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

Issue 2
February 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy 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, 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.
- Database License (DL). End User may install and use each copy 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 a single instance of the same database.
- CPU License (CP). End User may install and use each copy 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”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Virtualization

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

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 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:

- Added a note about the Communication Manager performance in the *Communication Manager virtual machine resource requirements* section.
- Added a note about the CM-duplicated pair configuration in the *Server role configuration* section.
- Added a note about the total number of supported endpoints in the *Duplex OVA Deployment* 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		
Implementing Avaya Aura® Communication Manager, 03-603558	Describes the implementation instructions for Communication Manager.	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		
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel

Title	Description	Audience
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 the Avaya Learning website at http://www.avaya-learning.com. To search for the course, log in to the Avaya Learning Center, enter the course code in the **Search** field, and then click **Go**.

Course code	Course title
ATI02348VEN	Avaya Aura® Communication Manager Implementation

Avaya Mentor videos

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

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

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

Support

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

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment overview

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

- simplifies IT management by providing 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.
- satisfies customer demand for Avaya products in a virtualized environment on customer-specified servers and hardware.
- enables business to 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 to expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

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

Note:

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

- server and host
- reservations and configuration values

Virtualized Environment applications

The Virtualized Environment supports the following Avaya products:

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

Customer deployment

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

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

Software delivery

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

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

Patches and upgrades

A minimum patch level can be required for each supported application. See the Compatibility Matrix at Compatibility Matrix for more information regarding the application patch requirements.

Important:

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

Performance and capacities

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

⚠ **Caution:**

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

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

Deployment guidelines

The high-level steps are:

1. Deployment of the .ova.
2. Configuration procedures.
3. Verification of the installation.

The following are deployment guidelines for the virtual machines:

- Deploy the virtual appliances on the same host as possible, depending on host size and VMs.
- Deploy the virtual appliances on the same cluster if it goes beyond the host boundary.
- Segment redundant elements on a different cluster. For example, Communication Manager duplication pair.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as Avaya Aura®, from other VMs.
- Ensure that you have enough resources for rainy day scenarios or conditions. Resources may only be configured for traffic or performance on an average day.
- Do not over-subscribe resources. Over-subscribing causes performance problems.
- Monitor the blade, host, and virtual appliance performance.

Important:

The values for performance, occupancy, and use can vary greatly. The blade may be running at 5% occupancy, but a VM may be running at 50%. Note that some VMs will behave differently at a higher CPU usage.

Chapter 3: Planning and configuration

Planning

Ensure that the customer has completed the following before deploying the Communication Manager OVA:

#	Action	Notes	✔
1	Get the required Communication Manager OVA.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/. See Configuration tools and utilities on page 18	
2	All required license have been purchased and are accessible. Register for PLDS and perform the following. • Obtain license file • Activate license entitlements in PLDS	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
3	Identify the Hypervisor and verify the capacity meets the OVA requirements.	See Server hardware and resources on page 18	
4	Staging and verification activities have been planned and resources assigned.	See Communication Manager virtual machine resource requirements on page 21	
5	Migrating from Communication Manager 5.2.1 or Communication Manager 6.2	See Migration data on page 18	

Server hardware and resources

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

Virtualized Environment requires VMware-certified servers to be running ESXi 5.0 and its updates. Releases prior to 5.0 are not supported and 5.1 is not supported.

Configuration tools and utilities

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

- Duplex OVA
- Simplex OVA
- Communication Manager 6.2 service packs
- a remote PC running the vSphere client
- a browser for accessing the Communication Manager SMI pages

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

For information about tools and utilities, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Migration data

If you want to migrate from standard Communication Manager Release 5.2.1 and 6.2 installation to Communication Manager 6.2 virtual open application deployment on VMware, you must first record the Communication Manager configuration information from the source system in the data collection worksheet. You can only restore the call processing translation data backup from a Communication Manager 5.2.1 or Communication Manager 6.x system on a Communication Manager virtual machine.

To record the required information for the migration, 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* on the Avaya Support website at http://support.avaya.com. When you open the spreadsheet, click **Enable Macros** when the dialog box displays.

After recording the Communication Manager migration information in the appropriate workbook, perform the steps for Migrating Communication Manager to Virtualized Environment on page 79.

Related topics:

Certificates on page 19
LDAP and AAA authentication on page 19

Certificates

Certificates provide identity to the virtual machine. When a license file or authentication file is loaded in Communication Manager you must install a unique certificate for each virtual machine. Based on the release, the license file or authentication file has the certificate information. These certificates are secure and work fine for most customers. Some customers generate and install their own certificates.

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

If you have custom certificates installed, you have to generate new certificates for your new Communication Manager VMware virtual machine. Certificates are tied to the virtual machine by a fully qualified domain name (FQDN) or IP address. If the FQDN or IP address is changed from the old virtual machine to the new virtual machine, you need new certificates on the VMware instance except in rare cases. If you want to use 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/.

Related topics:

Transferring files using WinSCP utility on page 21

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 for SCP access.
3. Click **OK** or **Continue** as necessary in the warning dialogue boxes.
4. Change the file transfer protocol from SFTP to **SCP**.
5. Click **Browse** to locate and select the file.
6. In the WinSCP destination machine window, browse to **/home/**.
7. Select **/home/<customerloginname>** as the destination location for the file transfer. This is likely to be the first destination when WinSCP opens.
8. Click and drag the file from the WinSCP source window to **/home/<customerloginname>** in the WinSCP destination window.
9. Click the WinSCP **Copy** button to start the file transfer.
10. When the copy completes, close the WinSCP window (**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. These resources are specified in the Communication Manager OVA.

VMware resource	Simplex values	Duplex values
CPU core	1	3

VMware resource	Simplex values	Duplex values
CPU reservation	2400MHz	8700MHz
CPU speed	2400MHz	2900MHz
Memory reservation	4.0GB	5.0GB
Storage reservation	30GB	30GB
Shared NIC(s)	One vmxnet3 @ 1000 Mbps	Two vmxnet3 @ 1000 Mbps

Note:

The Communication Manager OVA may be deployed on a host that does not have the resources to allocate to the virtual machine for power up. For a specific server speed, CPU reservations are assigned to the virtual machine through the OVA file.

In case of limited CPU resource limitations, the system displays the `Insufficient capacity on each physical CPU` pop-up message after the power-up request. To correct the CPU resources, edit the virtual machine properties.

1. Select and right click on the virtual machine and click **Edit Settings**.

   The Virtual Machine Properties window displays.

2. Click on the **Resources** tab to display the virtual machine resources, such as CPU, Memory, Disk, Advanced CPU, and Advanced Memory.
3. Adjust the CPU reservation in the *Resource Allocation* section and click **OK**.

You can 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

In some cases the CPU adjustments may not correct the power up conditions and you have to lower the CPU speed more. Also, you can follow the same procedure to lower other virtual machine resources as required.

Important:

Do not modify any other resource settings, for example, removing resources completely. Modifying these allocated resources could have a direct impact on the performance and capacity of the Communication Manager virtual machine. These resource size requirements must be met so that Communication Manager can run at full capacity. Removing or greatly downsizing resource reservations could put this requirement at risk. It is the responsibility of the customer to understand any modifications made to any resource reservation settings.

