Deploying Avaya Session Border Controller in Virtualized Environment

Release 7.2.2
Issue 9
October 2018

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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 is the

software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. 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 for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided

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

Avaya 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.

Contents

Chapter 1: Introduction

Purpose

This document contains Avaya SBCE installation, configuration, initial administration, and basic maintenance checklist and procedures.

This document is intended for people who install and configure a verified Avaya SBCE reference configuration at a customer site.

The audience includes and is not limited to implementation engineers, field technicians, business partners, and customers.

Change history

Issue	Date	Summary of changes
1	June 2017	Release 7.2 document
2	November 2017	Updated the configuring Avaya SBCE for network connectivity topic
3	November 2017	Updated the document for Release 7.2.1 for Nutanix support in Avaya SBCE
4	December 2017	Updated the Supported software and hardware topic for ESXi support in Release 7.2.1
5	January 2018	• Updated the document for Management interfaces and Dual stack IPv4 address support. • Added a new topic Avaya SBCE deploying options compatibility for VMware
6	June 2018	Updated the document for following Release 7.2.2 changes: • Updated the topic Deploying EMS on VSphere for Properties template. • Added the information about properties template in Configuring EMS in the CLI mode topic. • Added a new topic of Properties template field descriptions.

Table continues…

Issue	Date	Summary of changes
7	July 2018	Updated the Avaya SBCE virtual machine resource reservation specifications for VMware topic
8	September 2018	• Updated the Avaya SBCE virtual machine resource reservation specifications for VMware for Medium SBC support. • Updated the Supported software and hardware topic for Release 7.2.2 support for VMware ESXi versions
9	October 2018	Updated the supported hardware and software topic for vApp options.

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.

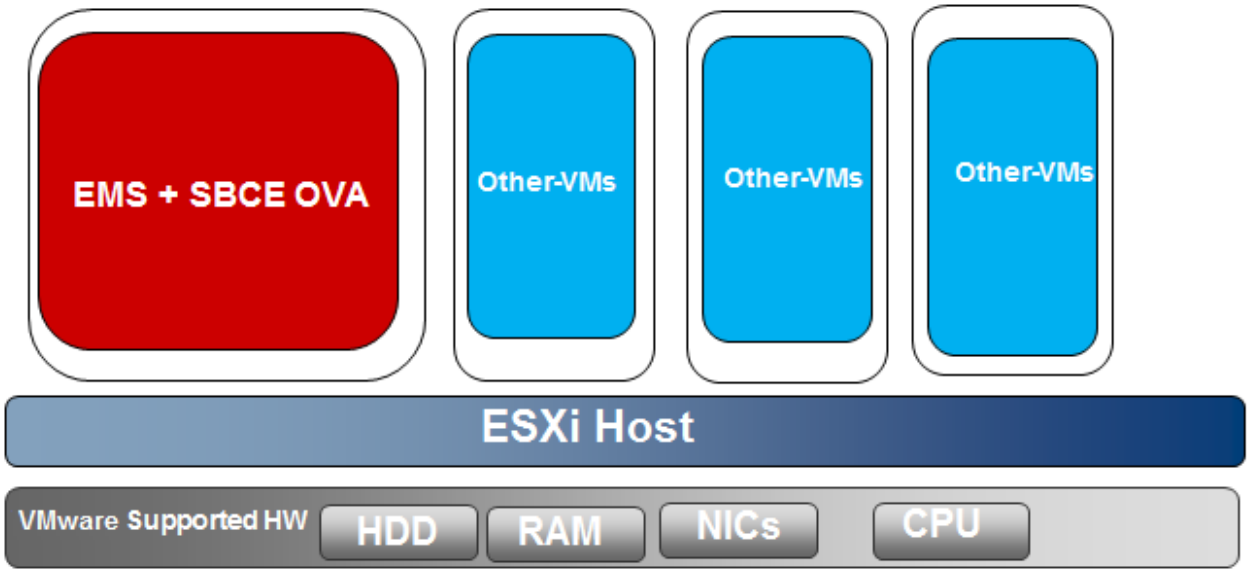
From Release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE.

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. The .ova file is available in Product Licensing and Delivery System (PLDS).

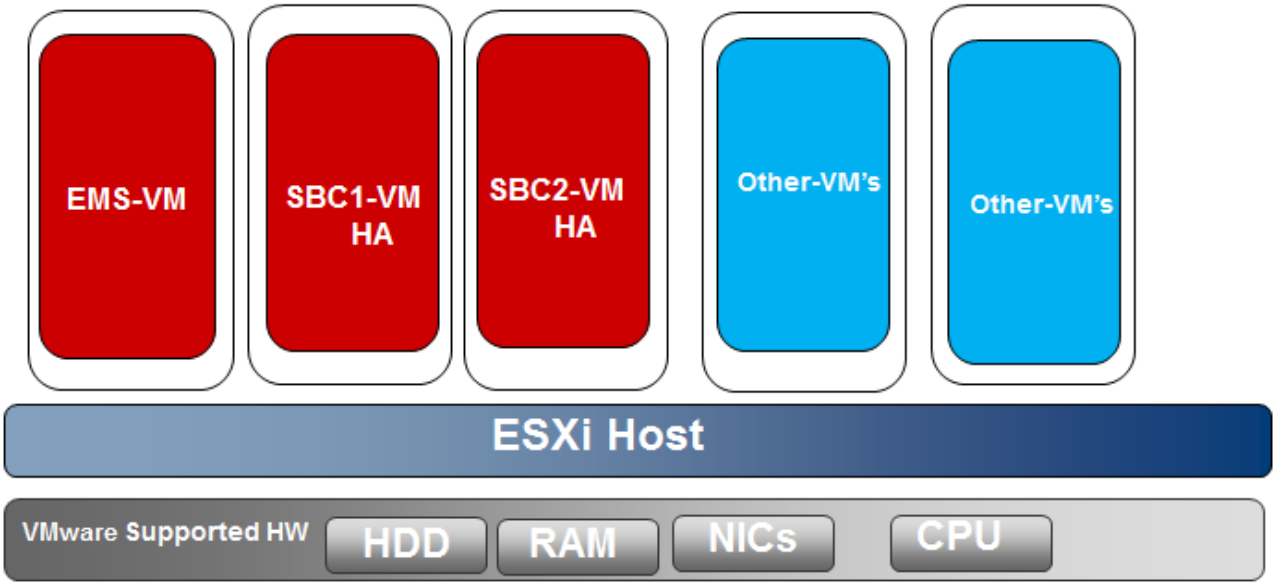
Avaya SBCE standalone mode

If you select a standalone deployment, the OVA file installs configurations for both Avaya SBCE and EMS.



