



Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment

Release 8.0.x
Issue 4
August 2019

© 2014-2019, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published 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](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](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. Unless otherwise stated, 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](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 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 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](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 | 8 |
| Purpose..... | 8 |
| Change history..... | 8 |
| Chapter 2: Architectural overview | 9 |
| Virtualization overview..... | 9 |
| Kernel-based Virtual Machine overview..... | 9 |
| Deployment modes..... | 10 |
| Chapter 3: Planning and preconfiguration | 12 |
| Supported software and hardware..... | 12 |
| Supported browsers..... | 13 |
| Deployment guidelines..... | 13 |
| Password policies..... | 13 |
| Supported tools for deploying the KVM OVA..... | 14 |
| Virtualized components..... | 14 |
| VMware and KVM resource reservation specifications..... | 15 |
| VMware deployment options..... | 15 |
| Customer configuration data..... | 16 |
| Chapter 4: Deploying and configuring Avaya SBCE on VMware | 17 |
| Checklist for deploying and configuring EMS and Avaya SBCE on vSphere..... | 17 |
| Deploying Avaya SBCE using vSphere Desktop client and vSphere web client..... | 19 |
| Deploying EMS on ESXi 6.x using vSphere Desktop client..... | 19 |
| Deploying SBCE on ESXi 6.x using vSphere desktop client..... | 22 |
| Deploying EMS and SBCE on single server on ESXi 6.x using vSphere desktop client..... | 24 |
| Deploying Avaya SBCE OVA on ESXi 6.x using vSphere web client..... | 26 |
| Deployment of cloned and copied OVAs..... | 26 |
| Migrating from a physical server to VMWare..... | 27 |
| Deploying Avaya SBCE using CLI..... | 27 |
| Deploying EMS and SBCE on single server using CLI..... | 27 |
| Deploying EMS using CLI..... | 30 |
| Deploying SBCE using CLI..... | 32 |
| Field descriptions..... | 35 |
| Configuring vSwitches on ESXi host | 37 |
| Configuring EMS for network connectivity..... | 38 |
| Configuring SBCE or EMS+SBCE for network connectivity..... | 39 |
| Configuring a time server..... | 40 |
| Configuring the virtual machine automatic startup settings on VMware..... | 40 |
| Chapter 5: Deploying and configuring Avaya SBCE on KVM | 42 |
| Overview..... | 42 |
| Prerequisites for deploying Avaya SBCE on KVM..... | 42 |

| | |
|---|-----------|
| Extracting KVM OVA..... | 42 |
| Deploying SBCE or EMS+SBCE on KVM OVA using Virt Manager..... | 43 |
| Deploying EMS on KVM OVA using Virt Manager..... | 44 |
| Deploying application by using Nutanix..... | 45 |
| Logging on to the Nutanix Web console..... | 45 |
| Transferring the files by using the WinSCP utility..... | 45 |
| Uploading the qcow2 image..... | 46 |
| Creating the virtual machine by using Nutanix..... | 46 |
| Starting a virtual machine..... | 48 |
| Configuring the virtual machine..... | 49 |
| Chapter 6: Post-installation verification..... | 50 |
| Successful deployment of SBCE verification..... | 50 |
| Logging on to the EMS web interface..... | 50 |
| Logging in to the EMS using SSH..... | 50 |
| Installing and verifying successful installation of EMS and Avaya SBCE..... | 51 |
| Chapter 7: Maintenance procedures..... | 52 |
| VMware Snapshots..... | 52 |
| Creating a snapshot for Vmware..... | 52 |
| Deleting a snapshot for VMware..... | 53 |
| Restoring a snapshot for VMware..... | 54 |
| Creating a snapshot for KVM..... | 54 |
| Deleting a snapshot for KVM..... | 55 |
| Restoring a snapshot for KVM..... | 56 |
| Removing an Avaya SBCE or EMS from VMware..... | 57 |
| Removing an Avaya SBCE or EMS from KVM..... | 57 |
| Determining whether Avaya SBCE is installed on VMware..... | 57 |
| Chapter 8: Licensing requirements..... | 59 |
| Avaya SBCE license features..... | 59 |
| License installation..... | 61 |
| Configuring WebLM server IP address on EMS..... | 62 |
| Configuring WebLM server IP address using CLI..... | 63 |
| Chapter 9: Resources..... | 64 |
| Documentation..... | 64 |
| Finding documents on the Avaya Support website..... | 65 |
| Accessing the port matrix document..... | 65 |
| Avaya Documentation Portal navigation..... | 66 |
| Training..... | 67 |
| Viewing Avaya Mentor videos..... | 67 |
| Support..... | 68 |
| Appendix A: Best Practices..... | 69 |
| Best practices for achieving a secure virtualized DMZ deployment | 69 |
| References..... | 70 |
| Best Practices for VMware performance and features..... | 71 |

| | |
|--|-----------|
| BIOS..... | 71 |
| VMware Tools..... | 72 |
| Timekeeping..... | 73 |
| Configuring the NTP time..... | 74 |
| VMware networking best practices..... | 74 |
| Storage..... | 75 |
| Thin vs. thick deployments..... | 75 |
| Running performance tune script on host..... | 76 |
| Best Practices for VMware features..... | 77 |
| Glossary..... | 80 |

Chapter 1: Introduction

Purpose

This document contains Avaya Session Border Controller for Enterprise installation, configuration, initial administration, and basic maintenance checklist and procedures for deploying Avaya SBCE on the following:

- VMware
- Kernel-based Virtual Machine

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

Change history

| Issue | Date | Summary of changes |
|-------|---------------|--|
| 1 | February 2019 | Release 8.0 document. |
| 2 | March 2019 | Updated the “VMware and KVM resource reservation specifications” section to include information about EMS+SBC. |
| 3 | July 2019 | <ul style="list-style-type: none">• Updated Resources map.• Updated Licensing map. |
| 4 | August 2019 | Updated the instances of 8.0 to 8.0.x. |

Chapter 2: Architectural overview

Virtualization 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.

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

You can deploy EMS and Avaya SBCE using a single OVA file.

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).

Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.

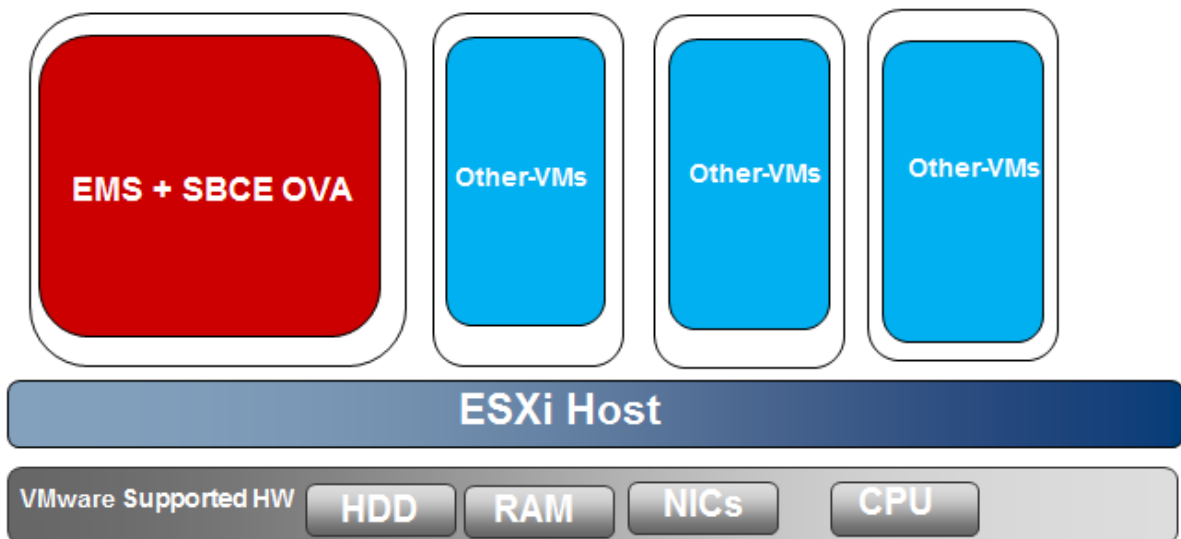
- Open source software that can be customized as per the changing business requirements of the customers.

