Avaya Aura® Virtualized Environment Solution Description

Release 6.2
Issue 7
November 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya 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.

Licence 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 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.

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. “Instance” means one unique copy of the Software. For example, if the end user customer or Avaya channel partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software 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 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 7
- Related resources 8
  - Documentation 8
  - Avaya Mentor videos 9
- Support 9

Chapter 2: Avaya Aura® Virtualized Environment Overview 11
- Customer requirements 12
- VMware components 13
- General engineering guidelines 14
- Avaya Collaboration Pod for Avaya Aura® Virtualized Environment 15
- Deployment guidelines 16
- Deployment of cloned and copied OVAs 17
- Storage sources (SAN, NFS) 17
- Distributed Resource Scheduler (DRS) 17
- Material Codes 18
- Upgrade strategies 19

Chapter 3: Design considerations 21
- Caveats and limitations 21
  - Licensing 21
  - Authentication files and ASG access 22
  - Potential issues 22
- Feature and capacity differences 23
- Virtualized Environment Footprint Flexibility 24
- Average network and disk utilization 24
- Solution use cases and capacities 25

Chapter 4: Topology 29
- Avaya Aura® Virtualized Environment 29
- Example ESXi Configuration 30
- Typical High Availability configuration 30
- Example for estimating a solution footprint 31

Chapter 5: Resource requirements and references 33
- Server hardware and resources 33
- Agile Communication Environment™ resource requirements 34
- Application Enablement Services resource requirements 35
- Communication Manager resource requirements 36
- Presence Services resource requirements 38
- SAL Gateway resource requirements 39
- Session Manager resource requirements 39
- System Manager resource requirements 41
- Utility Services resource requirements 42
- WebLM resource requirements 43

Appendix A: VMware Best Practices **45**
BIOS **45**
Intel Virtualization Technology support **45**
Dell PowerEdge Servers — BIOS settings **46**
HP ProLiant Servers — BIOS settings **46**
VMware Tools **46**
VMware networking best practices **47**
Thin vs. thick deployments **50**
Best Practices for VMware features **51**
VMware Snapshots **51**
VMware vMotion **52**
VMware Storage vMotion **53**
VMware High Availability **53**
Glossary **55**
Index **57**

Chapter 1: Introduction

Purpose

This document describes the Avaya Aura® Virtualized Environment market solution from a holistic perspective focusing on the functional view of the solution architecture. The Solution Description includes a high-level description of the solution as well as topology diagrams, customer requirements, and design considerations.

Intended audience

The primary audience for this document is the sales engineer. This document is intended to help sales engineers understand how the solution and its verified configurations meet customer needs at a high level.

This document can also be used by solution architects, implementation engineers, and support personnel.

Document changes since last issue

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

- Added the *Collaboration Pod* section.
- Added the *Footprint flexibility* section.
- In the **General engineering guidelines** section, added a note regarding the following: You cannot administer a core Session Manager OVA as a Branch Session Manager (remote survivable server). Deploy the Session Manager OVA as a core Session Manager OVA only.

Related resources

Documentation

The following are documents related to Virtualized Environment. Download the documents from the Avaya support website at Avaya Support website from the **Downloads & Documents** tab. The documents are listed under their product names and specific software release.

Title	Description	Audience
Avaya Agile Communication Environment™ using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Agile Communication Environment™ virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Aura® Application Enablement Services using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Application Enablement Services virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Communication Manager virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Presence Services virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Session Manager virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Aura® System Manager using VMware®	Describes the procedures for installing and configuring the System Manager virtual	Implementation Engineers, Field Technicians, Business

in the Virtualized Environment Deployment Guide	application in the Virtualized Environment.	Partners, Solution Providers, Customers
Avaya Aura® Utility Services using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Utility Services virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya Secure Access Link Gateway using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the Secure Access Link Gateway virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers
Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide	Describes the procedures for installing and configuring the WebLM virtual application in the Virtualized Environment.	Implementation Engineers, Field Technicians, Business Partners, Solution Providers, Customers

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 Avaya Mentor Videos 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 release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Avaya Aura® Virtualized Environment Overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with 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.

Customer requirements

Problem/ Symptoms What the customer experiences	**Cause of problem** Why it happens to customers	**Negative Business Impact** Consequences of inaction	**How we solve the problem** What we do to address the cause	**Positive Business Outcomes as a Result** Key operational/ financial metrics

Large number of individual servers and storage devices	Company Expansion	More cost for Rack and Stack space.	Multiple applications on one cluster.	Fewer racks required.
Electrical costs for cooling and power.	Electricity to run servers including air conditioning and fans.	Monthly reoccurring costs for AC and fans.	Reduce the number of servers, therefore reducing the costs for AC and additional fans.	Less power consumption for cooling.
Cost of servers and power as new functionality is added.	Adopting new technologies.	Additional servers and electrical costs.	Fewer servers and less cost.	Cost savings, both reoccurring and additional investment.
Avaya Applications do not integrate with a VMware Data Center from an OA&M perpsective.	Some Avaya applications were not available on VMware.	Technicians need to be familiar with several different ways of performing serviceability functions.	Allow seamless integration for Serviceability and Maintenance with VMware.	Standard operating procedures.
Customers want to control their own hardware and data centers.	Many of the applications in the Avaya Aura® portfolio ship as appliance-only solutions.	Customers may choose to deploy a solution from a competitor.	Provide a phased-in approach of Avaya Aura® virtual appliances.	Provide customers with what they are asking for.

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

VMware Software Component	Description
	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.

General engineering guidelines

The virtual application is packaged in a virtual appliance OVA that includes the following:

- guest operating system
- operation application image (except for Presence Services which needs to be installed after deployment)
- VMware tools package (5.0 or better)
- defined footprint resource parameters for successful application use
- use and configuration of VMXNET3 and NTP for VMware best practices

Virtualized Environment supports local or SAN storage. A customer can choose to use SAN or not.

All products can be deployed using any of the following methods:

- vSphere Client direct
- vCenter

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.

Important:

You can deploy the Communication Manager Simplex OVA and then administer the Communication Manager Simplex OVA as a survivable remote server. However, you cannot

administer a core Session Manager OVA as a Branch Session Manager (remote survivable server). Deploy the Session Manager OVA as a core Session Manager OVA only.

