Deploying Avaya Session Border Controller on ASP 130 R6.0.x (KVM on RHEL 8.10)

Release 10.2.1
Issue 1
December 2025

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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.

Service Provider

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 to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

Contents

Chapter 1: Introduction

Purpose

This document outlines the procedures for deploying Avaya Session Border Controller for Enterprise (Avaya SBC) applications on Avaya Solutions Platform 130 Appliance R6.0.x.

ASP 130 R6.0.x uses Kernel-based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) 8.10.

Background

In June 2024, Broadcom discontinued its Embedded OEM program. This decision affected Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 solutions, as Avaya was an Embedded OEM partner of VMware. Therefore, Avaya needed to identify a new hypervisor.

Avaya introduced KVM on RHEL 8.10 in the Avaya Solutions Platform 130 Appliance R6.0.x program. In addition to the new hypervisor, this release also introduced an updated server hardware platform based on Dell R660xs.

All Avaya Solutions Platform 130 Appliance R6.0.x solutions (Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300) now ship with the new KVM. Avaya Solutions Platform 130 Appliance R6.0.x does not support ESXi. For more information, see PSN020640u - Avaya Solutions Platform R6.0.x Introduction.

Note:

- Avaya Solutions Platform 130 Appliance R6.0.x with KVM on RHEL 8.10 supports Avaya SBC server KVM-specific images only.
- Do not deploy KVM-specific images on customer-provided KVM environments, including those based on RHEL.
- This document is specific to Avaya SBC R10.2 for Avaya Solutions Platform 130 Appliance R6.0.x (KVM on RHEL 8.10).