Deployment modes

Avaya SBCE supports following deployment modes:

- Avaya SBCE standalone mode:

If you select a standalone deployment, the OVA file installs configurations for both Avaya SBCE and EMS. In the standalone configuration, Avaya SBCE and EMS coreside in the same physical server.

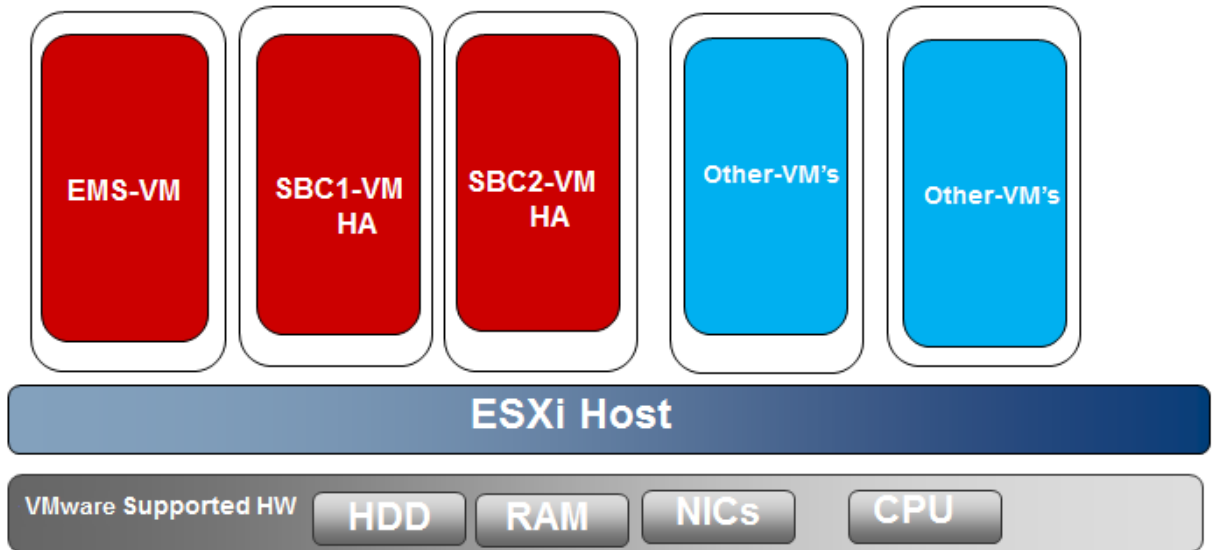


- Multiple server configuration:

In the multiple server configuration, EMS and Avaya SBCE are deployed on the separate physical servers.

- EMS and Avaya SBCE in High Availability mode:

For High Availability mode, deploy the OVA file separately for EMS and Avaya SBCE. You can also deploy EMS and Avaya SBCE using a single OVA file and select different configurations to deploy EMS and Avaya SBCE.



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 ESXi versions:

| VMware ESXi version | Avaya SBCE Release number | | |
|---------------------|---------------------------|--------------------------------|---------------|
| | Release 7.2 | Release 7.2.1 Release 7.2.2 | Release 8.0.x |
| 5.1 | √ | √ | x |
| 5.0 | √ | √ | x |
| 5U1 | √ | √ | x |
| 5.5 | √ | √ | x |
| 6.0 | √ | √ | √ |
| 6.5 | x | √ | √ |
| 6.7 | x | 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.

Avaya SBCE supports deployments on Linux Kernel based Virtual Machine (KVM) and KVM using Nutanix. Avaya SBCE uses KVM QEMU version 1.5.3 which runs on RedHat version 7.2 and Nutanix version 5.1.0.1.

Supported browsers

Avaya SBCE supports following browsers for accessing EMS:

- Microsoft Internet Explorer 11.0 or later
- Microsoft Edge 20.0 or later
- Mozilla Firefox 60.0/ 60.0 ESR or later
- Google Chrome 59.0 or later
- Apple Safari (4) 9.0 or later

Avaya SBCE supports following browsers for deploying OVA on VMHost:

- Microsoft Edge
- Mozilla Firefox version 60.0 and later
- Apple Safari (4) 9.0 or later

 **Note:**

Avaya recommends to use Microsoft Edge browser.

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>.

Deployment guidelines

- Deploy maximum number of virtualized environment on the same host.
- Deploy the virtualized environment 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 virtualized environment performance.

Password policies

The root and ipcs passwords are determined and set during product installation. The EMS GUI has a separate password. When you log in for the first time after installation, the system prompts you

to create a new password for accessing the EMS GUI. The default user ID and password is `ucsec`.

Password restrictions are enforced on the `ucsec` and `ipcs` accounts. The new password must meet the password criteria of minimum 8 characters, including:

- One uppercase letter, one lowercase letter, and one number.
- One special character from the hyphen (-), underscore (_), at sign (@), asterisk (*), and exclamation point (!). You must not use the number sign (#), dollar sign (\$), and ampersand (&).

*** Note:**

The customer network administrator determines the Avaya SBCE CLI root and `ipcs` passwords during the installation procedure. Two installation steps prompt the installer to enter a chosen password.

Supported tools for deploying the KVM OVA

You need one of the following tool to deploy KVM OVA.

- Virt Manager GUI
- `virsh` command line interface

Virtualized components

| Software component | Description |
|------------------------|---|
| ESXi Host | The physical machine running the ESXi Hypervisor software. |
| ESXi Hypervisor | A platform that runs multiple operating systems on a host computer at the same time. |
| vSphere Client | vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface. The installable vSphere Client is not available in vSphere 6.5 and later releases. |
| vSphere Web Client | Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. |
| vSphere Client (HTML5) | vSphere Client (HTML5) is available in vSphere 6.0 or later. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release. |

Table continues...

| Software component | Description |
|--------------------|---|
| vCenter Server | vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion. |

VMware and KVM resource reservation specifications

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

- SBC: Resource reservation equivalent to standalone Avaya SBCE 310 model.
- EMS: Resource reservation required for running only EMS

Table 1: Avaya SBCE resource requirements on VMHost and KVM:

| Resource | Variant | |
|--|---|---|
| | SBC | EMS |
| vCPU core | 4 dedicated cores | 3 floating cores |
| vCPU reservation | 8800 MHz to 9600 MHz | 6600 MHz to 7200 MHz |
| 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 Virtual Interfaces @ 100 Mbps or 1000 Mbps |

*** Note:**

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

You can run Avaya SBCE in SBC+EMS mode or SBC only mode. You can only combine SBCE +EMS when you have a single machine (HW or virtual) with no HA, that is small or medium configuration. This configuration requires only 1x 4cpu-8gig of RAM for both SBCE and EMS functions. For an HA pair, you need to separate the EMS function from SBC and you require 2x4vcpu + 8Gig (HA pair) and 1x3vcpu+8G (EMS).