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.

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 CMS, 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.

Deployment of cloned and copied OVAs

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

Storage sources (SAN, NFS)

The Avaya Aura® Virtualized Environment solution is compatible with any storage source that VMware supports. However, Avaya has focused mainly on iSCSI SAN testing as the preferred method of storage. Other technologies (for example, NFS), equipment, and network configurations may experience better or worse performance.

NFS is known to have lower performance characteristics. You need to understand the limits of your unique infrastructure. Follow IT best practices to achieve optimal operation within the limits of the specific technology that you use.

Distributed Resource Scheduler (DRS)

The Distributed Resource Scheduler (DRS) continuously monitors utilization across vSphere servers and intelligently allocates available resources among virtual machines.

DRS has not been fully tested by Avaya for Virtualized Environment 1.0. The customer bears the risk in using DRS. DRS rules allow much flexibility and can be customized for specific needs.

There is little risk in using DRS for start-up to direct affinity rules. Examples include

- partially automated or fully automated level 1.
- keeping redundancy pairs off the same server.

In general, DRS fully automated level 5 is not recommended. Virtual machine moves during a heavy production time could negatively impact performance and application experience.

Material Codes

The following are the new Material Codes that are associated with the OVAs and virtual appliances in the Avaya System Design tool (ASD).

SAP Material Code	Product	Description
271437	Application Enablement Services	AES R6 VE VAPP
271552	Session Manager	Avaya Aura® SM R6 VE VAPP
271535	Communication Manager (Simplex)	Avaya Aura® CM R6 VE VAPP
271841	Communication Manager (software duplex)	Avaya Aura® CM R6 DUP VE VAPP
271781	Utility Services	AVAYA R6 UTILSVCS VE VAPP SYS LIC
271489	Presence Services	Avaya Aura® TM PS R6 VE VAPP
271784	System Manager	SYSTEM MANAGER R6 VE VAPP
272695	Agile Communication Environment	ACE R6 VE VAPP
272750	Secure Access Link	SAL R2 STDALN GATEWAY VE VAPP
272801	WebLM	AVAYA WEBLM VE VAPP

Upgrade strategies

The following table describes the appliance vs. VMware upgrade strategies for each product.

Product	Server/Appliance upgrade process	VMware upgrade process
Agile Communication Environment™	New installation for Agile Communication Environment™	New installation for Agile Communication Environment™
Application Enablement Services	System Platform console, Application Enablement Services CLI commands	Application Enablement Services CLI commands
Communication Manager	System Platform console	New installation with translation migration
Presence Services	System Platform console, Presence Services CLI commands	Presence Services CLI commands
SAL Gateway	SAL CLI commands	SAL CLI commands
Session Manager	Session Manager CLI commands	Session Manager CLI commands
System Manager	System Platform console	System Manager CLI commands (data migration)
Utility Services	System Platform console	Utility Services CLI commands
WebLM	Not applicable. WebLM is not a separate product.	WebLM CLI commands

Chapter 3: Design considerations

Caveats and limitations

The Virtualized Environment solution is available to Service Providers, System Integrators, Authorized Partners, Certified Partners, Subject Matter Experts, and Service Delivery Specialized Partners. The solution can be ordered directly from Avaya or through a distributor.

The virtualized Avaya Aura® portfolio provides equivalent features and functionality as the appliance-based versions with the exception of management functions. Management functions were modified to support the VMware environment.

Avaya Aura® Virtualized Environment Release 1.0 only supports the specific product releases that are listed in each product requirements table.

Avaya and Business Partners access the Avaya Aura® virtualized products through the Secure Access Link (SAL).

Avaya continues to support the Avaya Aura® installation and services of applications, but the customer or certified Business Partner supports the VMware interfaces.

DVDs are not shipped.

Licensing

All software and licenses are available from the Avaya Product Licensing and Download System (PLDS).

Customers can move licenses from an appliance-based model to a virtual appliance of the same product. There is no charge for the software application. Licensing charges apply for appliance installations (licenses for new users, new features, expanded systems).

The virtual applications can use the WebLM infrastructure that is in place today.

Each OVA has a distinct ordering material code and is only available for the current versions of each OVA. See Material codes on page 18 for the list of applications and their material codes.

Virtualized Environment uses the Avaya Solution Designer (ASD) tool to quote and order the configuration.

All applicable licensing remains the same as it is today. No third-party licensing is required. Note that WebLM and SAL currently are not licensed applications.

Business Partners purchase virtual appliance licenses they install from Avaya using the same processes that are used for Avaya applications which are distributed in non-VMware environments.

Avaya does not provide VMware licenses on the virtual appliance.

WebLM provides licensing for the Avaya Aura® products. Each instance of Communication Manager requires its own WebLM instance. Multiple instances of WebLM may need to be deployed in a large enterprise environment.

Authentication files and ASG access

To provide full security, the authentication file must be changed on each application that is capable of accepting a unique file. To obtain the authentication file, log in to the Remote Activation Feature (RFA) website at http://rfa.avaya.com and access the Authentication File System (AFS) application.

Applications requiring an authentication file from the AFS are:

- Communication Manager (duplex and simple)
- Session Manager
- Utility Services
- WebLM
- System Manager

The authentication file installation is based on the installation model of the particular virtual application. See the deployment guide for a specific product for the AFS installation procedures.

Application Enablement Services, Presence Services, and Agile Communication Environment do not support the authentication files or Access Security Gateway (ASG) model.

Potential issues

Potential issues which could cause problems in the Virtualized Environment include:

- Server setup, server administration, and the VMware infrastructure are not under control of Avaya.
  - A virtual machine could be starved and not be able to provide Service Level Agreement (SLA).
  - Resources could be over-subscribed.

- Server BIOS could not be optimized.

- The VMware infrastructure can be modified by customer data center staff. A changed value could cause the system to not work properly.
- Servicing is more complex:
  - Is the problem related to the infrastructure (hardware or VMware)?
  - Is the problem related to the operating system?
  - Is the problem related to the application or software?

Feature and capacity differences

The following table describes the feature and capacity differences between an Avaya Virtualized Environment appliance and an Avaya Aura® appliance.