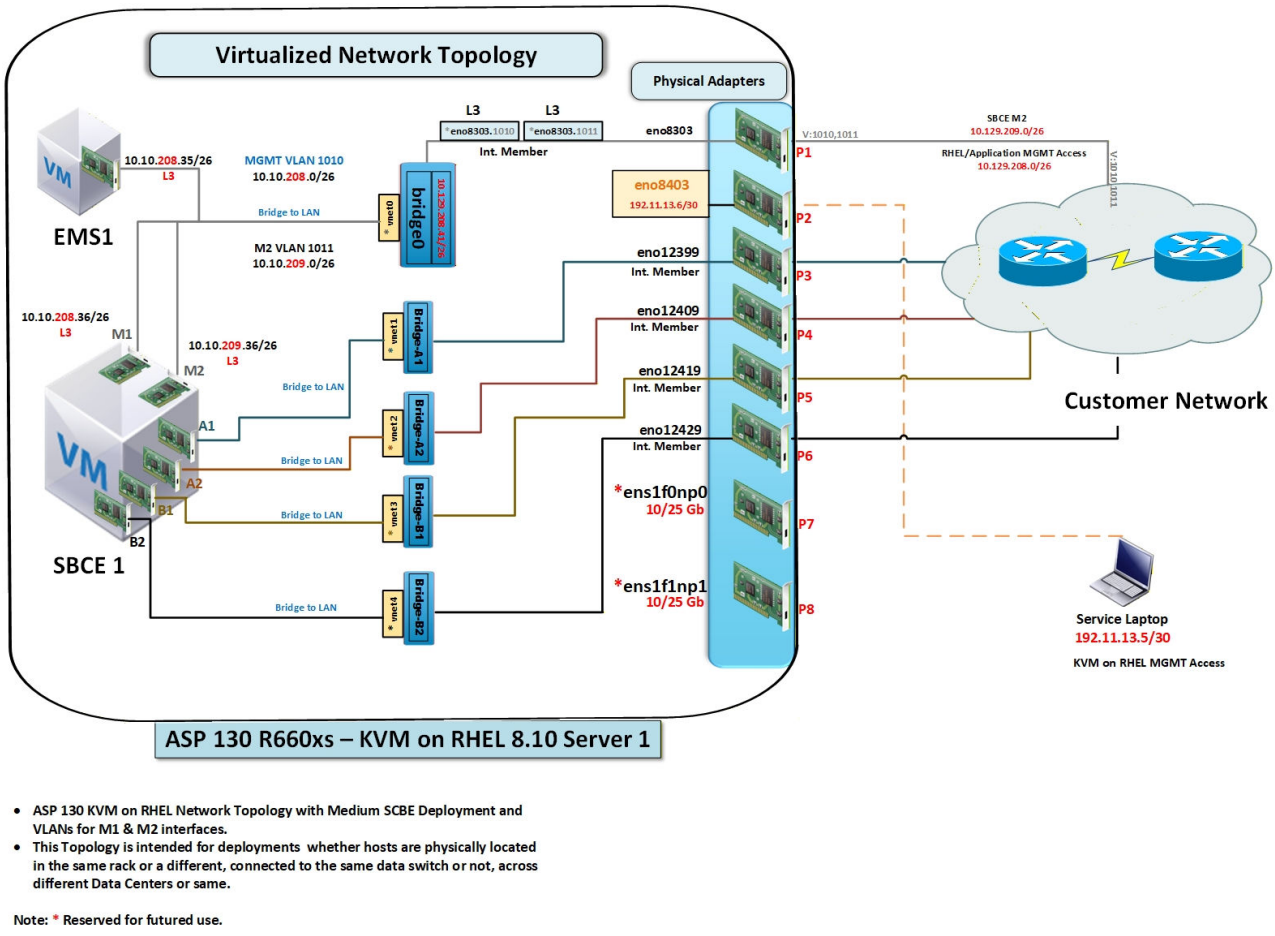
Change history

Issue	Date	Summary of changes
1	December 2025	Initial publication

Chapter 2: Architecture overview

Architecture

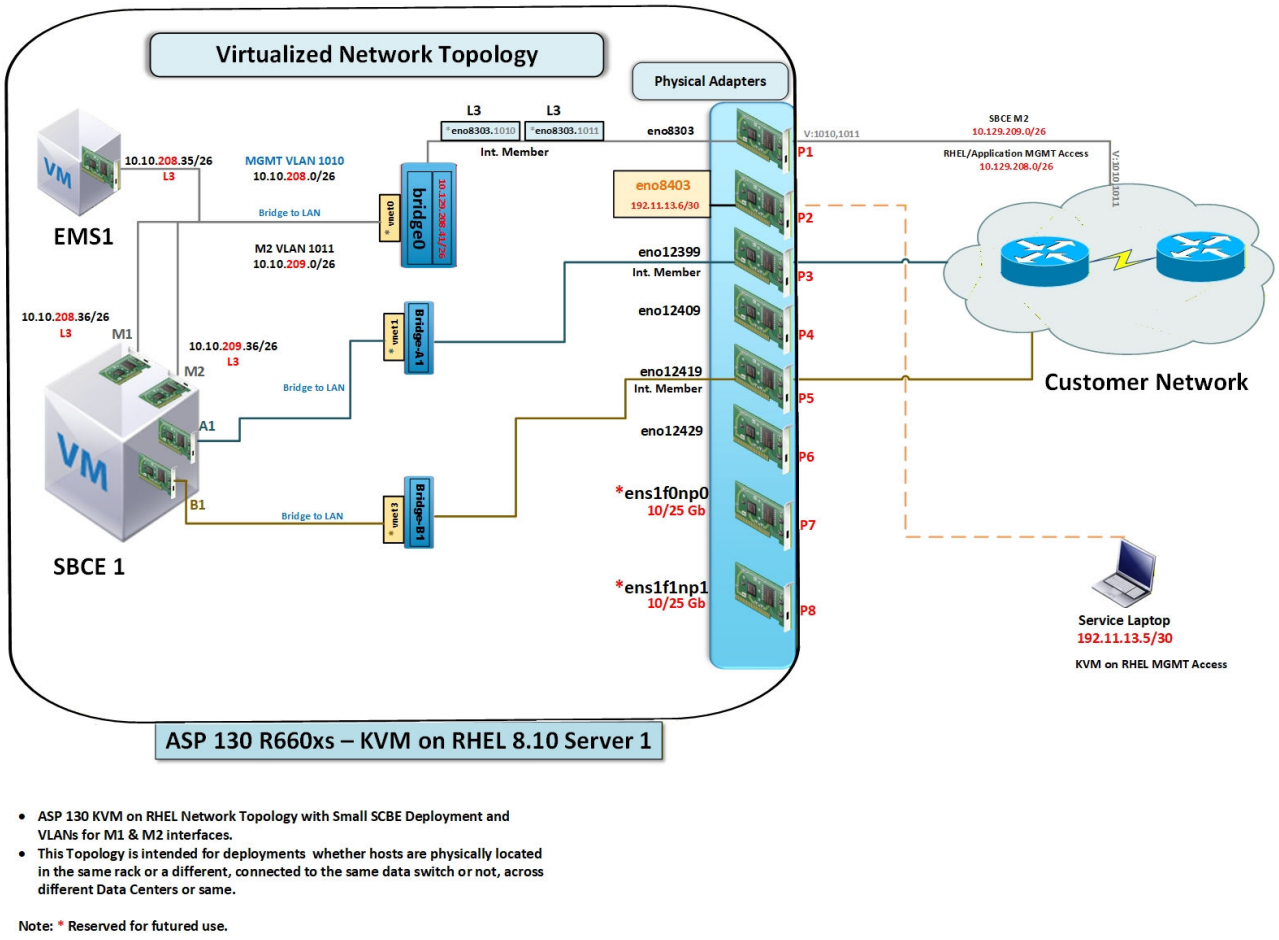
Avaya SBC deployment on Avaya Solutions Platform 130 Appliance R6.0.x (KVM on RHEL 8.10) uses a virtualized network model. Both the Element Management Server (EMS) and SBC instances run as Virtual Machines (VMs) on the Dell R660xs KVM host, with separate traffic using Linux bridges and VLANs.



