Deploying Avaya Session Border Controller in Virtualized Environment

Release 6.3
Issue 2
August 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides installation, configuration, initial administration, and basic maintenance checklists and procedures.

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 have been made to this document since the last issue:

- Included content related to deploying single ova file. From Avaya SBCE Release 6.3.2, a single ova file is available for deployment.

Related resources

Documentation

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

Title	Description	Audience
Implementation		
Deploying Avaya Session Border Controller for Enterprise	Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Virtual installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 6.3	Implementation engineers
Maintenance and Troubleshooting		
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers, Administrators
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures	Implementation engineers, and Sales engineers
Reference		
Avaya Port Matrix: ASBCE 6.3	Port information	Implementation engineers, Administrators, and Sales engineers

Training

The following course is available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

  Note:

  Videos are not available for all products.

Support

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

Related Links

Using the Avaya InSite Knowledge Base on page 8

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a Web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Enter the product in **The InSite Knowledge Base** text box.
4. Click the red arrow to obtain the Search Results.
5. Select relevant articles.

Related Links

Support on page 8

Warranty

Avaya provides a one-year limited warranty on Avaya SBCE hardware and 90 days on Avaya SBCE software. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the support details for Avaya SBCE in the warranty period is available on the Avaya Support website http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Architectural overview

Virtualization architecture overview

For deployment on VMware-certified hardware, Avaya SBCE is packaged as vAppliance ready (OVA) to run in the virtualized environment. Therefore, from Release 6.3, Avaya SBCE is also available for VMware-based deployments.

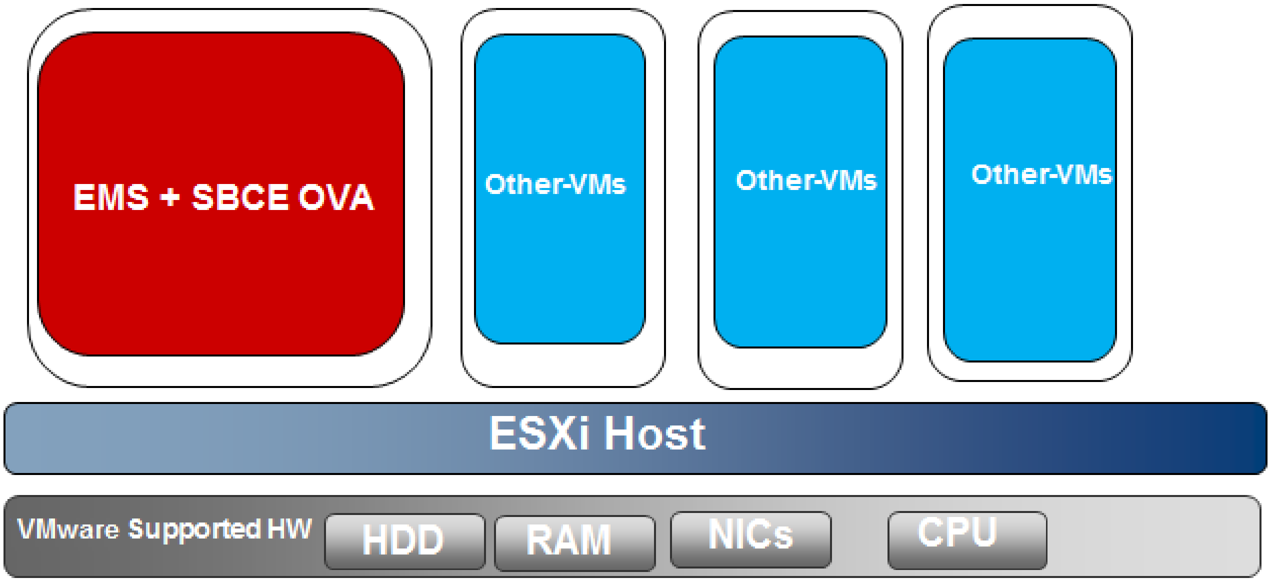
Avaya SBCE supports VMware features, such as vMotion, HA across data centers, and mixed hardware configurations.

The Avaya SBCE OVA files are offered as vAppliance for EMS and Avaya SBCE configurations. Use the EMS OVA file for EMS-only deployments. Use the Avaya SBCE OVA file for EMS plus Avaya SBCE or Avaya SBCE only deployments. The .ova file for each deployment is available in Product Licensing and Delivery System (PLDS).

From Release 6.3.2, a single ova file is available to deploy EMS and Avaya SBCE.