Product	Avaya Virtual Appliance (VE)	Aura Appliance
Communication Manager	• Communication Manager supports Avaya Aura® Contact Center Release 6.3 Service Pack 10. • Communication Manager does not support Communication Manager Messaging at this time. • The G250, G350, G430, G450, G650, and G700 Media Gateways are supported. • There is no virtual appliance for survivable remote (most of G-series gateways). Current hardware is supported.	
Session Manager	• Does not support virtual appliance for survivable remote (Branch Session Manager , most on G-series gateways).	

Agile Communication Environment™ (including Application Integration Engine)	• 15,000 users supported. • VMware HA (cold reboot) supported. • Avaya Media Server (AMS) on VMware is not supported.	• 15,000 users supported. • Agile Communication Environment HA offer (warm reboot) supported. • AMS is required to be on a separate server.
Application Enablement Services	• VMware HA (cold reboot) is supported. • Application Enablement Services supports Avaya Aura® Contact Center 6.3 SP10.	Machine Preserving HA (MPHA) hot standby offer is supported.
System Manager	No differences.	No differences.
Utility Services	No differences.	No differences.
WebLM	No differences.	No differences.

Virtualized Environment Footprint Flexibility

Virtualized Environment applications provide a fixed profile based on maximum capacity requirements. However, many customers require only a fraction of the maximum capacity.

Certain applications in the Virtualized Environment solution offer a flexible footprint profile based on the number of users that are supported. The customer can configure VMware CPU and RAM of a virtual machine according to a particular capacity line size requirement.

The applications that currently support Virtualized Environment Footprint Flexibility are:

- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

Average network and disk utilization

Certain virtual applications were tested at a high capacity. An average was determined for network and disk use for each application. The following table contains the name of the virtual

application that was tested at a high capacity, the average number of kilobits per second for network use, and the average number of disk input/output operations per second.

The average numbers for your system may differ.

Application Name	Network Usage	Average I/OPS
Application Enablement Services	75 Kbps	6
Communication Manager	3500 Kbps	4
Session Manager	3400 Kbps	7

Solution use cases and capacities

The Avaya Aura® Virtualized Environment product line addresses a broad section of the enterprise market, crossing several segments. The low end of the addressable market starts at the midsize with a user count of approximately 500 users. The high end of the market is characterized by Global Enterprise corporations with up to 250,000 endpoints and hundreds of locations worldwide with global contact center requirements.

The constants throughout the use cases are the following:

- A single corporate center where the Avaya Aura Core operates in a redundant configuration.
- At least one branch of a single of each type: Local Survivability and Midsize Enterprise
- A mix of endpoints that include:
    - Avaya 96xx-series and 96x1-series phones with One-X
    - Flare endpoints on Apple iPad, Windows/PC, and Avaya ADVD
    - One-X Software Clients on PC
    - Integration with MS MOC and OCS/Lync
    - A small percentage of HD video and Audio
- Audio, Video, and Web conferencing

Use Case 1: Large Global Enterprise

Application Core Configuration: includes Communication Manager, Session Manager, Application Enablement Services, and Presence Services with the Communication Manager duplication feature.

Endpoint configuration:

- Capacity is about 100K (3 Communication Managers at 36K per Communication Manager) all capable of standard IP telephony.
- 40% of endpoints are capable of video.
- 20% of video endpoints are capable of HD video.
- 25% of endpoints use soft clients along with a standard IP phone.
- 50% of endpoints use “extension to cellular” capabilities.

Corporate Center Configuration:

- 10,000 of the endpoints are at the Corporate Center have (LAN access to the facility housing the Aura Core applications).

Call Center Configuration:

- There are 5 call centers in 5 different time zones worldwide.
- Each call center houses 1000 IP Agents (5000 IP Agents total).
- The call centers are in a “follow the sun” configuration where two are “active” at all times (2000 IP Agents active concurrently).

Branch Configuration:

- 20 Branches of 400 endpoints. Half of these are Midsize Enterprise configurations and half are LSP configurations.
- 20 Branches of 200 endpoints. All branches are Survivable Remote Configurations.
- 20 Branches of 100 endpoints. All branches are Survivable Remote Configurations.

Trunk Capacities:

- Trunks at corporate center can be oversubscribed 6:1
- Trunks at call centers can be oversubscribed 2:1
- Trunks at branches can be oversubscribed 6:1

Use Case 2: Global Enterprise

This enterprise is smaller than the previous example. It is also less dispersed. Application Core Configuration includes Communication Manager, Session Manager, Application Enablement Services, and Presence Services.

Endpoint Configuration:

- Capacity is about 20,000 (1 Communication Manager) all capable of standard IP telephony.
- 40% of endpoints are capable of video.
- 20% of video endpoints are capable of HD video.
- 25% of endpoints use soft clients along with a standard IP phone.
- 50% of endpoints use “extension to cellular” capabilities.

Corporate Center Configuration:

- 5000 endpoints are at the Corporate Center (have LAN access to the facility housing the Aura Core applications).

Branch Configuration:

- 20 Branches of 400 endpoints. Half of these are Midsize Enterprise configurations and half are LSP configurations.
- 20 Branches of 200 endpoints. All branches are LSP Configurations.
- 20 Branches of 50 endpoints. All branches are LSP Configurations.

Use Case 3: Global Enterprise

Application Core Configuration: Communication Manager, Session Manager, Application Enablement Services, and Presence Services with the Communication Manager Duplication Feature.

Endpoint Configuration:

- Capacity is 2000, all capable of standard IP telephony.
- 40% of endpoints are capable of video.
- 20% of video endpoints are capable of HD video.
- 25% of endpoints use soft clients along with a standard IP phone.
- 50% of endpoints use `extension to cellular`capabilities.

Corporate Center Configuration:

- 500 endpoints are at the Corporate Center (have LAN access to the facility housing the Aura Core applications).

Call Center Configuration:

- There are 2 call centers in 2 different time zones nationwide (USA).
- Each call center houses 100 IP Agents (200 IP Agents total).
- The call centers are in a “follow the sun” configuration where one center is “active” at all times (100 IP Agents active concurrently).