- ASP 130 KVM on RHEL Network Topology with Medium SCBE Deployment and VLANs for M1 & M2 interfaces.
- This Topology is intended for deployments whether hosts are physically located in the same rack or a different, connected to the same data switch or not, across different Data Centers or same.

Note: * Reserved for futured use.

Figure 1: Medium SBC Deployment



- ASP 130 KVM on RHEL Network Topology with Small SCBE Deployment and VLANs for M1 & M2 interfaces.
- This Topology is intended for deployments whether hosts are physically located in the same rack or a different, connected to the same data switch or not, across different Data Centers or same.

Note: * Reserved for futured use.

Figure 2: Small SBC Deployment

To simplify deployment and eliminate variations, use the following validated architectural rules:

1. Use VLANs for M1 and M2. This ensures consistent behavior regardless of the host location (same rack, same switch, or different data centers).
2. Use bridge0 for management access. Use this default Cockpit/libvirt bridge to manage KVM host, manage VMs (M1), access EMS, and manage application networks.
3. Use 10/25 GbE ports only for high session capacity. Map A2 and B2 to high-speed 10/25 GbE ports only when needed. For small and medium deployments, 1 GbE on A1 and B1 is sufficient.

   Note:

   The 10/25 GbE Network Interface Cards (NICs) are not supported on Avaya Solutions Platform 130 Appliance R6.0.x. Support is planned for the future release.

   Any mention of 10/25 GbE NICs in this document refers to the future functionality.
4. Use of High availability (HA) and direct M2 cable connections is optional. The default option is M2 over a VLAN. Experienced integrators choose an L2 crossover between hosts.

Key design points

1. Tag M1 and M2 VLANs: Use the Management VLAN for M1 (1010) and the HA VLAN for M2 (1011). For example, refer to Figure 1 on page 7 and Figure 2 on page 8.

   This approach works for single-rack, multi-rack, or multi-switch scenarios.
2. Assign Bridges: Use A1 and B1 (1 GbE) for signaling and media. Use A2 and B2 for high-capacity traffic.
3. Use bridge0: Always use bridge0 as the management base bridge.
4. Attach NICs to Bridges: Attach all VM NICs to bridges rather than physical NICs to ensure deterministic network performance.

This approach reduces configuration errors and fully aligns with KVM best practices for deterministic network performance.

