Deploying Agile Communication Environment™ on VMware®

Release 6.2
NN10850-065
Issue 3
December 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 Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner 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 CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, 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

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.

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

Copyright

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

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances 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.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

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 deployment procedures for deploying the Avaya Agile Communication Environment™ virtual application in a virtualized environment.

This document includes deployment, 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 ACE™ on a VMware® vSphere ™ 5.0 or 5.1 virtualization environment at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Documentation changes since last issue

The following are the changes in the document for this release:

- Added information about additionally supported hypervisor versions.
- Added new procedure to change network parameters without requiring a reinstall.
- Added procedure to restart the ACE VM.
- Added procedures to Power on and Power off the ACE VM.
- Added procedures for migration of ACE Release 6.2 or 6.2.1 to Release 6.2.2.

ACE supports additional versions of VMWare Hypervisor

See *VMware software requirements* in the Planning and configuration chapter.

ACE supports change of network parameters without reinstall

See *Changing network parameters* in the Configuration chapter.

ACE supports two migration paths

You can migrate to ACE Release 6.2.2 from ACE Release 6.2 or 6.2.1

For procedures, see the *Migration* chapter.

Related resources

Documentation

This document is a part of the Avaya ACE documentation suite. Avaya ACE documents provide information on Avaya ACE fundamentals and planning, ordering ACE software, and ACE installation and administration. The documents also contain information on Avaya and third-party system solution integration, Web service application programming interfaces (APIs), security, fault, and performance management, and troubleshooting.

You can also find information on core applications or APIs delivered with the base software, for example, Message Drop, and Message Blast API.

Avaya ACE Release 6.2.2 documents

Title	Description	Audience
Overview		
Avaya Agile Communication Environment™ Overview and Specification	Provides a description of ACE including solution architecture, services, features, hardware, and software.	Sales engineers, Solution architects, Implementation engineers, and Support personnel
Avaya Agile Communication Environment™ Documentation Roadmap (NN10850–002)	Provides a list of documents in the Avaya ACE documentation suite for the release.	Sales engineers, Solution architects, Implementation engineers, and Support personnel
Installation, upgrades, migrations, and configurations		
Avaya Agile Communication Environment™ Planning and Installation (NN10850–004)	Describes network planning when integrating Avaya ACE with other applications. The document also contains information and procedures for installing and upgrading Avaya ACE software components.	Sales engineers, Solution architects, Implementation engineers, and Support personnel

Title	Description	Audience
Avaya Agile Communication Environment™ using VMware in the Virtualized Environment Deployment Guide (NN10850-065)	Describes the procedures for deploying the Avaya ACE vAppliance on VMware.	Sales engineers, Solution architects, Implementation engineers, Support personnel
Maintenance and Troubleshooting		
Avaya Agile Communication Environment™ Troubleshooting	Contains troubleshooting information and procedures for Avaya ACE.	Solution architects, Implementation engineers, Support personnel
Avaya Agile Communication Environment™ Fault and Performance Management	Describes how the fault and performance management system collects alarms and events generated by Avaya ACE. The document also describes how to monitor Avaya ACE.	Solution architects, Implementation engineers, Support personnel
Administration and system programming		
Avaya Agile Communication Environment™ Service Provider Administration	Provides information about the initial configuration, administration, and ongoing management of Avaya ACE service providers. The Avaya ACE host supports a Web-based GUI that administrators can use to perform the tasks.	Implementation engineers, Support personnel
Avaya Agile Communication Environment™ Secure Communication Fundamentals	Provides information on how Avaya ACE uses certificates for secure communication. The document also contains procedures that describe how to manage certificates using OpenSSL, IBM certificate management tools, and Avaya Aura® System Manager.	Implementation engineers, Support personnel
Avaya Agile Communication Environment™ User and Security Administration	Provides information about user management on Avaya ACE. The Avaya ACE host supports a Web-based GUI that administrators can use to perform system administration, configuration, fault management,	Implementation engineers, Support personnel

Title	Description	Audience
	performance management, and user management.	
Avaya Agile Communication Environment™ Message Drop and Message Blast Administration	Provides information about the administration of the Avaya ACE Message Drop and Message Blast service.	Implementation engineers, Support personnel
Administering Avaya WebLM (stand-alone)	Provides administration, configuration, and troubleshooting information for the Web-based license manager (WebLM).	Implementation engineers, Support personnel
Application developer		
Avaya Agile Communication Environment™Web Services	Describes the Web services supported by Avaya ACE.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Overview	Provides a general overview of Avaya ACE Foundation Toolkit.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Developer Guide	Describes the administration and maintenance of Foundation Toolkit.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Sample Java SE Application Guide	Describes the sample Java SE application delivered with Foundation SDK.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Sample Web Application Guide	Describes the sample Web application delivered with Foundation SDK.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Sample Basic Java SE Application Guide	Describes the Basic Java SE sample applications delivered with Foundation SDK.	Solution architects, Implementation engineers, Support personnel, Application developer
Avaya Agile Communication Environment™Foundation Toolkit Sample Web Application Guide Addendum Implicit Sequencing	Describes how to run sample Web applications in an implicit sequencing scenario.	Solution architects, Implementation engineers, Support personnel, Application developer

Training

Course code	Course title	Activity type
10U00010E	Avaya Agile Communication Environment(TM) (ACE) Core Implementation Virtual Campus Offering	On demand

Avaya Mentor videos

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

About this task

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

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

Note:

Videos are not available for all products.

Support

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

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment Overview

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

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

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

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

Note:

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

- server and host
- reservations and configuration values

Customer deployment

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

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

Software delivery

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

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

Patches and upgrades

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

Important:

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

Performance and capacities

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

Caution:

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

Avaya Collaboration Pod for Avaya Aura® Virtualized Environment

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

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

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

Documentation

The following table lists the Avaya Collaboration Pod for Avaya Aura® Virtualized Environment documents. These documents are available on the Avaya support website at http://support.avaya.com.

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

VMware components

VMware Software Component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	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 host in the case where vCenter Server is not used. Enables the installation and management of virtual machines.
vCenter Server	vCenter Server 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. vCenter Server provides VMware features such as High Availability and vMotion.

