Deploying Avaya Session Border Controller for Enterprise on Microsoft® Azure

Release 8.1.X
Issue 5
March 2023

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.

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

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.

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.

Contents

Chapter 1: Introduction

Purpose

This document describes the procedures to deploy Avaya Session Border Controller for Enterprise (Avaya SBCE) on a Microsoft® Azure (Azure) cloud services platform.

This document is intended for people who install and configure Avaya SBCE.

Change history

Issue	Date	Summary of changes
5	March 2023	Updated Converting a QCOW2 image to a VHD image on page 17
4	August 2021	Updated the following items: • About licensing requirements on page 50 • Avaya SBCE licensed features on page 51
3	December 2020	Updated the following items: • Fixed obsolete URLs to Microsoft articles. This change is in several places in the document. • Added a recommendation to use the Azure Command Line Interface (CLI) when deploying Avaya SBCE. This change is in several places in the document. • Added a recommendation to use the smaller Generation 2 QCOW files to ensure a clean download of the Avaya SBCE software. This change is in several places in the document. • Added a new section listing the files you need to download. See Software to download on page 13. • Updated the table in Network interfaces on page 14. • Updated information in Password policies on page 15. • Updated the network interface information in Configuring the network interfaces on page 25.

Table continues…

Issue	Date	Summary of changes
		• Updated the required options in Creating a managed disk from the VHD file on page 20. • Updated network interface descriptions in Configuring the network interfaces on page 25. • Updated the procedure in Running the first boot configuration on page 26. • Added the chapter *Deploying High Availability on Azure*. • Updated information about licensing a secondary EMS server in About licensing requirements on page 50.
2	September 2020	Made the following updates related to the new Generation 2 QCOW image: • Added a secondary password for the root login ID when using the Generation 2 QCOW image. For more information, see Password policies on page 15. • Added the file name for the Generation 2 version of the QCOW image. For more information, see Prerequisite procedures checklist on page 16. • Updated the options you use when creating a managed disk for a Generation 2 QCOW image. For more information, see Creating a managed disk from the VHD file on page 20.

Chapter 2: Architecture overview

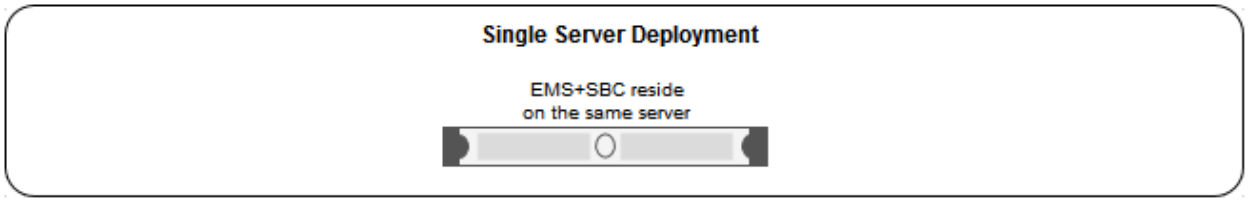
Avaya SBCE on Microsoft® Azure overview

Microsoft® Azure (Azure) is a cloud services platform that enables enterprises to run applications on the virtual cloud securely. By deploying Avaya SBCE on Azure, you get the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to an operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

Single server non-HA deployment

In a single server non-HA deployment, the Element Management System (EMS) and SBCE software are installed on a single server. Use this deployment scenario when you want to deploy Avaya SBCE in a basic mode.



Important:

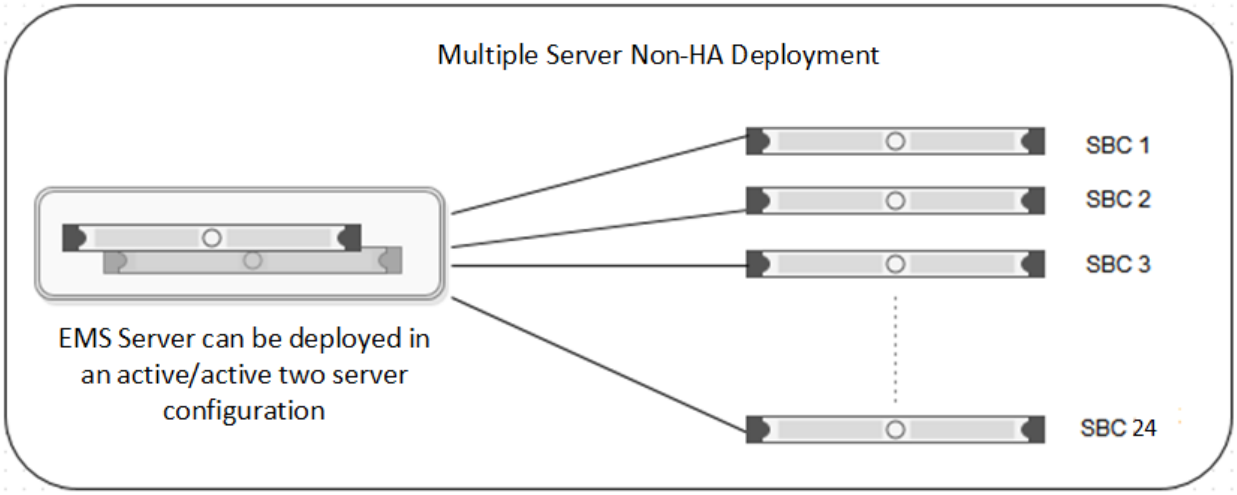
All hardware server types, virtualized environment platforms, and cloud platforms support the single-server non-HA deployment type.

Multiple server non-HA deployment

In a multiple server deployment, the EMS and SBCE software are installed on separate servers.

In a non-HA multiple server deployment, you can have one or more SBCE servers controlled by a single EMS server or a replicated EMS HA pair. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. When using a single EMS server, the EMS server is configured as Primary.

You can have up to 24 individual Avaya SBCE servers in this type of configuration.



If you start with a non-HA deployment and want to later move to an HA deployment, you must completely reconfigure the deployment.

Important:

All hardware server types (except Portwell servers), virtualized environment platforms, and cloud platforms support the multi-server non-HA deployment type.

Multiple server HA deployment

In a multiple server deployment, the EMS and SBCE software are installed on separate servers.

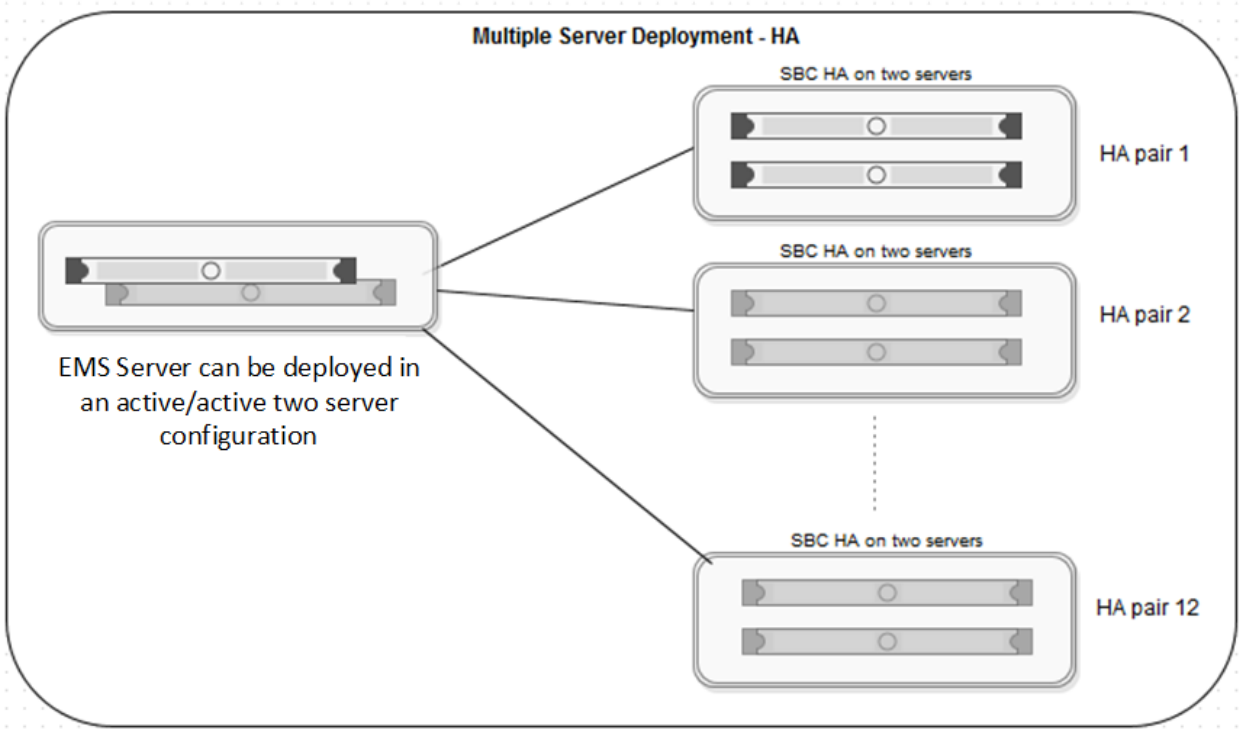
In an HA deployment, SBCE servers are deployed in pairs. Each pair has one SBCE server configured as Primary while the other is configured as Secondary.

Optionally, the EMS software can be replicated in an active/active HA pair deployment. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. An EMS HA pair must be reachable to each other and with the SBCE servers, and can be in different geographical locations.

One EMS server or an active/active pair of EMS servers can control up to 12 separate pairs of SBCE servers.

Note:

When deploying an HA configuration on Amazon Web Services, you only have to configure the SBCE software on the primary device



Important:

All hardware server types (except Portwell servers), virtualized environment platforms, and cloud platforms support the multi-server HA deployment type.

Although the HA pairs and non-HA deployments are shown separately in this figure, EMS can control both an SBCE HA server pair as well as a single SBCE server.

SBCE HA server pairs must adhere to the following requirements:

- You can enable and use the HA deployment feature only if the license file contains an HA license.
- The HA pair servers must reachable by the EMS or EMS HA pair servers over the Management Plane (M1).
- The HA pair servers must be reachable between the devices over the Management link (M1) .
- The HA pair servers must have the HA link (M2) reachable between the HA pair servers.
- The HA pair servers must set up to have all the data interfaces between the servers replicated so that the servers are connected in same subnets. For example, the A1 data interface in one SBCE server should be in the same subnet as the A1 data interface of the paired SBCE server. This allows you to meet the requirement that failover be functional in an active/standby mode.
- In a multiple server HA virtualized deployment, when there are multiple HA pairs and automatic IP addressing is being used on the HA link (M2), every HA pair should either have their own isolated vSwitch or each HA pair should use different IP addresses reachable with their HA pairs as stated previously for M2 connectivity.

Chapter 3: Planning

Prerequisite knowledge, skills, and tools

Before deploying the product, ensure that you have the following knowledge, skills and tools.

Knowledge

- Microsoft® Azure (Azure) setup
- Avaya SBCE setup
- Windows® Operating System
- Linux® Operating System

Skills

Ability to administer Azure and Avaya SBCE.

Tools and utilities

To deploy the Avaya SBCE software image and to configure the applications, you need the following tools and utilities:

- A browser for accessing the Azure Management Console.
- PuTTY, PuTTYgen, WinSCP, and WinZip.
- Linux QEMU tools.

Important:

Avaya recommends that you use the Azure Command Line Interface (CLI) when deploying Avaya SBCE with Azure. The setup of the management and data interfaces is critical and the CLI is the most reliable method.

Note:

The ASBC image supports only UEFI boot mode. Therefore, only Azure instance type gen 2 supports the deployment.

Supported virtual machine types

The Azure virtual machine (VM) environment is designed to support multiple options such as Generation 1 and Generation 2 VM types. Avaya SBCE supports both of these VM types.

Generation 1 uses BIOS-based boot architecture. Generation 2 uses newer UEFI-based boot architecture. Avaya SBCE Virtual Hard Disk (VHD) and QEMU Copy-on-Write (QCOW2) format supports only Generation 2 VMs.