EMS and SBC in High Availability (HA) mode

For HA mode, deploy the OVA file separately for EMS and Avaya SBCE. From release 7.0, a single OVA file is available to deploy EMS and Avaya SBCE. Therefore, you can use the same OVA file, but choose different configurations to deploy EMS and Avaya SBCE.



For more information, see *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*.

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can 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 applies only for VMware® and does not include any other industry hypervisor. Virtualized Environment project 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

Deployment considerations

VMware® vCenter and VMware® vSphere manage the deployment into the blade, cluster, and server.

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 version	Avaya SBCE Release number	
	Release 7.2	Release 7.2.1 Release 7.2.2
5.1	√	√
5.0	√	√
5U1	√	√
5.5	√	√
6.0	√	√
6.5	x	√

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.

Note:

Release 7.2.2 and earlier releases with ESXi 6.x do not support vApp options for deploying OVA.

From Release 7.2, Avaya SBCE supports deployments on Linux Kernel based Virtual Machine (KVM).

From Release 7.2.1 and later, you can deploy KVM using Nutanix.

Supported browsers

Avaya SBCE supports following browsers for accessing EMS:

- Microsoft Internet Explorer (5) 9.0+
- Microsoft Edge 13.0+
- Mozilla Firefox 38+ / 38.0 ESR+
- Google Chrome 47.0+
- Apple Safari (4) 7.0+

Avaya SBCE supports following browsers for deploying OVA on VMHost:

- Microsoft Edge
- Mozilla Firefox version 39 and later
- Apple Safari (4) 7.0+

Note:

Avaya recommends to use Microsoft Edge browser with version 38 and later.

For more information related to vSphere Web Client, see https://kb.vmware.com/s/article/2147929 and https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.install.doc/GUID-F6D456D7-C559-439D-8F34-4FCF533B7B42.html.

VMware specifications

Depending on resource reservation, the following variants are available to configure Avaya SBCE:

- Medium SBC: Resource reservation equivalent to standalone Avaya SBCE 310 model or Dell R210 II XL.
- EMS: Resource reservation required for running only EMS

Important:

Avaya recommends to use Medium SBC for deploying OVA on VMHost.

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

Table 1: Avaya SBCE OVA requirements on VMHost

VmWare Resource	Variant	
	Medium SBC	**EMS**
vCPU core	4 dedicated cores	3 floating cores
vCPU reservation	8800 MHz to 9600 MHz	6600 MHz to 7200 MHz

Table continues…

VmWare Resource	Variant	
	Medium SBC	**EMS**
Minimum CPU speed based on Xeon x5670 or equivalent processor	2.2 GHz	2.2 GHz
Memory reservation	8 GB	8 GB
Storage reservation	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)
Network Interfaces	6 Virtual Interfaces	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.

Avaya SBCE virtual machine resource reservation specifications for KVM

Avaya SBCE Release 7.0 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
- Medium SBC: Resource reservation equivalent to standalone Avaya SBCE 310 model or Dell R210 II XL.

  Note:

  Avaya recommends to configure only Medium SBC footprint for Nutanix.
- Large SBC: Used to support high-end deployments.
- EMS: Resource reservation required for running only EMS

The Avaya SBCE virtual machine requires the following set of resources :

Table 2: Avaya SBCE resource requirements on KVM

KVM Resource	Variant			
	Small SBC	**Medium SBC**	**Large SBC**	**EMS**
vCPU core	2 dedicated cores	4 dedicated cores	6 dedicated cores	3 floating cores
vCPU reservation	3320 MHz to 4400 MHz	8800 MHz to 9600 MHz	8800 MHz to 9600 MHz	6600 MHz to 7200 MHz

Table continues…

KVM Resource	Variant			
	Small SBC	**Medium SBC**	**Large SBC**	**EMS**
Minimum CPU speed based on Xeon x5670 or equivalent processor	1.66 GHz	2.20 GHz	2.20 GHz	2.20 GHz
Memory reservation	4 GB	8 GB	16 GB	8 GB
Storage reservation	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)	8.8 GB — thin provisioned 160 GB — thick provisioned (Recommended)
Network Interfaces	4 Virtual Interfaces	6 Virtual Interfaces	6 Virtual Interfaces	2 @ 100 Mbps or 1000 Mbps

VMware deployment options

VMware OVA type	Configuration type		
	EMS	**SBCE+EMS**	**SBCE**
Medium SBC	X	√	√

Supported hardware for VMware

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

- 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.

Configuring the virtual machine automatic startup settings on VMware

About this task

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 Web browser, type the vSphere vCenter host URL.
2. Click **Hosts and Clusters** or **VMs and Templates** icon.
3. In the left pane, select the host where the virtual machine is located.
4. Click **Configure**.
5. Under Virtual Machines, select **VM Startup/Shutdown**, and click **Edit**.

   The system displays the Edit VM Startup and Shutdown window.
6. Select **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Configuring vSwitches on ESXi host

About this task

This task creates a vSwitch that you can assign to a virtualized Avaya 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 the left navigation pane, click **Networking** > **Add Networking**.
3. In the Add Network Wizard window, do the following:
   a. In the Connection Type page, click **Virtual Machine**.
   b. In the Network Access page, click **Assign Physical NIC to vSwitch**.
   c. In the Connection Settings page, in the **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 servers 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*.

Chapter 4: Deploying EMS OVA

Deploying EMS on vSphere

Procedure

1. Download `sbce-7.2.x.0-xx-xxxxx.ova` from PLDS.
2. On the vSphere client, navigate to **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template dialog box, do one of the following:
   - 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 the name of the virtual machine.

   The name must not exceed 25 characters. For example, EMS-7-0-SingleBox is an appropriate name.
8. **(Optional)** If you logged in through vCenter, on the Host or cluster selection page, select a host and click **Next**.

   If one or more Resource Pools exist, Avaya SBCE displays a Resource Pool selection page.
9. **(Optional)** On the Resource Pool selection page, select the appropriate Resource Pool and click **Next**.

   The vSphere client displays the Deployment Configuration page.
10. In the **Configuration** field, click **EMS**.
11. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The vSphere client displays the data store that you select and sets the available space.
12. Select **Thin Provision** to minimize disk allocation. Use this option only in the lab environment.
13. Click **Next**.
14. **(Optional)** If you logged in through vCenter, in the Resource Allocation window, click **Next**.

15. On the Network Mapping page, in the **Source Network** column, configure Network 1 same as the management network in the **Destination Network** column.
16. In the **Properties** template, enter the requested information in the appropriate fields to deploy EMS on vSphere.