Deployment guidelines

The high-level deployment steps are:

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

The following are deployment guidelines for the virtual appliances:

- Deploy as many virtual appliances on the same host as possible.
- Deploy the virtual appliances on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure the redundant elements will not be on the same host.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as Avaya Aura® applications, from other virtual machines.

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

Important:

The values for performance, occupancy, and usage can vary greatly. The blade server may be running at 5% occupancy, but a virtual machine may be running at 50% occupancy. Note that a virtual machine will behave differently if the CPU usage is higher.

OVA deployment order

Deploy the application OVA files in the following order:

1. System Manager
2. Application Enablement Services
3. Communication Manager
4. Session Manager
5. Utility Services
6. Presence Services

Agile Communication Environment™, SAL, and WebLM can be deployed in any order after the application OVA files have been deployed.

Downloading software from PLDS

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

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

Note:

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

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.

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

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

13. (Internet Explorer only) If you receive an error message, click on the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

Chapter 3: Planning and configuration

Planning

Ensure that the following activities are complete before deploying the virtual appliance:

#	Action	Notes	✔
1	Coordinate with service providers.		
2	All required licenses have been purchased and are accessible.		
3	All required hardware has been purchased and delivered.		
4	Staging and verification activities have been planned and resources assigned.		
5	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation. Make sure the license file copies are accessible.		

Server hardware and resources

VMware offers compatibility guides that list servers, system, I/O, storage/SAN, and backup compatibility with VMware infrastructure. See http://www.vmware.com/resources/guides.html to view VMware-certified compatibility guides and product interoperability matrixes.

The VMware-certified servers must be running ESXi 5.0 and any of its updates, or ESXi 5.1 and any of its updates.

Configuration tools and utilities

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

- A remote PC running the VMware vSphere Client.
- A browser for accessing the Avaya ACE OAMP.
- Avaya Aura® System Manager Console

Customer configuration data

The following table identifies the key customer configuration information that are required throughout the deployment and configuration process for Avaya ACE.

Required data	Example value	Value for the system
FQDN host name of the ACE machine	soalaba175.aceott.avaya.com	
IPv4 address	135.20.245.175	
IPv4 netmask	255.255.255.0	
IPv4 gateway	135.20.245.1	
IPv4 address of the WebLM server	135.20.245.174	
(optional): IPv4 address for primary, secondary and tertiary DNS servers, if present	47.134.170.41 47.134.170.61 47.134.170.51	
SNMP v2c prompts		
IP address or fully qualified domain name (FQDN) of NMS location	135.20.244.56 or ace.avaya.com	
Port number of NMS location	10345	
Community string for SNMPv2c NMS	Public	
SNMP v3 prompts		

Required data	Example value	Value for the system
IP address or fully qualified domain name (FQDN) of NMS location	135.20.244.56 or ace.avaya.com	
Port number of NMS location	10345	
Username for v3 NMS	User name you have created on the NMS for SNMP usage.	
Authentication protocol for v3 user	md5 or sha	
Authentication password for specified protocol		
Privacy protocol for v3 user	AES or DES	
Privacy password for v3 user		

Default passwords on ACE

Avaya ACE is installed with the following default values:

Parameter	Default Value
Authentication mode	Basic
Websphere Application Server (Websphere) administrator username	admin
Websphere administrator password	admin
Avaya ACE database user name	root
Avaya ACE database password	admin
Linux console user name	root
Linux console password	agile
Linux console user name	sysadmin
Linux console password	agile
Avaya ACE GUI User name	admin
Avaya ACE GUI password	agile

Avaya ACE VM resource requirements

The Avaya ACE Virtual Machine (VM) requires the following set of resources to be available on the ESXi host before deployment.

VMware Resource	User profiles					
	500	1000	2400	5000	10000	15000
vCPU core	2	2	4	4	6 *	8
vCPU reservation (in MHz)	2330	4660	9320	9320	13980	18640
Minimum CPU speed (Minimum CPU speed based on Xeon E5620 or equivalent processor)	2.33 GHz	2.33 GHz	2.33 GHz	2.33 GHz	2.33 GHz	2.33 GHz
Memory reservation	4 GB	4 GB	6 GB	8 GB	12 GB	12 GB
Storage reservation (in GB)	300	300	300	300	300	300
Shared NIC(s)	1@1000 Mbps	1@1000 Mbps	1@1000 Mbps	1@1000 Mbps	1@1000 Mbps	1@1000 Mbps
IOPS	4	5	5	6	7	8
Average Network usage (Mbps)	0.5	1.5	2.5	4	5	6

Note:

Avaya ACE is tested at a high capacity. On an average, Avaya ACE at high capacity uses the values specified in the table for each profile in total network utilization and input/output operations per second (IOPS) in total disk utilization.

In a customer environment, Avaya ACE performance might vary from the average results.

Avaya ACE might be deployed on a host that does not have the resources to allocate to the VM for power up. There are CPU reservations assigned to the vAppliance, built into the OVA, that are specified for a specific server speed.

Adjusting Avaya ACE VM properties

About this task

If the system encounters CPU resource limitations, the system displays a message similar to `Insufficient capacity on each physical CPU`. To correct the CPU limitation, you must adjust the Virtual Machine (VM) properties.

If the CPU adjustments you made does not correct the power up conditions, reduce the CPU speed. Use the same procedure to reduce the value of other VM resources.

Do not modify the resource settings, for example, remove the resources altogether. Modifying the allocated resources can have a direct impact on the performance, capacity, and stability of the Avaya ACE VM. To run the Avaya ACE VM at full capacity, the resource size requirements must be met; removing or greatly downsizing reservations could put the resource size requirement at risk. Make deviations from the requirement is at your own risk.

Important:

Any deviation from the requirement is at your own risk.