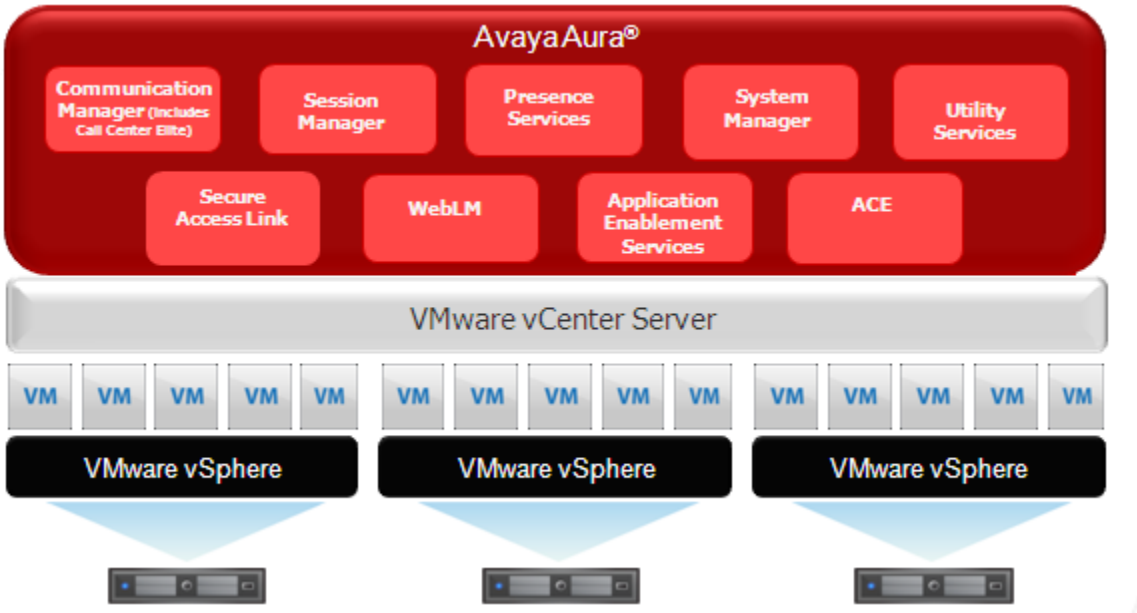
Branch Configuration:

- 10 Branches of 100 endpoints. All branches are LSP configurations.
- 6 Branches of 50 endpoints. All branches are LSP Configurations.

Chapter 4: Topology

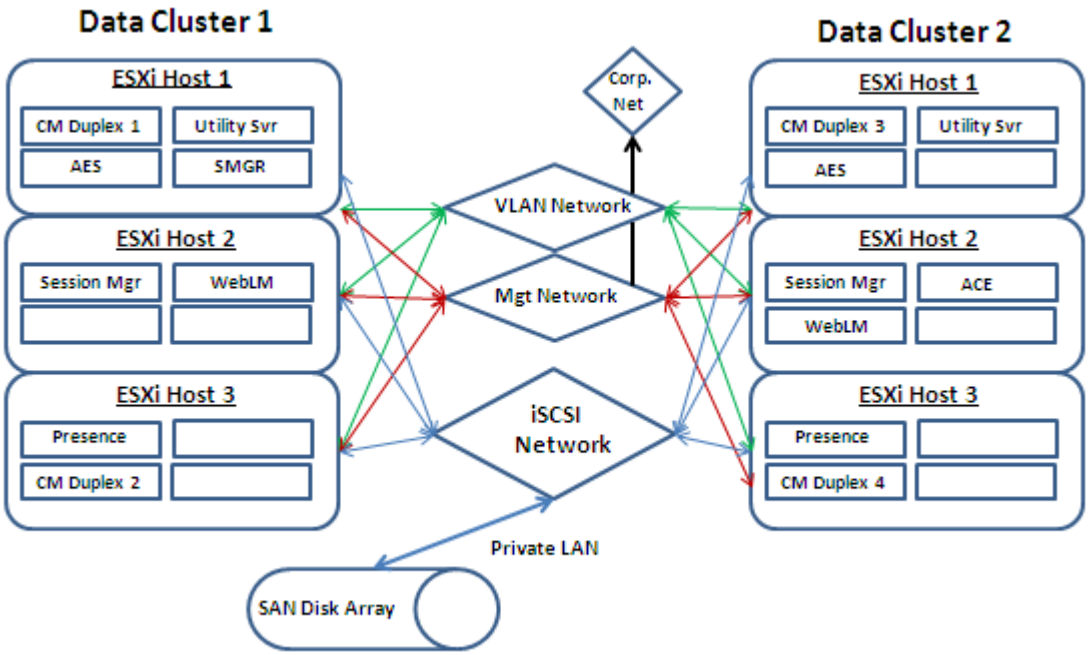
Avaya Aura® Virtualized Environment

The following diagram shows the Avaya Aura® applications supporting virtualization with VMware.



The Avaya Aura® applications are installed as separate virtual machines. The VMware virtualization platform, VMware vSphere, supports the virtual machines. The VMware vCenter Server management system manages the applications as virtual machines and provides management and implementation features in addition to the standard System Manager features.