Warning:

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

Note:

Communication Manager has been tested at a high capacity. On average, Communication Manager at high capacity uses 3500 Kilobits per second in total network utilization, and 4 input/output operations per second in total disk utilization. In the customer environment, Communication Manager performance might vary from the average results.

VMware software requirements

For optimal results, Virtualized Environment requires the following VMware software versions:

- VMware vCenter Server 5.0
- VMware vSphere Client 5.0
- VMware ESXi 5.0 Host and latest updates.

Software requirements

The Avaya Aura® Communication Manager uses the current release, 6.2, of software as its standard release on VMware vSphere 5.0. VMware vSphere 4.1 is not currently supported. The Communication Manager VMware virtualization environment is packaged as a virtual appliance ready for deployment on VMware certified hardware.

Communication Manager virtual appliance licensing on VMware

Communication Manager on VMware is deployed either as a simplex or as a duplicated Communication Manager software-duplication pair. In both cases only a single instance of WebLM license server should be used to host the Communication Manager license file. The first and preferred WebLM instance shall also be the WebLM located within System Manager (SMGR).

There can be cases when the standalone WebLM virtual appliance is used to host the Communication Manager license file and while it is expected that these cases will occur, it is expected to be the exception rather than the norm.

When there are multiple Communication Managers networked together, for example, to serve a larger community, each Communication Manager or Communication Manager software-duplication pair must have a license file for its own consumption. This will require that the first Communication Manager or Communication Manager software-duplication pair have its license file installed on System Manager (SMGR). But, because each Communication

Manager license file must be installed on a separate WebLM instance, and an enterprise cannot have multiple SMGR active instances, the second and subsequent Communication Manager license files would be installed on the stand-alone WebLM virtual appliance (per Communication Manager/Communication Manager software-duplication pair).

A second and less used case would be if the customer insists on not deploying a SMGR within their enterprise the first Communication Manager (or duplication pair) can use the license hosted on a WebLM virtual appliance.

Chapter 4: VMware best practices for performance

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

BIOS

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

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

Intel Virtualization Technology support

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

All Intel Xeon processors feature:

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

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

Note:

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

Other suggested BIOS settings

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

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

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

Dell PowerEdge Servers — BIOS settings

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

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

HP ProLiant Servers — BIOS settings

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

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

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 69.

Time keeping

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

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

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

In special situations, such as powering up the virtual machine, after vMotion, and after resuming a suspended virtual machine, the ESXi hypervisor will push an updated view of its clock into a virtual machine. If this view is very different from that received over the network (over 1000 seconds), the NTP service might not adjust to the network time and shutdown. In this situation, the guest administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest. The VMware recommendation is to add **tinker panic 0** 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 in setting the NTP configuration, you must configure the Domain Name Service in the guest before administering the NTP service. Otherwise, the NTP service will not be able to locate the time servers. If the NTP service is administered first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the **ntpstat** or **/usr/sbin/ntpq -p** command from a command window to verify the NTP service is getting time from a network time source. The results indicate which network time source is being used, how close the guest is to the network time, and how often the guest checks the time. The guest polls the time source between every 65 and 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

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

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

Related topics:

Setting up the network time protocol on page 45

VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The information in this section provides a few of the examples of the VMware networking possibilities. These examples are not the only supported networking configurations, and implement several best practices and recommendations from Avaya's perspective.

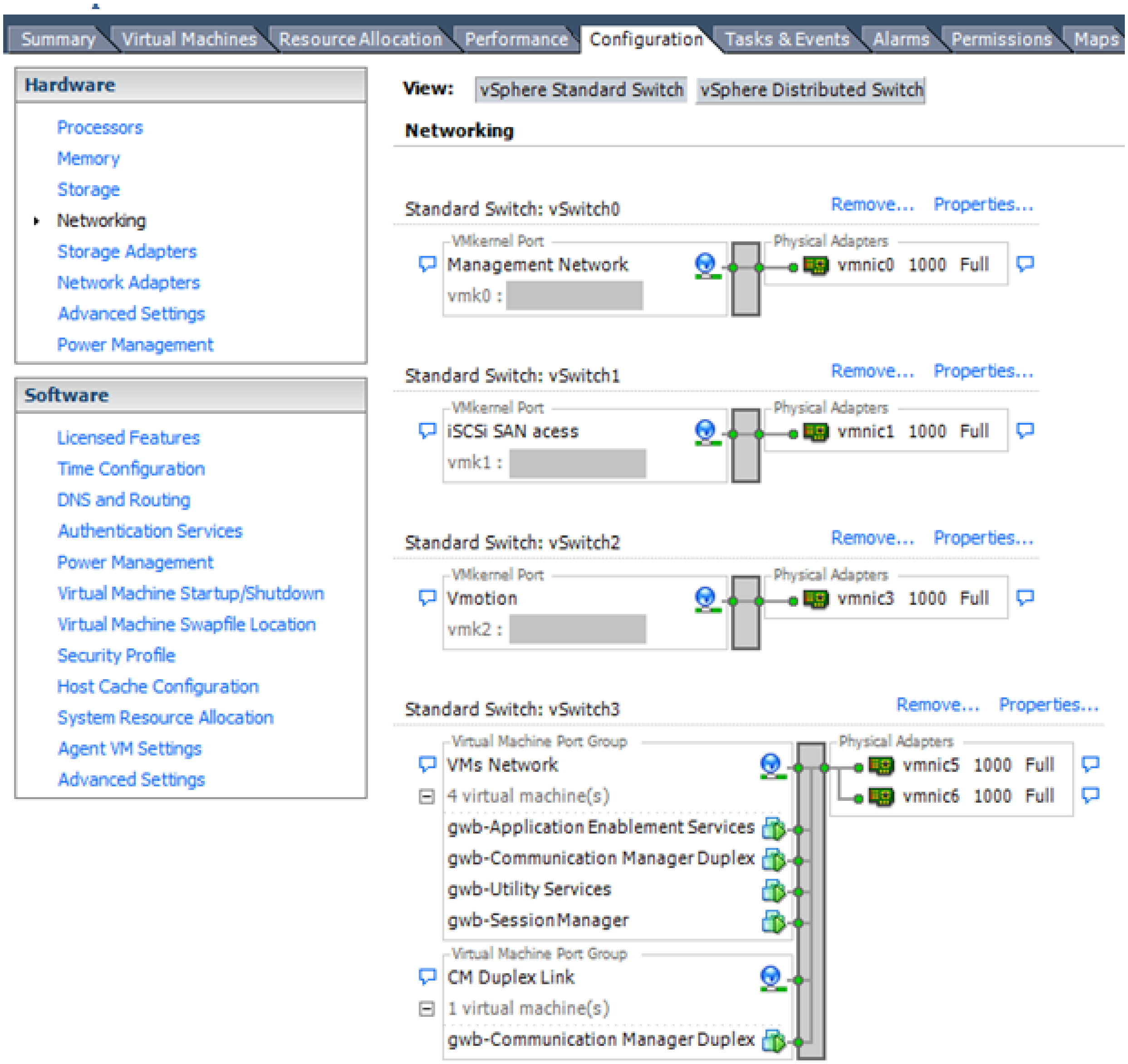
This section is not a substitute for the actual VMware documentation. If you do not have experience networking with VMware, you must review the VMware networking best practices before deploying any applications on an ESXi host.