SBC Capacity and NIC Requirements

SBC deployment size depends solely on session capacity, not the physical layout. The following table lists the recommended NIC usage for each deployment size:

Deployment Size	Recommended NIC Usage
Small SBC	A1/B1 (1 GbE) only
Medium SBC	A1/B1 (1 GbE) + A2/B2 (1 GbE) **Note:** 10/25 GbE is optional.
Large SBC	A2/B2 (10/25 GbE) required

System Architecture

Avaya SBC deployment on Avaya Solutions Platform 130 Appliance R6.0.x (KVM on RHEL 8.10) uses a virtual architecture model. In this model, the Element Management Server (EMS) and SBC instances run as separate Virtual Machines (VMs) on KVM hosts.

Dell R660xs platform powers each appliance host, configured for high-performance, low-latency networking and predictable SBC behavior. Depending on the deployment size and redundancy requirements, you can manage one or more SBC High-Availability (HA) pairs with either a single EMS or an EMS HA pair.

The following are the functions of the virtual components:

- EMS VM: Manages, configures, and monitors SBC instances from a centralized interface.
- SBC VM: Provides signaling and media processing for SIP sessions, secured through encryption and topology hiding.
- Each VM uses dedicated vCPUs, memory reservations, and network bridges that map directly to physical Network Interface Cards (NICs) on the host.

Virtualized network topology

You can deploy Avaya SBC on Avaya Solutions Platform 130 Appliance R6.0.x to support multiple topologies for both single and multiple data center environments.

The required SBC size depends only on session capacity, not on the number of switches or racks the servers use. Each topology enables you to separate management. You can also choose between VLAN or flat-LAN configurations for increased flexibility.

The following table describes the networking components for these virtualized environments:

Interface	Type	Transport	Purpose	Notes
M1	Management	VLAN over bridge0	EMS/SBC Management (10.10.x.x)	Always use a VLAN.
M2	HA/Sync	VLAN over bridge0 or dedicated bridge	Provides HA signaling.	A direct link is optional.
A1	Signaling/Media (Internal)	Bridge → 1 GbE NIC	Handles enterprise-side SIP and RTP.	This interface is required.
B1	Signaling/Media (External)	Bridge → 1 GbE NIC	Handles public/DMZ SIP and RTP.	This interface is required.
A2	High-capacity Media	Bridge → 10/25 GbE NIC or 1 GbE NIC	Supports additional media sessions.	Use for high-session deployments.
B2	High-capacity Media	Bridge → 10/25 GbE NIC or 1 GbE NIC	Supports additional media sessions.	Use for high-sessions deployments.

High Availability (HA) pairing

SBC High Availability pairing deployment

- Standard SBC deployment requires a pair of SBC Virtual Machines (VMs), wherein one device functions as Primary and the other as Secondary.
- SBC High Availability (HA) pairs must not be installed on the same physical host to avoid a single point of failure.

EMS high availability pairing deployment

- EMS can be deployed as a single instance or in a HA pair, wherein one device functions as Primary and the other as Secondary.
- EMS HA pairs must also be installed on different physical hosts.

When deploying both SBC HA pairs and EMS HA pairs, distribute SBC EMS HA pairs across at least two physical ASP 130 R6.0 hosts.