Example ESXi Configuration

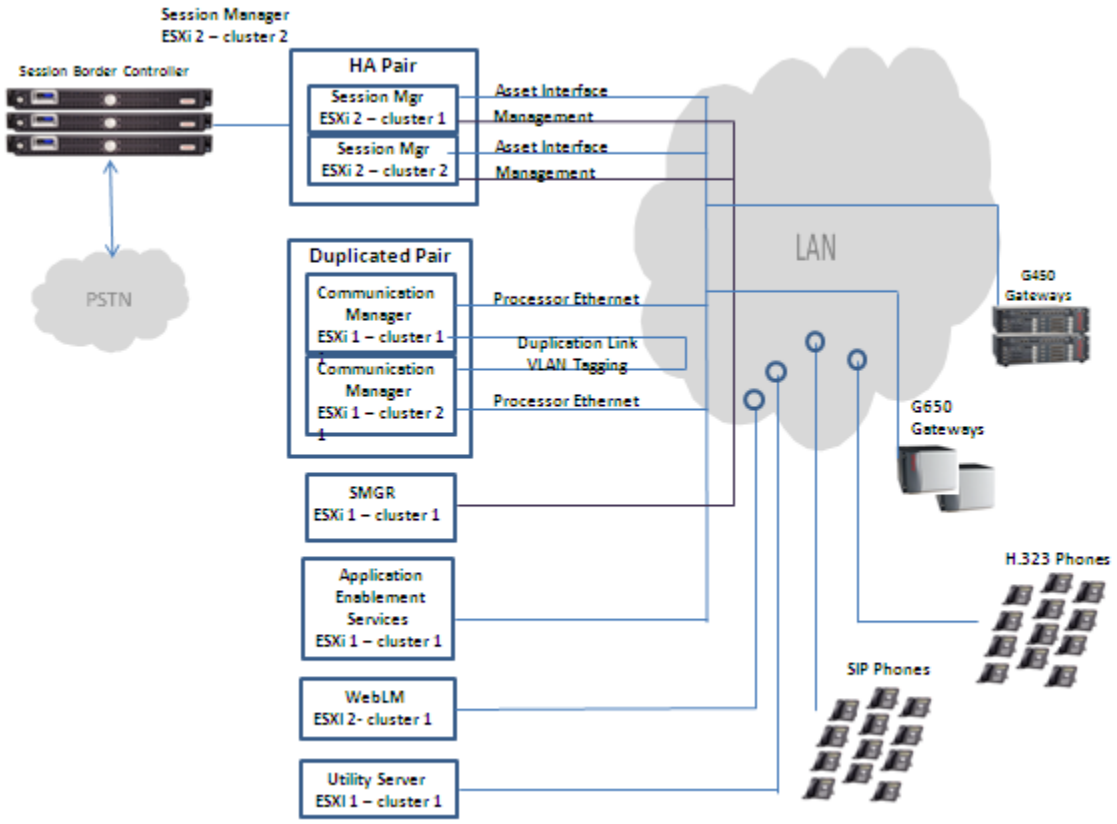


Network configuration notes:

- iSCSI:
  - Configured as VMware best practices recommends on a private and separate network.
  - In this environment, supporting vMotion activity.
- VLAN: supports all virtual application network interfaces.
- Management:
  - Interface between ESXi hosts and vCenter.
  - Command changes, for example HA enablement, are routed via this path.

Typical High Availability configuration

The following diagram is a logical depiction of the previous figure.



Example for estimating a solution footprint

When you are estimating a solution for a customer, note the following:

- You cannot fully load vCPUs due to ESXi overhead. Features such as vMotion and VMware HA require capacity.
- Actual CPU reservation is in MHz (vCPU x minimum CPU speed).
- VMware ESXi allows power up to only ~90% of the actual physical CPUs. Intel (hyper-threading) is handled differently than AMD.
- Each customer situation will be different.

The following section defines each product and its required footprint and resources per virtual machine. By multiplying the footprint of each VM with the quantity that is shown in the **# copies** column, you can estimate what will fit in a customer's situation (for example, server/host/cluster).

Note:

CM sw-dup requires two virtual machines. Only one copy of the software is required and can be used on both virtual machines.

Product	vCPUs per product VM	Mem (GB) per VM	Storage (GB) per VM	vNIC per VM	# copies	Total vCPU	Total Mem (GB)	Total Storage	Total vNIC
CM 6.2 sw-dup	3	5	30	2	1	6	10	60	4
SM 6.2	8	12	150	2	1	8	12	150	2
AES 6.2	4	4	20	1	1	4	4	20	1
PS 6.1	8	8	82	1	0	0	0	0	0
US 6.2	1	1	20	1	1	1	1	20	1
SMGR 6.2	4	6	70	1	1	4	6	70	1
WebLM 6.2	1	1	10	1	0	0	0	0	0
ACE 6.2	4	12	150	1	0	0	0	0	0
SAL 2.2	2	2	40	1	0	0	0	0	0
Solution Total						23	33 GB	320 GB	9
Total available						**24**	**96 GB**	**10 TB**	**NA**
This example uses a server with four sockets (each hex cores). 4x6 = 24 physical cores 96 GB RAM External SAN with 10 TB									

Chapter 5: Resource requirements and references

All Avaya Aura® virtual applications meet VMware Ready status. This status designates the highest level of endorsement from VMware for products and solution created by established partners such as Avaya. See http://www.vmware.com/partners/vmware-ready/home.html for more information regarding the VMware Ready Program.

Each Avaya Aura® application has individual resource requirements that must be met to run successfully on VMware. The following sections contain high-level resource requirement information for each application and a list of references to certain procedures regarding the application.

Note:

In the following tables, note the following:

- **vCPU** = the number of virtual machine CPU(s).
  - With Intel hyper-threading, there are two vCPUs per physical core/CPU.
  - With AMD, there is one vCPU per physical core CPU.
- The **minimum CPU speed** is based on Xeon E5620 or equivalent.

Server hardware and resources

VMware offers compatibility guides that list 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.

Agile Communication Environment™ resource requirements

Agile Communication Environment™ (ACE) and Application Integration Engine (AIE) were combined in Release 6.2 as a virtual appliance. AIE is not depicted in the nomenclature of the product.

Virtualized Environment Resource requirements for ACE	
Agile Communication Environment™ software	Release 6.2
Capacity (users)	4K
Virtual CPU reservation	4 @ 9320 MHz
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.3 GHz
Virtual Memory	12 GB
Virtual storage	150 GB
Shared NICs	1 @ 1000 Mbps

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Agile Communication Environment™ Planning and Installation*	Avaya ACE Migration
Migration	*Avaya Agile Communication Environment™ Planning and Installation*	Avaya ACE Migration
Upgrade (as a new install with ACE data restored from 5.x or 6.x)	*Avaya Agile Communication Environment™ using VMware® in the Virtualized Environment Deployment Guide*	Migration

Application Enablement Services resource requirements

Virtualized Environment Resource requirements for AES	
Application Enablement Services software	Release 6.2 / Release 6.3
Capacity (users) – 2.4K endpoints or 12K MOC/LCS	Virtual CPUs: 2 Virtual Memory: 2 GB Virtual Storage: 20 GB Minimum CPU speed: 2.4 GHz (based on Xeon E5620 or equivalent processor)
Capacity (users) – 4K endpoints or 20K MOC/LCS	Virtual CPUs: 4 Virtual Memory: 4 GB Virtual Storage: 20 GB Minimum CPU speed: 2.4 GHz (based on Xeon E5620 or equivalent processor)
CPU reservation	9600 MHz
Shared Network Interface Cards	1 @ 1000 Mbps
Average I/OPS	6
Average network usage	75 Kbps

Network Mapping	
AES VM Interface	**Application**
Eth0	AES Management and CM traffic in single NIC configuration
Eth1 (optional — recommendation is 2 CPUs X 2 GHz)	AES-CM traffic in dual NIC configuration

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® Application Enablement Services using VMware® in the Virtualized Environment Deployment Guide*	Backing up the AE Services server data
Migration	*Avaya Aura® Application Enablement Services using VMware® in the Virtualized*	Migrating

	Environment Deployment Guide	
Updating/patching	*Avaya Aura® Application Enablement Services using VMware® in the Virtualized Environment Deployment Guide*	Updating AE Services
Upgrading	*Avaya Aura® Application Enablement Services using VMware® in the Virtualized Environment Deployment Guide*	Upgrading AE Services

Communication Manager resource requirements

Communication Manager is offered in both a simplex and a duplex configuration as a virtual application. The duplex Communication Manager environment operates as it does today.