VMware deployment options

From Release 8.0, same OVA can be used to deploy all the below configurations.

| VMware OVA type | Configuration type | | |
|-----------------|--------------------|----------|------|
| | EMS | SBCE+EMS | SBCE |
| SBC | X | √ | √ |

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 |

Chapter 4: Deploying and configuring Avaya SBCE on VMware

Checklist for deploying and configuring EMS and Avaya SBCE on vSphere

| # | Action | Description | Link | ✓ |
|---|---|-------------|------|---|
| 1 | Download the following ova file from the PLDS website at https://plds.avaya.com : sbce-8.0.x.0-xx-xxxxx.ova | | | |

Table continues...

| # | Action | Description | Link | ✓ |
|---|--|--|--|---|
| 2 | <p>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 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.</p> <p>Ensure that you have a license file with the following feature:</p> <pre>FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1</pre> <p>* Note:</p> <p>You can enable and use the HA feature only when the license file contains an HA license.</p> | Applicable only to multiple server HA scenarios. | | |
| 3 | Install vSphere Client from the VMware website. | Download the third-party client from the VMware website. | | |
| 4 | Keep the configuration data ready. | | Customer configuration data on page 16 | |

Table continues...

| # | Action | Description | Link | ✓ |
|----|--|--|---|---|
| 5 | Deploy EMS OVA template. | | Deploying EMS on ESXi 6.x using vSphere Desktop client on page 19 | |
| 6 | Configure EMS. | | Deploying EMS on ESXi 6.x using vSphere Desktop client on page 19 Deploying EMS using CLI on page 30 | |
| 8 | Deploy Avaya SBCE. | | Deploying SBCE using CLI on page 32 Deploying SBCE on ESXi 6.x using vSphere desktop client on page 22 | |
| 10 | Create vSwitches. | Create virtual switches for M1, M2, and any of the following interfaces: A1, A2, B1, and B2. | Configuring vSwitches on ESXi host on page 37 | |
| 7 | Configure EMS for network connectivity. | | Configuring EMS for network connectivity on page 38 | |
| 9 | Configure Avaya SBCE for network connectivity. | | Configuring Avaya SBCE for network connectivity on page 39 | |
| 11 | Configure Avaya SBCE and EMS to start automatically after a power failure. | | Configuring the virtual machine automatic startup settings on page 40 | |
| 12 | Verify the installation of Avaya SBCE. | | Installing and verifying successful installation of EMS and Avaya SBCE on page 51 | |

Deploying Avaya SBCE using vSphere Desktop client and vSphere web client

Deploying EMS on ESXi 6.x using vSphere Desktop client

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 one of the following using the IP address and the password for the ESXi host:
 - ESXi host using vSphere
 - vCenter using vCenter Client

Ignore any security warning that the system displays.

2. Download `sbce-8.0.x.0-xx-xxxxx.ova` from PLDS.
3. On the vSphere client, navigate to **File > Deploy OVF Template**.
4. 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 and click **Next**.
 - Click **Browse**, navigate to the downloaded .ova file, and click **Next**.
5. On the OVF Template Details page, verify the details and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. On the Name and Location page, in the **Name** field, type the name of the virtual machine.
The name can contain up to 80 characters and it must be unique within the inventory folder.
9. **(Optional)** If you logged in through vCenter, then 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.
10. **(Optional)** On the resource pool selection page, select the appropriate resource pool and click **Next**.
The vSphere Client displays the Deployment Configuration page.
11. In the **Configuration** field, click **EMS..**

 **Note:**

For Thick Provision Lazy Zeroed and Thin Provision resource requirement information, see “VMware and KVM specifications” topic.

12. 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.
13. Select **Thin Provision** to minimize disk allocation.
Use this option only in the lab environment.
14. Click **Next**.
15. **(Optional)** If you logged in through vCenter then, in the Resource Allocation window, click **Next**.

16. On the Network Mapping page, in the **Source Network** column, configure Network 1 with the configuration information of the management network in the **Destination Network** column.
17. 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 configuration parameters properties template.

18. Click **Next**.
19. Select **Power on after deployment** to power on the system automatically after deployment.

Alternatively, you can power on the system manually after deployment is complete.

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

The system deploys the EMS.

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 options are: <ul style="list-style-type: none"> • IPV4 • DUAL STACK |
| Hostname | hostname | The host name of the device. |
| Appliance Type | apptype | The deployment type for the device. The options are: <ul style="list-style-type: none"> • 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 options are: <ul style="list-style-type: none"> • 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 time zone of the device. |
| NTP Server Address | ntpserver | 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 the EMS system. It is used only for separate SBCE deployments. |
| Root/Ipcs/Grub Passwords | rootpass/ipcspass/grubpass | The passwords for root, ipc, and grub. |

Deploying SBCE on ESXi 6.x using vSphere desktop client

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.
- Specify the network information in the OVA Template Details page, in the **Destination Network** column.

Procedure

1. Log on to one of the following using the IP address and the password for the ESXi host:
 - ESXi host using vSphere
 - vCenter using vCenter Client

Ignore any security warning that the system displays.

2. Download `sbce-8.0.x.0-xx-xxxxx.ova` from PLDS.

3. On vSphere Client, click **File > Deploy OVF Template**.
4. 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 .ova file.
 - Click **Browse** and navigate to the .ova file located on the local computer, network share, CD-ROM, or DVD and click **Enter**.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, type the name of the virtual machine.

The name can contain up to 80 characters and it must be unique within the inventory folder.

9. Click **Next**.

If one or more resource pools exist, the system displays a resource pool selection page.
10. Select the appropriate resource pool, and click **Next**.

The system displays the Deployment Configuration page.

11. In the **Configuration** field, select **SBCE**.

*** Note:**

For Thick Provision Lazy Zeroed and Thin Provision resource requirement information, see “VMware and KVM specifications” topic.

12. 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.

13. Click **Next**.

The system displays the Network Mapping page.

14. Click the network for management interface for each network that you specified in the OVA Template Details page, in the **Destination Network** column.

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 up to six interfaces.

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

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

16. Click **Next**.
17. Select **Power on after deployment** to power on the system automatically after deployment.
Alternatively, you can power on the system manually after deployment is complete.
18. Review the settings and click **Finish**.
19. Wait until the system deploys the OVA file successfully.
20. **(Optional)** Repeat steps 1 to 19 to deploy SBCE in HA mode.

Deploying EMS and SBCE on single server on ESXi 6.x using vSphere desktop client

Before you begin

- Install vSphere Client from the ESXi host web page. Type `https://ESXi host ip` in the address bar of the browser, 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 one of the following using the IP address and the password for the ESXi host:
 - ESXi host using vSphere
 - vCenter using vCenter ClientIgnore any security warning that the system displays.
2. Download `sbce-8.0.x.0-xx-xxxxx.ova` from PLDS.
3. On vSphere Client, click **File > Deploy OVF Template**.
4. 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 .ova file.
 - Click **Browse** and navigate to the .ova file located on the local computer, network share, CD-ROM, or DVD and press Enter.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.