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

- Separate network services to achieve greater security and performance. Create a vSphere standard or distributed switch with dedicated NICs for each service. If separate switches are not possible, consider port groups with different VLAN IDs.
- The vMotion connection must be located on a separate network devoted to vMotion.
- To protect sensitive VMs, deploy firewalls in the VM that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks to physical networks.
- Specify VM NIC hardware type **vmxnet3** for best performance. Avaya OVA files are built using **vmxnet3** by default.

- All physical NICs that are connected to the same vSphere standard or distributed switch must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).

Networking Avaya applications on VMware ESXi — Example 1



Standard Switch: vSwitch0

VMkernel Port: Management Network, vmk0 :

Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1

VMkernel Port: iSCSi SAN acess, vmk1 :

Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2

VMkernel Port: Vmotion, vmk2 :

Physical Adapters: vmnic3 1000 Full

Standard Switch: vSwitch3

Virtual Machine Port Group: VMs Network

4 virtual machine(s)

gwb-Application Enablement Services

gwb-Communication Manager Duplex

gwb-Utility Services

gwb-SessionManager

Virtual Machine Port Group: CM Duplex Link

1 virtual machine(s)

gwb-Communication Manager Duplex

Physical Adapters: vmnic5 1000 Full; vmnic6 1000 Full

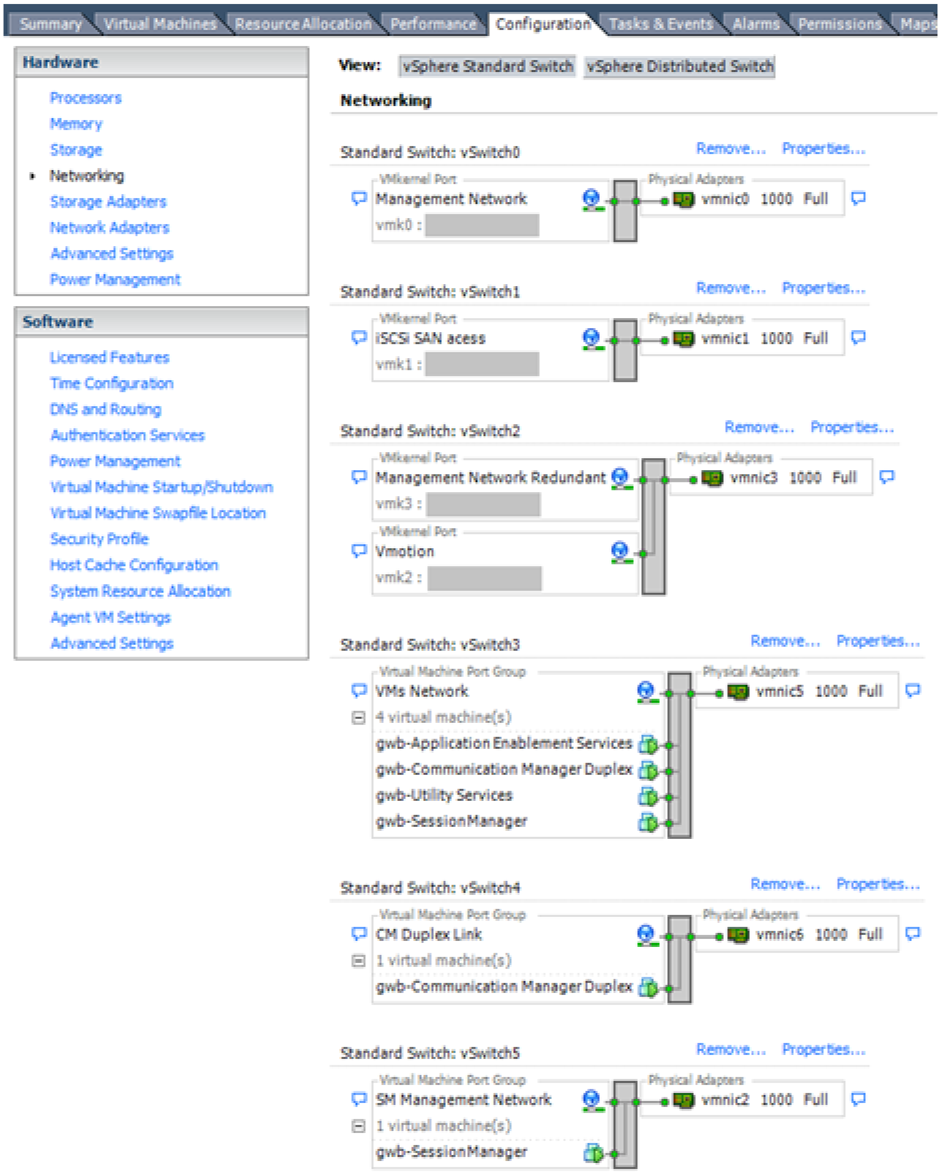
This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and VM networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the VMs Network. Load balancing provides additional bandwidth for the VMs

Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.

- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. There are several methods of doing this, but Example 1 displays separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements, detailed in Avaya PSN003556u at PSN003556u. Communication Manager software duplex connectivity minimum requirements are defined as:
    - 1 Gbps total capacity, or greater, with 50 Mbps of reserved bandwidth for duplication data.
    - 8 ms round-trip delay, or less.
    - 0.1% round-trip packet loss, or less.
    - Both servers duplication ports are on the same IP subnet.
    - Duplication link encryption must be disabled for busy-hour call rates that result in 9 greater than 40% CPU occupancy (`list measurements occupancy`, Static + CPU occupancy).
    - CPU occupancy on the active server (Static + CPU) must be maintained at less than 65% to provide memory refresh from the active to standby server.
- Session Manager vNIC mapping: The Session Manager OVA defines four separate virtual NICs within the VM. However, this example shows all of those interfaces networked 15 through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, it is possible to create a VLAN for the appropriate network.
- Virtual networking: Virtual machines which connect to the same vSwitch, as is the case in VMs Network of vSwitch 3, can communicate without ever entering the physical network. In other words, the network connectivity between these VMs is purely virtual. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi — Example 2



Networking

Standard Switch: vSwitch0
VMkernel Port: Management Network, vmk0 :
Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1
VMkernel Port: iSCSi SAN acess, vmk1 :
Physical Adapters: vmnic1 1000 Full

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

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

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

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

This configuration shows a more complicated situation of using more available physical network interface cards. Highlights which differ from Example 1 include:

- VMware Management Network redundancy: In this example, a second VMkernel Port has been added to vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for VMs Network: This example removes the teamed physical NICs on vSwitch3, which was providing more bandwidth and tolerance of a single NIC failure in favor of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 has been dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate

physical network, which still follows the requirements described in PSN003556u at PSN003556u.