The Communication Managervirtual application is offered as two separate OVA packages:

- Communication Manager simplex-only VM
- Communication Manager software duplication VM

The Communication Manager virtual application also supports the following:

- Communication Manager Survivable Core (formerly known as ESS).
- Communication Manager Survivable Remote (formerly known as LSP).

You can mix and match with Avaya System Platform-based products and branches, except for duplicated pairs. With the duplex OVA, the hardware/processors and all VM resources must be identical as well as on the same version of the hypervisor.

Note:

Communication Manager duplication bandwidth requires 1 Gbps for Communication Manager duplication link bursts. See *PSN003556u* at https://downloads.avaya.com/css/P8/documents/100154621 for more information regarding Communication Manager duplication bandwidth.

Virtualized Environment Resource requirements for Communication Manager	
Communication Manager software (includes Call Center Elite)	Release 6.2 / Release 6.3
Branches supported	Survivable Core and Survivable Remote

Capacity: 36K users – Simplex	Release: 6.2/6.3 Virtual CPUs: 1 Virtual CPU reservation: 2400MHz Virtual memory: 4 GB Virtual storage: 30 GB Minimum CPU speed: 2.4 GHz (based on Xeon E5620 or equivalent processor) Shared NICs: One @ 1000 Mbps
Capacity: 30K users – Software duplication	Release: 6.2/6.3 Virtual CPUs: 3 Virtual CPU reservation: 7200MHz Virtual memory: 5 GB Virtual storage: 30 GB Minimum CPU speed: 2.4 GHz (based on Xeon E5620 or equivalent processor) Shared NICs: Two @ 1000 Mbps
Capacity: 36K users – Software duplication	Release: 6.2/6.3 Virtual CPUs: 3 Virtual CPU reservation: 8700MHz Virtual memory: 5 GB Virtual storage: 30 GB Minimum CPU speed: 2.9 GHz (based on Xeon E5620 or equivalent processor) Shared NICs: Two @ 1000 Mbps
Average I/OPS	4
Average Network usage	3500 Kbps **Note:** Communication Manager duplication bandwidth requires 1 Gbps for Communication Manager duplication link bursts.

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*	Creating a backup
Patching	*Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*	Communication Manager patches

Migration	*Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*	Migrating Communication Manager to the Virtualized Environment
Upgrade	*Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*	Upgrading Communication Manager Open Virtual Application

Presence Services resource requirements

Virtualized Environment Resource Requirements for Presence Services	
Presence Services software	Release 6.1 / Release 6.2
Capacities	See the *Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide* for a complete list of the capacities and requirements.
Shared Network Interface Cards	1 @ 1000Mbps

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide*	Backup and restore
Migration	*Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide*	Migration
Patches/updates	*Avaya Aura® Presence Services Service Pack Release Notes*	
Upgrade (as a new install with Presence Services data restored from 5.x/6.x)	*Implementing Avaya Aura® Presence Services*	Upgrading

Changing Presence Services network identity	*Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide*	Changing Presence Services Network Identity

SAL Gateway resource requirements

Virtualized Environment Resource requirements for SAL Gateway	
SAL Gateway software	Release 2.2
Capacity	500 Elements
Virtual CPU	2
Virtual memory	2 GB
Virtual storage	40 GB
Minimum CPU speed based on Xeon E5620 or equivalent processor	2 GHz
Shared NIC	1 @ 1000Mbps

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Secure Access Link Gateway using VMware® in the Virtualized Environment Deployment Guide*	Backing up and restoring the virtual machine
Upgrade	*Avaya Secure Access Link Gateway using VMware® in the Virtualized Environment Deployment Guide*	Upgrading the SAL Gateway OVA

Session Manager resource requirements

Virtualized Environment Resource requirements for Session Manager

Session Manager software	Release 6.2 or Release 6.3
Capacities	See the *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* for information regarding capacities and resource requirements.
Network Interface Cards	Four virtual NICs @ 1000 Mbps, used for management and asset.
Average I/OPS	7
Average network usage	3400 Kbps

Network Mapping	
Session Manager VM Interface	**Application**
Eth0	Management
Eth1	Services Port (not used)
Eth2	Asset (SIP)
Eth3	Asset Bonding NIC

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide*	Accessing the backup and restore service
Migration	*Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide*	Migrating Session Manager
Patches and service packs	*Installing Service Packs for Avaya Aura® Session Manager*	
Upgrade	*Upgrading Avaya Aura® Session Manager*	
Changing network identity	*Maintaining and Troubleshooting Avaya Aura® Session Manager*	Changing the Session Manager IP address or host name

System Manager resource requirements

Any and all upgrade restrictions that exist today for System Manager remain in effect for the virtual appliance. Upgrades from applications with or without System Platform must perform a native backup and restore, similar to a new installation.

System Manager supports user interface and command line interface-based patching. Since the user interface will not be available using CLI access with validations, support personnel must execute the patch or install the service pack.