8. On the Name and Location page, in the **Name** field, type the name of the virtual machine.
The name can contain up to 80 characters and it must be unique within the inventory folder.
9. Click **Next**.
If one or more resource pools exist, the system displays a resource pool selection page.
10. Select the appropriate resource pool, and click **Next**.
The system displays the Deployment Configuration page.
11. In the **Configuration** field, select **SBCE**.
 - * **Note:**
For Thick Provision Lazy Zeroed and Thin Provision resource requirement information, see “VMware and KVM specifications” topic.
12. 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.
13. Click **Next**.
The system displays the Network Mapping page.
14. Click the network for management interface for each network that you specified in the OVA Template Details page, in the **Destination Network** column.
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 up to six interfaces.
15. In the **Properties** template, enter the requested information in the appropriate fields to deploy SBCE on vSphere.
The vSphere cClient does not display configuration through the CLI mode. The device is deployed according to the configuration parameters of the properties template..
16. Click **Next**.
17. Select **Power on after deployment** to power on the system automatically after deployment, otherwise you have to power on the system manually.
Alternatively, you can power on the system manually after deployment is complete.
18. Review the settings and click **Finish**.

19. Wait until the system deploys the OVA file successfully.
20. **(Optional)** Repeat steps 1 to 19 to deploy SBCE in HA mode.

Deploying Avaya SBCE OVA on ESXi 6.x using vSphere web client

Before you begin

If you are deploying Avaya SBCE using vCenter, then the following procedure is not required. You can use the procedure for deploying Avaya SBCE using vCenter of version 6.x.

Type `https://ESXi host IP` to access the ESXi host using the web interface.

Procedure

1. Click **Deploy a virtual machine from an OVF or OVA file** from the **Select creation type** field to create or register a Virtual Machine (VM).
2. Select the OVA file for the VM that you want to deploy and type the name for the VM.
3. Select storage and accept the license agreement.
4. Click **Deployment options** and do the following:
 - a. In **Network mappings** option, type a name for Network 1. Network 1 should be the management network.
 - b. Click **Thick** to select Thick Provision Lazy Zeroed, in the **Disk provisioning** field.
 - c. Clear the **Power on automatically** check box.
5. After the Avaya SBCE VM is deployed, do one of the following:
 - To deploy a standalone EMS server, power on the VM and complete the configuration.
 - To deploy a standalone SBC or EMS+SBCE server, perform the following steps before powering on the VM:
 - a. Select the VM option from left pane and navigate to **Actions > Edit settings**.
 - b. Click **Add Network Adapter** and add four new network adapters.
 - c. Click **X** to remove the CD or DVD drive option.
 - d. Click **Save** to save the changes.
 - e. Power on the VM and open the console.
 - f. Select the device type and configure the deployment. For more information, see *Deploying Avaya Session Border Controller for Enterprise*.

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 in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for creating snapshot for the EMS server or **SBCE** for device specific snapshot configuration.
3. In the navigation pane, click **Backup/Restore**.
4. On the Backup/Restore page, click the **Snapshots** tab.
5. Select the designated snapshot server.
6. Click **Create Snapshot**.

The EMS server displays the Create Snapshot window.

7. Enter a name for the snapshot, and click **Create**.
8. 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.

9. Turn off the power to the server on which EMS is deployed.
10. Deploy the EMS or the SBCE OVA file on VMWare with the same build number and management IP as on the physical server.

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

Deploying Avaya SBCE using CLI

Deploying EMS and SBCE on single server using CLI

Procedure

1. Connect to the system using the same mode that was used for software installation.
2. Turn on the system.
3. Wait for the configuration menu to appear.

The options are:

- 1-configure: Command line mode
- 2-Reboot SBCE
- 3-Shutdown SBCE
- 4-SBCE Shell Login

4. Type **1** for CLI mode.

5. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press **Enter**:

- IPv4
- DUAL STACK

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. The IP Address on Management interface (M1) supports only IPv4.address, it does not depend on the type of **IP Mode**.

6. Type the **Appliance Type** as **EMS+SBCE** and press **Enter**:

- EMS
- EMS+SBCE

7. Type a name for the appliance in the **Appliance Name** and press **Enter**.

8. Type the management IP address in the **Management IP address** field and press **Enter**.

9. Type the subnet mask in the **Management subnet mask** field and press **Enter**.

10. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press **Enter**.

11. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press **Enter**.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press **Enter**.

12. Type the prefix length in the **Management subnet network prefix length** field and press **Enter**.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press **Enter**.

13. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press **Enter**.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press **Enter**.

14. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press **Enter**.

15. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.
This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
16. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.
You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.
17. Type the domain suffix in the **Domain Suffix** field and press `Enter`.
18. Type appropriate value in the **First and Last Name** field and press `Enter`.
19. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
20. Type a name of your organizational unit in the **Organizational Unit** field and press `Enter`.
21. Type your organization name in the **Organization** field and press `Enter`.
22. Type your city or locality name in the **City or Locality** field and press `Enter`.
23. Type your state or province name in the **State or Province** field and press `Enter`.
24. Type the two characters code of your country in the **Country Code** field and press `Enter`.
25. Type the number of your country in the **Please select a country** field to select your country from the list.
26. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
27. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
28. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

Is the above information OK?

*** Note:**

If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:

29. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
30. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
31. Type and confirm the password for root user and then press `Enter`.
32. Type and confirm the same password for the ipcs user and press `Enter`.
Use this password for secure shell (ssh) to gain access to Avaya SBCE.
33. Type and confirm the grub password, and press `Enter`.

A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the

progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

Deploying EMS using CLI

Before you begin

Ensure that the software installation is complete. For more information, see the Installing Avaya SBCE software from a USB or DVD section.

Procedure

1. Connect to the system using the same mode that was used for software installation.
2. Turn on the system.
3. Wait for the configuration menu to appear.

The options are:

- 1-configure: Command line mode
- 2-Reboot SBCE
- 3-Shutdown SBCE
- 4-SBCE Shell Login

4. Type `1` for CLI mode.
5. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press `Enter`:
 - IPv4
 - DUAL STACK

If you are using dual stack for any of the data interfaces, then configure the system with dual stack. The IP Address on Management interface (M1) or (M2) supports only IPv4.address, it does not depend on the type of **IP Mode**.

6. Type the **Appliance Type** as `EMS` and press `Enter`:
7. Type the passphrase in the **Network Passphrase** field and press `Enter`.
8. Type a name for the appliance in the **Appliance Name** field and press `Enter`.
9. Type the installation type for EMS in the **Installation Type** field from the following choices and press `Enter`:
 - Primary
 - Secondary
10. Type the management IP address in the **Management IP address** field and press `Enter`.
11. Type the subnet mask in the **Management subnet mask** field and press `Enter`.

12. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press `Enter`.
13. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
14. Type the prefix length in the **Management subnet network prefix length** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
15. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
16. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press `Enter`.
17. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.
18. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.