Procedure

1. Right click the Avaya ACE Virtual Machine and select **Edit Settings…**.
   The system displays the Virtual Machine Properties dialog box.
2. Click **Resources** tab.
   The system displays the details for CPU, memory, disk advanced CPU, and advanced memory in the left pane.
3. To adjust CPU limitations, select **CPU**.
4. In the **Resource Allocation** area, perform one of the following to start the VM:
   - Adjust the slider to an appropriate position so that the VM can be started.
   - In the **Reservations** field, enter the exact number.

Software requirements

Avaya ACE™ uses the Release 6.2.2 software as the standard release on:

- VMware® vSphere ESXi 5.0 or ESXi 5.1
- VMware® vCenter ESXi 5.0 or ESXi 5.1

The system does not currently support VMware® vSphere 4.1. The Avaya ACE Virtualized Environment is packaged as a vAppliance ready for deployment on VMware certified hardware.

WebLM software requirements

With Avaya ACEVirtualized Environment solution, you can use only those WebLM versions that support virtualization.

The following are the supported versions of WebLM:

- System Manager WebLM versions
  - System Manager 6.2.0 - SP4. Build No 6.2.0.0.15669-6.2.12.408 and Software Update Revision No: 6.2.16.1.1993
  - System Manager 6.3.0 - FP2 Build No. - 6.3.0.8.5682-6.3.8.1627 Software Update Revision No: 6.3.2.4.1399
- Standalone WebLM versions
  - VE 1.0
  - VE 2.0

VMware software requirements

The following VMware software versions are supported:

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

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

Note:

ESXi 4.1 is not supported.

SAL gateway

Secure Access Link (SAL) Gateway provides Avaya support engineers and Avaya Partners with alarming and remote access to Avaya Agile Communication Environment™. Avaya ACE™ includes an embedded SAL Gateway. The SAL Gateway application on Avaya ACE provides remote delivery of support services. Avaya ACE can be serviced remotely, potentially eliminating the need for a service technician to visit the customer site. Avaya ACE uses the customer's existing Internet connectivity to facilitate remote support. All communication is outbound from the customer's environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS).

Note:

Avaya Partners and customers must ensure that SAL is always configured and registered with Avaya during Avaya ACE installation.

Avaya support will be delayed or not possible if SAL is improperly implemented or not operational.

Chapter 4: Deploying ACE

Deployment checklist

Use the following checklist for deploying the Avaya ACE vAppliance.

#	Action	Link/Notes	✔
1	Download the Avaya ACE OVA.	See Downloading the Avaya ACE OVA on page 27	
2	Deploy the Avaya ACE OVA	See Deploying the ACE OVA on page 28	
3	Modify resources, if applicable.	See Modifying the VM resources for user profile on page 29	
4	Start up the Avaya ACE VM.	See Powering on the virtual machine on page 30	
5	Keep the configuration data handy.	See Customer configuration data on page 20	
6	Configure Avaya ACE.	See Configuring ACE on page 33	
7	Verify Avaya ACE deployment.	See Verifying deployment on page 41	

Downloading the Avaya ACE OVA

Avaya ACE is packaged as a OVA. Use this procedure to download the OVA from the Avaya support site.

Procedure

1. Log in to the Avaya support site, https://support.avaya.com.
2. Click **Downloads & Documents**.

3. In the **Enter Your Product Here** field, enter `Avaya Agile Communication Environment` and from the drop down menu, select Release 6.2.2.
4. In the Select the content type section, select **Downloads** and click **Enter**.
5. In the resultant page, select the OVA file to download.
   The OVA file has the following naming convention:
   ```
   <product name>-<product build>-<ESXi version>-<OVA build iteration>
   ```
   For example, `ACE-6.2.0.79.30367-e50-00.ova`

Deploying the ACE OVA

Before you begin

Ensure that you:

- have installed vSphere client
- have obtained the Avaya ACE OVA file. See Downloading the Avaya ACE OVA on page 27.

Procedure

1. Log in to the vCenter or the ESXi server using the vSphere Client.
2. Select the ESXi host on which Avaya ACE will be deployed.
3. Navigate to **File** > **deploy OVF Template**.
4. In the Deploy OVF Template window, enter the path to the OVA file which is accessible from the Host and Click **Next**.
   You can enter the path to the OVA file in one of the following ways:
   - in the **Deploy from a file or URL** field, enter the URL path of the OVA file.
   - select **Browse** and navigate to the OVA file location.
5. Verify the OVA Template details and click **Next**.
6. Read the License agreement, click **Accept** and click **Next**.
7. Enter the VM name in the **Name** field and click **Next**.
8. If you do not have a host selected when you choose to Deploy OVF Template, the wizard prompts you for the host or cluster name to deploy the virtual appliance. Select the host or cluster to deploy the VM.
9. Select a data store for the VM files.
   For more information, see Storage on page 60

10. In the Disk Format window, select **Thick provisioned Eager zero format** to store the virtual machine virtual disks and click **Next**.

    For more information on virtual disks, see Thin vs. thick deployments on page 60.

11. For each network specified in the OVA Template, select a Host network by clicking the **Destination Network** column, click the entry in the **Destination Network** column, click the expansion arrow and select the desired Host network from the list displayed, Click **Next**.

    Note:

    This step is applicable if there is more than 1 Virtual Machine port group.

12. Review the settings and click **Finish**.
13. Check **Status** in the Recent Tasks window, and wait for the Deploy OVF template task to show `Completed`.

Modifying VM resources for user profile numbers

The Avaya ACE OVA is built with a default profile for 5000 users. If the number of users is less or more than the default profile, you must adjust the VM resources to suit your user profile.

For more information, see VM resource requirements on page 22.

Before you begin

Ensure that you have:

- Logged in to the correct vCenter or ESXi server.
- Successfully deployed the Avaya ACE OVA .
- Not powered on the Avaya ACE VM.

About this task

Use this procedure to adjust the VM resources based on the user profile.

Procedure

1. In the vSphere Client inventory, select the Avaya ACE virtual machine.
2. Right-click and select **Edit Settings**.
3. On the Hardware tab, select **Memory**.
4. Set the memory value by using any of the following techniques:
    - Click a colored triangle on the slider or in the legend.

- Use the slider control.
- Use the numeric field.