Virtualized Environment Resource requirements for System Manager	
System Manager software	Release 6.2 or Release 6.3
Capacity	250K users and 50 administrators simultaneously
Virtual CPUs	4
Virtual memory	Release 6.2: 6 GB Release 6.3: 9 GB
Virtual Storage	72 GB
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHz
Shared Network Interface Cards	1

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide*	Backup and restore System Manager data
Patches and updates	*Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide*	Installing the System Manager service pack or patch from CLI
Upgrade (as a new install with System Manager data restored from 5.x or 6.x)	*Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide*	Upgrading System Manager
Changing network identity	*Avaya Aura® System Manager using VMware® in*	Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI

	the Virtualized Environment Deployment Guide	

Utility Services resource requirements

Virtualized Environment Resource requirements for Utility Services	
Utility Services software	Release 6.2 or Release 6.3
Capacity	Supports 5K IP endpoints
Virtual CPU	1
Virtual Memory	1 GB
Virtual Storage	20 GB
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHz
Shared NIC(s)	One @ 1000 Mbps

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya Aura® Utility Services using VMware® in the Virtualized Environment Deployment Guide*	Avaya ACE Migration
Patches and updates	*Avaya Aura® Utility Services using VMware® in the Virtualized Environment Deployment Guide*	Updating patches and service packs
Change network identity	*Avaya Aura® Utility Services using VMware® in the Virtualized Environment Deployment Guide*	Post deployment reconfiguration.
Upgrade (as a new install with Utility Services data restored from 5.x or 6.x)	*Avaya Aura® using VUtility ServicesMware® in the Virtualized Environment Deployment Guide*	Upgrading the Utility Services virtual machine

WebLM resource requirements

The current software licensing structure remains the same for Virtualized Environment. Any application that uses WebLM for licensing continues to do so with the same functionality and services.

Eth0 is used for License Management.

Requirements for WebLM with Virtualized Environment	
WebLM software release	Release 6.2 / Release 6.3
Capacity	5K simultaneous requests
Virtual CPU	1
Virtual memory	1 GB
Virtual storage	30 GB
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHz
Shared Network Interface Cards	1

Documentation		
Procedure	**Document**	**Chapter/Section title**
Backup/restore	*Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide*	Performing WebLM backup
Patches and service packs	*Avaya Agile Communication Environment™ Planning and Installation Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide*	Installing a WebLM patch or a WebLM service pack
Changing the network identity	*Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide*	Changing the IP, FQDN, DNS, Gateway, or Netmask addresses

Appendix A: VMware Best Practices

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.

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.

VMware networking best practices

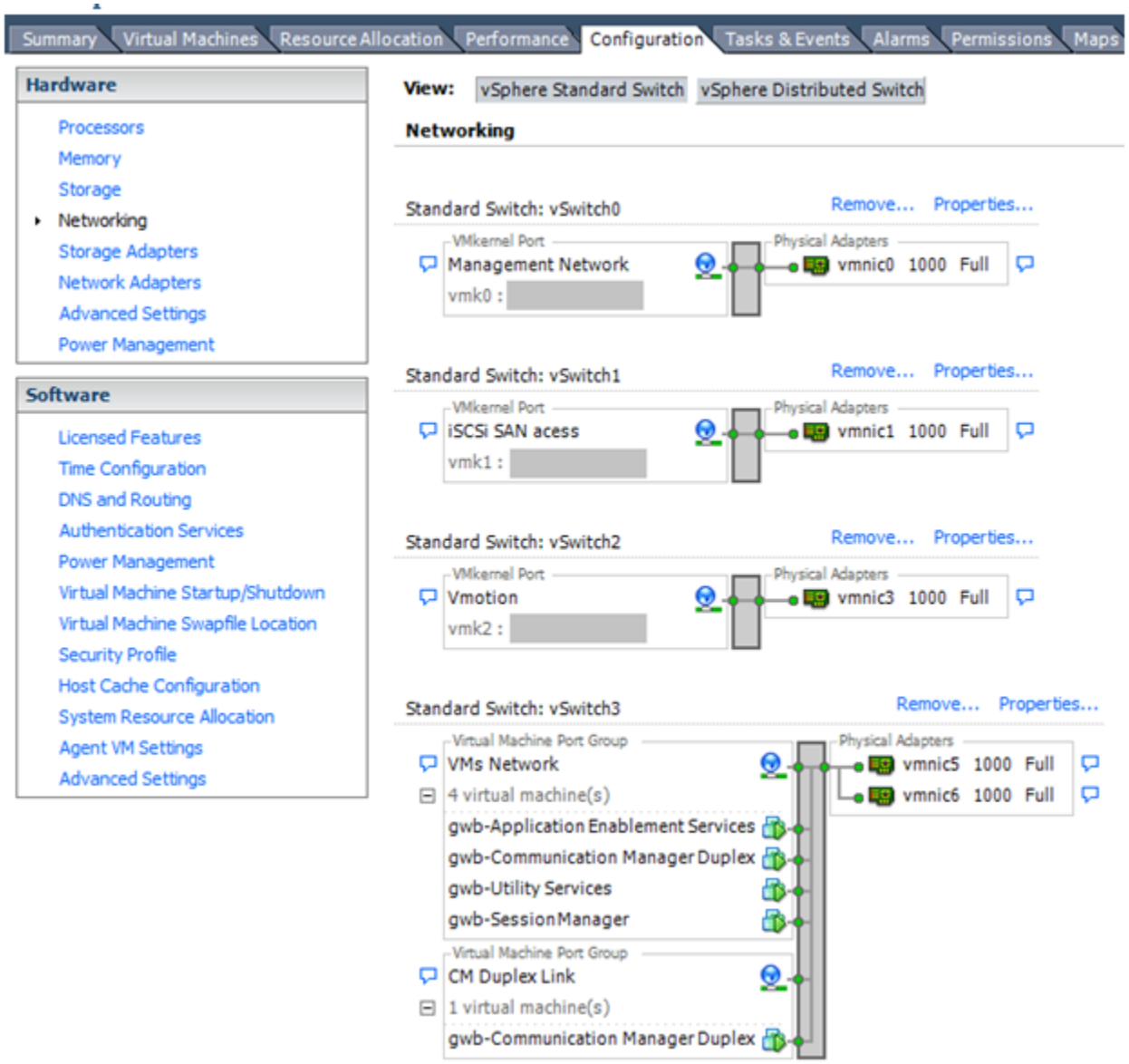
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities and are not the only supported networking configurations.