You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.
19. Type the domain suffix in the **Domain Suffix** field and press `Enter`.
20. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
21. Type appropriate value in the **First and Last Name** field and press `Enter`.
22. Type a number of your organizational unit in the **Organizational Unit** field and press `Enter`.
23. Type your organization name in the **Organization** field and press `Enter`.
24. Type your city or locality name in the **City or Locality** field and press `Enter`.
25. Type your state or province name in the **State or Province** field and press `Enter`.
26. Type the two characters code of your country in the **Country Code** field and press `Enter`.
27. Type the name of your country in the **Please select a country** field to select your country from the list.
28. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.

29. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
30. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

`Is the above information OK?`

*** Note:**

If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:

31. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
32. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
33. Type and confirm the password for root user and then press `Enter`.
34. Type and confirm the same password for the ipcs user and press `Enter`.

Use this password for secure shell (ssh) to gain access to Avaya SBCE.

35. Type and confirm the grub password, and press `Enter`.

A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

Deploying SBCE using CLI

Before you begin

Ensure that EMS is accessible over the network when Avaya SBCE is being configured.

Procedure

1. Connect to the system using the same mode that was used for software installation.
2. Turn on the system.
3. Wait for the configuration menu to appear.

The options are:

- 1-configure: Command line mode
 - 2-Reboot SBCE
 - 3-Shutdown SBCE
 - 4-SBCE Shell Login
4. Type `1` for CLI mode.

5. Depending on the IP address used in your network, type the **IP Mode** from the following choices and press `Enter`:

- IPv4
- DUAL STACK

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.

6. Type the **Appliance Type** as `SBCE` from the following choices and press `Enter`:

- SBCE
- EMS+SBCE

7. Type a name for the appliance in the **Appliance Name** field and press `Enter`.

8. Type the management IP address in the **Management IP address** field and press `Enter`.

9. Type the subnet mask in the **Management subnet mask** field and press `Enter`.

10. Type the IP address of the gateway in the **Management Gateway IP Address (IPv4)** field and press `Enter`.

11. Type the IP address of the gateway in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

12. Type the IP address of the EMS in **EMS IP address (IPv4)** and press `Enter`.

13. Type the IPv6 address of the EMS in **EMS IP address (IPv6)** and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

14. Type the prefix length in the **Management subnet network prefix length** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

15. Type the IPv6 address in the **Management Gateway IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

16. Type the IP address of the NTP server in the **NTP server IP Address (IPv4)** field and press `Enter`.

17. Type the IPv6 address of the NTP server in the **NTP server IP Address (IPv6)** field and press `Enter`.

This field is applicable only to the IPv6 addresses. Type the value only if you have selected DUAL STACK in the **IP Mode** field, otherwise press `Enter`.

18. Type the IP address of the DNS server in the **List of DNS Servers** field and press `Enter`.
You can either enter comma-separated list of DNS servers or single IP address if only one DNS server is present.
19. Type the domain suffix in the **Domain Suffix** field and press `Enter`.
20. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
21. Type appropriate value in the **First and Last Name** field and press `Enter`.
22. Type a name of your organizational unit in the **Organizational Unit** field and press `Enter`.
23. Type your organization name in the **Organization** field and press `Enter`.
24. Type your city or locality name in the **City or Locality** field and press `Enter`.
25. Type your state or province name in the **State or Province** field and press `Enter`.
26. Type the two characters code of your country in the **Country Code** field and press `Enter`.
27. Type the number of your country in the **Please select a country** field to select your country from the list.
28. Confirm the details and press `Enter`. Type `No`, if you want to re-enter the details.
29. Type the continent and ocean details in the **Continent** and **Ocean** fields for your timezone.
30. Type your choice in the **Set Timezone**. and when following message is displayed, type `Yes` to confirm.

Is the above information OK?

 **Note:**

If you have specified an NTP server that is not reachable, then system will prompt you to set the date and time manually and following two fields will be displayed:

31. Type date in yyyy/mm//dd format in the **Date** field and press `Enter`.
32. Type time in hh:mm:ss format in the **Time** field and press `Enter`.
33. Type and confirm the password for root user and then press `Enter`.
34. Type and confirm the same password for the ipcs user and press `Enter`.
Use this password for secure shell (ssh) to gain access to Avaya SBCE.
35. Type and confirm the grub password, and press `Enter`.




A series of scripts automatically run, which configure Avaya SBCE with the information that you type. As these scripts run, the video display shows a series of outputs reflecting the progress of the configuration. The configuration is successfully complete when the system displays the login prompt.

Next steps

After configuring Avaya SBCE, take a snapshot of the Avaya SBCE configuration. For information about backing up the Avaya SBCE database, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Field descriptions

Appliance Configuration field descriptions

| Name | Description |
|-------------------------------------|--|
| Appliance Name | <p>A descriptive name assigned to the EMS or Avaya SBCE.</p> <p> Note: Ensure that the appliance name is unique.</p> |
| Domain Suffix (Optional) | The domain within which this server is deployed. |
| List of DNS Servers | <p>The IP address of each Domain Name Server (DNS).</p> <p> Note: The list of DNS server names must be comma-separated, with no spaces. Only two IP addresses are allowed here.</p> |
| NTP Server IP Address (ipv4) | <p>The IPv4 IP address of the Network Time Protocol (NTP) server. If no NTP is present, configure manually. Only one IP address can be configured.</p> <p>For an HA pair, both Avaya SBCE servers must have the NTP address.</p> <p>You must configure NTP Server IP Address (ipv4) if TLS or encryption is enabled.</p> |
| Network Passphrase | <p>A unique password that the EMS server and Avaya SBCE security devices deployed throughout the network will use for authentication.</p> <p>This field is displayed for Avaya SBCE-only installations.</p> <p> Important: The same passphrase must be configured on all the SBCE instances that are managed by an EMS and on the managing EMS as well. Different passphrases prevent the EMS and Avaya SBCE security devices from communicating with one another.</p> |

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) | <p>The IPv6 address of the management network.</p> <p>The system displays this field only when you select Dual Stack on the Management IP Configuration screen.</p> <p> Note:</p> <p>In Dual Stack the IPv6 address is optional but the IPv4 address is compulsory.</p> |
| Management Network Pfx length | <p>The length of the prefix for the management network IPv6 address.</p> <p>The system displays this field only when you select Dual Stack on the Management IP Configuration screen.</p> |
| Management Gateway IP Address (ipv6) | <p>The IPv6 address of the gateway to the management network.</p> <p>The system displays this field only when you select Dual Stack on the Management IP Configuration screen.</p> <p> Note:</p> <p>In Dual Stack the IPv6 address is optional but the IPv4 address is compulsory.</p> |
| EMS Server IP Address (ipv4) | <p>The IP address of the EMS server.</p> <p>This field is displayed for Avaya SBCE only installations.</p> |
| Self-signed certificate fields | |
| First and Last Name | The name used to refer to or identify the company or group creating the certificate. |
| Organizational Unit | The group within the company organization creating the certificate. |
| Organization | The name of the company or organization creating the certificate. |
| City or Locality | The city or locality where the certificate is being created. |

Table continues...

| Name | Description |
|-------------------|--|
| State or Province | The state or province where the certificate is being created. |
| Country Code | The number to identify the country where the certificate is being created. |

! Important:

- When using SSL or VPN is configured on the M1 interface, 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. M1 is the management interface that is the required interface for SSL or VPN.
- All the self-signed certificate fields are applicable only on the management interface, for communication with the user interface and with the Avaya Aura[®] components. The values for self signed certificate are optional, if you will not provide any value then certificate will be generated by using the default values of the fields.