5. On the Hardware tab, select **CPUs**.
   - If the VM profile requirements is less than or equal to 4vCPU:
     - In the **Number of cores per socket** drop-down menu, click **1**.
     - In the **Number of virtual sockets** drop-down menu, select a value that will ensure the resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

     For example, if you need 2 vCPUs for your user profile, set **Number of cores per socket** to 1 and **Number of virtual sockets** to 2.

   - If the VM profile requirements is more than 4vCPU:
     - In the **Number of cores per socket** drop-down menu, click **2**.
     - In the **Number of virtual sockets** drop-down menu, select a value that will ensure the resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

     For example, if you need 8 vCPUs for your user profile, set **Number of cores per socket** to **2** and **Number of virtual sockets** to **4**.
6. Click **OK**.

Powering on the Avaya ACE virtual machine

Before you begin

Ensure that you have installed vSphere Client and are logged into the correct vCenter or ESXi server.

About this task

Use this procedure to power on the Avaya ACE virtual machine.

Procedure

1. In the vSphere Client inventory, select the Avaya ACE VM.
2. Click **Power On**.
3. In the Recent Tasks window, wait until the status of the **Power on virtual machine** shows **Completed**.

   The Recent Tasks window is displayed at the bottom of the page.

4. Right-click the Avaya ACE VM, and select **Open Console**. Wait for the Avaya ACE window VM to boot up.

Next steps

Continue with the deployment tasks on the Console window.

Powering off the Avaya ACE virtual machine

Procedure

1. In the vSphere Client inventory, select the Avaya ACE VM.
2. Right-click and select **Power** > **Shut Down Guest**.

Chapter 5: Configuration

Configuring ACE

Before you begin

Ensure that you:

- have installed vSphere Client.
- have deployed the Avaya ACE OVA and powered on the Avaya ACE VM. See Deploying the ACE OVA on page 28 and Powering on the virtual machine on page 30.
- know the value for the configuration parameters. You will be prompted for the configuration parameters during the first boot up of the Avaya ACE VM. For a list of configuration parameters, see Customer configuration data on page 20.

Procedure

1. Log in to the vSphere Client.
2. Select the Avaya ACE VM, right-click your mouse, and select **Open Console**.
3. Enter the parameters when prompted for it.
4. Review the settings for the parameters and enter `Yes` when prompted for it.

Result

After you confirm the parameter settings, the Avaya ACE VM will complete the boot process.

You can use the Avaya ACE GUI for any further configurations. For more information, see Verifying deployment on page 41.

Related topics:

Configuring the virtual machine automatic start and stop settings on page 33

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.

Note:

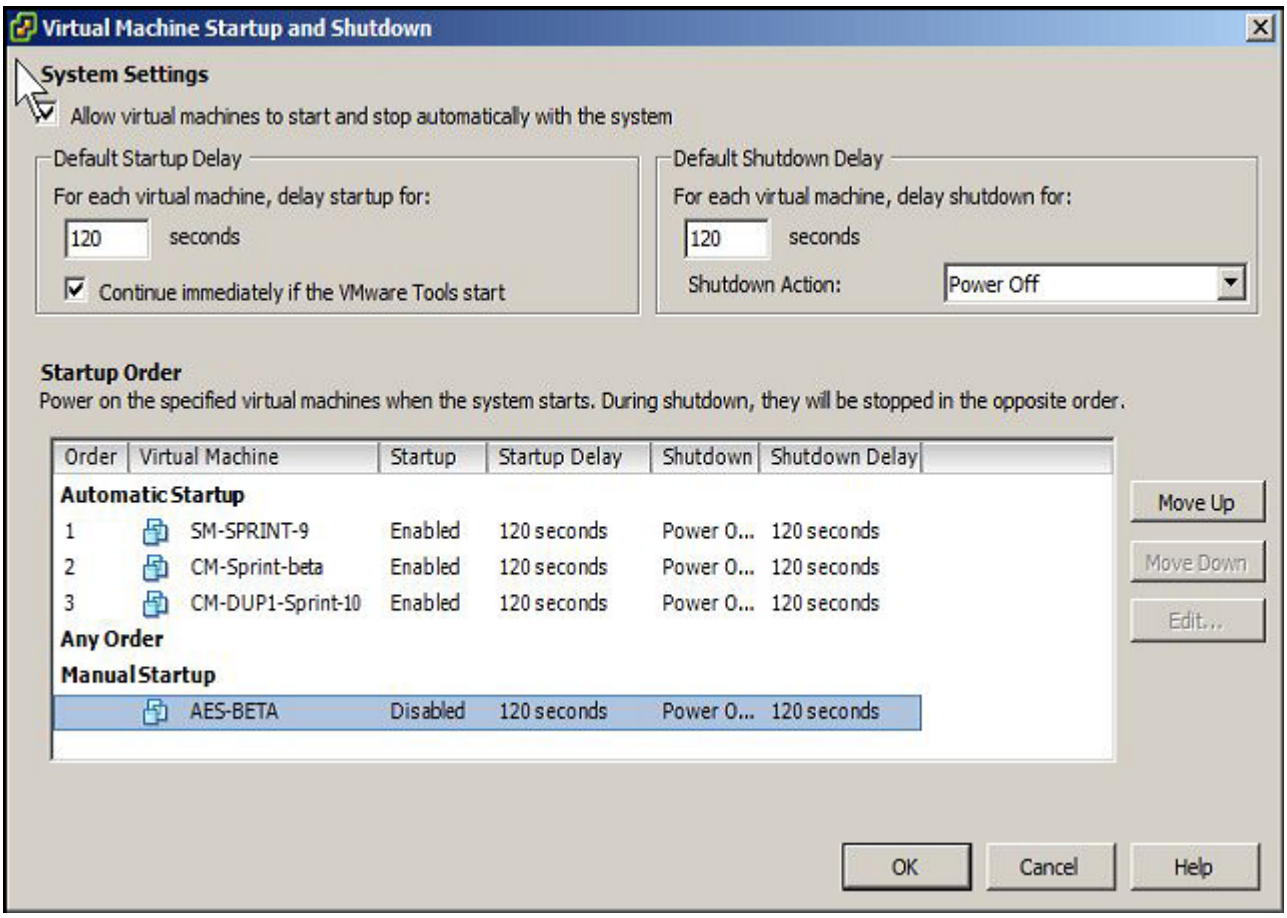
You can skip the this procedure, if you have enable the High Availability option for cluster.