- Session Manager Management Network: This example also shows the Session Manager Management network separated onto its own vSwitch, including a dedicated physical NIC which physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice — PSN003556u	PSN003556u
Performance Best Practices for VMware vSphere™ 5.0	Performance Best Practices for VMware vSphere™ 5.0
VMware vSphere 5.0 Basics	VMware vSphere Basics - ESXi 5.0

Thin vs. thick deployments

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

Some configurations require *eager-zeroed* thick disks. An eager-zeroed thick disk

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

Thin provisioned disks:

- can grow to the full size specified at the time of the virtual disk creation but do not shrink. The blocks cannot be unallocated after the blocks have been allocated.
- can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.

You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, thin disks are a viable option. Otherwise, the general recommendation is to deploy thick disks.

Best Practices for VMware features

VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshots are useful for short-term point-in-time copies of the running system before major upgrades or before patching the system.

Snapshots can:

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

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

- Snapshot operations can adversely affect service. The application that is running on the virtual machine should be stopped or set to out-of-service before you perform a snapshot operation. When the snapshot operation has completed, the application can then be restarted or brought back into service.
- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- **Do not run a virtual machine off of a snapshot**. Use no single snapshot for more than 24-72 hours. The recommended actions are to take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot as soon as the proper working state of the virtual machine is verified. Following the recommended actions prevents snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The length of time the host takes to write the memory onto the disk is relative to the amount of memory the virtual machine is configured to use and can add several minutes to the time it takes to complete the operation. If the snapshot is activated, saving memory will make calls appear to be active or in progress and can cause confusion to the user. When creating a snapshot, make sure that you
    - uncheck the **Snapshot the virtual machine’s memory** check box in the **Take Virtual Machine Snapshot** window.

  - select the **Quiesce guest file system (Needs VMware Tools installed)** check box to make sure all writes to the disks have completed. It gives a better chance of creating a clean snapshot image from which to boot.

- If you are going to use snapshots over a long period of time, you must consolidate the snapshot files on a regular basis to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  In the event of a consolidate failure, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, a warning is displayed 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 regarding snapshots:

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

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.

Duplex OVA

The Communication Manager Release 6.2 does not support (at this time) the usage of VMware High Availability with the Communication Manager Active and Standby virtual machines within the same data cluster. 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 73.

VMware vMotion

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

When you the use VMware vMotion, note the following:

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

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

Chapter 5: 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 Deploy OVF Template window displays.
3. You can use one of the following options to deploy the Communication Manager OVF package (CM-06.02.0.823.0-e50-04.ova):
   - Click **Browse** and provide the Communication Manager OVA file location.
   - If the Communication Manager OVA file is located on an http server, you can also deploy the Communication Manager OVA on VMware by entering the full URL in the **Deploy from a file or URL** field.
4. Click **Next**.
   The OVF Template Details window displays.
5. Verify the details about the installed OVA template and click **Next**.
   The End User License Agreement window displays.
6. Read the license agreement and click **Accept** to accept the license agreement.
7. Click **Next**.
   The Name and Location window displays.
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 do not have a host selected when you choose to **Deploy OVF Template**, the wizard will ask you which host or cluster you want to deploy the virtual appliance. Select the host or cluster you want to deploy on. If you have a host or cluster selected when you choose to **Deploy OVF Template**, the wizard assumes that you would like to install the virtual machine on that host.

9. Click **Next**.
The Storage window displays.
10. Select the data store location to store the virtual machine files and click **Next**.
The Disk Format window displays.
11. Accept the default disk format to store the virtual machine and virtual disks for Communication Manager OVA and click **Next**.

    For information about virtual disks, see Thin vs. thick deployments on page 32.
12. If there are multiple virtual machine networks configured 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 there is only a single virtual machine network on the host you are deploying the Communication Manager OVA, the wizard will not prompt.
The Ready to Complete window displays.
13. Verify the deployment settings and click **Finish**.

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

Duplex OVA Deployment

To deploy the Duplex OVA you must install the OVA twice, that is, the OVA must be installed on two different hosts in two different clusters. Similar to the Simplex OVA, the Duplex OVA has one network interface configured in the OVA. The Duplex OVA's 1st NIC and 2nd NIC are automatically assigned 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 power up the virtual machine, you must change the Communication Manager virtual machine settings to configure the 2nd NIC.

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

The system displays the Virtual Machine Properties window.

2. In the **Hardware** tab, select the Network adapter 1 that will be assigned to the *VM Network* under the *Network Connection*.
3. Next select the Network adapter 2 and then select the *CM_duplication_link* network name from the **Network label** drop down list under the *Network Connection*.

Note:

For the Communication Manager Duplex virtual appliance:

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

Chapter 6: Configuration

Configuration and administration checklist

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

#	Action	Link	✔
1	Start the Communication Manager virtual machine.	Starting the Communication Manager virtual machine on page 42	
2	Configure the Communication Manager virtual machine to start automatically after a power failure.	Configuring the virtual machine automatic start and stop settings on page 42	
3	Set up network configuration.	Administering network parameters on page 43	
4	Apply the latest Communication Manager 6.2 patch.	Applying Communication Manager patch on page 44	
5	Configure the time zone	Setting the time zone on page 44	
6	Set up Network Time Protocol.	Setting up the network time protocol on page 45	
7	Direct Communication Manager to the WebLM server.	Configuring WebLM Server on page 45	
8	Create an suser account.	Adding an administrator account login on page 49	
9	Load authentication files.	Installing an authentication file on page 50	

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

Configuring the virtual machine automatic start and stop settings

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

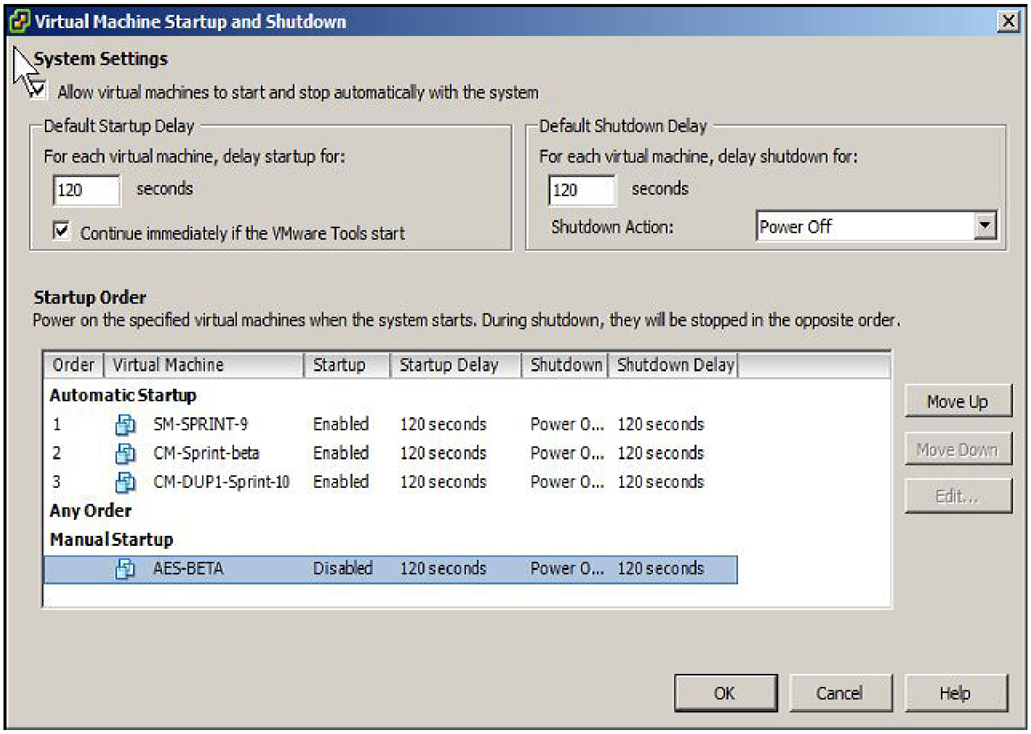
In high availability (HA) clusters, the VMware HA software ignores the Startup selections.