***** 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*.
- Network Security Agency: *Recommended IP Telephony Architecture*.
- National Institute of Standards and Technology (NIST): *Security Considerations for Voice Over IP Systems*.

Configuring vSwitches on ESXi host

About this task

- Use this procedure to create 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.
- You must repeat the following procedure for all the required vSwitches. For example, if your require interface M1 and A1 on different physical NIC then you will require three vSwitches to configure the interfaces.

Procedure

1. On vSphere client, click the **Configuration** tab.
2. In the Hardware section of the left navigation pane, click **Networking > Add Networking**.

The system displays the Add Network Wizard window.

3. In the Connection Type page, click **Virtual Machine**.
4. In the Network Access page, click **Assign Physical NIC to vSwitch** to select the physical NIC that provides connectivity to the network for the required vSwitch.

For example, if you are creating a vSwitch for management interface M1 then, the selected physical NIC provides external connectivity to the network.
5. In the Connection Settings page, in the **Network Label** field, type an interface name.
6. In the Connection Settings page, select the time zone.
7. In the Connection Settings page, in the **VLAN ID (optional)** field, click the VLAN ID.
8. Click **Finish**.

Next steps

Note:

For HA configuration, you require M2 interface for both Avaya SBCE systems. If the two SBCE instances are running on the same ESXi host, then the vSwitch for the M2 interface does not require a physical 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.

Configuring EMS for network connectivity

Before you begin

Deploy EMS by configuring the root and ipcs passwords and reboot the system.

Procedure

1. Log in to the EMS command line interface using the ipcs login and ipcs password.
To access root privileges, log in as root user.
2. To identify which MAC address is in use for M1 interface, type `ip link show M1`.
3. Note down the MAC address for future reference.
4. Right-click on the VMware user interface and click **Edit Settings**.
5. In the **Hardware** tab, compare the MAC address displayed in the **Network Adapter 1** field with the MAC address that is displayed using the `ip address` command. If the addresses do not match, contact Avaya support at <http://support.avaya.com>.
6. Select the vSwitch and in the **Network label** field, select the label corresponding to the management network.
7. In the **Network label** field, select the label corresponding to the management network.
8. Click **OK**.

Configuring SBCE or EMS+SBCE for network connectivity

Before you begin

Deploy SBCE or EMS+SBCE by configuring root and ipcs passwords and reboot the system.

Procedure

1. Log in to the EMS command line interface using ipcs login and ipcs password.
To access root privileges, login as root user.
2. To identify which MAC address is in use for M1 interface, type `ip link show M1`.
3. Note the MAC address.
4. Right-click on the Avaya SBCE virtual instance and click **Edit Settings**.
5. 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. If the addresses do not match then contact Avaya support at <http://support.avaya.com>.
6. Select the vSwitch and in the **Network label** field select the label corresponding to the management network.
7. Click **OK**.
8. To identify which MAC address is in use for M2 interface, type `ip link show M2`.
9. Note the MAC address.
10. Right-click on the Avaya SBCE virtual instance, and then click **Edit Settings**.
11. In the **Hardware** tab, in the **Network Adapter 2** field, confirm if the MAC address matches with the MAC address that is displayed by using the IP address command at step 9. If the addresses do not match then contact Avaya support at <http://support.avaya.com>.
12. Select the vSwitch and then in the **Network label** field, select the label corresponding to the HA network label.
13. Click **OK**.
14. Repeat Steps 8 to 12 for A1, A2, B1 and B2 interfaces by attaching the network adapter to their respective vSwitches.
15. Click **OK**.

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

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. Use this procedure to configure servers for different Avaya SBCE virtual machines when you have different NTP servers across locations

Procedure

1. In the vSphere Client inventory, choose the virtual machine and click **Power off**.
2. In the **Summary** tab, click **Edit Settings**.
3. Click **Options > General**.
4. Click **Configuration Parameters**.
5. Click **Add Row** and enter information in the following fields:
 - **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

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 does not use the startup selections.

Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Configure**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Properties**.
The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

Chapter 5: Deploying and configuring Avaya SBCE on KVM

Overview

You can deploy Avaya SBCE on KVM using one of the following:

- Virt Manager GUI
- Nutanix

Prerequisites for deploying Avaya SBCE on KVM

Before deploying the Avaya SBCE KVM OVA, ensure that you have the following knowledge, skills and tools.

Knowledge

- KVM hypervisor installation and set up
- Linux® Operating System
- Avaya SBCE
- Nutanix

Skills

To administer the KVM hypervisor and Avaya SBCE.

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

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 SBCE or EMS+SBCE on KVM OVA using Virt Manager

Before you begin

1. Download the KVM guest template image from PLDS on local deployment server.
2. Copy the downloaded KVM guest image to the KVM host in the storage directory.
3. Use the KVM guest image as a base to create new images for each new KVM based instance. For example, use `sbce-8.0.x.0-10-13055.qcow2` to create a new image with the following command: `cp -ap sbce-8.0.x.0-10-13055.qcow2 KVM-SBCE-8.0-qcow2`.

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.
The KVM host 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 as explained in the **Before you begin** section.
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 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. Avaya recommends to select **Device Model** as `virtio` and **Network Source** as the bridge type for better performance.

13. Click **Add Hardware**.
14. Click **Network**.
15. Provide a network source 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 15 four times to deploy SBCE or EMS+SBCE for a total of six NICs on KVM.

19. Click **Begin installation**.

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

Deploying EMS on KVM OVA using Virt Manager

Before you begin

- Download the KVM guest template image from PLDS on a 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-8.0.x.0-10-13055.qcow2` to create a new image with the following command: `cp -ap sbce-8.0.x.0-10-13055.qcow2 KVM-SBCE-8.0-qcow2`.

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, type `virt-manager`.
The KVM host displays the Virtual Machine Manager web interface.
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 as explained in the **Before you begin** section..
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 for 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. Avaya recommends to select **Device Model** as virtio and **Network Source** as the bridge type for better performance.

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 KVM host displays a console with Avaya SBCE kernel bootup messages. After the startup scripts run, the KVM host displays the Avaya SBCE configuration 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 Adapters (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 Adapters (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 6: Post-installation verification

Successful deployment of SBCE verification

You can verify the successful deployment of EMS using one of the following methods:

- Access the EMS server using the web interface.
- Access the EMS server through console.
- Establish a CLI session through a secure shell session (SSH).

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.

Logging in to the EMS using SSH

Procedure

1. Log in to SSH client using 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.

Installing and verifying successful installation of EMS and Avaya SBCE

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.
Following step is not applicable for the single server deployment of Avaya SBCE.
3. On the Device 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 Device Management page, the **Status** column of the Avaya SBCE device displays Registered.

4. Click **Install**.
5. In the Install Wizard, type the configuration. For more information, see *Administering Avaya Session Border Controller* document.
6. Click **Finish**.

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

Chapter 7: Maintenance procedures

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. For more information about snapshots for EMS or SBCE, see *Administering Avaya Session Border Controller for Enterprise* document.

Creating a snapshot for VMware

Before you begin

 **Warning:**

Snapshots can cause performance issues with Avaya SBCE. It is recommended to use snapshots for short periods of time.

 **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.

 **Caution:**

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

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 for VMware

*** 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 that you want to delete.
4. Select **Delete from Disk**.
5. When the system displays a dialog box for confirmation, click **Yes**.
6. If you are using the vSphere Web Client, click **Close** to close the Snapshot Manager.