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.



Next steps

For more information on the Presence Services VM Installation script using an X11 forwarding feature, see the *Implementing Avaya Aura® Presence Services* guide on the Avaya support website.

Logging in to Avaya ACE host

Avaya ACE does not support logging in to the server remotely with ***root*** user credentials. However, most of the administrative tasks need root credentials. To obtain ***root*** credentials, log in as ***sysadmin*** user and change to ***root*** user.

Before you begin

You must know the ***sysadmin*** and ***root*** credentials.

Procedure

1. Log in to the Avaya ACE host as ***sysadmin*** user.

For HA deployments, log in to the active host.

2. Change to ***root*** user. Type `su - root` and press **Enter**.

   When changing to the root user, always use the command syntax **`su - root`**. Using a dash ensures that you have the correct environment when entering commands as the root user.

3. Enter the ***root*** password when prompted for it.

Optional and customized functionality

Changing the WebLM IP

Before you begin

Ensure that you:

- Have installed vSphere Client and are logged in to the correct vCenter or ESXi server.
- Have Avaya ACE Release 6.2.x installed.
- Get the ***root*** and ***sysadmin*** user credentials.

About this task

During deployment of Avaya ACE OVA, you will be prompted to enter the IP address of the WebLM server. Use this procedure to change the IP address of the WebLM server you entered during deployment.

Important:

When you change the WebLM server address, the Avaya ACE application servers will be restarted for the update to take effect. During this time, there will be loss of service.

Procedure

1. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 35.
2. Change directories. At the command prompt, enter:

   ```
   cd /opt/avaya/ace/bin
   ```

3. Run the change IP tool. At the command prompt, enter:

   ```
   ./changeWebLM.sh
   ```

4. Enter the IP address of the WebLM server when prompted for it.

Result

The tool stores the logs in the file `WebLMServer_changes.log` located at `/var/avaya/ace/log/weblm`.

Changing the default passwords on ACE

Before you begin

Ensure that you:

- Have installed vSphere Client.
- Have logged in to the correct vCenter or ESXi server.
- Have Avaya ACE Release 6.2.2 installed.
- Get ***sysadmin*** and ***root*** user credentials.

About this task

When you deploy the Avaya ACE OVA, Avaya ACE database and the Linux console are installed with default passwords. Use this procedure to change the default passwords.

Important:

You must not use the ! symbol for mySQL passwords.

Procedure

1. On the Avaya ACE VM, select **Open Console**.
2. Log in to the Avaya ACE host as the ***sysadmin*** user.
3. To change the ***sysadmin*** user password, at the command line interface, enter:
   a. `passwd`.
   b. Enter the new password. Enter the new password again to confirm.
4. Change to ***root*** user.
   When changing to ***root*** user, always use the command **`su - root`**. Using a dash ensures that you have the correct environment when entering commands as root user.
5. To change the ***root*** user password, at the command prompt, enter:
   a. `passwd`
   b. Enter the new password. Enter the new password again to confirm.
6. To change the ACE database password, at the command line interface, enter:
   `mysqladmin -uroot -p``admin` **`password`** *`NewPassword`*

Where,

- *NewPassword* is the new password.
- *admin* is the default password for Mysql, the Avaya ACEdatabase.

7. To change the Websphere Application Server password:
   a. In your browser, open the Websphere administrative console using the following format
      `https://<ACE_IP or FQDN>:9043/admin`
      Example, `https://10.10.10.23:9043/admin` or `https://ace.avaya.com:9043/admin`
   b. Log in to Websphere Application Server console with default credentials:
      User ID: `admin`
      Password: `admin`
   c. On the left navigation pane, navigate to **Users and Groups** > **Manage Users**.
   d. Click **admin**.
   e. In the **Password** field, enter the new password. Enter the password again in the **Confirm password** field.
   f. Click **Apply** and then click **OK**.
   g. Log out and log back in to the Websphere Application server administrator web console with the new password to confirm the change in password.
   h. To renew the cached data, you must restart the Avaya ACE application servers. Perform the following steps:
      i. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 35.
      ii. Enter: `/opt/avaya/ace/bin/RestartAllServer.sh`

Changing network parameters

The Avaya ACE network parameters are set during the first boot after you deploy the Avaya ACE OVA. For information on first boot, see Configuring ACE on page 33.

Before you begin

Ensure that you:

- Have deployed the Avaya ACE OVA and powered on the Avaya ACE VM. . See Deploying the ACE OVA on page 28 and Powering on the virtual machine on page 30.
- Get ***sysadmin*** and ***root*** user credentials.
- Get the value for the network configuration parameters. You will be prompted for the configuration parameters during the task. For a list of configuration parameters, see Customer configuration data on page 20.

About this task

Use this procedure to change the network parameters you entered during first boot of Avaya ACE.

Important:

After you change the network parameters, you must reboot your system for the update to take effect. During this time, there will be loss of service.

Procedure

1. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 35.
2. Change directories. At the command prompt, enter:
   ```
   cd /opt/avaya/ace/bin
   ```
3. Run the change network parameter tool. At the command prompt, enter:
   ```
   ./ChangeHost.sh -a
   ```
4. Enter the values for the parameters when prompted.
5. Enter Yes or No when prompted to accept the entered values.

Next steps

Reboot for the changes to take effect. See Rebooting ACE on page 39.

Rebooting the Avaya ACE VM

Before you begin

Log in to the correct vCenter or ESXi server.

Procedure

1. In the vSphere Client inventory, select the Avaya ACE VM.

2. Right-click and select **Power** > **Restart Guest**

Chapter 6: Post deployment verification

Verifying Avaya ACE deployment

The Avaya ACE host exposes a Web-based operation, management, and provisioning (OAMP) console . Administrators can use the OAMP console to perform system administration, configuration, user, and license management tasks.