See the information on the following Microsoft web site to help you use the Azure tools to create a VM:

https://docs.microsoft.com/en-us/azure/virtual-machines/

Important:

Avaya recommends that you use the Azure Command Line Interface (CLI) when deploying Avaya SBCE with Azure. The setup of the management and data interfaces is critical and the CLI is the most reliable method.

Virtual machine specifications

Avaya SBCE on an Azure virtual machine (VM) requires a minimum of four (4) and a maximum of six (6) network interfaces. For an HA deployment, you must use a VM with six (6) network interfaces. For more information about Linux VMs used for Azure, see the following websites:

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

https://docs.microsoft.com/en-us/azure/virtual-machines/fsv2-series?toc=/azure/virtual-machines/linux/toc.json&bc=/azure/virtual-machines/linux/breadcrumb/toc.json

Table 1: Azure B-series VM specifications

Azure Size	vCPUs	Memory (GB)	Temporary Storage (GB)	NICs
Standard_B4ms	4	16	32	4
Standard_B8ms	8	32	64	4
Standard_B12ms	12	48	96	6

Table 2: Azure F-series high performance VM specifications

Azure Size	vCPUs	Memory	Temporary Storage	Maximum data disks	Maximum cached and temporary storage throughput	Maximum uncached disk throughput	NIC ports and Network Bandwidth
Standard_F2s_v2	2	4 GB	16 GB	4	4000 IOPS 31 Mbps 32 GB	3200 IOPS 47 Mbps	2 ports 875 Mbps

Table continues…

Azure Size	vCPUs	Memory	Temporary Storage	Maximum data disks	Maximum cached and temporary storage throughput	Maximum uncached disk throughput	NIC ports and Network Bandwidth
Standard_F4s_v2	4	8 GB	32 GB	8	8000 IOPS 63 Mbps 64 GB	6400 IOPS 95 Mbps	2 ports 1750 Mbps
Standard_F8s_v2	8	16 GB	64 GB	16	16000 IOPS 127 Mbps 128 GB	12800 IOPS 190 Mbps	4 ports 3500 Mbps
Standard_F16s_v2	16	32 GB	128 GB	32	32000 IOPS 255 Mbps 256 GB	25600 IOPS 380 Mbps	4 ports 7000 Mbps

Software to download

Download the ISO software image file from the Avaya Support Site or from the Avaya PLDS website:

https://support.avaya.com/downloads/

https://plds.avaya.com

Important:

The Generation 2 download files are significantly smaller than the Generation 1 download files. Unless you specifically require a Generation 2 file, you can download a Generation 2 file.

Release 8.1.2.0 Generation 1

- `sbce-8.1.2.0-31-19809.qcow2`
- `sbce-8.1.2.0-31-19809.qcow2.md5`

Release 8.1.2.0 Generation 2

- `sbce-8.1.2.0-31-19809-uefi.qcow2`
- `sbce-8.1.2.0-31-19809-uefi.qcow2.md5`

Release 8.1.1.0 Generation 1

- `sbce-8.1.1.0-26-19214.qcow2`
- `sbce-8.1.1.0-26-19214.qcow2.md5`

Release 8.1.1.0 Generation 2

- `sbce-8.1.1.0-26-19214-uefi.qcow2`
- `sbce-8.1.1.0-26-19214-uefi.qcow2.md5`

Capacities

An Avaya SBCE deployment on Azure supports the following system capacities:

Number of Remote Worker Registrations	Non-encrypted Calls with Trunking	Encrypted Remote Worker Sessions
5,000	5,000	1,800

Network interfaces

The number of network interfaces that you set up depends the type of Avaya SBCE instance that you are deploying.

The following table shows the relationship between the number of network interfaces and Avaya SBCE deployment configurations:

Number of network interfaces	Type of Avaya SBCE configuration	Interface ports
2	EMS only	M1, M2
4	Small SBCE (For VMware deployment only)	M1, A1, B1, M2
6	EMS+SBCE	M1, A1, B1, M2, A2, B2
6	For all other deployment types, such as High Availability (HA)	M1, A1, B1, M2, A2, B2

Supported browsers

For information about supported browser list and version, see the following website:

https://docs.microsoft.com/en-us/azure/azure-portal/

Password policies

The root and ipcs passwords are set during product installation. The EMS GUI has a separate password. The default user IDs and passwords are:

- `root/Avaya_123`
- `ucsec/ucsec`

Note:

For a Microsoft Azure or KVM platform, if the default root password is not accepted, try the following alternate password:

`@V@Y@_123`

Security alert:

You must change the default passwords for the CLI root and ipcs login IDs after first boot during the installation procedure. You are prompted to enter and confirm the new password. Password restrictions are enforced on the root, ucsec, and ipcs accounts. The new password must meet the following criteria:

- Minimum of 8 characters.
- One uppercase letter, one lowercase letter, and one number.
- One special character from the following: hyphen (-), underscore (_), at sign (@), asterisk (*), or exclamation point (!).You must not use the number sign (#), dollar sign ($), or ampersand (&).

Avaya SBCE features not supported in an Azure deployment

Avaya SBCE Release 8.1.1 deployed on Azure does not support the following features:

- EMS primary and secondary High Availability (HA) deployment
- Avaya SBCE HA deployment

HA on Azure is supported on Avaya SBCE Release 8.1.2 or later.

Chapter 4: Prerequisite procedures

Prerequisite procedures checklist

Ensure that you complete the following before deploying Avaya SBCE on Azure:

Task	Link/Notes	✔
Download the ISO software image file.	Software to download on page 13	
Purchase the required Avaya SBCE licenses. Register for PLDS and perform the following • Obtain the license file. • Activate license entitlements in PLDS.	https://plds.avaya.com/	
Convert the QCOW2 image to a VHD image.	Converting a QCOW2 image to a VHD image on page 17	

Downloading software from Avaya PLDS

About this task

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements. In addition to PLDS, you can download the product software from http://support.avaya.com/ by navigating to the Support by Product menu at the top of the page.

Procedure

1. To access the Avaya PLDS website, type http://plds.avaya.com/ in your web browser.
2. Type your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.

6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. In **Download Pub ID**, type the download pub ID.
8. In the **Application** field, click the application name.
9. In the **Download type** field, click one of the following:
   - **Software Downloads**
   - **Firmware Downloads**
   - **Language Packs**
   - **Miscellaneous**
10. In the **Version** field, click the version number.
11. Click **Search Downloads**.
12. Scroll down to the entry for the download file, and click the **Download** link.
13. Select a location where you want to save the file, and click **Save**.
14. **(Optional)** On Internet Explorer, if you receive an error message, click the install ActiveX message at the top of the page to start the download.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Converting a QCOW2 image to a VHD image

About this task

Depending on the type of VM you are using, you might need to convert a QCOW2 image to a VHD image. Use this procedure to do that conversion.

Before you begin

Download the QCOW2 image from PLDS as described in Downloading software from Avaya PLDS on page 16.

Confirm that you have access to Linux QEMU tools. For more information about QEMU tools, see the following website:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/virtualization_deployment_and_administration_guide/chap-using_qemu_img

Procedure

1. Log on as root to the Linux server.
2. Copy the QCOW2 image file to a temporary directory.
3. Run the following command convert the QCOW2 image to a raw file format:

   ```
   qemu-img convert -f qcow2 -O raw ASBCE.qcow2 ASBCE.raw
   ```

   ```
   MB=$((1024 * 1024))
   ```

4. Verify that the size of the raw image is aligned with 1 MB. If it is not, use the following commands to round it up to 1 MB:

   ```
   size=$(qemu-img info -f raw --output json "ASBCE.raw" | gawk
   'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}')
   ```

   ```
   rounded_size=$((($size/$MB + 1)*$MB))
   ```

   ```
   qemu-img resize ASBCE.raw $rounded_size
   ```

   Note:

   The **qemu-img** command sometimes displays the following message, but you can ignore the warning:

   ```
   WARNING: Image format was not specified for 'ASBCE.raw' and probing guessed
   raw.
   Automatically detecting the format is dangerous for raw images, write
   operations on block 0 will be restricted.
   Specify the 'raw' format explicitly to remove the restrictions. Image resized.
   ```

5. Run the following command to convert the raw file to a fixed-size VHD image:
   - If you are using QEMU Version 2.6 or later:

     ```
     qemu-img convert -f raw -o subformat=fixed,force_size -O vpc
     ASBCE.raw ASBCE.vhd
     ```

   - If you are using QEMU version earlier than 2.6:

     ```
     qemu-img convert -f raw -o subformat=fixed -O vpc ASBCE.raw
     ASBCE.vhd
     ```

Chapter 5: Deploying and configuring Avaya SBCE

Deployment checklist

Task	Reference	✔
Upload the VHD file to your system.	Uploading the VHD file on page 19	
Create a managed disk.	Creating a managed disk from the VHD file on page 20	
Create the virtual machine.	Creating the virtual machine on page 23	
Configure the network interfaces.	Configuring the network interfaces on page 25	
Run the first boot configuration.	Running the first boot configuration on page 26	
Configure the Avaya SBCE features.	Configuring Avaya SBCE features on page 27	

Important:

Avaya recommends that you use the Azure Command Line Interface (CLI) when deploying Avaya SBCE with Azure. The setup of the management and data interfaces is critical and the CLI is the most reliable method.

Uploading the VHD file

About this task

To use the VHD file as a VM image, you must upload it into a “page blob” storage type container on your Azure storage account. You can upload the VHD file using the Azure Storage Explorer. For more information about “page blobs”, see the following website:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-pageblob-overview?tabs=dotnet

Before you begin

Create the storage account and blob container in the Azure Portal, or use the Azure CLI or PowerShell user interfaces.

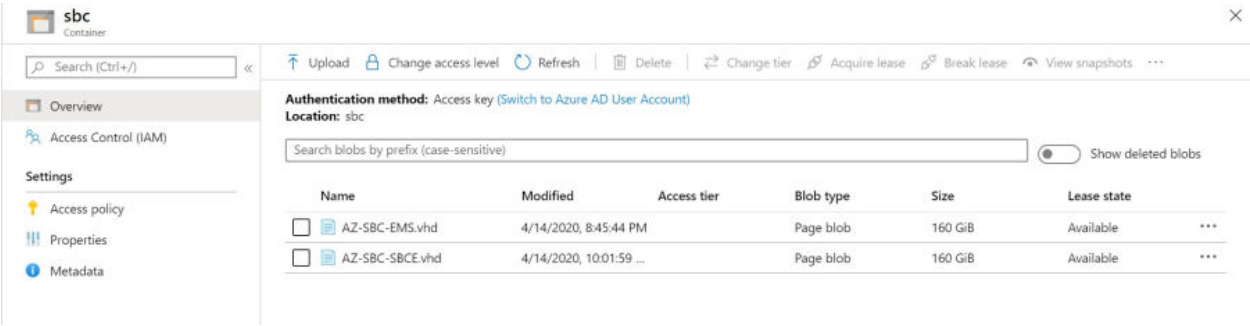
Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. Use one of the following commands to upload and convert the VHD file:
   - **`ConvertTo-MvmcAzureVirtualHardDisk`**
   - **`AzCopy`**

   For example:

   `azcopy cp` *PathToVHDfile* **`"https://storageaccount.blob.core.windows.net/container?sas" --blob-type PageBlob`**

   The upload program uploads the VHD file and converts it into the proper format. You can view the file in your Azure storage account. See the following example:



Creating a managed disk from the VHD file

About this task

Note:

The screen examples shown in this procedure are shown to assist you using the Azure user interface. Your actual screens may differ than those shown here.