Restoring a snapshot for VMware

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 system displays the `Completed` message

Creating a snapshot for KVM

About this task

Use the following procedure to create a snapshot for the virtual machine (VM) KVM-SBCE-8.0 where KVM SBCE 8.0 is an example of the filename.

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 powered off 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-8.0` command.

The system shuts down the KVM-SBCE-8.0 instance.

5. Take the snapshot by using the `virsh snapshot-create KVM-SBCE-8.0` command.

6. Enter a name to identify the snapshot.

7. View the snapshot, using the `virsh snapshot-list KVM-SBCE-8.0` 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-8.0 where KVM SBCE 8.0 is an example of the filename.

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 permission.

2. At the console, type `virt-manager`.

The system displays the Virtual Machine Manager GUI.

3. Type `2` for CLI mode.

4. List the created snapshots, using the `virsh snapshot-list KVM-SBCE-8.0` command.

The system displays the list of all the created snapshots.

5. Delete the snapshot, using the `virsh snapshot-list KVM-SBCE-8.0` command with the name of the snapshot.

```
virsh snapshot-delete KVM-SBCE-8.0 <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. Use the following procedure to delete a snapshot for the virtual machine (VM) KVM-SBCE-8.0 where KVM SBCE 8.0 is an example of the filename.

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-8.0` command.

The system shuts down the KVM-SBCE-8.0 instance.

5. List the created snapshots, using the `virsh snapshot-list KVM-SBCE-8.0` command.

The system displays the list of all the created snapshots.

6. Restore the snapshot, using the `virsh snapshot-revert KVM-SBCE-8.0` command where KVM SBCE 8.0 is an example of the filename.

```
#virsh snapshot-revert KVM-SBCE-8.0 <name of the snapshot>
```

The system restores the specified snapshot.

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**.

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-8.0` command.
The system shuts down the KVM-SBCE-8.0 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>
```

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.

Chapter 8: Licensing requirements

Avaya SBCE uses WebLM version 8.0.0.0 for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the Device 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. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBCE works normally during the grace period.

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

All hardware Avaya SBCE devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

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. |
| 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. |

License installation

You can install Avaya SBCE license on either of the following servers:

- The WebLM server on System Manager
- The local WebLM server

Installing a license on WebLM server on System Manager

Before you begin

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com/>.

About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering standalone Avaya WebLM*.

Procedure

1. Log in to the System Manager web interface.
2. On the home page, in the **Services** section, click **Licenses**.
3. In the left navigation pane, click **Install license**.
4. Browse to the location where you saved the license file, and select the file to upload.
5. Click **Install**.
6. Verify that the license is installed. If the installation is successful, a new menu item named **ASBCE** appears in the left navigation pane. Click **ASBCE** to view the licensed features.

Installing a license file on the local WebLM server

Procedure

1. Log in to the WebLM application. If you are logging in for the first time, the system prompts you to change the default password.
2. In the left navigation pane, click **Install License**.
The system displays the Install License page.
3. In the **Enter license path** field, select the downloaded license from your computer and click **Install**.
After the license is successfully installed, the system displays a new menu **ASBCE**.
4. Click **ASBCE** to view the license information.

Configuring WebLM server IP address on EMS

Before you begin

Install the Avaya SBCE license file on WebLM server installed on System Manager , local WebLM, or standalone WebLM server. For more information about installing license files and WebLM server, see *Administering Avaya Aura® System Manager* and *Administering standalone Avaya WebLM*.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation page, click **Device Management**.
3. On the Device Management page, click the **Licensing** tab.
4. Perform one of the following tasks:
 - For a WebLM server or standalone server installed on System Manager , in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

The url format of the WebLM server installed on System Manager is `https://<SMGR_server_IP>:52233/WebLM/LicenseServer` and the standalone WebLM server is `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.
 - For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.
5. Click **Refresh Existing License** to refresh the existing licenses.
6. Click **Verify Existing License** to verify the existing WebLM license to confirm it is trusted.

If the WebLM license is trusted, a pop window will display the certificate details. Otherwise, you can select the option to trust the WebLM certificate manually.
7. On the Dashboard screen, check the **License State** field.

If the configuration is successful, the **License State** field shows **OK**.
8. Click the **Devices** tab.
9. Locate the Avaya SBCE device you configured, and click **Edit**.

The EMS server displays the Edit Device dialog box.
10. In the **Standard Sessions**, **Advanced Sessions**, **Scopia Video Sessions**, **CES Sessions** and **Scopia Video Sessions** fields, type the number of licensed sessions depending on the license you purchased.
11. Click **Finish**.

Configuring WebLM server IP address using CLI

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. Run the following command to configure an external WebLM server URL:

```
sbceconfigurator.py config-weblm-url <WebLM URL>
```

Chapter 9: Resources

Documentation

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

| Title | Description | Audience |
|--|--|---|
| Design | | |
| <i>Avaya Session Border Controller for Enterprise Overview and Specification</i> | High-level functional and technical description of characteristics and capabilities of the Avaya SBCE. | Sales engineers, solution architects, and implementation engineers |
| <i>Avaya Converged Platform Overview and Specification</i> | Describes the key features of Avaya Converged Platform | IT Management, sales and deployment engineers, solution architects, and support personnel |
| Implementation and administration | | |
| <i>Installing the Dell PowerEdge R630 Server</i> | Hardware installation and preliminary configuration. | Implementation engineers |
| <i>Installing the HP ProLiant DL360 G9 Server</i> | Hardware installation and preliminary configuration. | Implementation engineers |
| <i>Upgrading Avaya Session Border Controller for Enterprise</i> | Procedures for upgrading to Avaya SBCE 8.0.x. | Implementation engineers |
| <i>Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment</i> | Procedure to deploy Avaya SBCE on VMware. | Implementation engineers |
| <i>Installing the Avaya Converged Platform 110 Series</i> | Describes how to install Avaya Converged Platform 110 Series. | Sales and deployment engineers, solution architects, and support personnel |
| <i>Administering Avaya Session Border Controller for Enterprise</i> | Configuration and administration procedures. | Implementation engineers and administrators |
| Maintenance and Troubleshooting | | |

Table continues...

| Title | Description | Audience |
|---|---|--|
| <i>Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise</i> | Troubleshooting and maintenance procedures for Avaya SBCE. | Implementation engineers and Sales engineers |
| <i>Maintaining and Troubleshooting the Dell PowerEdge R630 Server</i> | Troubleshooting and maintenance procedures for the Dell PowerEdge R630 Server. | Implementation engineers and Sales engineers |
| <i>Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server</i> | Troubleshooting and maintenance procedures for the HP ProLiant DL360 G9 Server. | Implementation engineers and Sales engineers |

Finding documents on the Avaya Support website

Procedure

1. Go to <https://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**.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
 - **Application & Technical Notes**

- **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.