Procedure

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

Example

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



System Settings

☑ Allow virtual machines to start and stop automatically with the system

Default Startup Delay

For each virtual machine, delay startup for: 120 seconds

☑ Continue immediately if the VMware Tools start

Default Shutdown Delay

For each virtual machine, delay shutdown for: 120 seconds

Shutdown Action: Power Off

Startup Order

Power on the specified virtual machines when the system starts. During shutdown, they will be stopped in the opposite order.

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	SM-SPRINT-9	Enabled	120 seconds	Power O...	120 seconds
2	CM-Sprint-beta	Enabled	120 seconds	Power O...	120 seconds
3	CM-DUP1-Sprint-10	Enabled	120 seconds	Power O...	120 seconds
Any Order					
Manual Startup					
	AES-BETA	Disabled	120 seconds	Power O...	120 seconds

Administering network parameters

Procedure

1. In the vSphere client, start the Communication Manager virtual machine console, and log in as `craft`.
2. As part of the very first login as `craft`, you must enter certain details according to the prompts.
   a. In the **IPv4 IP address** field, enter the IP address.
   b. In the **IPv4 subnet mask** field, enter the network mask IP address.
   c. In the **IPv4 Default Gateway address** field, enter 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 the Communication Manager System Management Interface as *craft* and navigate to the **Administration** > **Server (Maintenance)** > **Network Configuration** page.

   Note:

   If the initial network prompt for entering the IP address, Subnet mask, and Default gateway address is interrupted or incorrect data is specified, you can run the **`/opt/ecs/bin/serverInitialNetworkConfig`** command on the command line to reenter the data.

Applying Communication Manager patch

About this task

You must install and apply the Communication Manager 6.2 patch to set the time zone, to set up the network time protocol, to load the authentication file, or to configure a WebLM address by using the Communication Manager System Management Interface.

Procedure

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

Setting the time zone

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. Click **Administration** > **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 reboot the virtual machine to ensure that all 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. Click **Administration** > **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, enter the primary server, secondary server (Optional), and tertiary Server (Optional) details.
6. Click **Apply**.

Configuring WebLM Server

Procedure

1. Log in to Communication Manager System Management Interface as `craft`.
2. Click **Administration** > **Licensing**.
3. In the left navigation pane, click **WebLM Configuration**.
   The system displays the WebLM Configuration page.
4. In the **WebLM Server Address** field, enter the WebLM server IP address to fetch the license file.
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 *lock out* situation after loading the new authentication file. To add an administrator account, see Adding an administrator account login on page 49.

The Authentication File System (AFS) creates unique authentication files. You can start the AFS application from http://rfa.avaya.com and download the file. The file you are creating is generated by using the product type of System Platform. After you create and download the authentication file, you install the file from the Communication Manager System Management Interface.

Tip:

You can also email the file to your 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

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

Each survivable OVA must have its own unique authentication file.

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

Before you begin

AFS is available only to Avaya service personnel and Avaya Partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

You must have a login ID and password to start the AFS application. You can sign up for a login at http://rfa.avaya.com.

About this task

Procedure

1. Type `http://rfa.avaya.com` in your Web browser.
2. Enter your login information, and click **Submit**.
3. Click **Start the AFS Application**.
   The system displays a security message.
4. Click **I agree**.
   The AFS application starts.

Creating an authentication file for a new system

About this task

You can choose to 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 and log in to AFS. For more information, see Starting the AFS application on page 47.
2. In the **Product** field, select System Platform.
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **New System**, and then click **Next**.
5. Enter the fully qualified domain name (FQDN) of the host system where Communication Manager is installed. For duplicated Communication Manager virtual machines, enter the alias FQDN.
6. Enter the FQDN of the Utility Services.

Note:

The **Utility Services FQDN** field does not apply for the Communication Manager AFS.

7. If you want 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 where you want 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, release, and authentication file ID (AFID).

8. If you want to send the authentication file in an email message:

   a. Enter the email address in the **Email Address** field.

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

      AFS sends the email message that includes the authentication file as an attachment and 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 the file is saved and use WordPad to open the file.

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

Obtaining the AFID from Communication Manager SMI

Procedure

1. Log in to Communication Manager System Management Interface.

2. Click **Administration** > **Server (Maintenance)**.

3. Navigate to the **Security** > **Authentication File** page.
   The system displays the AFID in the **AFID** field.

Adding an administrator account login

Procedure

1. On the Communication Manager System Management Interface, click **Security** > **Administrator Accounts**.
2. Select **Add Login**.
3. From the list of logins, select the login that you want to add.
4. Click **Submit**.
5. On the Administrator Login - Add Login page, complete the following fields:

Fields	Description
Login name	The administrator login name.
Primary group	• For a limited access login, you must enter **users**. This group was formerly known as customer nonsuper-user login. • For a privileged login, you must enter **susers**. This provides extensive permissions to the server.
Additional groups (profile)	The field to administer an access profile. If the login does not need access to Communication Manager SAT or Web pages, this field must be left blank.
Linux shell & Home directory	The value populated in this field depends on the login name.
Lock this account	If you select this option, the system locks account details for editing.
Date on which account is disabled	If the feature is unused, you can leave this field blank.
Select type of authentication	• If the administrator must log in by using a password, you must select the **Password** option. • If the administrator must log in by using the ASG license key, you must select the **ASG** option. The system authenticates the login only when the ASG license is present on the server.
Enter password or key	The password for the administrator login.
Re-enter password or key	Enter the same password in the **Enter password or key** field.

Fields	Description
Force password/key change on next login	If you selected **Yes**, change the password after the first login.

6. Click **Submit**.

   If this is a new profile:

   - Define Communication Manager Web access permissions on the **Security** > **Web Access Mask** page.
   - Define Communication Manager SAT access permissions at SAT on the User Profile screen.

Installing an authentication file

Before you begin

You must create and download the authentication file from AFS.

About this task

To install the authentication file on Communication Manager, you must create an *suser* 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, and navigate to **Security** > **Load Authentication File**.
2. In the **Select the Authentication File** field, click **Browse**.
3. 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 date and time, select **Force load of new file** on the Authentication File page. Select this option if you:

   - Must install an authentication file that has a different unique AFID than the file that is currently installed, or
   - 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, AFID 7100000000, with a unique authentication file.