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

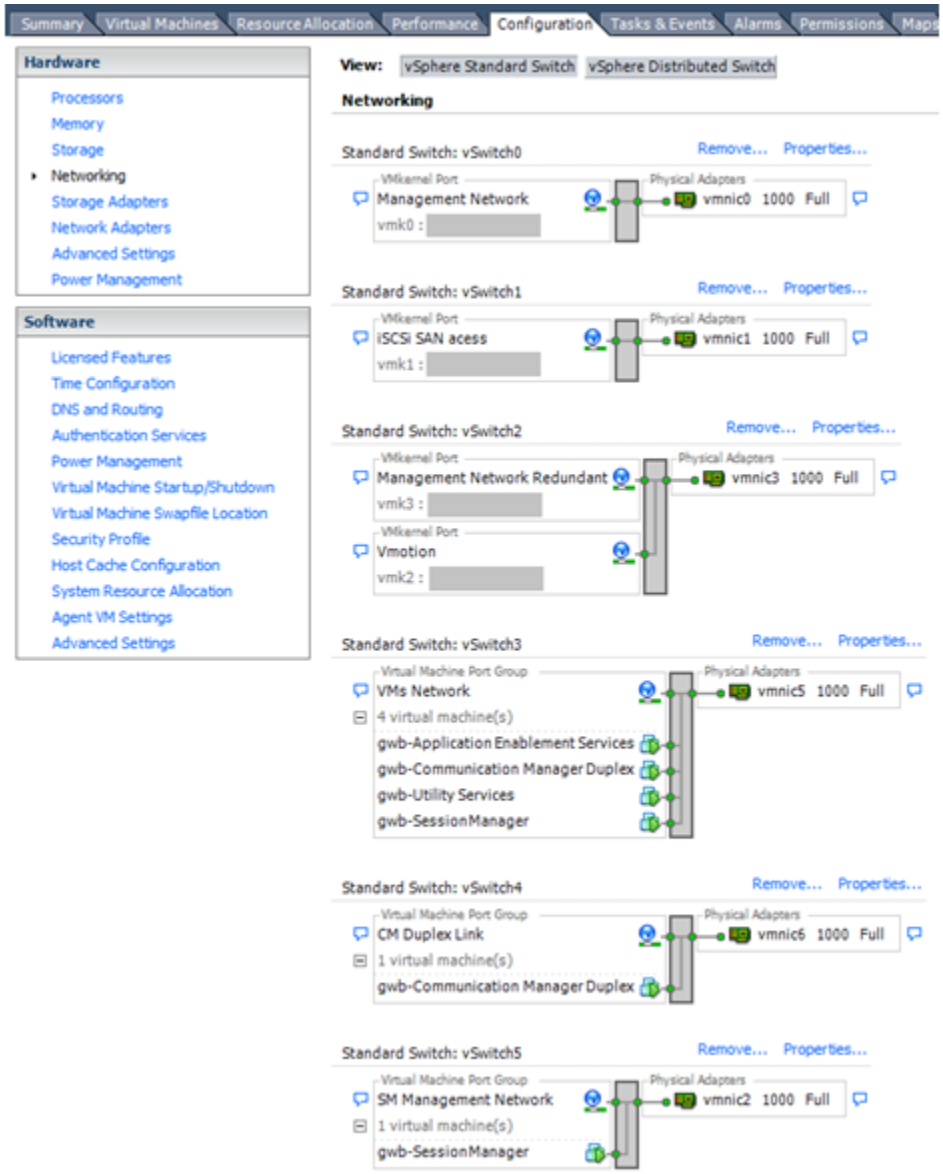


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- 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.
- 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

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.

Best Practices for VMware features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshot is a short-term copy of the running system that 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 uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a **hot-migration**, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can

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

Before using vMotion, you must:

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

VMware Storage vMotion

VMware Storage vMotion migrates virtual machine disk files within and across storage arrays while maintaining continuous service availability.

Features of Storage vMotion include:

- simplification of storage array migrations and storage upgrades.
- dynamic optimization of storage I/O performance.
- efficient utilization of storage and capacity management.

VMware High Availability

VMware vSphere High Availability (HA) provides automatic detection of hardware failures, server failures, and operating system failures. In the event of a physical server failure, affected virtual machines are automatically restarted on other production servers with spare capacity. In the case of an operating system failure, vSphere HA restarts the affected virtual machine on the same server.

VMware HA ensures that capacity is always available to restart all virtual machines affected by a server failure. HA continuously and intelligently monitors capacity utilization and reserves spare capacity to restart virtual machines.

VMware HA helps VMware vSphere users identify abnormal configuration settings detected within HA clusters. The VMware vSphere client interface reports relevant operating status and potential error conditions with suggested remediation steps.

See the VMware website: http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf for more information about VMware HA.

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

A

Access Security Gateaway 22
audience 7
Authentication File System 22
authentication files 22
Avaya System Design Tool 21
average disk utilization 24
average network utilization 24

B

best practices 47
  networking 47
BIOS 45
BIOS for Dell servers 46
BIOS for HP servers 46

C

capacities 25
capacity differences 23
  application and VE 23
caveats 21
clones 17
  deployment 17
Collaboration Pod 15
components 13
  VMware 13
customer requirements 12

D

deploying copies 17
deployment 50
  thick 50
  thin 50
deployment guidelines 16
Distributed Resource Scheduler 17
document changes 7
documentation 8
DRS 17

E

engineering guidelines 14
estimating a footprint 31
ESXi configuration 30

F

feature differences 23
  application and VE 23
flexible footprint 24
footprint example 31
footprint flexibility 24

G

guidelines 16
  deployment 16

H

high availability 53
high availability configuration 30

I

Intel VT support 45
intended audience 7

L

licenses 21
licensing 21
limitations 21

M

material codes 18, 21
Mentor videos 9

N

networking best practices 47
NFS 17

O

overview 11

P

PLDS 21
potential issue causes 22
purpose 7

R

requirements 12, 33–36, 38, 39, 41–43
ACE 34
AES 35
Communication Manager 36
customer 12
resource 33
Session Manager 39
System Manager 41
Utility Services 42
WebLM 43
Presence Services 38
resource requirements 33
resources 33
server 33

S

SAL Gateway requirements 39
SAN 17
SAP material codes 18
server hardware and resources 33
snapshots 51
storage sources 17
storage vMotion 53
support 9
contact 9

T

thick deployment 50
thin deployment 50

U

upgrade strategies 19
use cases 25

V

videos 9
Mentor 9
Virtualized Environment 29
diagram 29
vMotion 52
VMware Tools 46
VT support 45

W

WebLM 21