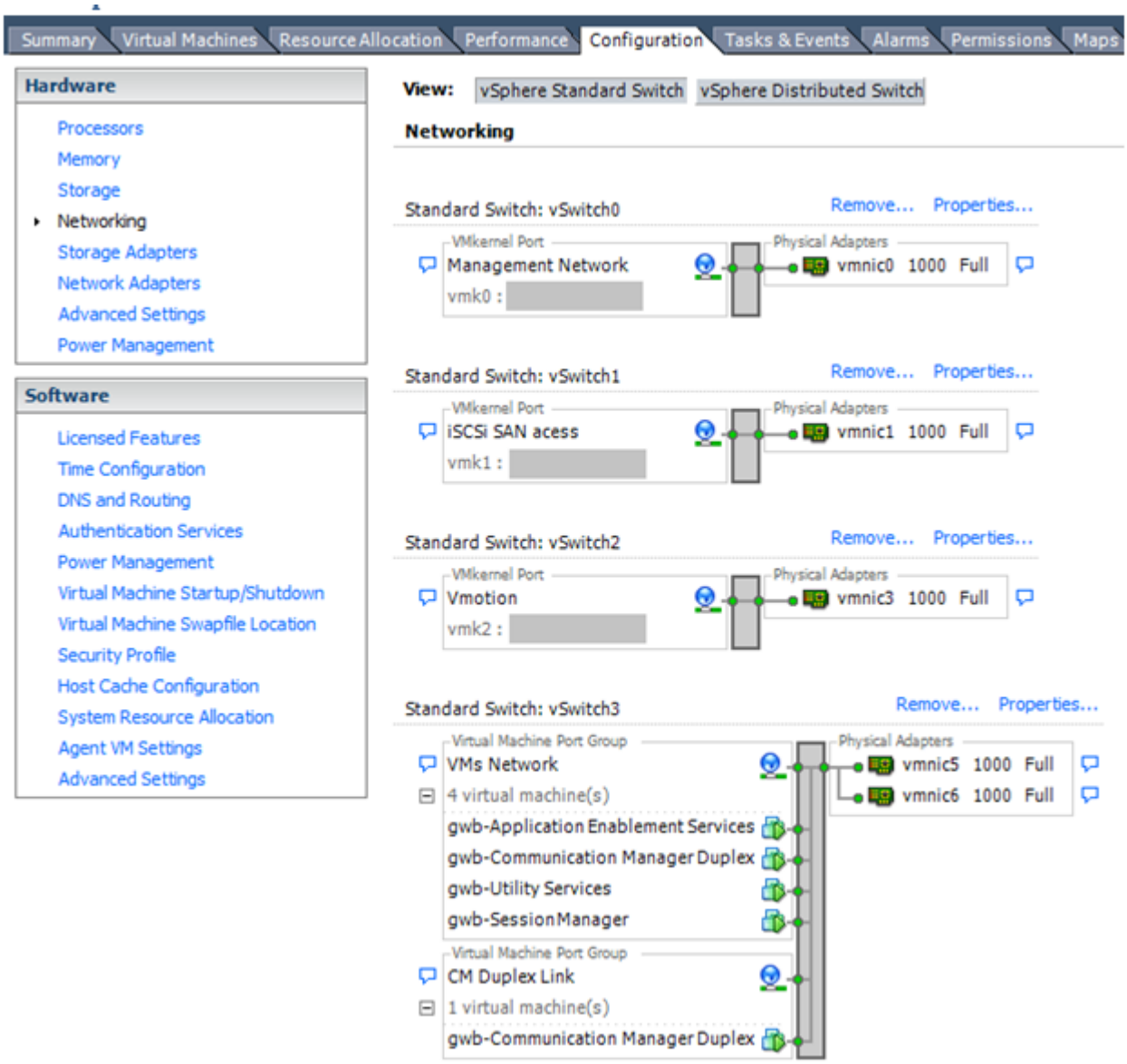
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

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

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.

- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernal vNICs to be the same IP Maximum Transmission Unit (MTU).

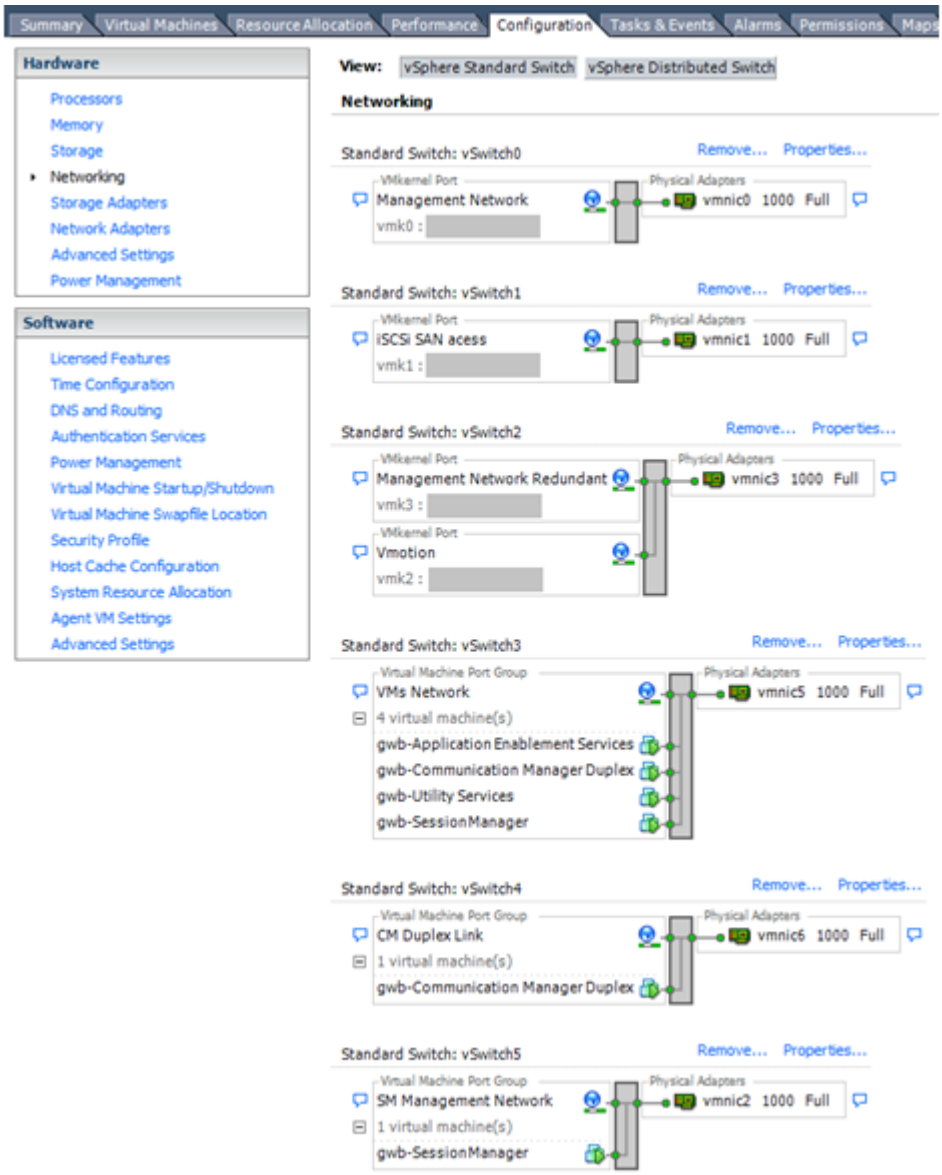
Networking Avaya applications on VMware ESXi – Example 1



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

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements. for more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:
  - The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
  - The round-trip delay must be 8 ms or less.
  - The round-trip packet loss must be 0.1% or less.
  - Both servers duplication ports must be on the same IP subnet.
  - You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
  - The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.
- Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, Example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