For more information, see:

- *Avaya Agile Communication Environment™ User and Security Administration* (NN10850–010).
- *Avaya Agile Communication Environment™ Service Provider Administration* (NN10850–005).

The Avaya ACE OAMP console is available after you install Avaya ACE and is accessible when you start the Avaya ACE application.

Procedure

In your Web browser, enter `https://<ACE_IP or FQDN>:9449/oamp`

If the Avaya ACE OVA is successfully deployed, the Avaya ACE Web console will open.

Example

https://135.32.12.181:9449/oamp

or

https://soalaba175.aceott.avaya.com:9449/oamp

Chapter 7: Maintenance

Backup and restore

Perform the native Avaya ACE backup and restore function for the long-term backup and recovery of the Avaya ACE VM data when running on VMware.

Avaya ACE runs an automated backup daily.

The automated backup process backs up:

- the ACE database.
- the ACE configuration files specified in the `backup_files.conf`file.
- the ACE network configuration files specified in the `backup_network.conf`file.

For more information on backup and restore procedures, see *Avaya Agile Communication Environment™ Planning and Installation* (NN10850–004).

VMware Snapshots

You can use VMware Snapshots for backup and recovery. However, do not rely on VMware Snapshots as a robust backup and recovery method. VMware Snapshots method is better suited to short-term point-in-time copies of the running system before performing major upgrades or patch upgrades to the system.

For more information on VMware Snapshots and how to use it, see VMware documentation.

Migration

Migration Data

Avaya ACE supports the following migration paths:

- Avaya ACE Release 6.2 or 6.2.1 to Avaya ACE Release 6.2.2.

Migration checklist for migrating from Release 6.2 or 6.2.1

Use the following checklist for deploying the Avaya ACE vAppliance.

#	Action	Link/Notes	✔
1	Backup Avaya ACE database and configuration data. **Note:** Store the backed up tar file on a different machine.	See backup procedures in *Avaya Agile Communication Environment™ Planning and Installation* (NN10850–004).	
2	Power off Avaya ACE VM.	See Powering off a VM on page 31.	
3	Deploy the Avaya ACE Release 6.2.2 OVA	See Deploying the ACE OVA on page 28	
4	If you are changing user profile numbers from earlier release, adjust VM resource allocation.	See Modifying the VM resources for user profile on page 29	
5	Start up the Avaya ACE VM.	See Powering on the virtual machine on page 30	
6	Keep the configuration data handy. **Note:** Use the same network parameters you had in your earlier release.	See Customer configuration data on page 20	
7	Configure Avaya ACE.	See Configuring ACE on page 33	

#	Action	Link/Notes	✔
8	Verify Avaya ACE deployment.	See Verifying deployment on page 41	
9	Copy the backup tar file to a location on the newly started Avaya ACE VM.		
10	Migrate the backed up data and configuration.	See Migrating ACE on page 45	

Migrating from Avaya ACE Release 6.2 or 6.2.1

Before you begin

Ensure that you:

- transfer the stored Avaya ACEbackup file to a directory on the Avaya ACEhost.
- know the root and sysadmin user credentials.
- define the following parameters. The migration procedure will prompt you for the values of the parameters.

Parameter	Description	Value
WAS admin user name	WebSphere admin user ID.	
WAS admin user password	Password for the WebSphere admin user ID.	
Database username with restore privilege	root user ID.	
Database password	Password for the root database user.	
Directory that holds the ACE backup file	Location on the local ACE host, where the backup file containing the Avaya ACERelease 6.2 or 6.2.1 database and configuration data is stored.	
ACE backup file name	Name of the backup file containing the Avaya ACE Release 6.2 or 6.2.1 database and configuration data	
Valid PASSWORD in Active Directory For User DN *AD_USER_DN*	Password for user *AD_USER_DN* **Note:** *AD_USER_DN* is a user created in the Active Directory for authentication purposes. For more information, see *Avaya Agile Communication*	

Parameter	Description	Value
	Environment™ User and Security Administration (NN10850–010). This prompt appears only if the Avaya ACERelease 6.2 or 6.2.1 system had IWA authentication.	
Valid PASSWORD in Active Directory For User DN *SECONDARY_AD_USER_DN*	Password for user *SECONDARY_AD_USER_DN* **Note:** *SECONDARY_AD_USER_DN* is a user created in the Active Directory for authentication purposes. For more information, see *Avaya Agile Communication Environment™ User and Security Administration* (NN10850–010). This prompt appears only if the Avaya ACERelease 6.2 or 6.2.1 system had IWA authentication in multiple domains.	
Directory BINDING PASSWORD for Binding User *AD_BINDING_USER*	Password for user *AD_BINDING_USER* **Note:** *AD_BINDING_USER* is a user created in the Active Directory for authentication purposes. For more information, see *Avaya Agile Communication Environment™ User and Security Administration* (NN10850–010). This prompt appears only if the Avaya ACERelease 6.2 or 6.2.1 system had LDAP authentication.	

About this task

Use this procedure to migrate from Avaya ACE release 6.2 or 6.2.1 to Avaya ACE release 6.2.2.

Procedure

1. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 35
2. Change directories. Enter:
   ```
   cd /opt/avaya/ace/install
   ```
3. Run the migrate tool. Enter:
   `./migrate62to622Vm.sh`

4. Enter the values for the parameters when prompted.

Chapter 8: Troubleshooting

Troubleshooting

To troubleshoot issues faced during deployment of the Avaya ACE OVA, see VMware documentation.

To troubleshoot Avaya ACE issues, see *Avaya Agile Communication Environment™ Troubleshooting* (NN10850–026).

Appendix A: 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 the best performance BIOS settings for a few specific servers from the VMware-certified server list. In general, turn off power-saving server options for optimal performance. Consult the manufacturer technical data for your particular server.

Related topics:

Intel Virtualization Technology support on page 51
Dell PowerEdge Servers — BIOS settings on page 52
HP ProLiant Servers — BIOS settings on page 52

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

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

The tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing
- Startup/Shutdown

See *Overview of VMware Tools* at http://kb.vmware.com/kb/340 for more information regarding VMware tools.