    The vSphere client does not display configuration through the CLI mode. The device is deployed according to the properties template configuration parameters.
17. Click **Next**.
18. Review the settings and click **Finish**.
19. Wait until the system deploys the EMS successfully.

Related links

Properties template field descriptions on page 20

Properties template field descriptions

Name on web interface	Name on Command Line Interface (CLI)	Description
IP Mode	ipmode	The IP mode of the device. The available options are: • IPV4 • DUAL STACK
Hostname	hostname	The host name of the device.
Appliance Type	apptype	The deployment type for the device. The available options are: • EMS • SBCE • EMS+SBCE
Network Passphrase	nwpass	The password for the network.
EMS Instance Type	ems_inst_type	The instance type for the EMS deployment type. The available options are: • Primary • Secondary • None
Management IPv4 Address	ip0	The IPv4 management address.
Netmask	netmask0	The network mask for management address.

Table continues…

Name on web interface	Name on Command Line Interface (CLI)	Description
Default Gateway	gateway	The default gateway address for management address.
IPv6 Address	ipv6address0	The IPv6 management address.
Ipv6 Prefix	ipv6prefix0	The IPv6 prefix for management interface.
IPv6 Gateway	ipv6gateway	The gateway address for IPv6 management address.
TimeZone	timezone	The timezone of the device.
NTP Server Address	ntpservers	The NTP server address for the device.
NTP Server Address(IPV6)	ntpipv6	The NTP server IPv6 address.
DNS Address	dns	The DNS server address.
EMS Address	emsip	The IP address of the EMS system. **EMS Address** is not valid for primary EMS and single box deployments.
EMS IPv6 Address	emsip_v6	The IPv6 address of EMS system.
Root/Ipcs/Grub Passwords	rootpass/ipcspass/grubpass	The passwords for root, ipcs, and grub.

Related links

Deploying EMS on vSphere on page 19

Deploying EMS on KVM

Before you begin

- Download the KVM guest template image from PLDS on local deployment server.
- Copy the downloaded KVM guest image to the KVM host in the storage directory.

  Give a unique name to the KVM instance.
- Use the KVM guest image as a base to create new images.

  For example, use sbce-7.2.x.0-10-13055.qcow2 to create a new image with the following command: **`cp -ap sbce-7.2.x.0-10-13055.qcow2 KVM-SBCE-7.2-qcow2`**.

  Then, use KVM-SBCE-7.2–qcow2 to create an instance called KVM-SBCE-7.2.

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

The system displays the Virtual Machine Manager GUI.

3. Click **File** > **New Virtual Machine**.
4. Click **Importing existing disk image**.
5. In the **Provide the existing storage path** field, type the storage path for the KVM image.
6. In the **OS Type** field, click **Generic**.
7. In the **Version** field, click **Generic**.
8. Click **Forward**.
9. Based on the type of deployment, select the RAM and CPU.
10. In the **Name** field, type a unique name of the EMS instance.
11. Select **Customize configuration before install**.
12. Click **Finish**.

    Virtual manager displays only one NIC card by default. Depending on the type of deployment, you can add more network cards. For better performance, choose **Device Model** as virtio and **Network Source** as the bridge type.
13. Click **Add Hardware**.
14. Click **Network**.
15. Provide a network source, MAC address, and Device model, and click **Finish**.
16. Click **CPUs**.
17. In the **Model** field, click **Hypervisor Default**.
18. Click **Apply**.
19. Click **Begin installation**.

    The system displays a console with Avaya SBCE kernel bootup messages. After the startup scripts run, the system displays the SBCE Config menu.

Configuring EMS

Configuring EMS in the text mode

Before you begin

Turn on the EMS server.

Procedure

1. In the VSphere client inventory, right-click a virtual instance of EMS and click **Open Console**.
2. When the system displays, **Enter your choice**, type `2` to configure in the text mode.
3. In the Select Device Type window, do the following:
   a. Select **EMS**.

      The system displays a confirmation message.

   b. Select **YES**.

      The system displays the `Installing as EMS device` message.

   c. Select **OK**.
4. On Device Configuration screen, do the following:
   a. Select **Configuration**.
   b. If you use only IPv4 addresses, select **IPv4** or **Dual Stack** and click **Select**.
   c. Based on the deployment, select an installation type.
   d. Select **Primary** or **Secondary** and click **OK**.

      This option specifies whether the EMS is primary or secondary.

   e. Click **EMS Appliance Configuration**.

      The system displays the Appliance Configuration screen.

   f. In the **EMS Host name** field, type a name for the EMS host.
   g. In the **List of DNS Servers** field, type the IP address of the DNS server.
   h. In the **NTP Server IP Address (ipv4)** field, type the NTP Server IP address.
   i. In the **Network Passphrase** field, type the passphrase.
   j. In the **Network Passphrase (Again)** field, retype the passphrase.

      You must use the same network passphrase while configuring Avaya SBCE.

   k. Select **OK**.
5. Select **Management Interface Setup**.
6. On the Management Interface Setup page, type appropriate values for Management IP address, Management Network Mask, and Management Gateway IP Address.

   Voice interfaces (A1, A2, B1, B2) support both IPv4 and IPv6 address configuration. If you are using dual stack for any of the data interfaces, then configure the system with dual stack and the IP Address on Management interface (M1) must be the IPv4.address.
7. Select **OK**.
8. Based on the customer location, select the appropriate time zone.

   If required, follow steps 9 to 11 to enter details for a self-signed certificate.

9. **(Optional)** Select **Configure self-signed certificate**.
10. **(Optional)** Type appropriate values in the **First and Last Name**, **Organizational Unit**, **Organization**, **City or Locality**, **State or Province**, and **Country Code** fields.
11. **(Optional)** Select **OK**.
12. Return to the previous page.
13. Click **Done**.
14. When the system displays prompts for changing the root and grub passwords, enter new root and grub passwords.

    If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set the EMS to factory default settings. Then, after starting the EMS, enter the configuration data again to complete the configuration process.