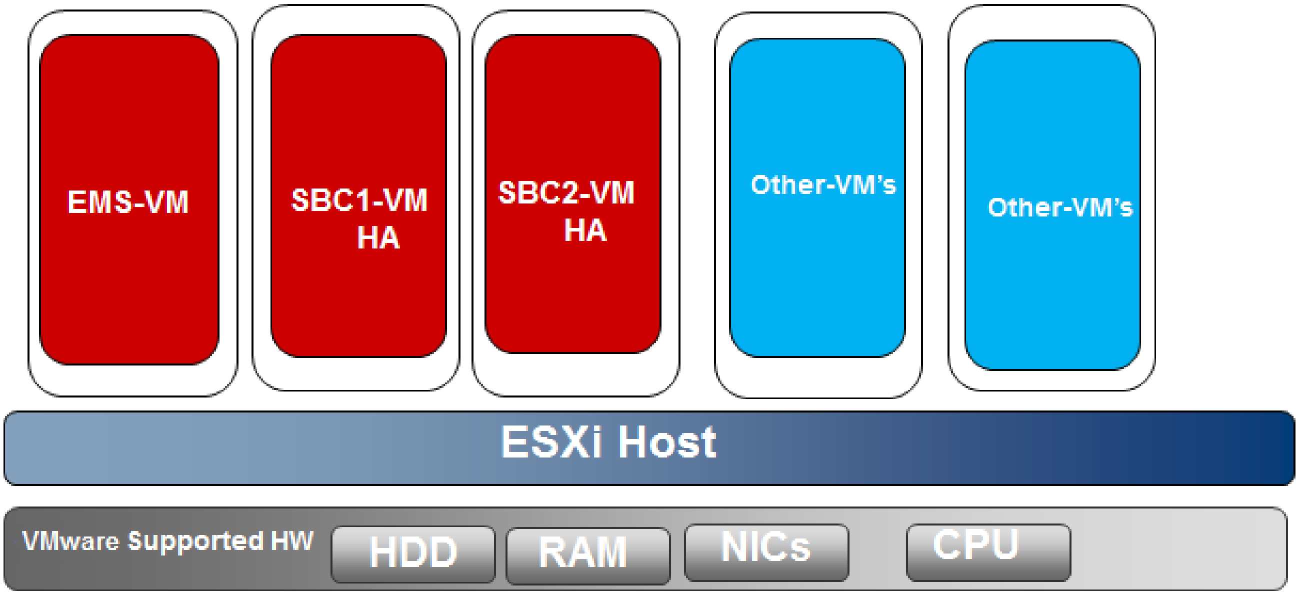
Avaya SBCE standalone mode

The OVA file for standalone deployments includes OVA configurations for both Avaya SBCE and EMS. For Avaya SBCE mode, use the Avaya SBCE OVA file for installation. From Release 6.3.2, you can use the single ova file for both standalone and Avaya SBCE deployments.



EMS and SBC in High Availability (HA) mode

For HA mode, use separate OVA files for EMS and Avaya SBCE.



Avaya Aura® Virtualized Environment Overview

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

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

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

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

Note:

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

- server and host
- reservations and configuration values

Customer deployment

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

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

Software delivery

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

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

Patches and upgrades

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

Important:

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

Performance and capacities

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

Caution:

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

Chapter 3: Planning and preconfiguration

Supported software and hardware

Software

The virtualization feature insulates Avaya applications from the specifics of the underlying server hardware and its infrastructure.Avaya SBCE virtualized application provides the resource footprint such as memory, required number of CPUs, and NICS. For more information about hardware components compatible with VMware, go to http://www.vmware.com/resources/compatibility/search.php.

Hardware

You can deploy Avaya SBCE software on the following VMware software versions:

- VMware ESXi 5.1
- VMware ESXi 5.0
- VMware ESXi 5U1
- VMware ESXi 5.5

ESXi is specific about the hardware that it runs on. You can optimize the server resources as Hypervisor uses few resources. You can manage ESXi with VMware vCenter and set up clusters that support vMotion and high availability.

Avaya SBCE virtual machine resource reservation specifications

The Avaya SBCE virtual machine requires the following set of resources on the ESXi host before deployment:

Table 1: SBCE EMS OVA requirements on VMHost

VMware resource	Minimum value
vCPU core	3 floating cores
vCPU reservation	7200 MHz
Minimum CPU speed based on Xeon x5670 or equivalent processor	2.4 GHz
Memory reservation	4 GB or 8 GB

Table continues…

VMware resource	Minimum value
Storage reservation	160 GB
Shared NIC	2 @ 100 Mbps or 1000 Mbps

Note:

If the ESXi host does not have the minimum resources to allocate to the virtual machine, the system does not start the Avaya SBCE virtual machine.

Table 2: SBCE OVA requirements on VMHost (includes standalone EMS and SBCE)

VMware resource	Minimum value
vCPU cores	4 dedicated cores
vCPU reservation	9600 MHz
Minimum CPU speed based on Xeon x5670 or equivalent processor	2.9 GHz
Memory reservation	8 GB
Storage reservation	160 GB
Shared NIC	4 @ 1000 Mbps and 2 @ 100 Mbps or 1000 Mbps

Avaya SBCE Release 6.3.2 onwards, you can install EMS and Avaya SBCE by using a single OVA file. Depending on resource reservation, the following variants are available to configure Avaya SBCE:

- Small SBC: Resource reservation equivalent to Micro - Portwell CAD-0208
- EMS: Resource reservation required for running only EMS
- Large SBC: Resource reservation equivalent to standalone Avaya SBCE 310 model or Dell R210 II XL.