Important:

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

Time keeping

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

The NTP servers can be local to the LAN or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open 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.

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:

Configuring a time server on page 54

Configuring a time server

Before you begin

- You must know the IP address of the NTP server. If you are configuring multiple NTP servers, you must know the IP addresses of all of them.
- You must know the ***root*** user credentials.

About this task

Configuring a network time protocol (NTP) server is normally performed during installation of Linux. However, you can also use this procedure to ensure that your ACE host is NTP synchronized before joining a federation.

Procedure

1. Log in to one of the ACE hosts. See Logging in to the Avaya ACE host on page 35.
2. Open the NTP configuration file `/etc/ntp.conf` in a text editor.
3. Configure the primary NTP server. Edit the following line and insert the appropriate IP address.
   ```
   server <primary_NTP_server_IP> prefer
   ```
4. **(Optional)** Configure a secondary NTP server. Edit the following line and insert the appropriate IP address.
   ```
   server <secondary_NTP_server_IP>
   ```
5. If you are configuring an NTP server for the first time, add the following line.
   ```
   driftfile /etc/ntp/ntp.drift
   ```
6. Save and close the file.
7. To synchronize with the NTP server, you must restart the NTP service. First, stop the NTP service. Enter
   ```
   service ntpd stop
   ```
8. Enter the following command.
   ```
   ntpd -q
   ```
9. Configure the NTP service for run level init. Enter
   ```
   chkconfig --level 35 ntpd on
   ```
10. Start the NTP service. Enter
    ```
    service ntpd start
    ```
11. Verify that the NTP service is running. Enter
    ```
    pgrep ntpd
    ```
    The process ID for **ntpd** should be returned.
12. Verify that the NTP service is synchronized with the NTP server. Enter
    ```
    ntpq -p
    ```
    The delay and offset values should be nonzero. The jitter value must be less than 100.

VMware networking best practices

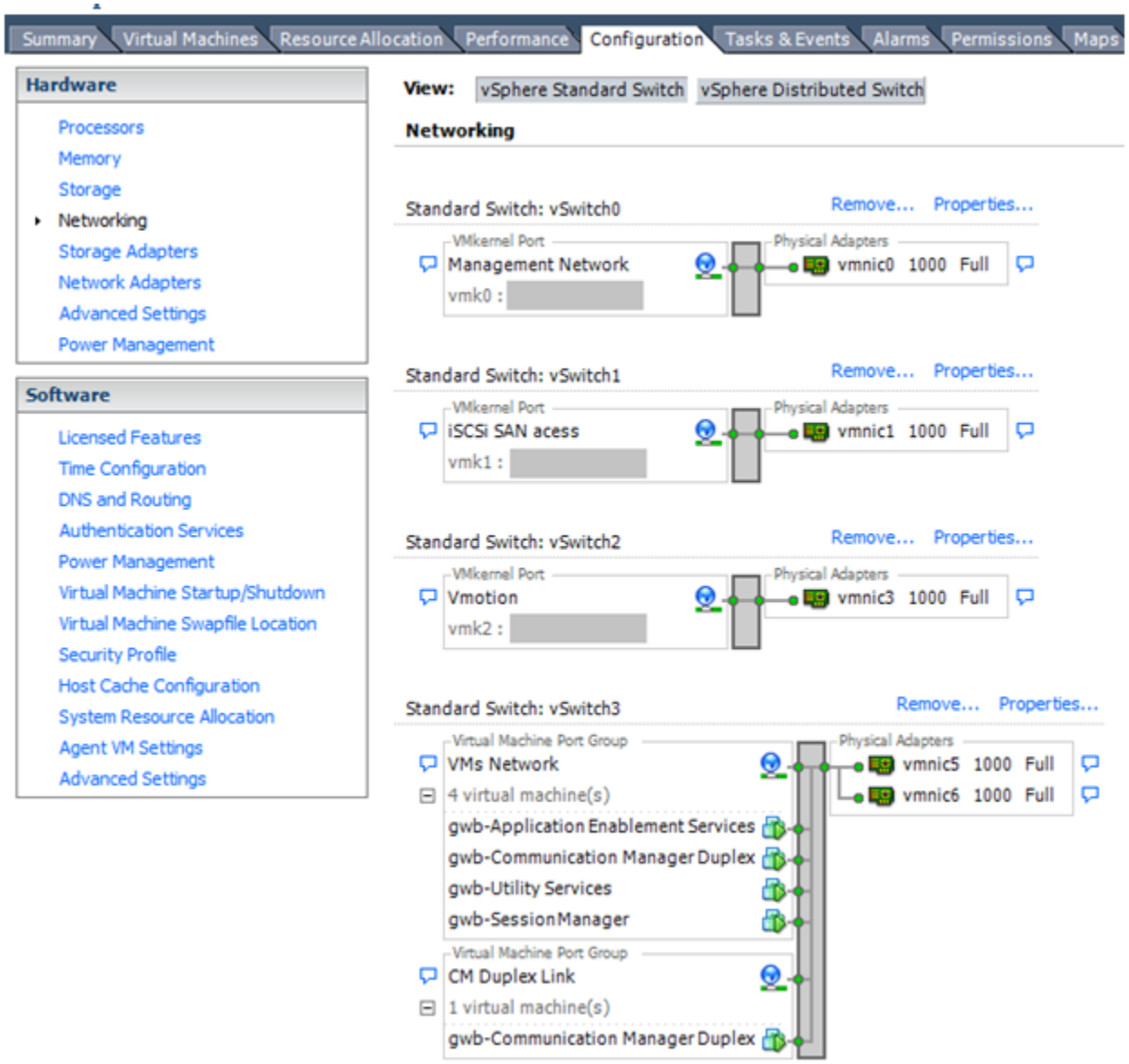
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities and are not the only supported networking configurations.