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

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

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

References

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

Related Links

VMware best practices for performance on page 80

Thin vs. thick deployments

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

In contrast, a thin virtual disk does not pre-allocate all of the space. Blocks in the VMDK file are not allocated and backed by physical storage until they are written during the normal course of operation. A read to an unallocated block returns zeroes, but the block is not backed with physical storage until it is written. Consider the following when implementing thin provisioning in your VMware environment:

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

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

Related Links

VMware best practices for performance on page 80

Storage

Fibre Channel SAN arrays and iSCSI SAN arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs and are the preferred storage technology for Communication Manager. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

Related Links

VMware best practices for performance on page 80

Best Practices for VMware features

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshot is a short-term copy of the running system that you can create before a 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 that 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. When creating a snapshot, perform the following;
  - 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 consolidate failure occurs, you 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, the system displays a warning in the UI.

If the Duplex OVA is in use, you must take the snapshot on the standby virtual machine when the standby is refreshed. If the snapshot is taken on the active virtual machine under a heavy load there is a possibility an interchange of virtual machine can occur.

Related resources

See the following resources for more information about snapshots:

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

Related Links

VMware best practices for performance on page 80

High availability

Simplex OVA

Communication Manager Simplex open virtual application (OVA) deployment supports VMware high availability. If the ESXi host fails where the Communication Manager virtual machine is installed, the Communication Manager virtual machine is moved to another ESXi host. The Communication Manager virtual machine powers up, boots, and continues to process the new call processing requests.

Related Links

VMware best practices for performance on page 80

Duplex OVA

The VMware (non HA) environment configuration supports an Active (ACT) Communication Manager virtual machine deployed on one stand alone Host with the Standby (STB) Communication Manager virtual machine deployed on a second stand alone Host with the software duplication link (NIC) directly linked together.

Communication Manager software duplication works with VMware HA as long as the Communication Manager Active and Standby virtual machines are in different data clusters.

For example, if an active Communication Manager virtual machine is deployed on a host in one data cluster (A) and standby Communication Manager virtual machine is deployed on a second host in another data cluster (B). The Communication Manager virtual machines are configured on the same sub network. The connectivity requires the software duplication link (NIC) to be tied together through a private network switch or VLAN.

For information about VMware HA in each data cluster, see Communication Manager software duplication with VMware high availability on page 63.

Related Links

VMware best practices for performance on page 80

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one ESX host to another 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.

Before using VMware 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.

With vMotion, you can:

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

Using VMware vMotion with Communication Manager virtual machine moves its current host to a new host and call processing continues with no call failures.

Related Links

VMware best practices for performance on page 80

Appendix G: PCN and PSN notifications

PCN and PSN notifications

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

Viewing PCNs and PSNs

To view PCNs and PSNs, perform the following steps:

Procedure

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

   Note:

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

2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   Note:

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

Signing up for PCNs and PSNs

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

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

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

Glossary

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

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

Index

A

accessing
    SMI 55
activating
    connection preservation during an upgrade 71
activating connection preservation during an upgrade 71
adding
    administrator account 39
administering
    network parameters 33
AFID
    obtaining from SMI 41
AFS
    starting 36
applying patch
    patch 34
Authentication
    LDAP and AAA 20
authentication file
    creating for new system 38
authentication files
    ASG 36
automatic restart
    virtual machine 32
Avaya courses 9

B

Backing up
    system data 70, 71
backup
    restore 19
Back up the system data 75
best practices
    performance 80
    VMware networking 83
BIOS 80
BIOS for HP servers 81
BIOS settings
    for Dell servers 81
busying out
    busied-out equipment 74
busying out previously busied-out equipment 74
busying out server 71
busyout equipments 69