⚠ **Caution:**

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

4. Click **Install**.
   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.
5. To confirm that the authentication file is installed on Communication Manager, log in to Communication Manager System Management Interface and check the Authentication File page.

Network port considerations

The main virtual machine, survivable remote virtual machines, and each survivable core virtual machine use specific ports across a customers network for registration and translation distribution. You can modify the firewall settings from the command line using the **`firewall`** command with *suser* level access.

Note:

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

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

Port	Used by	Description
20	ftp data	
21	ftp	
22	ssh/sftp	
23	telnet server	
68	DHCP	
514	This port is used in Communication Manager 1.3 to download translations.	
1719 (UDP port)	The survivable core virtual machine to register to the main virtual machine.	A survivable core virtual machine registers with the main virtual machine using port 1719. For more

Port	Used by	Description
		information on survivable core virtual machine registration, see *Avaya Aura® Communication Manager Survivability Options*, 03-603633.
1024 and above	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 to download translations to the survivable core virtual machine.	A main virtual machine uses port 21874 to download translations to the survivable core virtual machine and the survivable remote virtual machines.

Server Role

To complete the installation, you must use Communication Manager System Management Interface (SMI) to complete the configuration tasks.

The primary areas are:

- Server role: Use to indicate whether the virtual machine is a main, survivable core, or survivable remote virtual machine.
- Network configuration: Use to configure the IP-related settings for the virtual machine. Many of the fields are prepopulated with data generated as part of the OVA template installation.
- Duplication parameters: Use to configure the duplication settings if you installed the Duplex Main/Survivable Core OVA.

Related topics:

Server role configuration on page 53

Configuring server role on page 53
Server Role field descriptions on page 54

Server role configuration

A telephony system may be made up of several virtual machines, each fulfilling 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 individual virtual machine roles. Depending on the virtual machine role, configure at least two of the following data:

- Virtual machine settings
- Survivable data
- Memory

OVA type and virtual machine role

The Communication Manager OVA type that is deployed determines which roles are available.

The Communication Manager Simplex OVA can be configured as one of the following:

- Main Server
- Enterprise Survivable Server (ESS)
- Local Survivable Server (LSP)

> **Note:**
>
> For a CM-duplicated pair configuration, both of the Communication Manager duplicated servers must be deployed either on the VMware platform or on the non-VMware hardware. However, you can mix and match the deployment of the survivable core server (ESS), the survivable remote server (LSP), 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.

The Communication Manager Duplex OVA can be configured as one of the following:

- Main Server
- Enterprise Survivable Server (ESS)

Configuring server role

Before you begin

You must be logged into the Communication Manager System Management Interface.

Procedure

1. From the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server Configuration** > **Server Role**.
3. In the Server Role page, fill-in the fields from the following sets:
   a. **Server Settings**
   b. **Configure Survivable Data**, if the **a main server** button is not selected, the **Configure Survivable Data** field displays.

      Note:

      If you are configuring virtual machine role for the main virtual machine, this set will not be displayed.
   c. **Configure Memory**
4. Click **Change** to apply the virtual machine role configuration.

Server Role field descriptions

Server Settings Field descriptions

Name	Description
This Server is	Specifies the role of the server. The possible virtual machine roles are: • **a main server:** Select this role if a primary virtual machine. • **an enterprise survivable server (ESS):** Select this role if a survivable core virtual machine. • **a local survivable server (LSP):** Select this role if a survivable remote virtual machine.
SID	Is 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	Is the module ID. The main server module ID must be 1 and that of other server must be unique and 2 or

Name	Description
	above. If a survivable remote server, the MID must match the Cluster ID/MID for that server.

Configure Survivable Data Field descriptions

Name	Description
Registration address at the main server (C-LAN or PE address)	Are the IP addresses of the Control LAN (C-LAN) or the Processor Ethernet (PE). These addresses are registered with the main server.
File Synchronization address at the main cluster (PE address)	Are the IP addresses of the NICs of the main server and the second redundant server connected to a LAN to which the Survivable Remote or the Survivable Core server is also connected. **Note:** If a second server is not used, do not fill in this field. 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)	Is the IP address of the interface to be used as alternate file synchronization interface. Refer to the **File Synchronization address at the main cluster (PE Address)** field description for information on how to fill in this field.

Configure Memory Field descriptions

Name	Description
This Server's Memory Setting	Is this server's boot time memory setting, that is, small, medium or large.
Main Server's Memory Setting	Is the main server's boot time memory setting, that is, small, medium or large.

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 may escalate to a full Communication Manager reboot.

Network

Network configuration

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

> **Note:**
>
> Some of the changes made on the Network Configuration page may affect the settings on other pages under **Server Configuration**. Make sure that all the pages under **Server Configuration** have the appropriate configuration information.

The Network Configuration page enables you to configure or view the settings for 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 from the Network Configuration page.

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

The Network Configuration page displays the network interfaces that will be used by Communication Manager. This will be eth0 for all Communication Manager OVAs except CM_Duplex. For CM_Duplex, the network interfaces will be eth0 and eth1.

To activate the new settings in the virtual machine, you must restart Communication Manager. Make sure that you restart Communication Manager only after configuring the complete settings of the virtual machine. Too many restarts may escalate to a full Communication Manager reboot.

Configuring the Communication Manager network

Before you begin

Log in to Communication Manager System Management Interface on the virtual machine on which you want to configure the network.

About this task

For the Duplex Survivable Core OVA, additional fields display for configuring Communication Manager for duplication. This enables Communication Manager to duplicate data on the second virtual machine.

Procedure

1. From the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server Configuration** > **Network Configuration**.
3. Fill in all the fields.
4. Click **Change** to save the network configuration.
5. Click **Restart CM**.

   Note:

   If configuring for duplication, do not restart Communication Manager yet. Wait until after you configure the duplication parameters.

   It takes about 2 minutes to start and stabilize the Communication Manager processes. Additional time is required to start the port networks, the gateway, and the phones, depending on your enterprise configuration.

Network Configuration field descriptions

Field descriptions

Name	Description
Host Name	Is the host name of the virtual machine and is often aligned with the DNS name of the virtual machine.

Name	Description
Alias Host Name	Is the alias host name for duplicated virtual machines only. When the virtual machine is duplicated and is running in survivable mode, make sure that the alias host name field is populated.
DNS Domain	Is the domain name server (DNS) domain of the virtual machine.
Search Domain List	Is the DNS domain name for the search list. If more than one search list name, separate them with commas.
Primary DNS	Is the primary DNS IP address.
Secondary DNS	Is the secondary DNS IP address. This field is optional.
Tertiary DNS	Is the tertiary DNS IP address. This field is optional.
Server ID	Is the unique server ID, which is a number between 1 and 256. If a duplicated virtual machine or survivable virtual machine, the number cannot be 1.
Default Gateway	Is the default gateway IP address.
IP Configuration	Is the set of parameters for configuring an Ethernet port. The parameters are: • IP Address • Subnet Mask • Alias IP Address (for duplicated virtual machines only) • Functional Assignment. Choices are - Corporate LAN/Processor Ethernet/ Control Network - Corporate LAN/Control Network - Duplication Link **Note:** You may configure as many Ethernet ports as available on the NICs of your virtual machine.