Avaya SBCE 6.3.2 onwards, virtual machine requires the following set of resources on the ESXi host before deployment:

Table 3: Avaya SBCE OVA requirements on VMHost

VmWare Resource	Variant		
	Small SBC	**EMS**	**Large SBC**
vCPU core	2 dedicated cores	3 floating cores	4 dedicated cores
vCPU reservation	3320 MHz to 4400 MHz	6600 MHz to 7200 MHz	8800 MHz to 9600 MHz
Minimum CPU speed based on Xeon x5670 or equivalent processor	1.66 GHz	2.2 GHz	2.2 GHz
Memory reservation	4 GB	8 GB	8 GB
Storage reservation	160 GB	160 GB	160 GB

Table continues…

VmWare Resource	Variant		
	Small SBC	EMS	Large SBC
Network Interfaces	4 Virtual Interfaces	2 @ 100 Mbps or 1000 Mbps	6 Virtual Interfaces

Server hardware and resources

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

Customer configuration data

The following table identifies the key customer configuration information that you must provide throughout the deployment and configuration process:

	Required data	Example
Network configuration	IP address	172.16.1.10
	Default netmask	255.255.0.0
	Default gateway	172.16.1.1
	DNS Server IP address	172.16.1.2
	Short host name	myhost. The host name must be a valid short name.
	Domain name	mydomain.com
	Default search list	mydomain.com
	NTP server	172.16.1.100
	Time zone	America/Denver

Deployment guidelines

The high-level deployment steps are:

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

The deployment guidelines for the virtual appliances are:

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

Important:

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

Deployment and configuration checklist

Use the following checklist to deploy the Avaya SBCE vAppliance by using vSphere:

#	Action	Description	Link	✔

1	Download the following Avaya SBCE ova and EMS ova files from the PLDS website at https://plds.avaya.com:
	`EMS-sbce-6.3.xxx-xx-xxxx.ova`
	`SBC-sbce-6.3.xxx-xx-xxxx.ova`			

2	High availability requires GARP support on the connected network elements. In scenarios where GARP is not supported, use a GARP-aware router or switch between the elements and Avaya SBCE for the switch to handle GARP packets sent from Avaya SBCE.	Applicable only to multiple server HA scenarios.		

Table continues…

#	Action	Description	Link	✔
3	Install vSphere Client 5.0, 5.1 or 5.5.	Download the third-party client from the VMware website.		
4	Keep the configuration data ready.		Customer configuration data on page 16	
5	(Optional) Download the authentication file from http://rfa.avaya.com.			
6	Create vSwitches.	Create virtual switches for M1, M2, A1, and B2 network.		
7	Deploy EMS OVA template.		Deploying SBCE on page 27	
8	Configure EMS.		Configuring EMS in text mode on page 22, Configuring EMS in CLI mode on page 24	
9	Configure EMS for network connectivity.		Configuring EMS for network connectivity on page 26	
10	Deploy Avaya SBCE OVA template.		Deploying SBCE on page 27	
11	Configure Avaya SBCE.		Configuring SBCE on page 29	
12	Configure Avaya SBCE for network connectivity.		Configuring Avaya SBCE for network connectivity on page 30	
13	Configure Avaya SBCE and EMS to start automatically after a power failure.		Configuring the virtual machine automatic startup settings on page 20	
14	Verify the installation of Avaya SBCE.			

Chapter 4: Deploying EMS OVA

Deploying EMS

Before you begin

- Install vSphere Client.
- Ensure that the computer on which vSphere Client is installed can access the VMware ESXi servers of all devices on the network.

Procedure

1. On the destination device, using a web browser download EMS ova from PLDS.

   From Release 6.3.2, Avaya SBCE has one ova file to deploy EMS and Avaya SBCE.

2. On vShpere Client, click **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, type the path to the downloaded .ova file.
   - Click **Browse**, navigate to the downloaded .ova file, and click **Next**.
4. On the OVF Template Details page, verify the details, and click **Next**.
5. On the End User License Agreement page, click **Accept**.
6. Click **Next**.
7. On the Name and Location page, in the **Name** field, type a name for the virtual machine.

   The virtual machine name must not exceed 25 characters. For example, EMS-6-2-SingleBox is an appropriate name.

   If you have logged in to vCenter, the system displays a Host/cluster selection page.

8. Select a host, and click **Next**.
9. On the Resource Pool page, click **Next**.
10. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you select and set the available space.

    Note:

    Use **Thin Provision** to minimize disk allocation. Use this option only in the lab environment.

11. Click **Next**.

12. In the Resource Allocation window, click **Next**.
13. On the Network Mapping page, in the **Source Network** column, map Network 1 to the management network in the **Destination Network** column.
14. Click **Next**.
15. Review the settings and click **Finish**.
16. Wait until the system deploys the EMS successfully.