Related links

Configuring a time server on page 24
Management Interface Setup field descriptions on page 25

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

Management Interface Setup field descriptions

Name	Description
Management IP Address (ipv4)	The IPv4 address of the management network.
Management Network Mask	The network mask of the management network.
Management Gateway IP Address (ipv4)	The IPv4 address of the gateway to the management network.
Management IP Address (ipv6)	The IPv6 address of the management network. The system displays this field only when you select Dual Stack on the Management IP Configuration screen. **Note:** In Dual Stack the IPv6 address is optional but the IPv4 address is compulsory.
Management Network Pfx length	The length of the prefix for the management network IPv6 address. The system displays this field only when you select Dual Stack on the Management IP Configuration screen. For example, 2001:1234:5678:1234:5678:ABCD:EF12:1234/64 is a 128 bit IPv6 address. Out of the 128 bits IPv6 address, 64 bits that is, 2001:1234:5678:1234: is the prefix and 5678:ABCD:EF12:1234 is the host name. So correct way to write the 128 bits IPv6 prefix is 2001:1234:5678:1234::/64.
Management Gateway IP Address (ipv6)	The IPv6 address of the gateway to the management network. The system displays this field only when you select Dual Stack on the Management IP Configuration screen. **Note:** In Dual Stack the IPv6 address is optional but the IPv4 address is compulsory.
EMS Server IP Address (ipv4)	The IP address of the EMS server. This field is displayed for Avaya SBCE-only installations.

Note:

Management interface (M1) supports only IPv4 address configuration, so following fields are not supported in Release 7.2.1 or earlier:

- **Management IP Address (ipv6)**
- **Management Network Pfx length**
- **Management Gateway IP Address (ipv6)**

Important:

When using SSL/VPN as configured on the M1 interface, ensure that the IP address associated with the M1 interface will need *outbound* internet access. The M1 interface requires *outbound* internet access to initiate connectivity with the Avaya VPN Gateway (AVG) server (FQDN: plavg0(x).sal.avaya.com. M1 is the management interface that is the required interface for SSL/VPN.

Note:

For security reasons for Voice Over IP (VoIP) systems, segment the data or data management network from the voice network. For Avaya SBCE deployments, segmentation means configuring the Management Interface (M1) on a separate subnet from the subnet used for the Voice Interfaces (A1, A2, B1, and B2). Avoid placing M1 IP address on a PBX core network. For more information about this recommendation, see

- Avaya: *Security Best Practices Checklist*, in the Network section at https://downloads.avaya.com/css/P8/documents/100070101
- Network Security Agency: *Recommended IP Telephony Architecture*, at http://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf
- National Institute of Standards and Technology (NIST): *Security Considerations for Voice Over IP Systems* at http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Related links

Configuring EMS in the text mode on page 22

Configuring EMS in the CLI mode

About this task

Use this procedure to configure EMS using command line interface. If you have configured the ova properties from **Properties** template, configuring the same properties from CLI mode is not required.

Procedure

1. Right click the virtual machine instance of EMS and click **Power**.
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. In the **IP Mode** field, depending on the type of addresses used in your network, type `IPV4` or `DUAL_STACK`.
5. In the **Appliance Type** field, type `EMS` and press `Enter`.
6. In the **Network Passphrase** field, type the passphrase.

   You must use the same network passphrase while configuring Avaya SBCE.
7. In the **Appliance Name** field, type application name and press `Enter`.
8. In the **Installation Type** field, type primary or secondary, as applicable.
9. Type network details in the following fields: **Management IP address**, **Management subnet mask**, **Management Gateway IP address**, **Management subnet prefix length**, **NTP Server IP Address**, **List of DNS Servers**, and **Domain suffix**.
10. **(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.
11. Select the appropriate time zone.
12. When the system displays, `Changing password for user root New password:`, type the new password and confirm the password.
13. When the system displays, `Changing password for user ipcs New password:`, type the new password and confirm the password.
14. When the system displays, `Changing password for user grub New password:`, type the new password and confirm the password.
15. Log in using ipcs credentials.

    If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set the EMS to factory default settings. Then, after starting the EMS, enter the configuration data again to complete the configuration process.

Configuring EMS for network connectivity

Before you begin

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

Configure password for root and ipcs users.

Procedure

1. Log in to virtual machine using ipcs login and ipcs password.
2. To access root privileges, login as root user.
3. 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.

4. Note the MAC address.
5. Right-click on the EMS virtual instance, such as EMS -VM, and then click **Edit Settings**.
6. 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.
7. Select the vSwitch and then in the **Network label** field, click the appropriate network label for M1 to be available on network.
8. Click **OK**.

Configuring the virtual machine automatic startup settings on VMware

About this task

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 Web browser, type the vSphere vCenter host URL.
2. Click **Hosts and Clusters** or **VMs and Templates** icon.
3. In the left pane, select the host where the virtual machine is located.
4. Click **Configure**.
5. Under Virtual Machines, select **VM Startup/Shutdown**, and click **Edit**.

   The system displays the Edit VM Startup and Shutdown window.
6. Select **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Configuring vSwitches on ESXi host

About this task

This task creates a vSwitch that you can assign to a virtualized Avaya 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 the left navigation pane, click **Networking** > **Add Networking**.
3. In the Add Network Wizard window, do the following:
    a. In the Connection Type page, click **Virtual Machine**.
    b. In the Network Access page, click **Assign Physical NIC to vSwitch**.
    c. In the Connection Settings page, in the **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 servers 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*.

Chapter 5: Deploying and configuring Avaya SBCE on vSphere

Checklist for deploying and configuring Avaya SBCE on vSphere

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

#	Action	Description	Link	✔
1	Download the following ova file from the PLDS website at https://plds.avaya.com: `sbce-7.2.x.0-xx-xxxxx.ova` **Note:** Avaya SBCE Release 7.0 onwards, a single ova file is available for installing EMS and Avaya SBCE.			
2	High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication. For example, to handle GARP, branch	Applicable only to multiple server HA scenarios.		

Table continues…

#	Action	Description	Link	✔
	gateways, Medpro, Crossfire, and some PBXs/IVRs must be deployed in a different network from Avaya SBCE, with a router or L3 switch. If you do not put the Avaya SBCE interfaces on a different subnet, after failover, active calls will have a one-way audio. Devices that do not support GARP continue sending calls to the original primary Avaya SBCE. Ensure that you have a license file with the following feature: FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1 **Note:** You can enable and use the HA feature only when the license file contains an HA license.			
3	Install vSphere Client from the VMware website.	Download the third-party client from the VMware website.	Configuring vSwitches on ESXi host on page 17	
4	Keep the configuration data ready.		Customer configuration data on page 15	
5	Create vSwitches.	Create virtual switches for M1, M2, and any of the following interfaces: A1, A2, B1, and B2.		
6	Deploy EMS OVA template.		Deploying EMS on vSphere on page 19	
7	Configure EMS.		Configuring EMS in text mode on page 22, Configuring EMS in CLI mode on page 26	
8	Configure EMS for network connectivity.		Configuring EMS for network connectivity on page 27	
9	Deploy Avaya SBCE OVA template.		Deploying SBCE on page 32	
10	Configure Avaya SBCE.		Configuring SBCE on page 35	

Table continues…

#	Action	Description	Link	✔
11	Configure Avaya SBCE for network connectivity.		Configuring Avaya SBCE for network connectivity on page 39	
12	Configure Avaya SBCE and EMS to start automatically after a power failure.		Configuring the virtual machine automatic startup settings on page 17	
13	Verify the installation of Avaya SBCE.		Verifying successful installation of EMS and Avaya SBCE on page 48	

Deploying Avaya SBCE OVA

Deploying Avaya SBCE on vSphere

Before you begin

- Install vSphere Client from the ESXI host web page. Type `https://ESXI host ip` in the browser address bar, and locate the download link from the **Getting Started** section.
- Ensure that the computer on which vSphere Client is installed can access the VMware ESXi servers of all devices on the network.