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

The following are the suggested best practices for configuring a network supporting applications that are 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



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

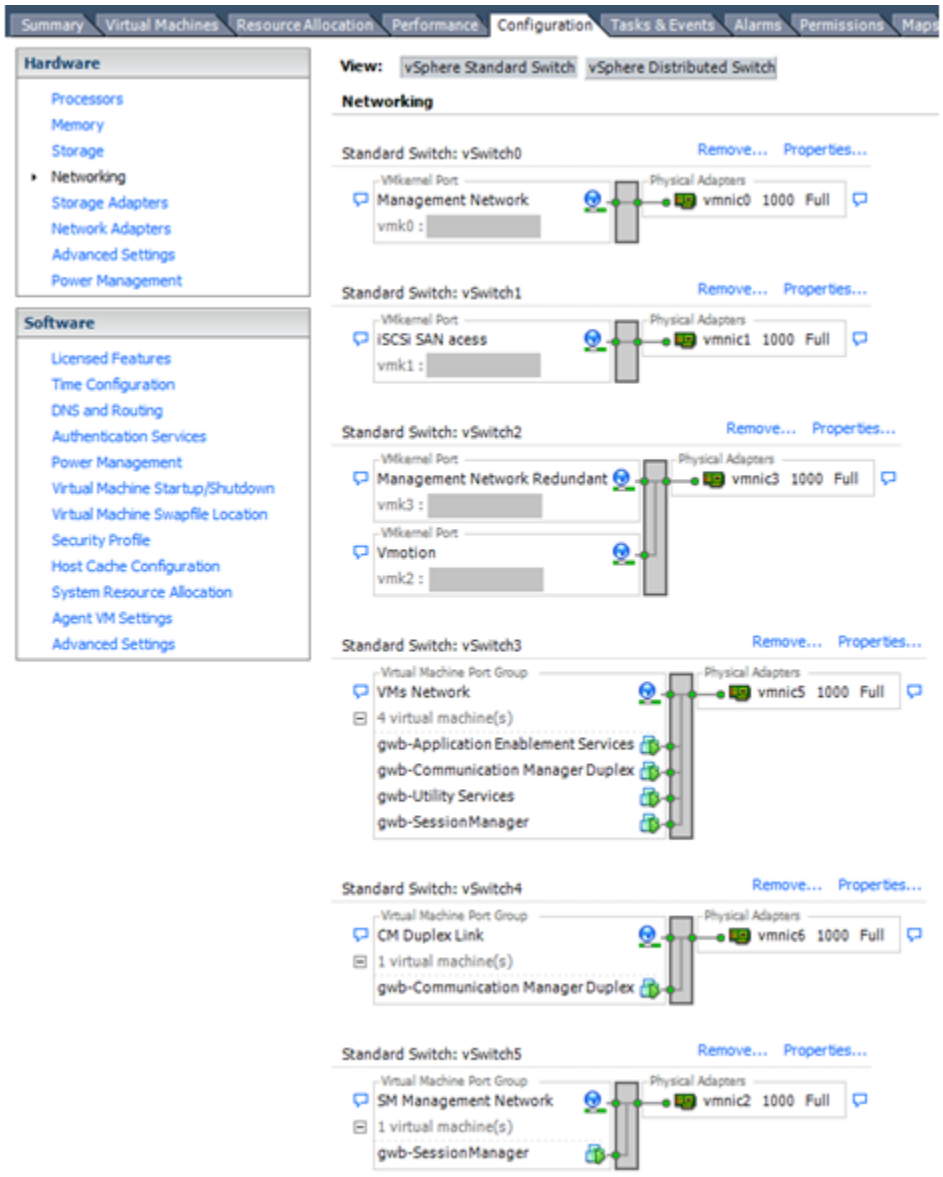
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and VM networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the VMs Network. Load balancing provides additional bandwidth for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



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
VMware 5.1 Documentation	http://pubs.vmware.com/vsphere-51/index.jsp

Storage

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are different storage technologies supported by VMware vSphere to meet different datacenter storage needs.

The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning these resources to virtual machines.

The data store can be local to the host or a mounted shared storage such as SAN. The virtual machine configuration file and virtual disk files are stored on the data store.

Note:

Avaya ACE does not support being deployed on or migrated to Network File System (NFS) mounted data stores.

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.
- results in the best performance, even on the first write to each block.
- has a longer disk creation time. Because of the extra time required to deploy an eager zero disk, it is not uncommon for the deployment operation to time out and fail.

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

VMware features used in Avaya ACE

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshot is a short-term copy of the running system that is created before a major upgrade or a patch installation.

Snapshots can:

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

Verify that the patch installation or upgrade is successful, and ensure that the virtual application is functional. You can then delete the snapshot

Caution:

Snapshot operations can adversely affect service. The application that is running on the virtual machine must 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.

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

- *Do not* rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- **Do not run a virtual machine off of a snapshot.** Do not use a single snapshot for more than 24-72 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 virtual machine is verified to be working properly. 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.

Related resources

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

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

VMware vMotion

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

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

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

VMware High Availability

VMware High Availability (HA) provides easy-to-use, cost effective high availability for all applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other host machines in the cluster that have spare capacity.

HA minimizes downtime and IT service disruption while eliminating the need for dedicated standby hardware and installation of additional software. VMware HA provides uniform high availability across the entire virtualized IT environment without the cost and complexity of failover solutions tied to either operating systems or specific applications.

Avaya ACE VMware Solution will support the HA of the ACE VMs where all the ACE virtual machines are monitored for failures and will be restarted on the other hosts when the current host fails.

VMware HA is a viable option for Avaya ACE recovery in the VMware environment. If the ESXi host on which Avaya ACE VM is installed fails, Avaya ACE is moved to a standby host. Once the cold boot of Avaya ACE on the standby host is complete, Avaya ACE will continue to process new web service requests.

Note the following when configuring to use VMware HA:

- All VMs and their configuration files must be on shared storage, for example, Fibre Channel SAN, iSCSI SAN, or iSCSI NAS
- To have reliable failure detection for HA clusters, the console network should have redundant network paths. This is because VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses virtual machine priority to decide order of restart.

Note:

Avaya ACE VMware HA solution will not support the monitoring of applications running within the ACE VMs.

Glossary

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

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

Index

R

S

T

V

W