Configuring the virtual machine automatic startup settings

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

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

Before you begin

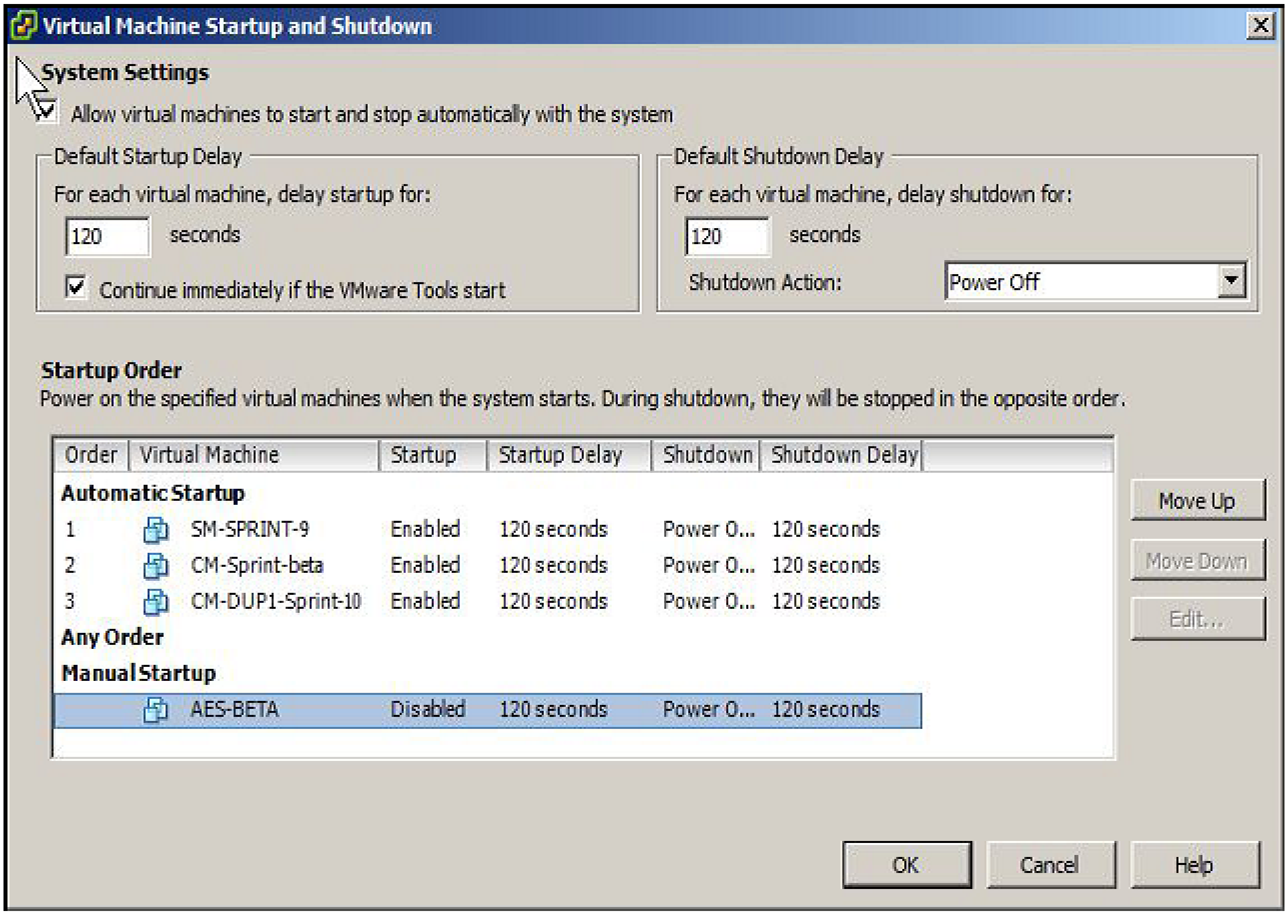
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

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

Example

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



System Settings

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

Default Startup Delay

For each virtual machine, delay startup for: 120 seconds

☑ Continue immediately if the VMware Tools start

Default Shutdown Delay

For each virtual machine, delay shutdown for: 120 seconds

Shutdown Action: Power Off

Startup Order

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

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

Configuring vSwitches on ESXi host

About this task

This task creates a vSwitch that you can assign to a virtualized Avaya SBCE SBCE interface.

Use this procedure to configure A1, A2, B1, B2, M1, and M2 interfaces.

Procedure

1. Log on to the ESXi host interface by using vSphere or vCenter client and click the **Configuration** tab.
2. In the Hardware section of left navigation pane, click **Networking** > **Add Networking**.
3. In the Add Network Wizard window, do the following:
    a. In the Connection Type page, select **Virtual Machine**.
    b. In the Network Access page, select **Assign Physical NIC to vSwitch**.
    c. In the Connection Settings page, in the select **Network Label** field, type an interface name.

   d. In the Connection Settings page, select the time zone.
   e. In the Connection Settings page, in the **VLAN ID (optional)** field, click the VLAN ID.
4. Click **Finish**.

Next steps

Note:

- For HA configuration, you require M2 interface for both Avaya SBCE systems. If the vSwitch is running on the same ESXi host, then the vSwitch for M2 interface does not require a NIC association. You must assign the same M2 vSwitch without NIC to both Avaya SBCE systems in HA mode, because M2 connection is on layer 2.
- If you want to use a specific interface through default VM Network, skip additional vSwitch configuration for the interface.

VSwitches for Avaya SBCE in High Availability

Deploying Avaya SBCE serves in high availability requires connecting M2 network interfaces of both the Avaya SBCE virtual machines. You must first create a virtual network not connected to any physical interface. Then assign M2 interfaces of both Avaya SBCE virtual machines to this virtual switch. For information about mapping the correct network interface to M2, see *Configuring Avaya SBCE for network connectivity*.

Note:

Both the Avaya SBCE virtual machines must reside on the same VMware host.

Configuring EMS

Configuring EMS in the text mode

Before you begin

Turn ON Avaya SBCE.

Procedure

1. When the system displays, **Enter your choice**, type `2` to configure in the text mode.
2. In the Select Device Type window, do the following:
   a. Select **EMS**. For a standalone box, select **EMS + SBC**.

      The system displays a confirmation message.
   b. Click **YES**.

      The system displays the `Installing as EMS device` message.
   c. Click **OK**.

3. On Device Configuration screen, do the following:
    a. Click **EMS Configuration**.
    b. Based on the deployment, select an installation type.
    c. Click **EMS Appliance Configuration**.