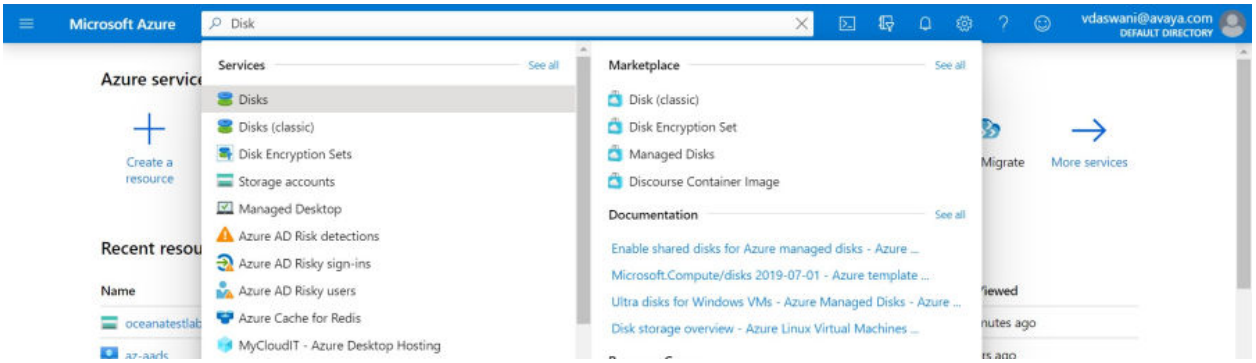
Before you begin

Create a resource group in the Azure Portal.

Procedure

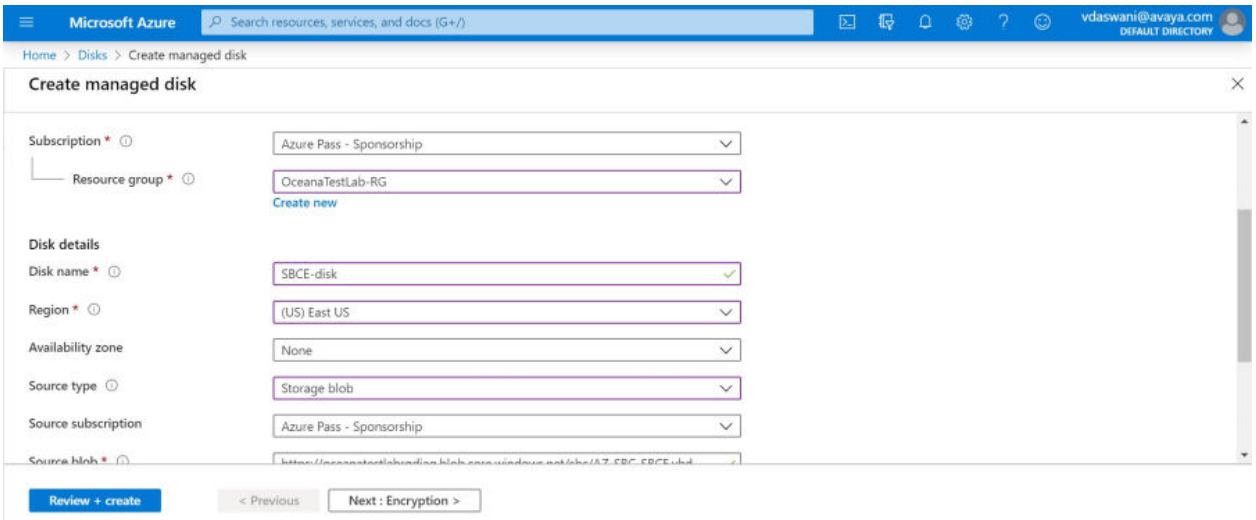
1. Log on to the Azure Portal using your Azure logon credentials.
2. In the Azure Portal search box, enter “disks” and press **Enter**.

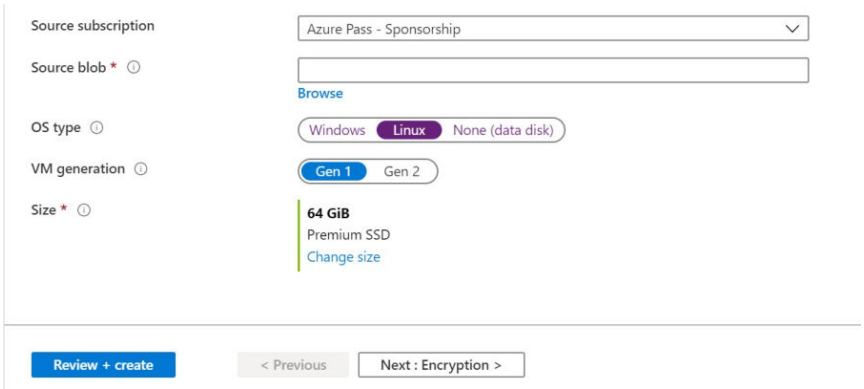
   The system displays various results similar to the following example:



3. Select **Disks**.
4. Click **Add**.

   The system displays the Create managed disk windows similar to those shown in the following examples:





5. On the Create managed disk window, configure the following options:
   - In the **Resource group** field, select a resource group you have configured.

- In the **Disk name** field, enter the name of the disk you uploaded and converted.
- In the **Region** field, select the region where the system is located. If you have an HA pair, you must have them located in the same region.
- In the **Availability zone** field, an HA pair should be assigned to the same zone. Use **None** for all other configurations.
- In the **Source type** field, select **Storage blob**.
- In the **Source subscription** field, select the subscription you have purchased from Microsoft.
- In the **Source blob** field, browse to where you stored the VHD file.
- In the **OS type** field, select the operating system you want to use.

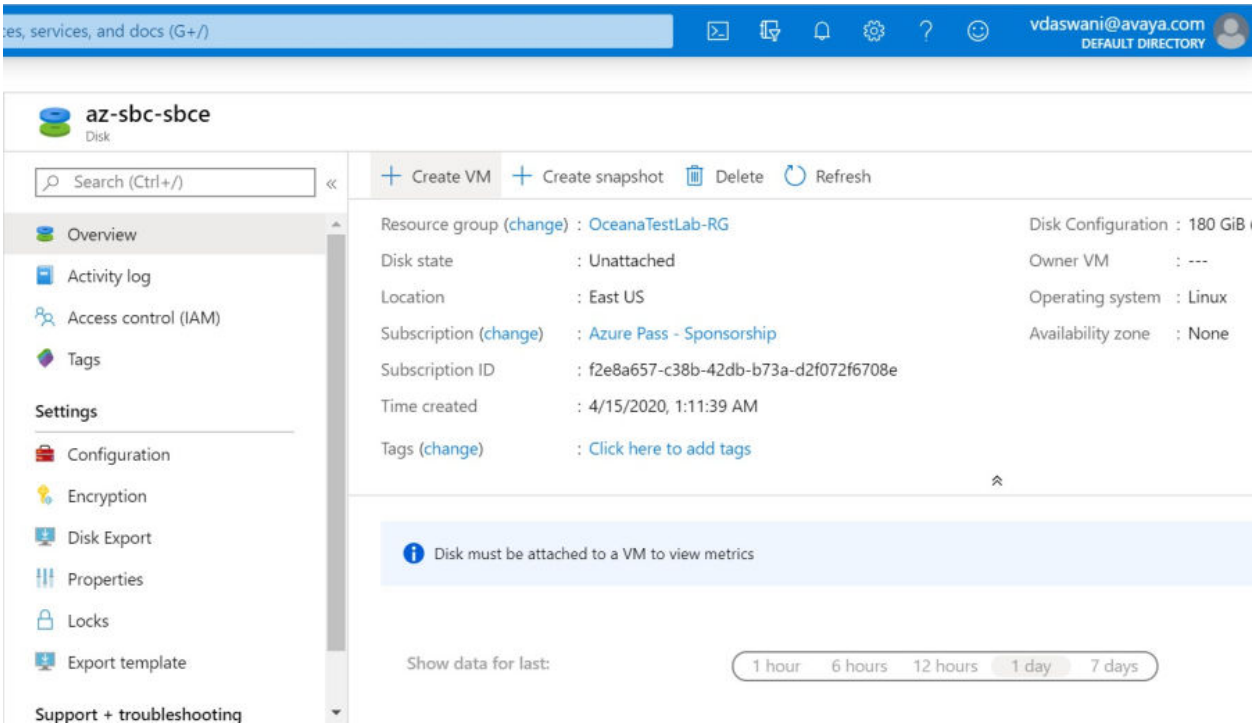
  Important:

  For disk0, you must select an operating system. Do not use **None (data disk)**. The rest of the disk will be a data disk. When using a Generation 2 QCOW image, you must select **Linux**.

- In the **VM generation** field, select **Gen 1** for the original Generation 1 QCOW image. Select **Gen 2** for the Generation 2 QCOW image.
- In the **Size** field, click the **Change size** link and select a size that is the same or larger than the size of the VHD file. Round up any values to the next highest round number value.

6. Click **Create**.

   The system displays a screen similar to the following example:



Creating the virtual machine

About this task

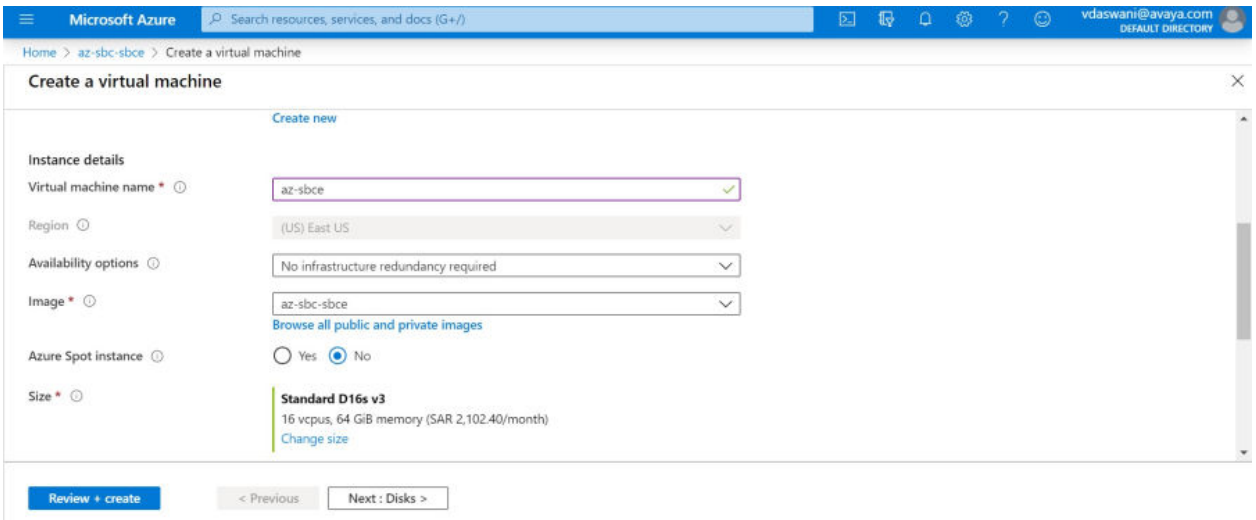
Note:

The screen examples shown in this procedure are shown to assist you using the Azure user interface. Your actual screens may differ than those shown here.

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. Click **Create VM**.

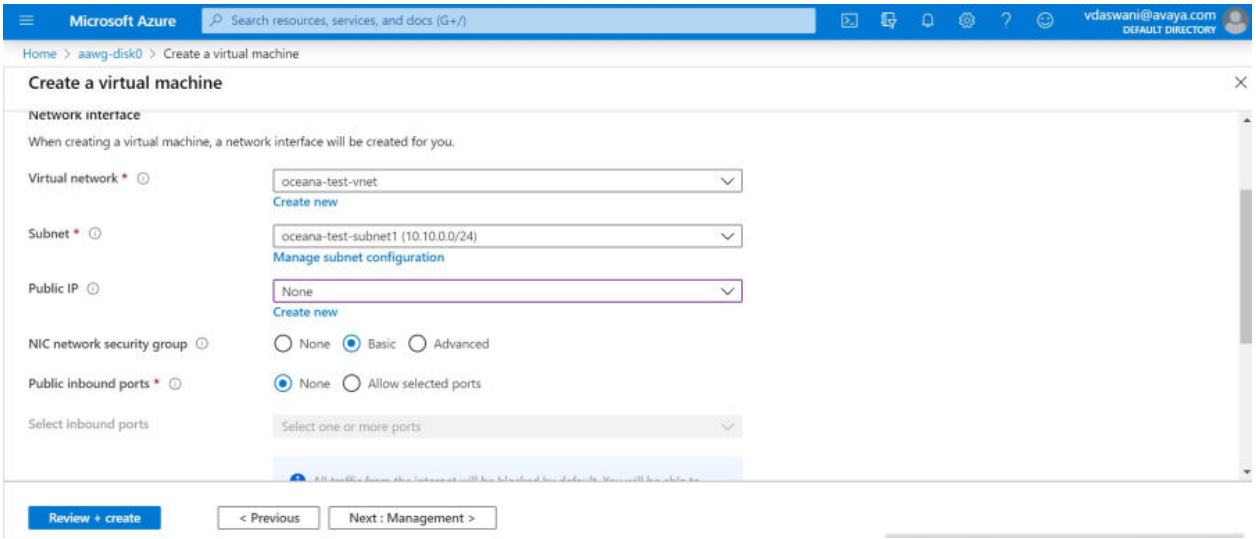
   The system displays the Create a virtual machine window.