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 may escalate to a full Communication Manager reboot.

Duplication parameters configuration

Duplication parameters

The Duplication Parameters page is available only when the Duplex OVA is installed. Configuring duplication parameters ensures that your telephony applications run without interruption even as the primary virtual machine faces operational problem.

The duplication type setting must be the same for both virtual machines. If you are changing the already configured duplication parameters, make sure that you do it in the following order:

1. Busy-out the standby virtual machine and 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:

Changing the duplication parameters on the active virtual machine results in the standby virtual machine becoming the active virtual machine. Moreover, the new active virtual machine will not be available for call processing.

In the Duplication Parameters page, configure the following settings for the virtual machine:

- Duplication type for the virtual machines: Communication Manager supports two virtual machine duplication types—software-based duplication and encrypted software-based duplication.
- Duplication parameters of the other virtual machine: Configure the hostname, virtual machine ID, Corporate LAN IP address and the duplication link IP address for the other virtual machine.
- Processor Ethernet parameters: Configure the Processor Ethernet interchange priority level for the virtual machine and the IP address that enables the virtual machine to determine whether its Processor Ethernet interface is working or not.

Configuring duplication parameters

Before you begin

Log in to Communication Manager System Management Interface.

Procedure

1. From the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server Configuration** > **Duplication Parameters**.
3. Fill in all the fields for the virtual machine.
4. Click **Change**.
5. Click **Restart CM**.
   In the pop-up confirmation page, click **Restart Now** if you want to restart the virtual machine immediately. Click **Restart Later**, if you want to restart the virtual machine later.

Duplication Parameters field descriptions

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

Name	Description
	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	Is the host name of the other virtual machine.
Server ID	Is the unique virtual machine ID of the other virtual machine, which must be an integer between 1 and 256.
Corporate LAN/PE IP	Is the IP address for the Corporate LAN/ Processor Ethernet interface for the other virtual machine.
Duplication IP	Is the IP address of the duplication interface of the other virtual machine. This is typically 192.11.13.13 for the first virtual machine and 192.11.13.14 for the second virtual machine.
PE Interchange Priority	Is a simple 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 consider the Processor Ethernet in virtual machine interchange decisions.
IP address for PE Health Check	Is the IP address that enables the virtual machine to determine whether its PE interface is working or not.

Name	Description
	Note: The network gateway router is the default address. However, the IP address of any other device on the network that will respond can be used.

Button descriptions

Name	Description
Change	Updates the system configuration files with the current values on the page and restarts the Communication Manager processes. A dialog box is displayed 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 may escalate to a full Communication Manager reboot.
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 may escalate to a full Communication Manager reboot.

Chapter 7: Postinstallation verification and testing

Installation tests

You need to perform a number of post installation administration, verification, and testing tasks to ensure that the various system components are installed and configured as desired as part of Communication Manager installation.

This section provides a list of tasks for testing the OVA, virtual machine, and system component installation and configuration. Some tests cannot be performed until the complete solution is installed and configured, including port networks.

Perform the following post installation administration and verification tasks:

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

The following tests can be done only after the port networks and UPS are installed and configured.

- Testing the IPSI circuit pack
- Testing the IPSI LEDs

Refer to the relevant server installation document for your server-specific postinstallation administration and verification tasks. Also refer to *LED Descriptions for Avaya Aura® Communication Manager Hardware Components* for understanding the states that LEDs on different components of your system denote.

Verifying the license status

Accessing the Communication Manager System Management Interface

About this task

You can gain access to the SMI remotely through the corporate LAN connection. The virtual machine must be connected to the network.

Procedure

1. Open a compatible Web browser.

   Currently, 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 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 you are certain 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 gain access to this virtual machine or other Communication Manager virtual machine again, click Install **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.
4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), 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 your password, and click **Logon**.

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

Viewing the license status

Before you begin

Log in to the Communication Manager System Management Interface (SMI).

About this task

Use this procedure to view the status of the license for Communication Manager and Communication Manager Messaging. The license can be installed and valid, unlicensed and within the 30-day grace period, or unlicensed and the 30-day grace period has expired. The License Status page also displays the System ID and Module ID.

Procedure

1. In the menu bar, click **Administration** > **Licensing**.
2. In the navigation pane, click **License Status**.
   The License Status page displays the license mode and error information.

License Status field descriptions

Name	Description
CommunicaMgr License Mode	Status of the license. Possible statuses are: • Normal: The Communication Manager license mode is normal and there are 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 you can correct license errors (for example, reducing the number of stations).
checking application CommunicaMgr version	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 greater. 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.

Name	Description
	Avaya provides the system ID when you submit the Universal Install/SAL Product Registration Request form.

Verifying the software version

Before you begin

Log in to the Communication Manager System Management Interface.

About this task

Since the system is running on a new software release, you must log in with the super user login that was configured just prior to installing the AFS file. To add an administrator account, see Adding an administrator account login on page 49.

Procedure

1. From the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server** > **Software Version**.
3. Verify that the **CM Reports as:** field shows the correct software load.
4. In the menu bar, click **Log Off**.

Verifying survivable virtual machine registration

Before you begin

Log in to a Communication Manager SAT session.

About this task

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 could take several minutes to complete.

Procedure

1. Enter **`list survivable-processor`** to open the Survivable Processor screen.
2. Verify that the **Reg** field is set to **y**, indicating that the survivable virtual machine has registered with the main virtual machine.

3. Verify that the **Translations Updated** field shows the current time and date, indicating that the translations have been pushed down to the survivable virtual machine.

Verifying the mode of the virtual machine

Before you begin

Log in to the Communication Manager System Management Interface.

About this task

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

Procedure

1. From the **Administration** menu, click **Server (Maintenance)**.
2. In the left navigation pane, click **Server** > **Status Summary**.
3. Verify the **Mode** field:
    - `Active` on an active virtual machine.
    - `StandBy` on a standby virtual machine.
    - `BUSY OUT` on a virtual machine that is busied out.
4. To verify the process status, click **Server** > **Process Status**.
5. Under **Frequency**, click **Display Once**.
6. Click **View**.
7. Verify 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

About this task

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. 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

About this task

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 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

About this task

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 72.

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 74, 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 74:

- 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.