       The system displays the Appliance Configuration screen.
    d. In the **EMS Host name** field, type a name for the EMS host.
    e. In the **List of DNS Servers** field, type the IP address of the DNS server.
    f. Select a time zone.
    g. In the **NTP Server IP Address (ipv4)** field, type the NTP Server IP address.
    h. In the **Network Passphrase** field, type the passphrase.
    i. In the **Network Passphrase (Again)** field, retype the passphrase.
    j. Click **OK**.
4. Click **Management Interface Setup**.
5. Type appropriate values in the **management ip address (ipv4)**, **management network mask**, and **management gateway ip address (ipv4)** fields.
6. Click **OK**.
7. Based on the customer location, select the appropriate time zone.
8. Click **Configure self-signed certificate**.
9. Type appropriate values in the **first and last name**, **organizational unit**, **organization**, **city or locality**, **state or province**, and **country code** fields.
10. Click **OK**.
11. Return to the previous page.
12. Click **Done**.

Related Links

Configuring a time server on page 23

Configuring a time server

About this task

By default Avaya SBCE OVA synchronizes time with the NTP server of the ESXi host if the VMWare tools are installed and running on the system. To configure a different time server for Avaya SBCE, disable the SYNC options for VMware tools on the Avaya SBCE virtual machine. Perform this procedure when you have different NTP servers across locations and you need to configure these servers for different Avaya SBCE virtual machines.

Procedure

1. Select the virtual machine in the vSphere Client inventory and power it off.
2. In the **Summary** tab, click **Edit Settings**.

3. Click **Options** > **General**.
4. Click **Configuration Parameters**.
5. Click **Add Row** and enter the following information.
   - Name: *Value*
   - tools.syncTime: `0`
   - time.synchronize.continue: `0`
   - time.synchronize.restore: `0`
   - time.synchronize.resume.disk: `0`
   - time.synchronize.shrink: `0`
   - time.synchronize.tools.startup: `0`
   - time.synchronize.tools.enable: `0`
   - time.synchronize.resume.host: `0`

Related Links

Configuring EMS in the text mode on page 22

Configuring EMS in the CLI mode

About this task

Perform the procedure after you deploy EMS or SBCE ova.

Procedure

1. Deploy EMS and turn ON the EMS.
2. In the vSphere Client inventory, right-click a virtual instance of EMS and click **Open Console**.
3. Type `1` for the CLI mode and then press **Enter**.
4. When the system prompts, **Applicance Type**, type `EMS` and press **Enter**.
5. When the system prompts, **Enter Network Passphrase**, type the passphrase.
6. When the system prompts, **Application Name**, type application name and then press **Enter**.
7. When the system prompts, **Installation Type**, type primary or secondary, as applicable.
8. When the system prompts, network details, type the **Management IP address**, **Management Subnet mask**, **Management Gateway IP address**, **NTP Server IP address**, list of **DNS servers**, and **Domain suffix** and click **OK**.
9.

   The system displays the Device configuration screen.
10. Select the **Time Zone** option.

The system displays the Select Time Zone screen.

11. Select the appropriate time zone.

    The system displays the Device Configuration screen.

12. (Optional) Select the **Self-Signed Certificate** option.
13. (Optional) Enter the self-signed certificate details.

    The self-signed certificate is used to enforce Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) access for the web interface.

14. When the system displays, `Changing password for user root` `New password:`, type the new password and confirm the password.

    The system displays a message to confirm the timezone.

15. Type `Y` to continue or type `N` to enter the details again.
16. When the system displays, `Changing password for user ipcs` `New password:`, type the new password and confirm and confirm the password.

    The system prompts, `EMS login:`.

17. Log in using ipcs credentials.

Configuring the management interface

Before you begin

Turn ON Avaya SBCE.

About this task

Perform this task to assign an IP address to the EMS.

Procedure

1. On the Device Configuration screen, click **EMS Configuration** > **Management Interface Setup**.

    The system displays the Management Interface Setup screen.

2. In the **Management IP Address (ipv4)** field, type the IP address of the EMS server.
3. In the **Management Network Mask** field, type the subnet mask of the EMS server.
4. In the **Management Gateway IP Address (ipv4)** field, type the gateway IP address of the EMS server.
5. Click **OK**.
6. Click **Done**.

Configuring EMS for network connectivity

Before you begin

Configure EMS and management interface, and then power ON EMS.

Procedure

1. Configure password for root and ipcs users.
2. Log in to virtual machine using ipcs login and ipcs password.
3. To access root privileges, type `sudo su`.
4. To identify the MAC address is in use for M1 interface, type `ip address`.

   The **`ip addr | awk '/[ABM][12]:/ {dev=$2;getline;mac=$2;print dev,mac}'`** command displays concise results.
5. Note the MAC address.
6. Right-click on the EMS virtual instance, such as EMS -VM, and then click **Edit Settings**.
7. In the **Hardware** tab, in the **Network Adapter 1** field, confirm whether the MAC address matches with the MAC address that is displayed using the **`ip address`** command.
8. Select the vSwitch and then in the **Network label** field, click the appropriate network label for M1 to be available on network.
9. Click **OK**.

Chapter 5: Deploying Avaya SBCE OVA

Deploying Avaya SBCE

Before you begin

- Install vSphere Client.
- Ensure that the computer on which vSphere Client is installed can access the VMware ESXi servers of all devices on the network.

Procedure

1. On the destination device, log on to ESXi Host or vCenter using vSphere or vCenter Client by typing the IP address and the password for the ESXi host.

   Ignore any security warning that the system displays.
2. On vSphere Client, click **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, type the path to the .ova file.
   - Click **Browse** and navigate to the .ova file from the local computer, network share, CD-ROM, or DVD.