Procedure

1. 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.
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 up to 25 characters.

   For example, SBCE-6-2-SingleBox is an appropriate name.

8. Click **Next**.

   If one or more Resource Pools exist, the system displays a Resource Pool selection page.

9. Select the appropriate Resource Pool, and click **Next**.

   The system displays the Deployment Configuration page.

10. In the **Configuration** field, select one of the following options:

    - Small SBC: 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.
    - Medium SBC: Medium SBC option is preferable when you require features such as HA and capacity less than Large SBC deployment. For the Medium SBC deployment option, the M1, M2, B1, B2, A1 and A2 interfaces are available.
    - Large SBC: Large SBC option is preferable when you require features such as HA. For the Large SBC deployment option, the M1, M2, B1, B2, 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**.

    The system displays the Network Mapping page.

13. 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. In the **Properties** template, enter the requested information in the appropriate fields to deploy SBCE on vSphere.

    The vSphere client does not display configuration through the CLI mode. The device is deployed according to the properties template configuration parameters.

15. Click **Next**.
16. Review the settings and click **Finish**.
17. Wait until the system deploys the OVA file successfully.

18. Turn on the machine.
19. Repeat steps 1 to 17 to deploy SBC1 and SBC2 templates for HA mode.
20. In the navigation pane, select the newly deployed virtual instance of Avaya SBCE.
21. 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.

Migrating from a physical server to VMWare

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. Select **Backup/Restore** from the Task Pane.

   The system displays the Backup/Restore screen in the content area.
3. Click **Create Snapshot**.

   The system displays the Create Snapshot window.

   In a deployment with multiple Avaya SBCEs, if any of the Avaya SBCEs is out of service, you cannot create a snapshot.
4. Enter a name to designate this snapshot (backup) file, and click **Create**.

   A snapshot (backup) of the EMS security configuration is made and sent to all the configured snapshot servers. A banner is displayed on the Create Snapshot pop-up window informing you that the snapshot has been successfully created. When the process is complete, the newly created snapshot is displayed in the content area of the snapshots screen.
5. Select the snapshot file that you created, and click **Download**.

   Save the snapshot file for Avaya SBCE deployed on the physical server. You can then use this snapshot to restore the same configurations to VMware.
6. Turn off the power to the server on which EMS is deployed.
7. Deploy the EMS ova file on VMWare with the same build number and management IP as on the physical server.

After the EMS deployed on VMWare is up, you can restore the snapshot you saved from the physical server.

8. Log on to the EMS web interface with administrator credentials.
9. In the Task pane, click **Backup/Restore**.

   The Content area displays the Backup/Restore screen.
10. Select the corresponding **Restore by File** option.

    The system displays the Restore by File pop-up window.
11. Click **Browse**.

    The system displays a dialog pop-up window.
12. Select the desired snapshot file, and click **Open**.

    The system enters the selected snapshot file in the **Restore Point File** field of the Restore by File window.
13. Click **Finish**.

    The system displays a warning window for confirmation to proceed with the restoration procedure.
14. Click **OK**.

    The EMS server goes offline and the snapshot file transferred to the EMS server, where the file is uncompressed and used to reconfigure the EMS software to a previous configuration.

    Note:

    After the system successfully restores a snapshot, in an HA configuration both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The system takes 2 to 3 minutes to reboot after backup configuration.

Configuring Avaya SBCE

Configuring Avaya SBCE in the text mode

Procedure

1. After you power ON, select the text mode.
2. Select **SBCE**.

   Use the SBCE option to deploy Avaya SBCE when the device is managed by a separate EMS server, for example, in an HA deployment.
3. Select **OK**.
4. On the Device Configuration screen, select **Configuration**.

5. Depending on the IP addresses used in your network, do one of the following:
   - If you use only IPv4 addresses, select **IPv4** and click **Select**.
   - If you use both IPv4 and IPv6 addresses, select **Dual Stack** and click **Select**.
6. Select **Appliance Configuration**.
7. In the **Appliance name** field, type an appliance name.
8. **(Optional)** In the **Domain Suffix** field, type the domain suffix.
9. In the **List of DNS Servers** field, type the list of DNS servers.
10. In the **NTP Server IP Address** field, enter the NTP server IP address.
11. If you selected the Dual Stack installation mode, in the **NTP Server IP Address (ipv6)** field, type the NTP server Ipv6 IP address.
12. In the **Network passphrase** field, type a passphrase and confirm the passphrase.

    This network passphrase must match the password you provided while installing EMS.
13. Select **Management Interface Setup**.

    The system displays the Management IP Configuration screen.
14. On the Management Interface Setup page, type appropriate values for IP addresses.
15. Select a time zone.
16. Select **Back**.
17. Select **Done**.
18. When the system displays **Enter the password**, type the password for root, ipcs, and grub users.
19. To access root privileges of the Avaya SBCE device, login as root user.
20. In the root privileges, type the `ip address` command.

    The system displays all six mapping interfaces.
21. Verify the network adapters for A1, B1, M1, M2, A2, and B2 and note the MAC address for each interface.
22. In vSphere, right-click the Avaya SBCE instance and click **Edit Settings**.
23. In the **Hardware** tab, click the interface.
24. Click the appropriate virtual network interface for the Avaya SBCE virtual machine.
25. Click **OK**.

    If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set Avaya SBCE to factory default settings. Then, after starting Avaya SBCE, enter the configuration data again to complete the configuration process.

Configuring Avaya SBCE in the CLI mode

About this task

Perform the procedure after you deploy Avaya SBCE ova.