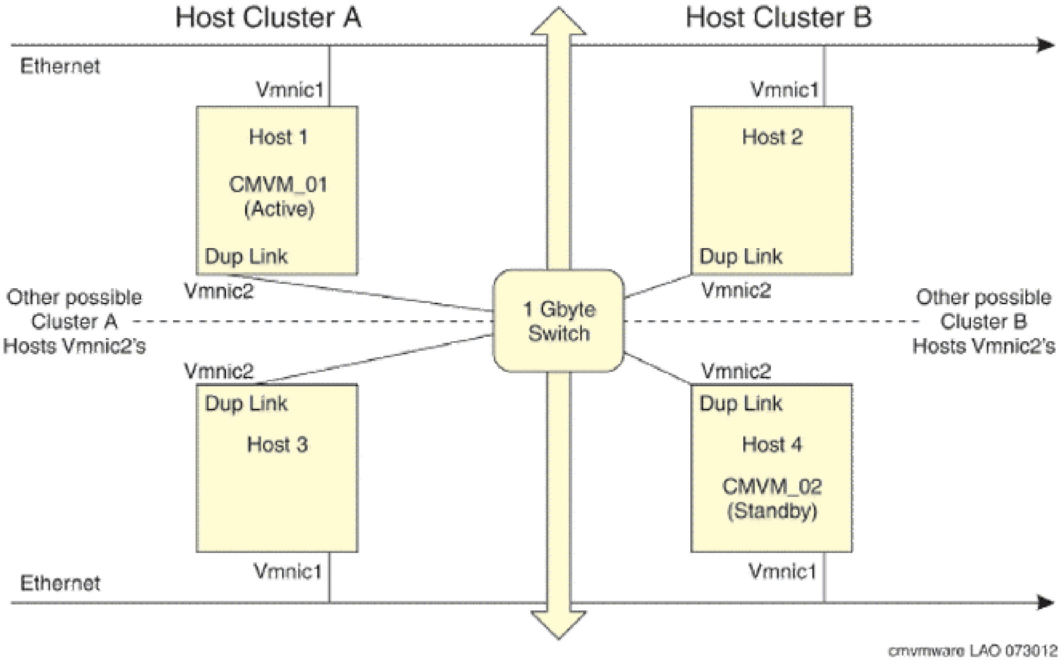


Figure 1: VMware cluster configuration with four ESXi hosts

Appendix D: Upgrading Communication Manager Open Virtual Application

Upgrading Communication Manager using full backup

About this task

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. Deploy the new Communication Manager virtual machine on a host server.
2. Start the new Communication Manager virtual machine.
3. Take the full backup 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. Give the existing Communication Manager IP address to the new Communication Manager virtual machine.
7. On the new Communication Manager virtual machine, log in to Communication Manager System Management Interface.
8. Restore the full backup on the new Communication Manager virtual machine.
9. Reboot the new Communication Manager virtual machine.

Upgrading an existing Communication Manager virtual machine and restoring the existing translations

About this task

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

The following procedure requires a SMI web page 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. Log in to the new Communication Manager virtual machine console with the *craft* login.
4. Specify a new (unused) IP address for the new Communication Manager virtual machine.
5. 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 up the network time protocol.
   e. Add an suser account.
   f. Load an authentication file.
6. Save the translations of the existing Communication Manager virtual machine.
7. Shutdown the existing Communication Manager virtual machine.
8. On the new Communication Manager virtual machine, log in to Communication Manager System Management Interface and set the network identity of the new Communication Manager virtual machine with the existing Communication Manager virtual machine.
9. Log in to Communication Manager System Management Interface of the new Communication Manager virtual machine.
10. Restore the translations on new Communication Manager virtual machine.
11. Reboot the new Communication Manager virtual machine.

12. Log in to Communication Manager System Management Interface of the new Communication Manager virtual machine and configure the WebLM Server.

Creating a backup

Procedure

1. Log in to the Communication Manager System Management Interface as `craft`.
2. From the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Data Backup/Restore** > **Backup Now**.
   The Backup Now page displays.
4. Click the `Full Backup` option and select the backup method.
5. Click **Start Backup**.

Communication Manager patches

You can unpack, activate, validate, and apply the updates through the Communication Manager System Management Interface from the **Adminstration** > **Server(Maintenance)** > **Server Upgrades** > **Manage Updates** page.

The Communication Manager Simplex and Duplex OVAs might not include the latest Communication Manager Service Pack. Once the OVA is deployed 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.

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.

Appendix E: Migrating Communication Manager to the VMware Virtualized Environment

Before you begin

VMware is not supported on the S8300D. 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.

Procedure

1. Ensure any Survivable Remote server is the same version as the Communication Manager virtual application version. The survivable remote must remain at 6.2. Use the 6.2 media if you must update the version.
2. Download and save the translation 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.
3. Record the required Communication Manager data in the workbook.
4. Navigate to the Communication Manager SMI page of the existing main Communication Manager server.
5. Backup existing translations from the SMI page:
   - Communication Manager 5.2.1 or 6.x translation files
   - Utility Services (if applicable) translations files (only available in 6.2 and later. See the Utility Services deployment guide for the backup procedure.)
6. 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.

7. Download and install the following virtual application OVA files but *do not* turn on the applications. See the appropriate deployment guide for downloading and installing the virtual application OVA file.
   - Communication Manager
   - Utility Services (if applicable)
   - WebLM (if applicable)
   - Secure Access Link (not needed if a Standalone SAL Gateway is in place)
8. If SAL is in use on System Platform:
   a. Login to the SAL Gateway.
   b. Capture settings using screen capture.
9. Turn off the existing server.
10. 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.
11. 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)
12. Download and activate the latest Communication Manager service pack.
13. Navigate to the Communication Manager SMI page.
14. 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 call processing translations (XLN file only). Re-enter SNMP data if needed.
    e. Retranslate the WebLM server destination, if applicable. Navigate to **Administration** > **Licensing** > **WebLM Configuration**.
15. Restore Utility Services (6.2 and later) or retranslate Utility Services, as applicable.
16. Retranslate the Utility Services server destination, if applicable.
17. Set up System Manager or WebLM as applicable to provide licensing support for Communication Manager. The MAC address from the previously used server *cannot* be used. See the appropriate deployment guide for the licensing procedures. A new PLDS license is required. Log in to WebLM and click **Properties** to obtain the MAC address information (or equivalent).

18. Complete the SAL registration spreadsheet in the migration workbook.
19. Reregister Communication Manager as a virtual application.
20. Remove records for Communication Manager as System Platform. This step must be performed by the Avaya Registration Team.
21. Add records. This step must be performed by the Avaya Registration Team.
22. Verify SAL connectivity after the new SAL Gateway is communicating to the data center.
23. Test an alarm and verify that alarming is working properly.
24. Verify survivability with existing LSP(s) or ESS(es).
25. If there were multiple SAL Gateways in use on System Platform before the migratio, 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.
26. 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.
27. 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.
28. 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: PCN and PSN notifications

PCN and PSN notifications

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

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

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

   Note:

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

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

Note:

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

Signing up for PCNs and PSNs

About this task

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

To sign up for notifications:

Procedure

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

Glossary

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.

Avaya Services VM

A virtual machine that supports Avaya services applications. Currently the services virtual machine is part of System Platform which uses a non-VMWare hypervisor.

Blade

A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.

DRS

Distributed Resource Scheduler. A VMware feature that intelligently places workloads based on available virtual resources.

ESXi

A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.

HA

High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.

Hypervisor

A hypervisor is also known as 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 Application. An OVA is 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 is the amount of physical RAM, CPU cycles, or memory that are reserved for a virtual machine.

SAN

Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.

Snapshot

Capture a virtual appliance configuration 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

An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.

virtual appliance

A virtual appliance is a single software application bundled with an operating system.

VM

Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.

vMotion

A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.

vSphere

< < v

vSphere is VMware’s computer cloud virtualization operating system.

Index