     ✱ **Note:**

     Choose appropriate template: SBC-sbce-xx format for SBCE or EMS+SBCE deployments.
4. On the OVF Template Details page, verify the details, and click **Next**.
5. On the End User License Agreement page, click **Accept**.
6. Click **Next**.
7. On the Name and Location page, in the **Name** field, type a host name for SBCE.

   The host name does not exceed 25 characters. For example, SBCE-6-2-SingleBox is an appropriate name.
8. Click **Next**.
9. On the Resource Pool page, click **Next**.

10. **(Optional)** To deploy Avaya SBCE 6.3.2 or later, by using a single ova file , in the **Configuration** field, click one of the following options:

    - Small SBC: For smaller deployments reserved with minimum resources. With the Small SBC option, you can achieve lower capacity, but some features such as HA will not work. For the Small SBC deployment option, the M1, A1, A2, and B1 interfaces are available.

    - Large SBC: For large deployments reserved with maximum resources. Using the Large SBC option is preferable when you require features such as HA. For the Large SBCE deployment option, the M1, M2, B1, B1, A1 and A2 interfaces are available.

11. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you select and the available space.

    ✱ **Note:**

    Use **Thick Provision Lazy Zeroed** for better usage of memory resources.

12. Click **Next**.

13. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, click the network for management interface.

    Map the source virtual machine network to the network for management interface. After installation, you can specify other networks for A1 or B1 interfaces.

    ✱ **Note:**

    By default, the Network mapping page displays one VM Network destination, as default. However, actual network interfaces are available post deployment. For SBCE, you can map six interfaces.

14. Click **Next**.

15. Review the settings and click **Finish**.

16. Wait until the system deploys the OVA file successfully.

17. Turn on the machine.

18. In the left-navigation pane, select the newly deployed virtual instance of the SBCE.

    Repeat steps 1 to 16 to deploy SBC1 and SBC2 templates for HA mode.

19. On the right pane, in the Getting Started tab, in the Basic Tasks section, click **Power on the virtual machine**.

    The system starts in factory reset mode.

Deployment of cloned and copied OVAs

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

Configuring Avaya SBCE

Configuring Avaya SBCE in the text or CLI mode

Before you begin

- Deploy EMS OVA and SBCE OVA, and then configure EMS.

Procedure

1. After you power ON, select the text mode or the CLI mode.
2. In the **Device type** field, click one of the following:
   - **SBCE**: To deploy Avaya SBCE on a separate EMS server.
   - **EMS+SBCE**: To deploy EMS and Avaya SBCE on the same server.
3. On the Device Configuration screen, click **EMS Configuration** > **EMS Appliance** > **Configuration**.

   The system displays the Appliance Configuration screen.
4. In the **Appliance name** field, type an appliance name.
5. In the **DNS IP address** field, type the DNS IP address.
6. In the **Network passphrase** field, type a passphrase and confirm the passphrase.
7. In the **Management interface** field, type a management interface.
8. Click **Done**.
9. When the system displays, **Enter the password**, type the password for root and ipcs users.
10. To access root privileges of the Avaya SBCE device, type `sudo su` to access root privileges.
11. In the root privileges, type the `ip address` command.

    The system displays all six mapping interfaces.
12. Verify the network adapters for A1, B1, M1, M2, A2, and B2 and note the MAC address for each interface.

13. In vSphere, right-click the Avaya SBCE instance and click **Edit Settings**.
14. In the **Hardware** tab, click the interface.
15. Click the appropriate virtual network interface for the Avaya SBCE virtual machine.
16. Click **OK**.

Configuring Avaya SBCE for network connectivity

Before you begin

Configure and power ON Avaya SBCE.

Procedure

1. Configure password for root and ipcs users.
2. Log in to virtual machine using ipcs login and ipcs password.
3. To access root privileges, type `sudo su` .
4. To identify the MAC address is in use for M1 interface, type `ip address` .

   The

   ```
   ip addr | awk '/[ABM][12]:/ {dev=$2;getline;mac=$2;print dev,mac}'
   ```

   command displays concise results.
5. Note the MAC address.
6. Right-click on the EMS virtual instance, such as EMS -VM, and then click **Edit Settings**.
7. In the **Hardware** tab, in the **Network Adapter 1** field, confirm if the MAC address matches with the MAC address that is displayed using the ip address command at step 3.
8. Select the vSwitch and then in the **Network label** field, click the appropriate network label for M1 to be available on network.
9. Click **OK**.

Chapter 6: Maintenance procedures

Snapshots

Snapshots capture the state of the virtual machine when you take the snapshot. To avoid problems, ensure that you take a snapshot when no applications in the virtual machine are communicating with other computers. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file. But when you revert to the snapshot, the file transfer fails.

⚠ **Warning:**

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, you can then restart or set the application back into service.

Creating a snapshot

⚠ **Caution:**

Do not perform any activity on the virtual application until the snapshot backup is complete. Snapshot operations can adversely affect service.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Create snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the following steps accordingly.

Procedure

1. Select a virtual machine.
    - If you are using the vSphere Web Client:
        a. Search for a virtual machine and select it from the search results list.
        b. Stop the application that is running on the virtual machine or set to out-of-service.
        c. Right-click the virtual machine and select **Snapshot** > **Take Snapshot**.

- If you are using the vSphere Client:
    a. Stop the application that is running on the virtual machine or set to out-of-service.
    b. Click **Inventory** > **Virtual Machine** > **Snapshot** > **Take Snapshot**.

2. In the **Name** field, enter a name for the snapshot.
3. In the **Description** field, enter a description for the snapshot.
4. Disable **Snapshot the virtual machine's memory**.
5. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
6. Click **OK**.