3. Select the resource group you created earlier.
4. Configure the following options:
   - In the **Virtual machine name** field, enter a name for the machine you are creating.
   - In the **Size** field, select the Azure machine size you want to use. For more information, see Virtual machine specifications on page 12.
   - In the **Inbound port rules** options, administer any inbound ports you wish to allow. In most cases, you would not allow any public interface or public inbound ports open.
5. Click **Next : Disks**.

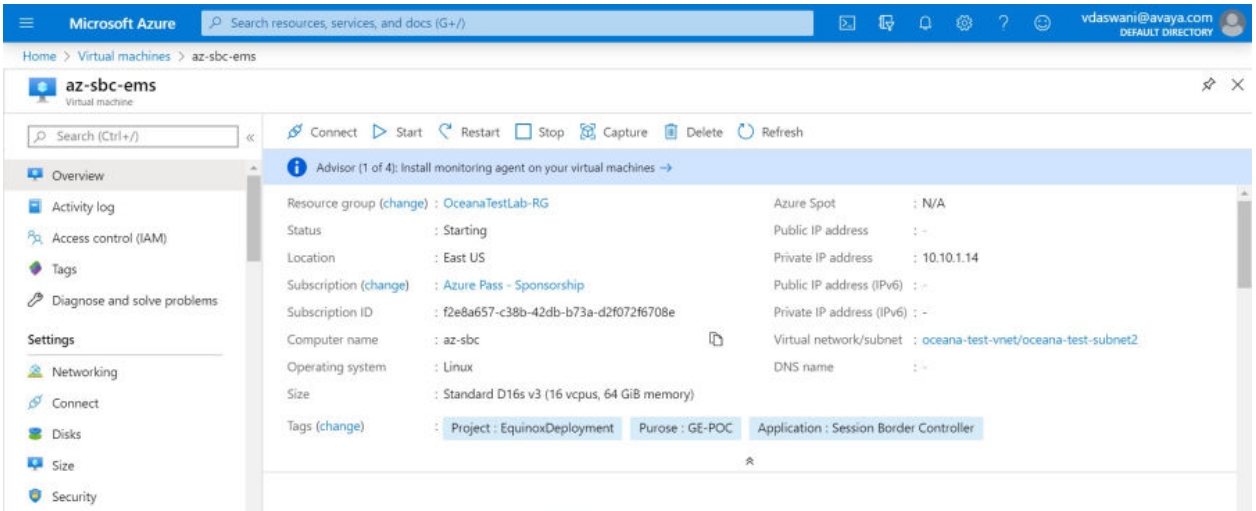
   Accept all disk defaults.
6. Click **Next : Network interface**.

   The system displays the **Network Interface** options window.



7. Configure the following options:
   - In the **Virtual network** field, select a virtual network to use for the system.
   - In the **Subnet** field, select the subnet you want to use.
   - In the **Public IP** field, select **None**.
8. Leave all other options defaulted.
9. Click **Review + create**.

   The system displays a screen similar to the following example:



Next steps

Verify that the following configuration items are valid:

- The host name must be in the `/etc/hosts` file in the correct format.
- The DNS server must be in the `/etc/resolv.conf` file.

- The VMware IP address must not exist in any of these configuration files.
- Verify the SSH configuration in the `/etc/ssh/sshd_config` file.

Configuring the network interfaces

About this task

Before you install and configure the Avaya SBCE software, you must configure the network interfaces on Azure as follows:

- For an EMS+SBCE deployment – Four network interfaces (M1, A1, B1, M2)
- For all other deployments, including HA – Six network interfaces (M1, M2, A1, A2, B1, B2)

By default, Azure creates only the one M1 interface automatically, so you have to manually create the rest of the interfaces required by your deployment.

Important:

You must verify that none of the network interfaces have already been assigned prior to configuring them for use with Avaya SBCE. If you have not verified this before you configure the network interfaces, you might need to follow a special procedure to detach and then attach the network interfaces. For more information, see the following KB article:

Note:

The screen examples shown in this procedure are shown to assist you using the Azure user interface. Your actual screens may differ than those shown here.

Before you begin

Create three different subnets, one each for Avaya SBCE Management, Avaya SBCE external, and Avaya SBCE internal networks.

Procedure

1. Verify that you can SSH to the Avaya SBCE virtual machine from the subnet that is enabled for your system. Use the password `Avaya_123` or `@V@Y@_123`.

   `ssh root@`<*SBCE_VM_IP_ADDRESS* **`-p 22`**

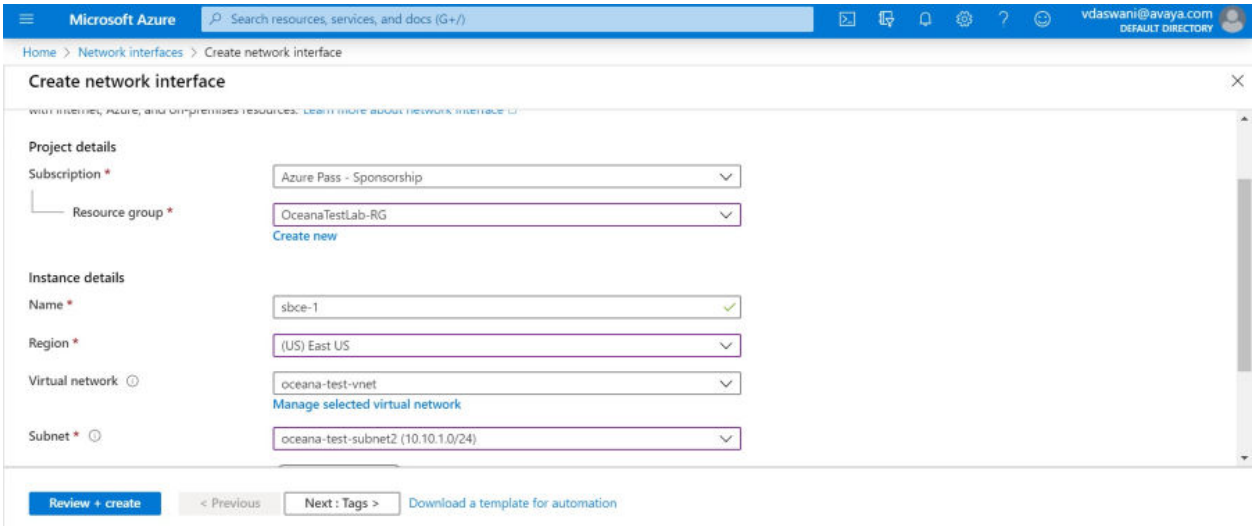
   If there is a problem using SSH, you can use the Serial Console in Azure.

2. Log on to the Azure Portal using your Azure logon credentials.
3. In the search box, enter “network interfaces” and press **Enter**.

   The system displays the results based on the search.

4. Select **Network interfaces**.

   The system displays the Create network interface window.



5. Do one of the following depending on if you are adding a total of four or six interfaces:

   Important:

   The M1 management network interface was automatically configured when you first created the VM. You do not need to create the M1 network interface again.

   - Add three network interfaces for EMS+SBCE in the following order: SBC_A1, SBC_B1, and SBC_M2.
   - Add five network interfaces for all other SBCE configurations, including HA, in the following order: SBC_M2, SBC_A1, SBC_B1, SBC_A2, and SBC_B2.

   For detailed instructions on how to add network interfaces using Azure, see the following website:

   https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm

Running the first boot configuration

Before you begin

In the Azure Portal, verify that the Overview window for the VM you created earlier is open. You can find the VM under All Resources if you need to open it. The Overview window allows you to see whether the VM is running, stop or restart the VM, get the public IP address of the VM, and see the activity of the CPU, disk, and network components.

Be prepared to change the password during the first boot configuration. You cannot keep the default password.

Procedure

1. Log on to the console using SSH to the Avaya SBCE virtual machine from the subnet that is enabled for your system. Use the password `Avaya_123` or `@V@Y@_123`.

   `ssh root@<SBCE_VM_IP_ADDRESS> -p 22`

   If there is a problem using SSH, you can use the Serial Console in Azure.

2. Run the following command:

   `/usr/local/ipcs/icu/scripts/CloudConfigurator.py -s`

   The system displays a prompt to accept the EULA agreement and then displays a configuration screen similar to configuration on VMware and hardware. For more information, see *Deploying Avaya SBCE in Virtualized Environment* document.

3. After the system reboots, wait for several minutes for the system processes to stabilize and you receive the “Boot process complete” message.
4. Power off and power on the VM from the Azure Portal page.

Configuring Avaya SBCE features

Procedure

1. Use any Windows machine that is accessible as a remote desktop from the client machine to configure the Avaya SBCE instance from EMS.

   You can access EMS from `https://<Avaya SBCE IP address>/` by using following credentials:

   - Username : ucsec
   - Password: ucsec

   You can login to the Avaya SBCE instance CLI by using port 222 and 'ipcs' user with the password set during installation stage.

   Note:

   At your first login, you must change the default password.

2. Configure the Avaya SBCE features as required for this deployment.

   For more information, see the following documents that explain how to administer and configure different Avaya SBCE features and solutions:

   - *Avaya Session Border Controller for Enterprise Overview and Specification*
   - *Administering Avaya Session Border Controller for Enterprise*
   - *Working with Avaya Session Border Controller for Enterprise Multi-Tenancy*

- *Working with Avaya Session Border Controller for Enterprise and Microsoft® Teams*

Chapter 6: Deploying High Availability on Azure

About deploying High Availability on Microsoft® Azure

With Avaya SBCE Release 8.1.2 and later, you can deploy Avaya SBCE in a High Availability (HA) configuration on Microsoft® Azure.

Important:

You must be on Avaya SBCE Release 8.1.2 or later to configure HA on Microsoft® Azure. You cannot configure HA using Avaya SBCE Release 8.1.1 or earlier.

Basic concepts for HA on Microsoft® Azure

To understand how HA will work on Microsoft® Azure, you must understand the following concepts:

Virtual Private Cloud (VPC)

A VPC is a private subnet in the Azure cloud available to the client when an Azure account is created. By default, the VPC is associated with a pool of IPv4 addresses in a predefined range based on the region where you are located. For example, 172.31.0.0 through 172.31.0.16 is reserved for the U.S. Central region (uscentral). You can further create a subnet in a VPC network for connecting various services with the Internet.

Network Interface (NI)

When you create an Azure virtual machine instance in a region as part of a subnet, an elastic NI is created and attached to the virtual machine by default. The NI will be assigned a default IP (its Primary IP) from the subnet if one is not assigned while deploying the Azure virtual machine instance. You can create an additional NI and attach it to the Azure virtual machine instance depending upon the instance type.

Secondary IP

You can assign more than one IP address (known as the Secondary IP) to an NI attached to the Azure virtual machine instance. You must assign these Secondary IP addresses to the same subnet in which the NI is associated. You can associate these Secondary IP addresses in a floating arrangement with the NI attached to another Azure virtual machine instance in the same subnet.

Public IP

The Public IP is a static IP address available within a VPC. You can assign a static IP address from the pool of addresses valid for your region in the Azure VPC. You can then associate these static IP addresses with an Azure virtual machine instance.