C

changing
    virtual machine settings 29
checking
    clock synchronization 69
checklist
    deployment procedures 31
    planning procedures 15
clearing
    alarms 69
Clearing alarms 71
clock synchronization
    check 69
clones
    deployment 28
Collaboration Pod 12
Communication Manager
    duplication parameters 50
    installation tests 54
    migrating to Virtualized Environment 76
    patches 67
    upgrade 72
components 13
    VMware 13
configuration
    server role 44
    tools and utilities 17
configuring
    duplication parameters 50
    network 48
    server role 45
    virtual machine automatic restart 32
    WebLM Server 35
creating
    backup 66
Creating
    core images 61

D

Debug
    Communication Manager core files 61
Deploying
    Open Virtual Application 27
    OVA 27
deploying copies 28
deployment
    thick 87
    thin 87
deployment guidelines 14
deployment procedures
    checklist 31
disabling
    IPv6 42
    scheduled maintenance 70
document changes 7
document purpose 7
Downloading

Downloading *(continued)*
default authentication file 37
downloading software
using PLDS 15
duplex
OVA deployment 29
Duplex
OVA 90
duplex OVA
upgrade 68
Duplication Parameters
field descriptions 51

E

Editing
CPU resources 23
enable
scheduled maintenance 74
enabling
IPv6 41

F

field descriptions
Duplication Parameters 51
Network Configuration 48
server role 45

G

guidelines
deployment 14

I

identify
corrupted Communication Manager VMware vSphere Tools 59
installing
authentication file 40
Intel Virtualization Technology 80
intended audience 7
interchange servers 73

L

legal notice .....
license
viewing status 56
virtual appliance 24
License Status
field descriptions 56
Log off
administration applications 75

M

migrating
Communication Manager Release 5.2.1 to 6.3 18
Communication Manager Release 6.2 to 6.3 18
Communication Manager to Virtualized Environment .. 76
release 5.2 17
release 6.2 17
minimum resource requirements 21

N

network
configuration 47
Network Configuration
field descriptions 48
network port
open port 42
NTP time source 82

O

overview 11

P

PCN 92
PCN notification 92
PCNs 92
performance best practices 80
Performing
an integrity check 72, 73
Performing an integrity 72
Performing an integrity check 73
planning procedures
checklist 15
PLDS
downloading software 15
presite upgrade
checklist, ... 68
PSN 92
PSN notification 92
PSNs 92
purpose of document 7

R

Reconfigure the Communication Manager server 72
recording 69
reducing reservations
Communication Manager 30
related documentation 8
releasing server 72
releasing the server 72
requirements
resources 21

requirements *(continued)*
software 24
reservations
reducing for Communication Manager 30
Resolve alarms 75
Resolving
alarms 74
resource requirements 21
resources
server 16
restoring
backup 19
VMware vSphere tool 60

S

S8300E server 13
SAL Gateway 25
SAT session 69
Save translations 74
saving
translations 70
server; busy out 71
server; release 72
server hardware and resources 16
server role
field descriptions 45
servers
interchange 73
service packs 67
setting
network time protocol
NTP 35
time zone 34
signing up
PCNs and PSNs 93
Simplex
OVA 90
software
requirements 24
software duplication
duplicated servers 64
Software Duplication
VMware HA 63
starting
SAT session 69
virtual machine 31
storage
Fibre Channel SAN 88
iSCSI SAN 88
support
contact 10
supported versions
VMware 23
survivable virtual machine
registration 58

T

thick deployment 87
thin deployment 87
timekeeping 82
training 9
Transferring files
WinSCP 21

U

upgrade
Communication Manager 72
upgrading
full backup 65
translations 66
virtual machine 65, 66

V

verifying
mode of virtual machine 58
software version 57
survivable virtual machine registration 58
videos 10
virtual machine
automatic restart configuration 32
certificates 19
configuration 43
roles 44
VMware
snapshots 88
vMotion 91
VMware generated core images 62
VMware networking
best practices 83
VMware software
supported 23
VMware Tools 82
VT support 80

W

WebLM
centralized licensing 25