    The system displays `Completed` to indicate that the snapshot backup is complete.

Deleting a snapshot

Note:

Differences exist between the vSphere Web Client versions. Modify the steps accordingly.

Before you begin

Verify the required privilege **Virtual machine.State.Remove snapshot** is available on the virtual machine.

Procedure

1. Open the **Snapshot Manger**.
    - If you are using the vSphere Web Client:
        a. Search for a virtual machine and select it from the search results list.
        b. Right-click the virtual machine and select **Snapshot** > **Snapshot Manager**.
    - If you are using the vSphere Client:
        a. Select **Inventory** > **Virtual Machine** > **Snapshot** > **Snapshot Manager**.
2. In the **Snapshot Manager**, click a snapshot to select it.
3. Select **Delete from Disk** to delete the single snapshot from the Snapshot Manager and the virtual machine.
4. Click **Yes** in the confirmation dialog box.
5. If you are using the vSphere Web Client, click **Close** to close the Snapshot Manager.

Restoring a snapshot

Use this procedure to return the memory, settings, and state of the virtual machines to the state when you took the snapshot. The power and data states of the virtual machines return to the state when you took the parent snapshot.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Important:

Do not perform any activity on the virtual application until the snapshot restoration is complete.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Revert to snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the steps accordingly.

Procedure

1. Click **Inventory** > **Virtual Machine**.
2. Right-click the virtual machine name on which you want to restore the snapshot, and click **Snapshot**.
3. Open **Snapshot Manager**.
4. Select the snapshot version that you want to restore.
5. Click **Go to**.
6. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task.

   Wait until the message `Completed` displays.

Chapter 7: Postinstallation verification and testing

Verifying EMS operation

You can verify the operational status of the EMS by:

- Attempting to access the EMS server using the web interface.
- Establishing a CLI session via a secure shell session (SSH) and manually checking the status of various internal processes.

Logging on to the EMS web interface

Procedure

1. Open a new browser tab or window by using any of the following web browsers:
    - Microsoft Internet Explorer (5) 8.0+
    - Mozilla Firefox [ESR] 24.0+
    - Google Chrome 25.0+
    - Apple Safari (4) 6.0+
2. Type the following URL:

    ```
    https://<Avaya EMS IP address>
    ```

3. Press **Enter**.

    If the Welcome screen is displayed, the EMS is operating normally and available for use. You can log in to EMS and perform normal administrative and operational tasks. See *Administering Avaya Session Border Controller for Enterprise*.

Verifying successful installation of EMS and Avaya SBCE

Before you begin

Deploy EMS and Avaya SBCE, and configure EMS and Avaya SBCE by using vSphere Client.

About this task

Use this procedure to add an Avaya SBCE device. Configure Avaya SBCE devices from the web interface for High Availability.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **System Management**.
3. On the System Management page, do the following:
   a. In the **Devices** tab, click **Add**.
   b. In the Add Devices window, type the Avaya SBCE details, such as the serial number and the management IP address.
   c. Click **Finish**.

   On the System Management page, the **Status** column of the Avaya SBCE device displays Registered.
4. Click **Install**.
5. In the Install Wizard, type the configuration.
6. Click **Finish**.

   In the **Devices** tab, the **Status** column of the device displays **Commissioned** indicating that the device is successfully deployed and configured.

Logging in to Avaya SBCE through SSH connection

Before you begin

Ensure that Avaya SBCE is installed and available on the network.

Procedure

1. Open an SSH client, such as PuTTy.
2. Type the IP address for Avaya SBCE.
3. Specify the port as **222**.
4. Select the connection type as SSH and press `Enter`.
5. Enter the user name and password to log in.

   Note:

   You cannot gain access to shell with user account `ucsec`.

   User account `ipcs` or user accounts that have shell access can be used for logging in to Avaya SBCE.

Chapter 8: Licensing requirements

Avaya SBCE uses WebLM for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the System Management page. Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. To install a license file on a newly installed or upgraded EMS, you have a 30-day grace period from the day of installation or upgrade.

Important:

Virtual EMS cannot run a local WebLM.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features
- Licensed capacity

For mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use an ova WebLM or System ManagerWebLM.

Note:

Grace period is no longer available for licenses. Customers can use the trial license until obtaining a production license.

Avaya SBCE license features

License feature	Description
VALUE_SBCE_STD_SESSION	Specifies the number of trunking session licenses.

Table continues…

License feature	Description
VALUE_SBCE_ADV_SESSION	Specifies the number of session licenses for remote worker, media recording, and encryption.
VALUE_SBCE_ELEMENTS_MANAGED	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_ENCRYPTION	Specifies the Avaya SBCE encryption.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION	Specifies the maximum number of Avaya SBCE video conferencing sessions.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG	Specifies the configuration of HA for the setup.

Appendix A: Best practices for achieving a secure virtualized DMZ deployment

Most security issues do not occur from the virtualization infrastructure, but from administrative and operational challenges. The primary risks are caused by a loss of separation of duties. When this occurs, people who lack the necessary experience and capabilities can introduce vulnerabilities through misconfiguration such as, they can accidentally put the virtual NIC of a virtual machine in the wrong trust zone. This risk can also occur in purely physical environments and can breach the isolation between networks and virtual machines of different trust levels.

Best practice security policies and procedures for configuring DMZ in a virtualized environment are not overly complex. However, you must know the critical challenges and best practice methods to reduce risk.