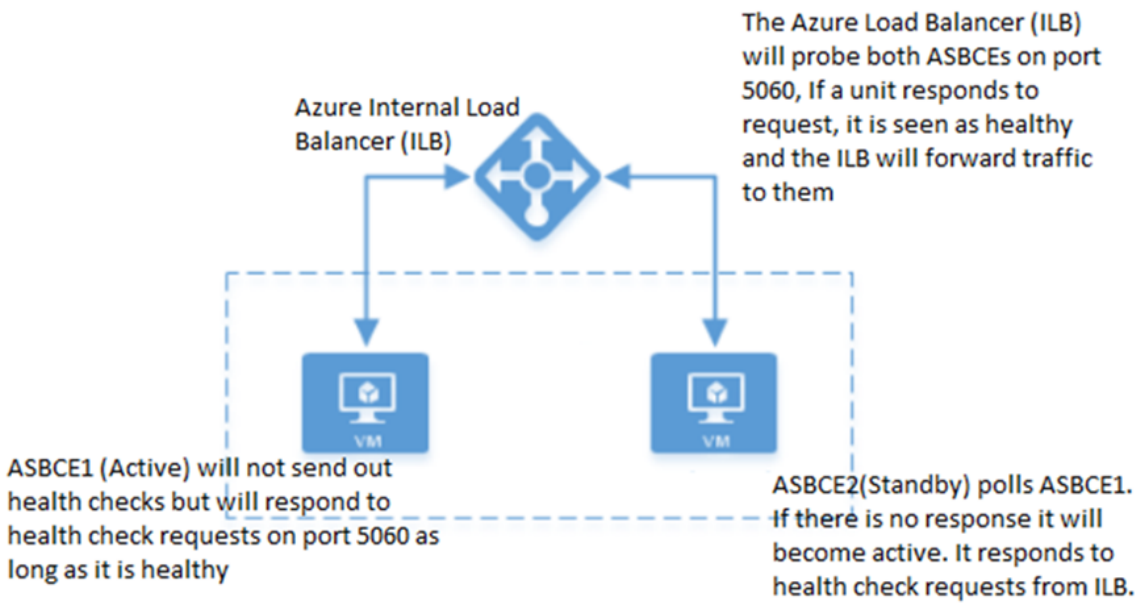
You can associate the Public IP with Primary IP or Secondary IP addresses of an NI attached to an Azure virtual machine instance. This way, the Public IP can “float” from one NI attached to one Azure virtual machine interface to another NI attached to a different Azure virtual machine instance. You can assign more static Public IP addresses to every extra Secondary IP configured on an NI, and the number is only limited by the availability of the Public IP addresses predefined in the VPC pool.

Functional differences when using Avaya SBCE on Microsoft® Azure HA

When using Avaya SBCE with HA on Microsoft® Azure, HA operates similar to how it operates on non-cloud platforms except for the following key differences:

- Avaya SBCE HA on Microsoft® Azure involves a load balancer that synchronizes (replicates) the administrative settings bidirectionally. Changes made to the active system are replicated to the standby system, and changes made to the standby system are replicated to the active system.
- The replication of administrative settings from the active system to the standby system is not always instantaneous and might take a few moments to complete. The same is true for replication of administrative settings from the standby system to the active system.
- When synchronizing the GEO settings from the active system to the standby system, any FQDN or cluster IP addresses that match the active system's IP address are replaced with the standby system's IP address. The same is true when synchronizing from the standby system to the activer system. The standby system's IP address is replaced with the active system's IP address.
- All user-defined settings are synchronized, with the exception of the following:
  - Default gateway (both IPv4 and IPv6)
  - IP addresses and netmasks
  - Hostname
  - Name server
  - Domain
  - Admin default gateway
  - Administrative certificate settings (`.cert`, `.pem` and `.setadmin` files)
  - Network interface settings: Link Status (Speed and Duplex), MTU, and additional addresses
  - Virtual LAN (VLAN) configuration
  - Virtual Extensible LAN (VXLAN) configuration
  - Additional routes
- Depending on the design of the Network Security Groups, you must ensure the necessary ports are open inbound to allow for the traffic.

The following diagram shows how the Microsoft® Azure load balancer operates with Avaya SBCE:



How HA connectivity is administered on Microsoft® Azure

The following is the basic administrative flow for setting up HA on a Microsoft® Azure deployment:

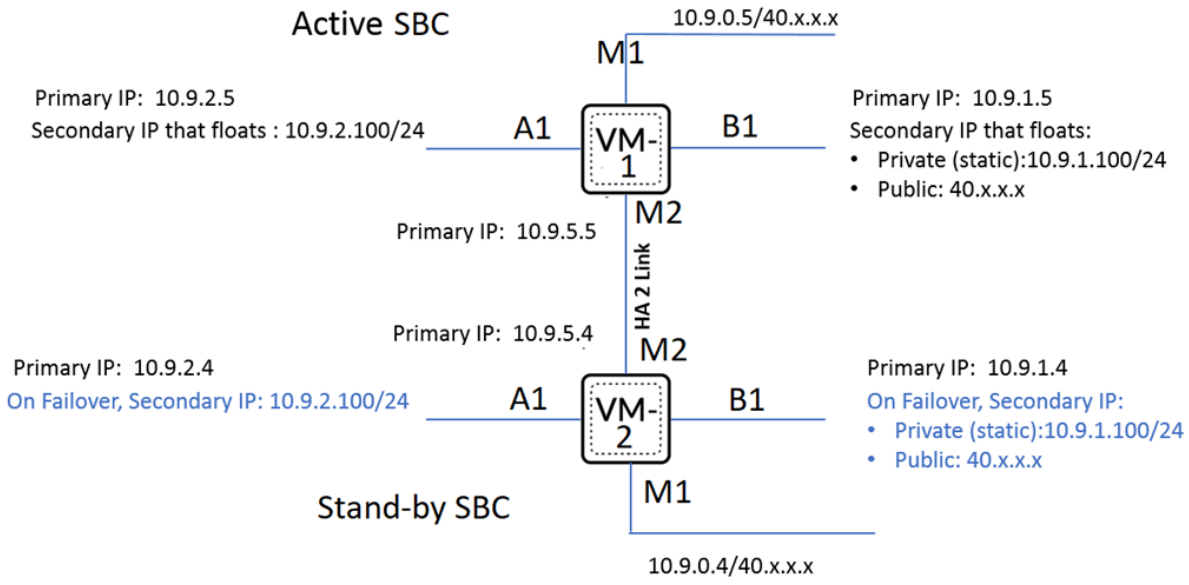
1. When an SBCE is deployed from the Avaya SBCE VHD, the SBCE gets a Network Interface attached to the virtual instance, which is later automatically used as the M1 interface. After attaching three to five more interfaces (depending on the size of the deployment), the SBCE comes up in operational mode. The order in which the interfaces are administered are either M2, A1, and B1 when you use only four interfaces, or M2, A1, B1, A2, and B2 when you are using all six interfaces.
2. While creating additional interfaces for the active and standby SBCE, there are several items you must administer:
   - You must create an NI to attach data interface A1. The NI must have the same subnet on the active and standby SBCE.
   - The Network Interfaces for M1, A2, B1, and B2 must be created and attached to both the active and standby SBCEs.
   - You must assign all data interfaces on the Primary IP to the Network Interface when administering the SBCEs. The Primary IP is not used while adding network, signaling, or media interfaces on SBCE.
3. You must assign the Secondary IP address to the data interfaces (A1, A2, B1, and B2) on the active SBCE. When configuring the network, signaling, and media interfaces for the flow through EMS on SBCEs, you must use these Secondary IP addresses assigned for each data interface. You do not have to assign any Secondary IP addresses on the standby SBCE data interfaces. When failover occurs, these Secondary IP addresses will “float” and be reassigned to the standby SBCE through the SSYNDI process.

4. Attaching a floating IP address to a Secondary IP address is done when the Azure VPC is not connected through a Direct VPN connection to be part of the organization's VPN network. In this scenario, the static Public IP is obtained from the Azure VPC pool and is associated with the NI that is exposed to the Internet cloud. You must configure this subnet on the EMS to assign a static Elastic IP as the Public IP for that particular NI subnet. For failover, you must administer SSYNDI code to reassign the Elastic IP with the floated Secondary IP attached to the other corresponding NI attached to the standby SBCE.

   The floating IP address is used for failover scenarios. A floating IP is reassigned to a standby server in case the active server fails. Floating IP is required for Avaya SBCE AlwaysOn. On the Microsoft® Azure administration portal, the load balancer **Floating IP (direct server return)** option must be set to **Disabled**.

Functional diagram for HA on Microsoft® Azure

The following diagram illustrates a typical HA deployment on Azure:



Deploying HA checklist

Task	Reference	✔
Do all prerequisite procedures.	Required prerequisite configuration on page 33	

Table continues…

Task	Reference	✔
Create the first virtual Avaya SBCE.	Creating the first virtual Avaya SBCE in Azure on page 35	
Create the second virtual Avaya SBCE.	Creating the second virtual Avaya SBCE in Azure on page 39	
Configure the network interfaces, run the first boot configuration, and configure Avaya SBCE features	Configuring the network interfaces on page 25 Running the first boot configuration on page 26 Configuring Avaya SBCE features on page 27	

Required prerequisite configuration

You must configure the following items before you start administering HA on Microsoft® Azure.

ARM virtual network

Create an Azure Resource Manager (ARM) (V2) Virtual Network to put the Avaya SBCE virtual machines. For more information, see the following website:

https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-template

Azure internal load balancer

Deploy an Azure internal load balancer to create the HA pair. For more information, see the following website:

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

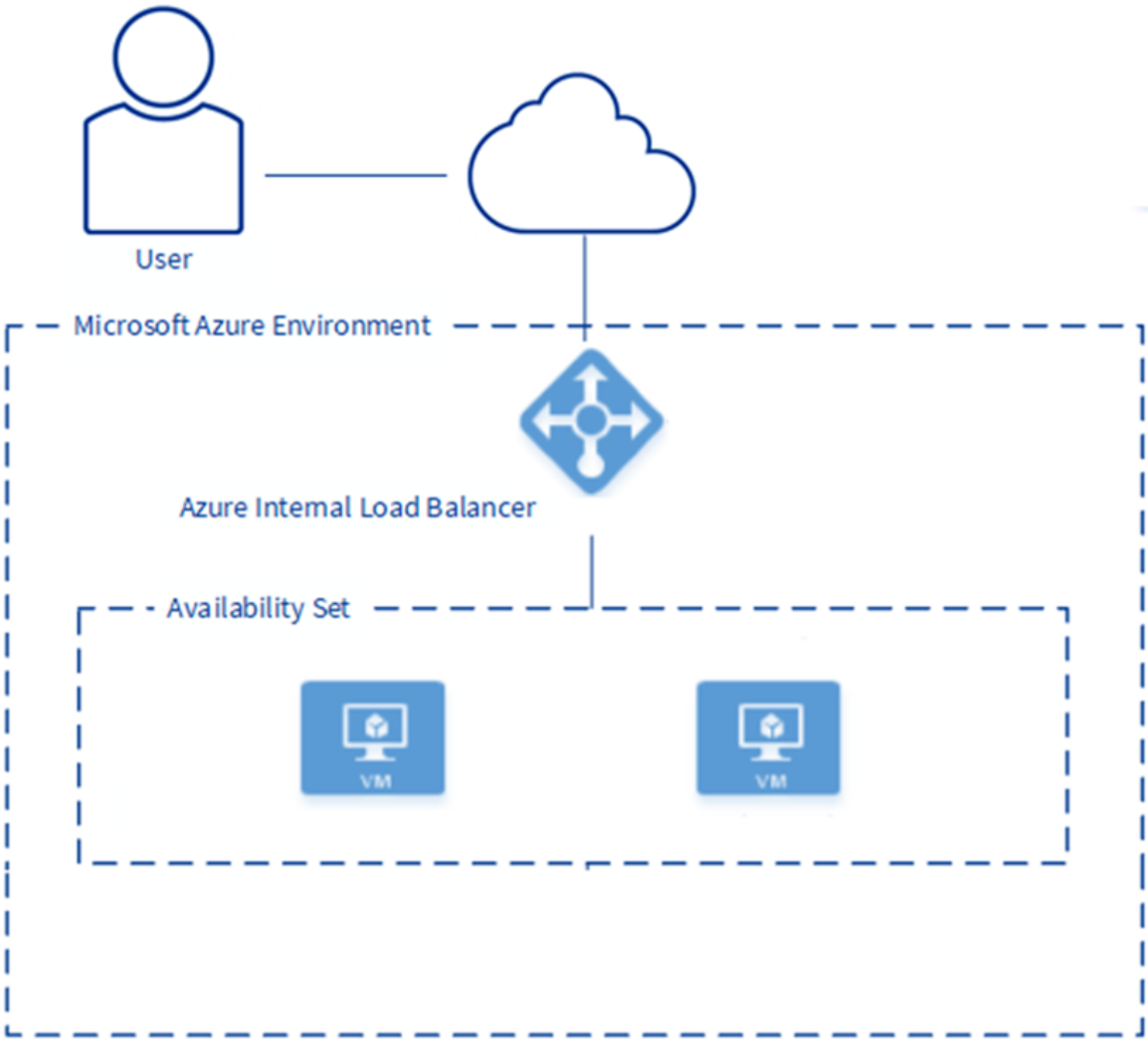
Deploy Avaya SBCE systems

Deploy two Avaya SBCE systems in ARM on the same virtual network. Both Avaya SBCE systems must be configured as part of an availability set. For more information, see the following website:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets

Configuration notes

The following diagram provides overview of this required prerequisite configuration:



To configure high availability using a load balancer, you must have the following items in place:

- Deploy two Avaya SBCE systems.