7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at <https://documentation.avaya.com>.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
 - Type a keyword in the **Search** field.
 - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
 - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **My Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
 - Add content from various documents to a collection.
 - Save a PDF of selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

Navigate to the **My Content > Watch list** menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

*** Note:**

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

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 |
|-------------|---|
| 2060W | What is new for Avaya Session Border Controller for Enterprise |
| 2066W | Administering the Avaya Session Border Controller for Enterprise |
| 2080C | Implementing and Supporting Avaya Session Border Controller — Platform Independent |
| 2080T | Avaya Session Border Controller for Enterprise Platform Independent and Support Test |
| 2080V | Implementing and Supporting Avaya Session Border Controller — Platform Independent |
| 26160W | Avaya Session Border Controller for Enterprise Fundamentals |
| 7008T | Avaya Session Border Controller for Midmarket Solutions Implementation and Support Test |
| 7008W | Avaya Session Border Controller for Midmarket Solutions Implementation and Support |
| 2035W | Avaya Unified Communications Roadmap for Avaya Equinox Clients |
| 43000W | Selling Avaya Unified Communications Solutions |

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 <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://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.

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 70

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 69

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, “Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs” at <https://www.vmware.com/>.

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

Following are the BIOS recommendations for Dell PowerEdge Servers supported by Avaya SBCE:

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 G8 and G9 Servers

The following are the recommended BIOS settings for the HP ProLiant G8 and G9 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 VMkernel 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

VMware ESXi uses a thick virtual disk by default when it creates a virtual disk file.. The thick disk preallocates the entire amount of space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are preallocated for that virtual disk.

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

- Thin-provisioned disks can grow to the full size as specified at the time of virtual disk creation, but they cannot shrink. Once you allocate the blocks, you cannot deallocate them.
- Thin-provisioned disks run the risk of overallocating 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 formatting process 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 format tool in Microsoft Windows writes information to all sectors on the disk, which in turn inflates the thin-provisioned disk to full size.

Thin-provisioned disks can overallocate storage. If the storage is overallocated, 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 consumed to its full capacity. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin-provisioned 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 |

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 <i>bare-metal hypervisor</i> . 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 Web client version is VMware 6.5 and later. |

Index

A

| | |
|----------------------------------|----|
| accessing port matrix | 65 |
| Appliance Configuration | |
| field descriptions | 35 |
| automatic restart | |
| virtual machine | 40 |
| Avaya Aura products | |
| license file | 16 |
| Avaya SBCE | |
| overview | 9 |
| Avaya SBCE on KVM | 42 |
| Avaya SBCE or EMS from KVM | 57 |
| Avaya support website | 68 |

B

| | |
|--------------------------------|----|
| best practices | |
| cloning | 78 |
| DMZ deployment | 69 |
| performance and features | 71 |
| storage | 75 |
| VMware HA | 78 |
| BIOS | 71 |
| BIOS for HP servers | 72 |
| BIOS settings | |
| for Dell servers | 72 |

C

| | |
|---|----|
| checklist | |
| deploying and configuring | 17 |
| clones | |
| deployment | 26 |
| collection | |
| delete | 66 |
| edit name | 66 |
| generating PDF | 66 |
| sharing content | 66 |
| components | |
| virtualized | 14 |
| VMware | 14 |
| configuration data | |
| customer | 16 |
| configure | 74 |
| configure VM | |
| Launch Console | 49 |
| configuring | |
| virtual machine automatic restart | 40 |
| WebLM server IP address using CLI | 63 |
| configuring a time server | 40 |
| configuring Avaya SBCE | |
| network connectivity | 39 |

| | |
|-----------------------------------|----|
| content | |
| publishing PDF output | 66 |
| searching | 66 |
| sharing | 66 |
| watching for updates | 66 |
| creating | |
| application virtual machine | 46 |
| snapshot for KVM | 54 |
| snapshot for VMware | 52 |
| customer configuration data | 16 |

D

| | |
|---|--------|
| data | |
| network configuration | 16 |
| VFQDN | 16 |
| deleting | |
| snapshot for KVM | 55 |
| snapshot for KVM deletion | 55 |
| deleting a snapshot | 53 |
| deploying | |
| SBCE OVA on ESXi 6.x using vSphere web client | 26 |
| Deploying | 42 |
| SBCE | 32 |
| deploying copies | 26 |
| deploying EMS | |
| KVM | 43, 44 |
| deployment | |
| thick | 75 |
| thin | 75 |
| deployment and configuration procedures | |
| checklist | 17 |
| deployment guidelines | 13 |
| deployment modes | 10 |
| determining | |
| installation on VMware | 57 |
| documentation portal | 66 |
| finding content | 66 |
| navigation | 66 |
| document changes | 8 |

E

| | |
|----------------------------|----|
| EMS | |
| connect to network | 38 |
| deploying | 30 |
| installing | 30 |
| network availability | 38 |
| verification | 50 |
| EMS, | |
| GUI | 50 |
| EMS+SBCE | |
| deploying | 27 |

EMS+SBCE (continued)

- installing27
- EMS on ESXi, deploy on single server with SBCE, using vSphere24
- EMS on ESXi 6.x using vSphere desktop client deployment19
- extracting
 - KVM OVA42

F

- features best practices71
- finding content on documentation portal66
- finding port matrix65

G

- guidelines
 - deployment13

I

- installing a license on WebLM on System Manager61
- installing the license file61
- Intel Virtualization Technology71

K

- KVM9
 - deploying43, 44
- KVM OVA deployment tools14
- KVM snapshot creation54
- KVM specification15

L

- license administration
 - WebLM support59
- license feature
 - SBCE59
- license file
 - Avaya Aura products16
- logging in EMS50
- log on
 - Nutanix Web console45

M

- Management Interface Setup
 - field descriptions36
- migrating
 - from physical server to VMWare27
- My Docs66

N

- NTP time74
- NTP time source73

O

- order
 - restoring VMware snapshot78
- overview42

P

- password
 - policies13
- performance best practices71
- port matrix65
- power on VM48
- properties template field descriptions21

R

- references70
- related documentation64
- removing57
 - Avaya SBCE from VMware57
- restoring56
- restoring a snapshot54
- running
 - performance tune script76

S

- SBCE13
 - license feature59
- SBCE on ESXi, deploy on single server with EMS, using vSphere24
- SBCE on ESXi 6.x
 - deploying22, 24
 - vSphere desktop client22, 24
- searching for content66
- sharing content66
- snapshot
 - deleting53
 - restoring54
- snapshot for KVM56
- snapshot for KVM restoration56
- snapshots77
- software/hardware
 - supported12
- start VM48
- support68
- supported browsers13

Index

T

| | |
|------------------------|--------------------|
| thick deployment | 75 |
| thin deployment | 75 |
| timekeeping | 73 |
| training | 67 |
| transferring files | |
| using WinSCP | 45 |

U

| | |
|------------------------------|--------------------|
| uploading | |
| qcow2 image on Nutanix | 46 |

V

| | |
|---|--------------------|
| verify EMS installation | 51 |
| verifying EMS and SBCE installation | 51 |
| verify SBCE installation | 51 |
| videos | 67 |
| Virtualized components | 14 |
| virtual machine | |
| automatic restart configuration | 40 |
| virtual machine specifications | 15 |
| vMotion | 79 |
| VMware | |
| best practices | 74 |
| snapshots | 52 |
| VMware components | 14 |
| VMware deployment options | 15 |
| VMware snapshot | |
| restoration order | 78 |
| VMware Tools | 72 |
| vswitches | |
| configuring | 37 |
| VT support | 71 |

W

| | |
|-------------------------------|--------------------|
| watch list | 66 |
| ways to install license | 61 |
| WebLM Server | |
| configuration | 62 |