At every stage, you must remember that virtual machines need the same types of protections as the physical counterparts including antivirus software, host intrusion protection, configuration management, and patching in a timely manner. Virtual machines need to be secured in the same manner as physical machines.

After you decide to either partially or completely virtualize DMZ, the first step is to map out which virtual servers reside on which physical ESX hosts and to establish the level of trust for each system. The second step is to follow the guidelines in this section.

Harden and isolate the service sonsole

This step is important in DMZ because access to the service console of an ESX host allows full control over the virtual machines on that host. Although access to the service console is secured through authentication, you must provide more security against unauthorized access by following the guidelines in VMware Infrastructure 3 Security Hardening.

In addition, you must physically isolate the service console. Ensure that the network to which the service console is isolated is firewalled, and is accessible to only authorized administrators. You can use a VPN or other access control methods to restrict access to the management network. Although VMware ESXi does not have a service console and much of the hardening is unnecessary, you must isolate the management interface, which provides access to the ESXi APIs.

You should also isolate SAN connections and the VMotion networks from the management network.

Clearly label networks for each zone within DMZ

Clearly labeling networks for each zone within DMZ is critical because accidentally connecting virtual servers to the wrong networks can undermine all other security efforts. By clearly labeling the networks, you can avoid this problem.

Set Layer 2 security options on virtual switches

Protect against attacks such as, data snooping, sniffing, and MAC spoofing, by disabling the promiscuous mode, MAC address changes, and forged transmissions capabilities on virtual network interfaces. These capabilities are rarely needed and create opportunities for exploitation. With the VMware infrastructure, you have full control over these options, which is not the case in purely physical environments.

Enforce separation of duties

Reduce configuration mistakes by using VirtualCenter to define roles and responsibilities for each administrator of the VMware Infrastructure 3 environment. By distributing rights based on skills and responsibilities, you can reduce the chance of misconfiguration. This method also limits the amount of authority any one administrator has over the system as a whole.

Best practice also dictates that you use administrator or root access only in emergency situations. This practice reduces the potential for accidental or malicious misconfiguration by an administrator and helps limit the number of people who know the password for this type of account, which provides full control.

Use ESX resource management capabilities

Denial of service within a virtual environment can occur if each virtual machine uses a disproportionate share of ESX host resources. It starves other virtual machines running on the same ESX host. Such denial of service can occur accidentally or because of malicious intent, you can avoid this problem by setting resource reservations and limits for virtual machines by using VirtualCenter.

Regularly audit virtualized DMZ configuration

Regular audit of configurations is essential in both physical and virtual environments. When virtualizing DMZ or any part of the infrastructure, it is important to regularly audit the configurations of the components including VirtualCenter, virtual switches, virtual and physical firewalls, and any other security devices. You must conduct the audits to ensure that changes to configurations are controlled and that the changes do not cause a security hole in the configuration. The configuration management and compliance tools can assist with the audit process. Audits are important for the second and third options because the risk of misconfiguration is higher in those topologies.

Related Links

References on page 39

References

VMware Infrastructure 3 Security Hardening, http://www.vmware.com/resources/techresources/726

VMware Security Center, http://www.vmware.com/

Related Links

Best practices for achieving a secure virtualized DMZ deployment on page 38

Appendix A: Best Practices for VMware performance and features

BIOS

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

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

The following sections describe the recommended BIOS settings for:

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

Intel Virtualization Technology

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

All Intel Xeon processors include:

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

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

Note:

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

Other suggested BIOS settings

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

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

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

Dell PowerEdge Server

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

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

HP ProLiant Servers

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

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

VMware Tools

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

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

❗ **Important:**

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

Timekeeping

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

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

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

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system.

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

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

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

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

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

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

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

Configuring the NTP time

Procedure

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

The date and time of the System Manager virtual machine synchronizes with the NTP server.

6. Select the **Restart NTP service to apply changes** check box.
7. Click **OK**.

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

VMware networking best practices

You can administer networking in a VMware environment for many different configurations.

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

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

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type `vmxnet3` for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernal vNICs to be the same IP Maximum Transmission Unit (MTU).

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware VSphere™ 5.0	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf
Performance Best Practices for VMware VSphere™ 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf

Table continues…

Title	Link
VMware VSphere™ 5.0 Basics	http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-basics-guide.pdf
VMware VSphere™ 5.0 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi/vcenter-server-pubs.html
VmWare Documentation Sets	https://www.vmware.com/support/pubs/

Storage

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

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

Thin vs. thick deployments

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

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

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

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

Best Practices for VMware features

VMware Snapshots

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

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

⚠ **Caution:**

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

Snapshots can:

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

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

- *Do not* rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- *Do not run a virtual machine off of a snapshot.* Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent

snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.

- When taking a snapshot, *do not* save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
    - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the virtual machine's memory** check box.
    - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

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

Related resources

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

VMware Cloning

System Manager does not support VMware Cloning.

VMware High Availability

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

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

VMware vMotion

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

With vMotion, you can:

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

Before using vMotion, you must:

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

Note:

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

Glossary

AFS

Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.

Application

A software solution development by Avaya that includes a guest operating system.

Avaya Appliance

A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.

Blade

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

ESXi

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

Hypervisor

A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.

MAC

Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.

OVA

Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.

PLDS

Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.

Reservation

A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.

RFA Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.

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

Snapshot The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.

Storage vMotion A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.

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

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

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

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

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

vSphere Client The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

Index