  Important:

  The HA Check Port must be set to the same port on both the active and standby systems for HA to work correctly. The same port must be configured as the probe port on the internal load balancer.

- The following management Load Balanced NAT Rules might be needed to access the Avaya SBCE systems:
  - TCP Port 22 for SSH access
  - TCP Port 5060 for Application access
  - Additional Load Balanced Rules for any traffic that is being transmitted through the Load Balancer

Use this table to record the necessary information required to create the Avaya SBCE pair in Azure:

Active Avaya SBCE name	
Standby Avaya SBCE name	
Pricing Tier	
Password for Avaya SBCE	
Availability Service Name	
Resource Group Name	
Virtual Network	
Internal Load Balancer Name	
Internal Load Balancer Public IP Address (PIP), if required	

Note:

It is not possible to bond interfaces on an Avaya SBCE pair in Azure.

Creating the first virtual Avaya SBCE in Azure

About this task

Information about the procedures in this section are found on the following website:

https://docs.microsoft.com/en-us/azure/virtual-machines/?WT.mc_id=azureportalcard_Service_Virtual%20Machines_-inproduct-azureportal

Refer to the following procedures used when creating non-HA deployments:

- Uploading the VHD file on page 19
- Creating a managed disk from the VHD file on page 20
- Creating the virtual machine on page 23

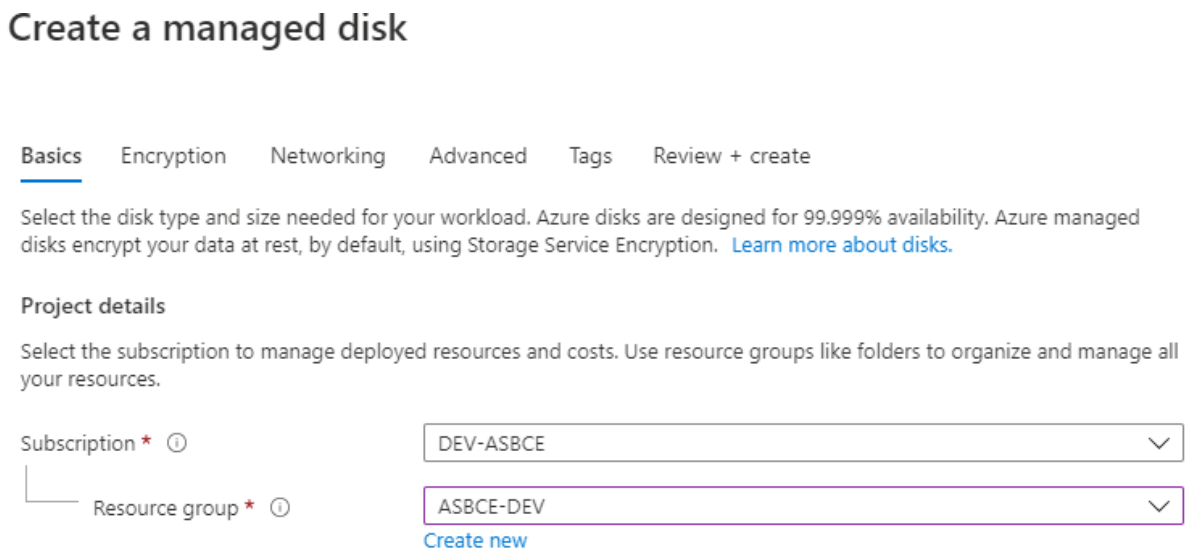
Note:

The screen examples shown in this procedure are shown to assist you using the Azure user interface. Your actual screens may differ than those shown here.

Procedure

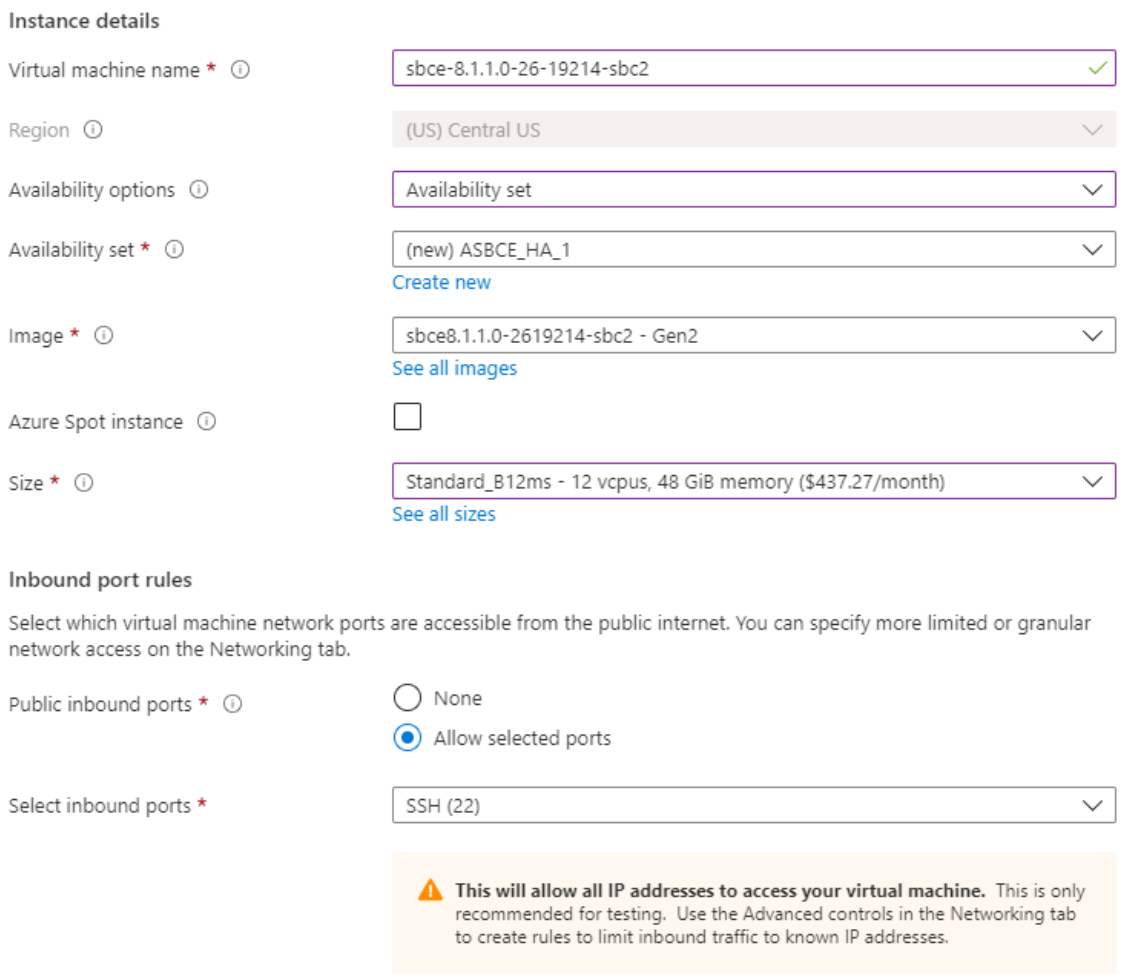
1. Log on to the Azure Portal using your Azure logon credentials.
2. Select **Disks**.
3. Click **Add**.

   The system displays a screen similar to the following example:



4. Configure the following options:
   - In the **Subscription** field, select the Azure subscription.
   - In the **Resource group** field, select an existing group or create a new group by clicking **Create new**. The is the group to which you deploy the first Avaya SBCE system for HA.
5. Move to the **Instance details** window.

   The system displays a screen similar to the following example:

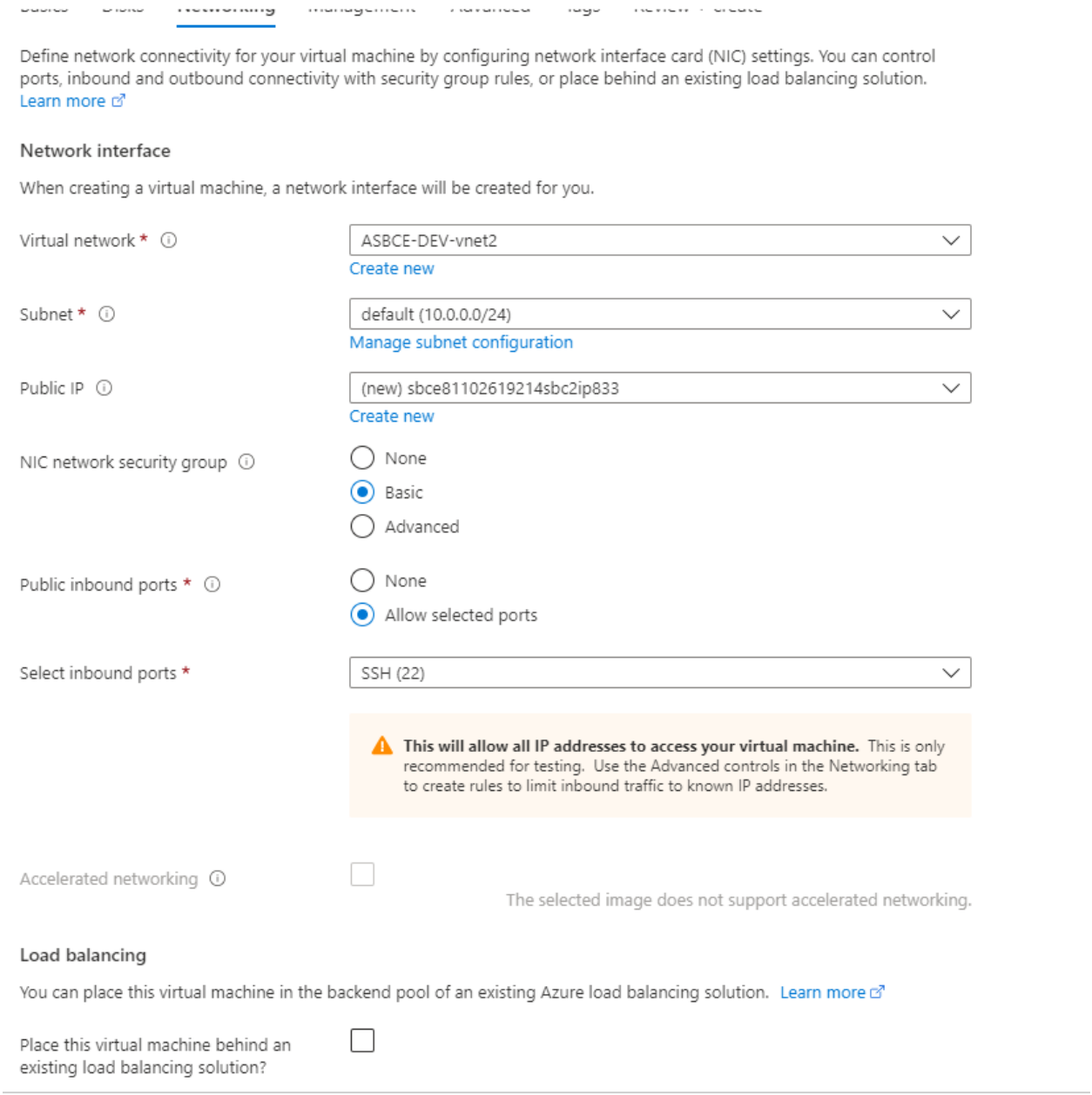


6. Configure the following options:
   - In the **Virtual machine name** field, enter a name for the Avaya SBCE virtual machine.
   - In the **Region** field, select the location of the system.
   - In the **Availability options** field, select **Availability set**.
   - In the **Availability set** field, create a new set or select an existing set for the HA pair.
   - In the **Image** field, select the Avaya SBCE software image that you downloaded and converted.
   - In the **Azure Spot instance** field, enable the feature if required for your deployment. By default, this option is disabled.
   - In the **Size** field, select the Standard_B12ms Azure virtual machine type, which is the only machine type that supports six network interfaces.
7. Click **Next : Disks**.