Procedure

1. Deploy Avaya SBCE and turn ON the Avaya SBCE.
2. In the vSphere Client inventory, right-click a virtual instance of Avaya SBCE and click **Open Console**.
3. Type `1` for the CLI mode and then press `Enter`.
4. In the **IP Mode** field, depending on the type of addresses used in your network, type `IPV4` or `DUAL_STACK`.
5. In the **Appliance Type** field, type `EMS` and press `Enter`.
6. In the **Network Passphrase** field, type the passphrase.
7. In the **Appliance Name** field, type application name and press `Enter`.
8. In the **Installation Type** field, type primary or secondary, as applicable.
9. Type network details in the following fields: **Management IP address**, **Management subnet mask**, **Management Gateway IP address**, **Management subnet prefix length**, **NTP Server IP Address**, **List of DNS Servers**, and **Domain suffix**.
10. **(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.
11. Select the appropriate time zone.
12. 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 password.
13. Type `Y` to continue or type `N` to enter the details again.
14. When the system displays, `Changing password for user ipcs New password:`, type the new password and confirm and confirm the password.

    The system prompts, `Avaya SBCE login:`.
15. When the system displays prompts for changing the root and grub passwords, enter new root and grub passwords.
16. Log in using ipcs credentials.

    If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set the Avaya SBCE to factory default settings. Then, after starting the Avaya SBCE, enter the configuration data again to complete the configuration process.

Configuring standalone Avaya SBCE

Procedure

1. Power on the Avaya SBCE instance and select the text mode.
2. In the **Device Type** field, select **EMS+SBCE**.

   Use the **EMS+SBCE** option to deploy EMS and Avaya SBCE on the same server.
3. On the Device Configuration screen, select **Configuration**.
4. If you use only IPv4 addresses, select **IPv4** or **Dual Stack** and click **Select**.
5. Select **Appliance Configuration**.
6. In the **Appliance name** field, type an appliance name.
7. **(Optional)** In the **Domain Suffix** field, type the domain suffix.
8. In the **List of DNS Servers** field, type the list of DNS servers.
9. In the **NTP Server IP Address** field, enter the NTP server IP address.
10. If you selected the Dual Stack installation mode, in the **NTP Server IP Address (ipv6)** field, type the NTP server Ipv6 IP address.
11. Select **Management Interface Setup**.

    The system displays the Management IP Configuration screen.
12. On the Management Interface Setup page, type appropriate values for IP addresses.
13. Select a time zone.
14. Enter self-signed certificate details in the **First and Last Name**, **Organizational Unit**, **Organization**, **City or Locality**, **State or Province**, and **Country Code** fields.
15. Select **Done**.
16. When the system displays **Enter the password**, type the password for root, ipcs, and grub users.
17. To access root privileges of the Avaya SBCE device, login as root user.
18. In the root privileges, type the `ip address` command.

    The system displays all six mapping interfaces.
19. Verify the network adapters for A1, B1, M1, M2, A2, and B2 and note the MAC address for each interface.
20. In vSphere, right-click the Avaya SBCE instance and click **Edit Settings**.
21. In the **Hardware** tab, click the interface.
22. Click the appropriate virtual network interface for the Avaya SBCE virtual machine.
23. Click **OK**.

If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set Avaya SBCE to factory default settings. Then, after starting Avaya SBCE, enter the configuration data again to complete the configuration process.

Configuring standalone Avaya SBCE in the CLI mode

About this task

Perform the procedure after you deploy Avaya SBCE ova.

Procedure

1. Deploy Avaya SBCE and turn ON the Avaya SBCE.
2. In the vSphere Client inventory, right-click a virtual instance of Avaya SBCE and click **Open Console**.
3. Type `1` for the CLI mode and then press `Enter`.
4. In the **IP Mode** field, depending on the type of addresses used in your network, type `IPV4` or `DUAL_STACK`.
5. In the **Appliance Type** field, type `EMS+SBCE` and press `Enter`.
6. In the **Appliance Name** field, type application name and press `Enter`.
7. Type network details in the following fields: **Management IP address**, **Management subnet mask**, **Management Gateway IP address**, **Management subnet prefix length**, **NTP Server IP Address**, **List of DNS Servers**, and **Domain suffix**.
8. **(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.
9. Select the appropriate time zone.
10. When the system displays, `Changing password for user root New password:`, type the new password and confirm the password.
11. When the system displays, `Changing password for user ipcs New password:`, type the new password and confirm and confirm the password.
12. When the system displays prompts for changing the root and grub passwords, enter new root and grub passwords.
13. Log in using ipcs credentials.

    If the virtual machine shuts down abruptly before you complete the initial configuration steps, you must set the Avaya SBCE to factory default settings. Then, after starting the Avaya SBCE, enter the configuration data again to complete the configuration process.

Configuring Avaya SBCE for network connectivity

Before you begin

Configure and power ON Avaya SBCE.

Use M2 interface as HA link.

Ensure connection between M1 interfaces of both Avaya SBCE instances in the HA pair.

Procedure

1. Log in to virtual machine using ipcs login and ipcs password.
2. To access root privileges, type `sudo su`.
3. 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.
4. Note the MAC address.
5. Right-click on the Avaya SBCE virtual instance, and then click **Edit Settings**.
6. In the **Hardware** tab, in the **Network Adapter 1** field, confirm if the MAC address matches with the MAC address that is displayed by using the ip address command at step 4.
7. Select the vSwitch and then in the **Network label** field, click the appropriate network label for M1 to be available on network.
8. Click **OK**.

   For information about configuring Avaya SBCE, and for remote worker and trunk configuration, see *Administering Avaya Session Border Controller for Enterprise*.

Chapter 6: Deploying and configuring Avaya SBCE on Kernel-based virtual machine

Extracting KVM OVA

Procedure

1. Create a folder on the KVM host and copy the application KVM OVA in the created folder.
2. Type the command **`tar -xvf`** *<application_KVM.ova>*.

   The system extracts the files from the application KVM OVA.

Deploying Avaya SBCE KVM OVA using Virt Manager

Before you begin

- Download the KVM guest template image from PLDS on local deployment server.
- Copy the downloaded KVM guest image to the KVM host in the storage directory.

  Give a unique name to the KVM instance.
- Use the KVM guest image as a base to create new images.

  For example, use sbce-7.2.x.0-10-13055.qcow2 to create a new image with the following command: **`cp -ap sbce-7.2.x.0-10-13055.qcow2 KVM-SBCE-7.2-qcow2`**.

  Then, use KVM-SBCE-7.2–qcow2 to create an instance called KVM-SBCE-7.2.

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

   The system displays the Virtual Machine Manager GUI.
3. Click **File** > **New Virtual Machine**.
4. Click **Importing existing disk image**.
5. In the **Provide the existing storage path** field, type the storage path for the KVM image.

6. In the **OS Type** field, click **Generic**.
7. In the **Version** field, click **Generic**.
8. Click **Forward**.
9. Based on the type of deployment, select the RAM and CPU.
10. In the **Name** field, type a unique name of the EMS instance.
11. Select **Customize configuration before install**.
12. Click **Finish**.