   Accept all disk defaults.

8. Click **Next : Networking**.

   The system displays a screen similar to the following example:



9. Configure the following options:
   - In the **Virtual network** field, select an existing network or create a new network.
   - In the **Subnet** field, select an existing subnet or create a new subnet.
   - (Optional) In the **Public IP** field, assign the public IP address of the system unless you are using load balancing as described later in these procedures.

- In the **NIC network security group** field, keep the default setting. The security group must contain rules for port 443 (management), 22 (SSH), and any other ports that are required for your deployment.
- In the **Accelerated networking** field, select **On** if the VM type supports accelerated networking.
- (Optional) In the **Load Balancing** options, enable load balancing if you already have a load balancer, or follow the load balancing procedure provided later in this section.

10. Click **Next : Management**.
11. If required for your deployment, configure the **Monitoring**, **Identity**, or **Shutdown** options. Otherwise, use the default settings.
12. Click **Next : Advanced**.
13. If required for your deployment, configure the **Extensions** or **Custom data** options. Otherwise, use the default settings.
14. Click **Next : Tags**.
15. If required for your deployment, configure the **Tags** options. Otherwise, use the default settings.
16. Click **Next : Review + create**.
17. Review all of your changes and correct any settings before you continue.
18. If required for your deployment, select **Download a template for automation** to download an ARM template.
19. Click **Create**.

    If you chose to create a new SSH key pair, you are now prompted to store the private key for the public key you created. Azure does not store the private key. After the SSH key is created, you will not be able to download the private key.

Creating the second virtual Avaya SBCE in Azure

About this task

Information about the procedures in this section are found on the following website:

https://docs.microsoft.com/en-us/azure/virtual-machines/?WT.mc_id=azureportalcard_Service_Virtual%20Machines_-inproduct-azureportal

Refer to the following procedures used when creating non-HA deployments:

- Uploading the VHD file on page 19
- Creating a managed disk from the VHD file on page 20
- Creating the virtual machine on page 23

Note:

The screen examples shown in this procedure are shown to assist you using the Azure user interface. Your actual screens may differ than those shown here.

Procedure

Follow the same procedures in Creating the first virtual Avaya SBCE in Azure on page 35 except for the following differences:

- You must select the same **Resource group** that was used when configuring the first virtual Avaya SBCE.
- You must select the same **Availability set** that was used when configuring the first virtual Avaya SBCE.
- You must select the same **Virtual network** that was used when configuring the first virtual Avaya SBCE.

Important:

You must configure all other options uniquely for the second virtual Avaya SBCE except for those options noted above.

Configuring the network interfaces, first boot, and Avaya SBCE features

About this task

After you configure the first and second virtual Avaya SBCE machines, you must do the procedures shown in this task.

Procedure

1. For both systems, configure the network interfaces as described in Configuring the network interfaces on page 25.
2. For both systems, run the first boot configuration as described in Running the first boot configuration on page 26.
3. For both systems, configure the required Avaya SBCE features as described in Configuring Avaya SBCE features on page 27.

About configuring the load balancer components

You must configure several settings to provide HA for the Avaya SBCE systems in your deployment:

- Create an Internal Load Balancer.
- Create a back-end address pool and add the Avaya SBCE systems to the pool.
- Create inbound NAT rules to direct traffic to the appropriate Avaya SBCE system.
- Create a probe to monitor the health of the Avaya SBCE systems.
- Create load balancing rules to control traffic flow.

Related links

Creating an Internal Load Balancer on page 41
Creating a backend address pool on page 43
Creating inbound NAT rules on page 43
Creating a probe to monitor the health of the Avaya SBCE HA pair on page 44
Creating load balancing rules to manage traffic on page 45

Creating an Internal Load Balancer

About this task

You must deploy an Internal Load Balancer to monitor the health of the Avaya SBCE systems and adjust traffic accordingly. For more information about this process, see the following website:

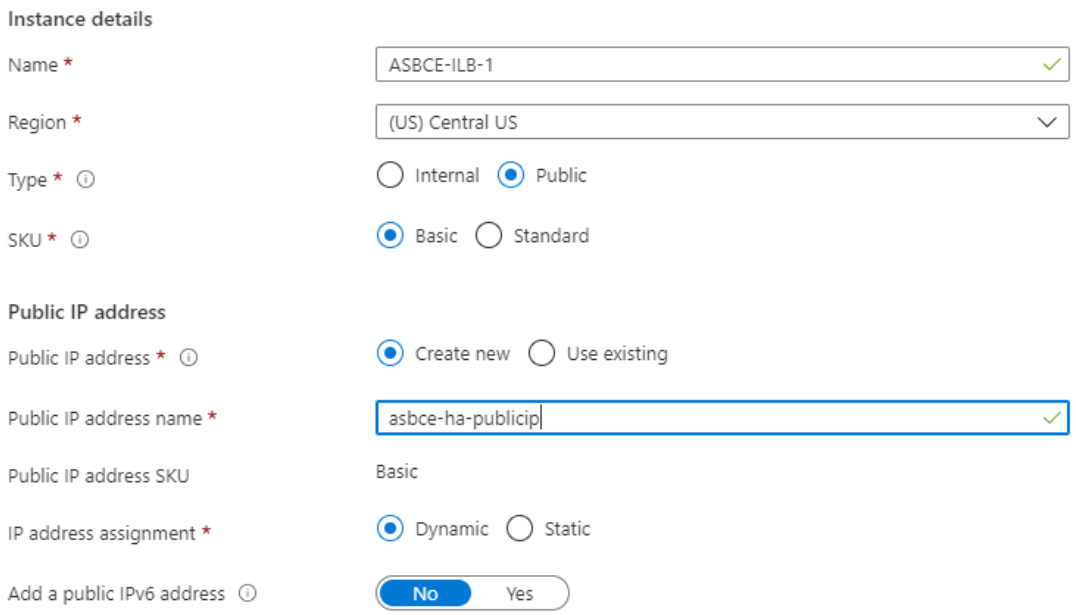
(http://portal.azure.com

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. From the Azure Management Portal dashboard, click **Create a resource**.
3. 2. Enter the phrase `Load Balancer` in the search bar and press **Enter**.

   The system displays the **Load Balancer** option.
4. Click **Create**.
5. Under **Project details**, configure the following options:
   - In the **Subscription** field, select the Azure subscription created for this deployment.
   - In the **Resource group** field, select the existing group to which you deployed the Avaya SBCE systems for HA.
6. Move to the **Instance details** window.

   The system displays a screen similar to the following example:



7. Configure the following options:
   - In the **Name** field, enter a name for the load balancer.
   - In the **Region** field, select the location of the system.
   - In the **Type** field, select either **Internal** or **Public**. Use **Internal** when the systems are within you private network. Use **Public** when the systems are located on the public network.
   - In the **SKU** field, select the type of SKU.
   - If creating a load balancer in the public network, configure the following options:
     - In the **Public IP address** field, either use an existing IP address or create a new IP address.
     - In the **Public IP address name** field, enter a name for the address.
     - In the **IP address assignment** field, select whether the IP address is dynamic or static.
     - In the **Add a public IPv6 address** field, select **No** or **Yes**. If you select **Yes**, the system displays additional fields to enter the IPv6 address.
8. Click **Next : Tags**.

   Either accept all Tags defaults, or make changes if required for your deployment.
9. Click **Next : Review + create**.
10. Review all of your changes and correct any settings before you continue.

11. If required for your deployment, select **Download a template for automation** to download an ARM template.
12. Click **Create**.

    The system creates the Internal Load Balancer, which might take some time to propagate throughout the system. If you chose to use a Public IP address, the front-end IP configuration is created automatically.

Creating a backend address pool

About this task

The backend address pool is a collection of virtual machines (Avaya SBCE systems) that are load balanced to provide HA.

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. 2. Enter the phrase `Load Balancer` in the search bar and press **Enter**.

   The system displays any load balancers administered on the system. The load balancer you created in Creating an Internal Load Balancer on page 41 should be displayed in the list.
3. Select that load balancer.
4. Click **Backend pools**.
5. Click **Add**.
6. Under **Add backend pool**, configure the following options:
   - In the **Name** field, enter a name for the pool.
   - In the **Virtual network** field, select the virtual network set up for HA.
   - In the **IP version** field, select either **IPv4** or **IPv6**.
   - In the **Associate to** field, select **virtual machines**.
7. Under **Virtual machines**, click **Add**.

   The system displays the list of configured virtual machines.
8. Select the two Avaya SBCE systems you want to be part of the HA pair.
9. Click **Add**.

   The system displays the two virtual machines in the backend pool.

Creating inbound NAT rules

About this task

The Azure cloud uses the Internal Load Balancer to create the Shared IP address (SIP), and to probe and route traffic to the Avaya SBCE virtual machine instances. To allow public access to

the service of each Avaya SBCE system, you must create Internal Load Balancer NAT rules. For example:

- *SIP*:5060 maps to the active Avaya SBCE port 5060
- *SIP*:5061 maps to the standby Avaya SBCE port 5060

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. 2. Enter the phrase `Load Balancer` in the search bar and press **Enter**.
3. Navigate to **Settings** > **Inbound NAT rules**.
4. Create four inbound NAT rules.
5. Click **Create**.

   The system displays the inbound NAT rules.