    Virtual manager displays only one NIC card by default. Depending on the type of deployment, you can add more network cards. For better performance, choose **Device Model** as virtio and **Network Source** as the bridge type.
13. Click **Add Hardware**.
14. Click **Network**.
15. Provide a network source, MAC address, and Device model, and click **Finish**.
16. Click **CPUs**.
17. In the **Model** field, click **Hypervisor Default**.
18. Click **Apply**.

    Repeat step 13 to step 18 four times to deploy Large Avaya SBCE and two times to deploy Small and Medium Avaya SBCE on KVM.
19. Click **Begin installation**.

    The system displays a console with Avaya SBCE kernel bootup messages. After the startup scripts run, the system displays the SBCE Config menu.

Deploying application by using Nutanix

Logging on to the Nutanix Web console

Procedure

1. To log on to the Nutanix Web console, in your web browser, type the PRISM URL.

   For example, http://<PRISM_IPAddress>/.
2. In **username**, type the user name.
3. In **password**, type the password.
4. Press **Enter**.

The system displays the Home page.

Transferring the files by using the WinSCP utility

About this task

Use the following procedure to transfer the files from a remote system to a Nutanix container by using the WinSCP utility.

Procedure

1. Use WinSCP or a similar file transfer utility to connect to the Nutanix container.
2. In **File protocol**, click **SCP**.
3. Enter the credentials to gain access to SCP.
4. Click **Login**.
5. Click **OK** or **Continue** as necessary in the warning dialog boxes.
6. In the WinSCP destination machine pane, browse to `/home/<Container_Name>` as the destination location for the file transfer.
7. Click and drag the `qcow2` image from the WinSCP source window to `/home/<Container_Name>` in the WinSCP destination window.
8. Click the WinSCP **Copy** button to transfer the file.
9. When the copy completes, close the WinSCP window (**x** icon) and click **OK**.

Uploading the qcow2 image

Procedure

1. Log on to the Nutanix Web console.
2. Click **Settings icon (**  **) > Image Configuration**.

   The system displays the Image Configuration dialog box.
3. Click **+ Upload Image**.

   The system displays the Create Image dialog box.
4. In **NAME**, type the name of the image.
5. In **ANNOTATION**, type the description of the image.
6. In **IMAGE TYPE**, click **DISK**.
7. In **STORAGE CONTAINER**, click the storage container of the image.

8. In **IMAGE SOURCE**, perform one of the following:
   - Select **From URL**, type the exact URL of the qcow2 image. For example: `nfs://<127.0.0.1>/<Storage Container Name>/<Image Name>`
   - Select **Upload a file**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
9. Click **Save**.

   The system displays the created image on Image Configuration.

Creating the virtual machine by using Nutanix

Before you begin

- Upload the `qcow2` image.
- Configure the network.

Procedure

1. Log on to the Nutanix Web console.
2. Click **Home** > **VM**.
3. Click **+ Create VM**.

   The system displays the Create VM dialog box.
4. In the General Configuration section, perform the following:
   a. In **NAME**, type the name of the virtual machine.
   b. In **DESCRIPTION**, type the description of the virtual machine.
5. In the Compute Details section, perform the following:
   a. In **VCPU(S)**, type the number of virtual CPUs required for the virtual machine.
   b. In **NUMBER OF CORES PER VCPU**, type the number of core virtual CPUs required for the virtual machine.
   c. In **Memory**, type the memory required for the virtual machine.

      The value must be in GiB.

   You must select the CPU and Memory according to the application footprint profile.
6. In the Disk section, perform the following:
   a. Click **+ Add New Disk**.

      The system displays the Add Disk dialog box.
   b. In **TYPE**, click **DISK**.
   c. In **OPERATION**, click **Clone from Image Service**.

d. In **IMAGE**, click the application image.

e. In **BUS TYPE**, click **IDE**.

f. Click **Add**.

The system displays the added disk in the **Disk** section.

7. In the Disk section, select a boot device.
8. In the Network Adopters (NIC) section, perform the following:

a. Click **Add New NIC**.

The system displays the Create NIC dialog box.

b. In **VLAN NAME**, click the appropriate NIC.

The system displays **VLAN ID**, **VLAN UUID**, and **NETWORK ADDRESS / PREFIX** for the selected NIC.

c. Click **Add**.

The system displays the added NIC in the Network Adopters (NIC) section.

You must select the number of NIC according to the application footprint profile.

If you are configuring Out of Band Management, select one more NIC.

9. In the VM Host Affinity section, perform the following:

a. Click **Set Affinity**.

The system displays the Set VM Host Affinity dialog box.

b. Select one or more host to deploy the virtual machine.

c. Click **Save**.

The system displays the added hosts in the VM Host Affinity section.

10. Click **Save**.

The system displays the message: `Received operation to create VM <name of the VM>`.

After the operation is successful, the system displays the created virtual machine on the VM page.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Power On**.

   The system starts the virtual machine.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

---

Configuring the virtual machine

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Launch Console**.
5. Follow the prompt to configure the virtual machine.

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.

If the Avaya SBCE installation fails, you can restore the system data. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Logging on to the EMS web interface

Procedure

1. Open a new browser tab or window.
2. Type the following URL:

   `https://<Avaya EMS IP address>`
3. Press **Enter**.

   The system displays a message indicating that the security certificate is not trusted.
4. Accept the system message and continue to the next screen.

   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*.
5. Type the username and password as `ucsec`.

   On first login, system prompts you to change the password.
6. Enter a new password and login with the new password.

Verifying successful installation of EMS and Avaya SBCE

Before you begin

Deploy EMS and Avaya SBCE, and configure EMS and Avaya SBCE.

About this task

Use this procedure to add an Avaya SBCE device.

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 host name 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 EMS 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: Maintenance procedures

Maintenance procedures for Avaya SBCE on VMware

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.

This section contains information about creating, restoring, and deleting snapshots from VMware. You can also back up and restore system information by using the Backup/Restore option on the EMS web interface. The problems mentioned in this section are for VMware snapshots, and not for the snapshots that you can take from the Avaya SBCE web interface.

For more information about VMware snapshots, see the VMware Snapshots section.

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.

Warning:

Take a VM snapshot when the application is powered off to avoid .war file corruption on Avaya SBCE. If the .war file is corrupted, some GUI pages might not display correctly.

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. To select a virtual machine 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 make the application out-of-service.
   c. Right-click the virtual machine and select **Snapshot** > **Take Snapshot**.
2. To select a virtual machine using the vSphere Client:
   a. Stop the application that is running on the virtual machine or make the application out-of-service.
   b. Click **Inventory** > **Virtual Machine** > **Snapshot** > **Take Snapshot**.
3. In the **Name** field, enter a name for the snapshot.
4. In the **Description** field, enter a description for the snapshot.
5. Disable **Snapshot the virtual machine's memory**.
6. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
7. Click **OK**.

   The system displays `Completed` when 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. To open the **Snapshot Manager** using the vSphere Web Client:
   a. Search for a virtual machine.
   b. Select the virtual machine from the search results list.
   c. Right-click the virtual machine and select **Snapshot** > **Snapshot Manager**.
2. To open the **Snapshot Manager** using the vSphere client, select **Inventory** > **Virtual Machine** > **Snapshot** > **Snapshot Manager**.
3. In the **Snapshot Manager**, click a snapshot to select it.

4. Select **Delete from Disk** to delete the single snapshot from the Snapshot Manager and the virtual machine.
5. Click **Yes** in the confirmation dialog box.
6. 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.

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.

Removing an Avaya SBCE or EMS from VMware

About this task

You might need to remove an Avaya SBCE or EMS from VM when the device is no longer required.

Procedure

1. Locate the Avaya SBCE or EMS.
2. Right-click the Avaya SBCE or EMS.

3. Click **Power** > **Power Off**.
4. When the system displays a dialog box for confirmation, click **Yes**.
5. Right-click the Avaya SBCE or EMS, and click **Delete from Disk**.
6. When the system displays a dialog box for confirmation, click **Yes**.

Determining whether Avaya SBCE is installed on VMware

Procedure

1. Log in as a root user to get root privileges.
2. Type `dmidecode | grep 'VMware'.`

   If Avaya SBCE is installed on VMware, the system displays `Product Name: VMware`.

   If Avaya SBCE is installed on any other server, the system does not display any data.

Maintenance procedures for Avaya SBCE on KVM

Creating a snapshot for KVM

About this task

Use the following procedure to create a snapshot for the virtual machine(VM) KVM-SBCE-7.2.

Before you begin

Caution:

Do not perform any activity on KVM until the snapshot backup is complete. Snapshots operations can adversely affect service.

It is recommended that VM is suspended or shut down to take a clean snapshot.

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

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. Shutdown the VM by using the **`virsh shutdown KVM-SBCE-7.2`** command.

The system shuts down the KVM-SBCE-7.2 instance.

5. Take the snapshot by using the **`virsh snapshot-create KVM-SBCE-7.2`** command.
6. Enter a name to identify the snapshot.
7. View the snapshot, using the **`virsh snapshot-list KVM-SBCE-7.2`** command.

   The system displays the **Name**, **Creation Time** and the **State** of the snapshot.

Deleting a snapshot for KVM

About this task

Use the following procedure to delete a snapshot for the virtual machine(VM) KVM-SBCE-7.2.

Before you begin

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

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. Shutdown the VM by using the **`virsh shutdown KVM-SBCE-7.2`** command.

   The system shuts down the KVM-SBCE-7.2 instance.
5. List the created snapshots, using the **`.virsh snapshot-list KVM-SBCE-7.2`** command.

   The system displays the list of all the created snapshots.
6. Delete the snapshot, using the **`virsh snapshot-list KVM-SBCE-7.2`** command with the name of the snapshot.

   # virsh snapshot-revert KVM-SBCE-7.2 <Name of the snapshot>

   The system deletes the specified snapshot.

Restoring a snapshot for KVM

About this task

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

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. Shutdown the VM by using the **`virsh shutdown KVM-SBCE-7.2`** command.

   The system shuts down the KVM-SBCE-7.2 instance.
5. Restore the snapshot, using the **`virsh snapshot-revert KVM-SBCE-7.2`** command.

   #virsh snapshot-revert KVM-SBCE-7.2 <name of the snapshot>

   The system restores the specified snapshot.

Removing an Avaya SBCE or EMS from KVM

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. Shutdown the VM by using the **`virsh shutdown KVM-SBCE-7.2`** command.

   The system shuts down the KVM-SBCE-7.2 instance.
5. Stop the virtual machine using the **`virsh destroy VM_NAME`** command.
6. To delete the virtual machine from KVM use the **`virsh undefine VM_NAME`** command.

   #virsh undefine <Name of the KVM Guest Machine>

Chapter 9: 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 Manager WebLM.

Avaya SBCE license features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.

Table continues…

License feature	Description
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that download of VMware OVA files is permitted for Avaya SBCE.
VALUE_SBCE_ENCRYPTION_1	Specifies the Avaya SBCE encryption, and is required for advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies encryption Avaya SBCE encryption only for signaling.

Chapter 10: 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 7.2.	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 7.2	Port information.	Implementation engineers, Administrators, and Sales engineers

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.

3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Training

The following courses are 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.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller
5U00160E	Knowledge Collection Access: Avaya Unified Communications Core Support

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 http://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.

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 without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any 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 system displays the Avaya Support page.

3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Best Practices

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 console

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 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 63

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 62

Best Practices for VMware performance and features

The following sections describe the 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 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-tuning-latency-sensitive-workloads-white-paper.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. 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.

- 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.

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
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 Documentation Sets	https://www.vmware.com/support/pubs/

Storage

When you deploy Avaya SBCE in a virtualized environment, observe the following storage recommendations:

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

Running performance tune script on host

About this task

Reset the tuning parameters by running the script for optimization.

Procedure

1. Log in to the Avaya SBCE virtual machine as root.
2. Type `scp /usr/local/ipcs/icu/scripts/tunevmxnet3.py` *`username`*`@`*`hostname`*`:/opt`, where *username* and *hostname* are the host credentials.

   The system copies the script `tunevmxnet3.py` to the VM host.
3. Type `/opt/tunevmxnet3.py` *`SBCE-VM`*, where *SBCE-VM* is the name of the Avaya SBCE VM instance.
4. Type `ethtool -G vmnic0 rx 4078`.

   Vmnic0 is the virtual network for VM.

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 from 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, the system displays a warning on the user interface.

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

Order for restoring VMware snapshot

If you revert the VMware snapshot before upgrading, ensure that you restore the VMware snapshots in the following order:

1. EMS
2. Avaya SBCE

VMware cloning

Avaya SBCE does not support VMware cloning.

High Availability

In Virtualized Environment, use the VMware High Availability (HA) method to recover Avaya SBCE when an ESXi host failure occurs. For more information, see the High Availability document for VMware.

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

Application	A software solution development by Avaya that includes a guest operating system.
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.
EASG	Enhanced Access Security Gateway. The Avaya Services Logins to access your system remotely. The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.
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.
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 an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based client version is VMware 6.5 and later.

Index

K

L

M

N

O

P

R

S

T

U

V