Creating a probe to monitor the health of the Avaya SBCE HA pair

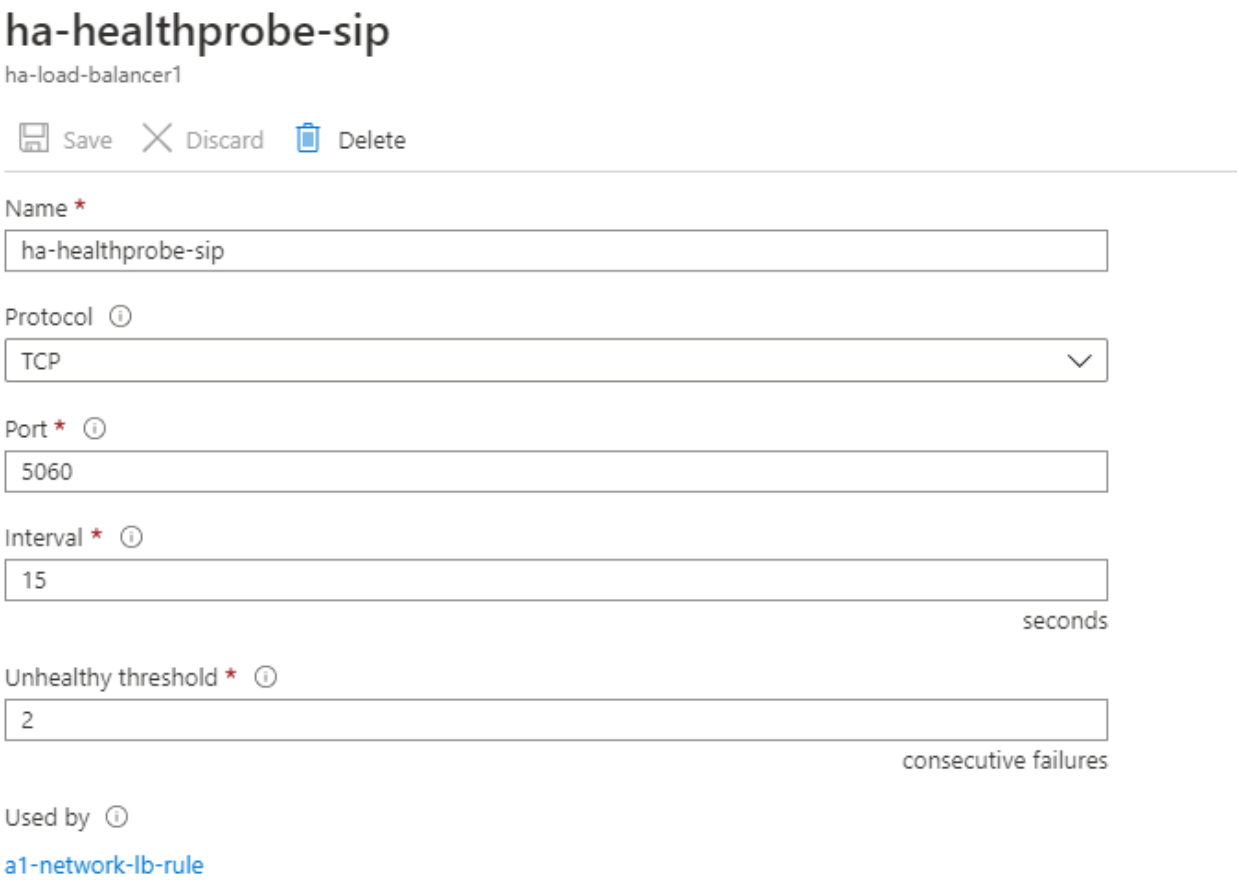
About this task

You must create a probe to monitor the health of the Avaya SBCE HA pair. This probe determines which Avaya SBCE is active and sends the traffic to the active Avaya SBCE. Should the active Avaya SBCE go offline, the probe takes that Avaya SBCE out of service and directs all traffic to the standby Avaya SBCE.

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. 2. Enter the phrase `Load Balancer` in the search bar and press **Enter**.
3. Navigate to **Settings** > **Health probes**.
4. Click **Add**.

   The system displays a screen similar to the following example:



5. Configure the following options:
   - In the **Name** field, enter a name for the probe.
   - In the **Protocol** field, select **TCP**.
   - In the **Port** field, select **5060**.
   - In the **Interval** field, select **5**.
   - In the **Unhealthy threshold** field, select **2**.
6. Click **OK**.

Creating load balancing rules to manage traffic

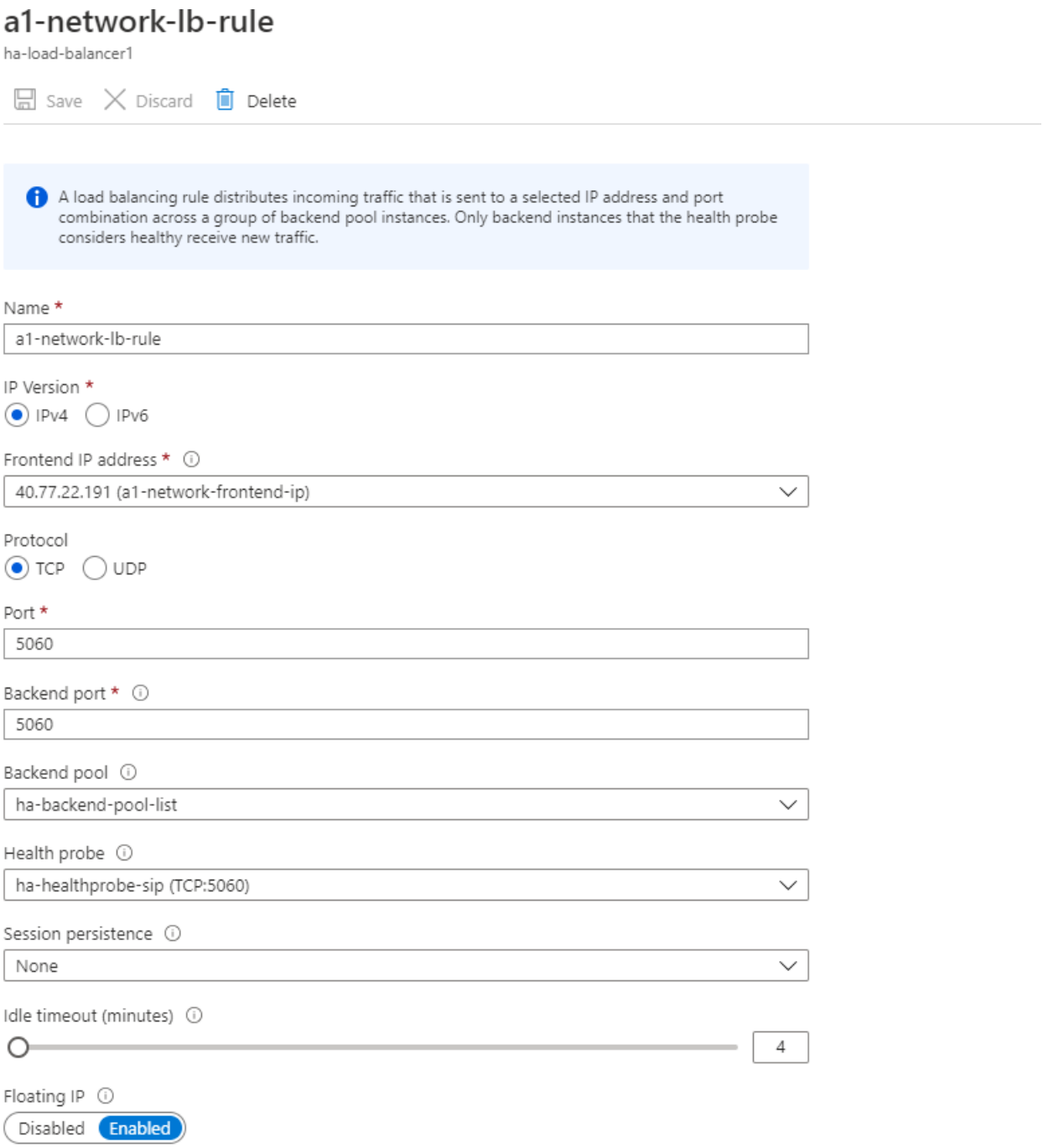
About this task

You must configure load balancing rules to manage any traffic that is published through the Avaya SBCE. A rule is set up for port 5060 which can be used to check the state of the Avaya SBCE within the backend pool.

Procedure

1. Log on to the Azure Portal using your Azure logon credentials.
2. 2. Enter the phrase `Load Balancer` in the search bar and press **Enter**.
3. Navigate to **Settings** > **Load balancing rules**.
4. Click **Add**.

   The system displays a screen similar to the following example:



5. Configure the following options:
   - In the **Name** field, enter a name for the rule.
   - In the **IP version** field, select either **IPv4** or **IPv6**.
   - In the **Frontend IP address** field, select the system that serves as your public access point.

- In the **Protocol** field, select **TCP**.
- In the **Port** field, select **5060**.
- In the **Backend port** field, select **5060**.
- In the **Backend pool** field, select the backend pool you created in Creating a backend address pool on page 43.
- In the **Health probe** field, select the health probe you created for port 5060 in Creating a probe to monitor the health of the Avaya SBCE HA pair on page 44.
- In the **Session persistence** field, select **None**.
- In the **Idle timeout** field, enter **4**.
- In the **Floating IP** field, select **Disabled**.

6. Click **OK**.
7. Create additional load balancing rules for any other traffic that is published through the Avaya SBCE.

Configuring network security groups

About this task

Network security groups are used in Azure to control what traffic is allowed or denied access to virtual machines. Depending on your configuration, you must update one or more network security groups.

Procedure

Follow the procedures found at the following website:

https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

Testing the HA configuration

About this task

Use this task to emulate system failures so you can verify that the HA failover is working as expected.

Procedure

1. Restart the active SBCE server using the following command:

   ```
   /etc/init.d/ipcs-init restart
   ```

When you restart the active SBCE, the following processes occur to transfer control of call processing to the standby SBCE:

- The system begins a graceful shutdown of sockets towards the end points and Session Manager.
- Failover occurs within about 2.8 seconds.
- Application keep alive messages are exchanged between the active SBCE and the standby SBCE to determine the health of the application on primary SBCE. Keep alive messages are exchanged every 500ms with maximum number of 3 retransmissions. These values are configurable on Avaya SBCE.

2. Disconnect the network cable on the active SBCE to simulate a break in network communication. When you do this, the following occurs:
   - There is no graceful shutdown of sockets. All active connections are lost.
   - Failover occurs within about 250 ms.

   Note:

   A failover will also occur if there is a TCP link bounce, which is not a complete loss of network connection.

3. Restart the active SBCE server by cycling power. This would simulate a loss of power.

   When you cycle power on the active SBCE, the following processes occur to transfer control of call processing to the standby SBCE:

   - There is no graceful shutdown of sockets. All active connections are lost.
   - Failover occurs within about 2.8 seconds.
   - Application keep alive messages are exchanged between the active SBCE and the standby SBCE to determine the health of the application on the active SBCE. Keep alive messages are exchanged every 500ms with maximum number of 3 retransmissions. These values are configurable on Avaya SBCE.

Chapter 7: Licensing requirements

About licensing requirements

Avaya SBCE uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBCE software. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBCE:

- Standard Services delivers non-encrypted SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication, and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBCE.

Avaya SBCE uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBCE license file on a primary Element Management System (EMS) using the Device Management page.

Important:

You must not enable the local WebLM option and install an Avaya SBCE license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **Grace Period State**.

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.

Important:

Licenses and a WebLM server are required for new installations or upgrades.

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.

For integration with Microsoft® Teams, Avaya SBCE requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBCE requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

Avaya SBCE licensed 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_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.

Table continues…

License feature	Description
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server 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 the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBCE. This license is required when using any 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. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBCE encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

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 the WebLM server IP address using the EMS web interface

Before you begin

Install the Avaya SBCE license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Licensing**.
3. Do 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`

     The URL format of 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**.
4. Click **Refresh Existing License** to refresh the existing licenses.
5. 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.
6. On the Dashboard screen, check the **License State** field.

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

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

Configuring the WebLM server IP address using CLI

Before you begin

Install the Avaya SBCE license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log on to the CLI with administrator credentials.
2. Run the following command to configure an external WebLM server URL:

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

About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBCE connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBCE setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBCE setup.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBCE.

Note:

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBCE setup.

Chapter 8: Verifying a successful deployment

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.

Installing and verifying successful installation of EMS and SBCE

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.

   Note:

   The 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, enter 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, enter the configuration. For more information, see *Administering Avaya Session Border Controller for Enterprise*.
6. Click **Finish**.

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

Logging in to 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.

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		
Avaya Session Border Controller for Enterprise Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBCE.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller for Enterprise Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller for Enterprise on a Hardware Platform	Describes how to plan and deploy an Avaya SBCE system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBCE system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on an Avaya Aura® Appliance Virtualization Platform	Describes how to plan and deploy an Avaya SBCE system on a virtualized appliance.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller for Enterprise on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBCE system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller for Enterprise on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBCE system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller for Enterprise Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller for Enterprise	Describes how to upgrade to the latest release of Avaya SBCE.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller for Enterprise	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise	Describes troubleshooting and maintenance procedures for Avaya SBCE.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller for Enterprise and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBCE with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller for Enterprise Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBCE Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller for Enterprise Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBCE Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

For Portwell documentation, go to https://portwell.com/.

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 the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for 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 both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

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

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - 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 website.

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

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

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
20600W	Avaya SBCE 8.1.x Technical Delta
21098W	Avaya SBCE 8.0.x Technical Delta
20660W	Administering Avaya SBCE Release 8 for SIP Trunking
60660W	Administering Avaya SBCE Release 8 for Remote Worker
20660T	Administering Avaya SBCE Release 8 Test
20800C	Implementing and Supporting Avaya SBCE — Platform Independent
20800T	Avaya SBCE Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBCE — Platform Independent
26160W	Avaya SBCE Fundamentals
7008T	Avaya SBCE for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBCE for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

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.

- 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.

Index

M

N

O

P

R

S

T

U

V

W