Example

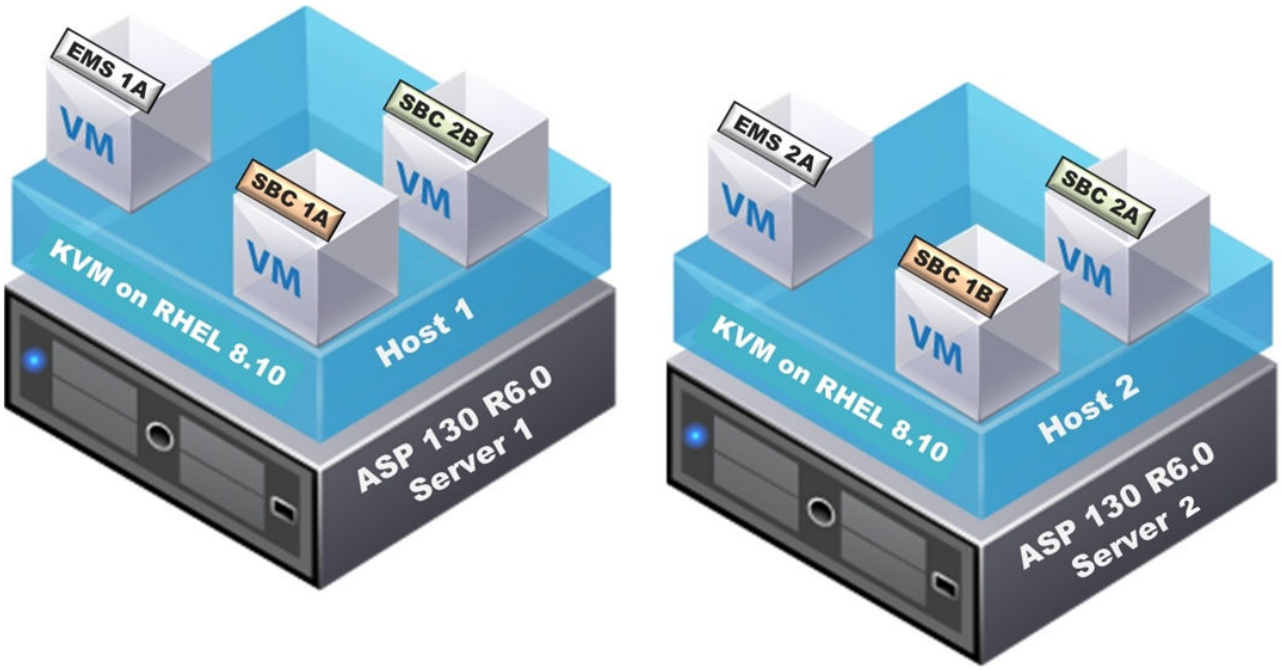


Figure 3: The virtual deployment of two ASP 130 R6.0 servers

As shown in the image:

- ASP 130 R6.0 Host 1: EMS 1A, SBC 1A, SBC 2B
- ASP 130 R6.0 Host 2: EMS 2A, SBC 1B, SBC 2A

This ensures redundancy at both the application layer (HA) and the infrastructure layer (separate ASP 130 hosts).

Network connectivity between an EMS pair and an SBC HA pair

The diagram shows the network connectivity between an EMS pair and an SBC HA pair:

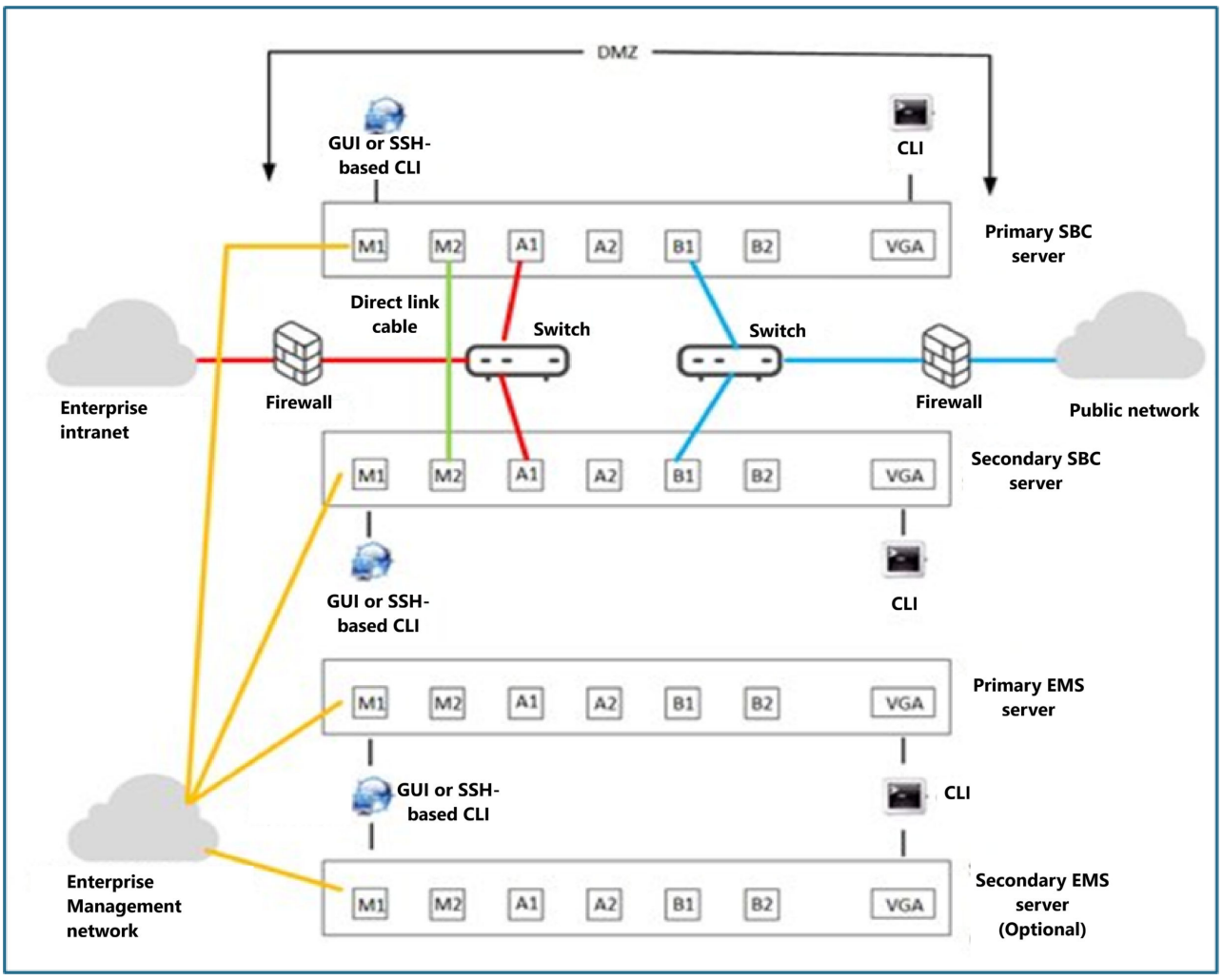


Figure 4: EMS and SBC HA pair

Network interface	Name	Description
Management interfaces	M1 (Yellow)	M1 connects both SBCs and EMS servers to the enterprise management network for configuration, monitoring, and administration through GUI or SSH. EMS servers use M1 to connect to the SBCs over the enterprise management network. This channel provides all management and monitoring communications between EMS and the SBC HA pair.

Table continues…

Network interface	Name	Description
	M2 (Green)	M2 is used as the HA heartbeat link between the Primary and Secondary SBC servers. A dedicated direct link cable ensures synchronization.
Access network	A1/A2 (Red)	A1 and A2 connect to the enterprise intranet through a firewall and switch to carry latency-sensitive access-side traffic from enterprise users toward the SBC.
Core network	B1/B2 (Blue)	B1 and B2 connect to the public network through a firewall and switch to carry core-side traffic between SBC and external service providers or the internet.

Chapter 3: Deployment recommendations for SBC and EMS

Software compatibility

The following table provides the supported version of Avaya SBC deployed on Avaya Solutions Platform 130 Appliance R6.0.x (KVM on RHEL 8.10):

Avaya Solutions Platform 130 Appliance (KVM on RHEL 8.10) version	Avaya SBC server release
Avaya Solutions Platform 130 Appliance R6.0.0.2 and later	Avaya SBC 10.2.1.x

Requirements for deploying Avaya SBC on ASP R6.0.x

Before you deploy Avaya SBC on Avaya Solutions Platform 130 Appliance R6.0.x, ensure that you meet the following requirements:

- Only Avaya Solutions Platform 130 Appliance R6.0.0.2 and later supports Avaya SBC R10.2.1.x. If you are using Avaya SBC on Avaya Solutions Platform 130 Appliance R5.x, upgrade to R6.0.0.2 or later before deployment.
- Follow the required deployment rules when installing Avaya SBC R10.2.1.x on Avaya Solutions Platform 130 Appliance R6.0.0.2 or later. Review the deployment documentation to ensure compliance.
- Use the Avaya One Source Configurator (A1SC) to order new installations, perform migrations, or add applications. If A1SC recommends multiple servers, deploy applications according to its configuration output.
- During migration, you need additional hardware to maintain optimal application performance. Only Avaya ASP-certified applications can be deployed on ASP servers. Third-party applications are not supported.

Supported footprints of Avaya SBC server on Avaya Solutions Platform 130 Appliance R6.0.x

Avaya SBC R10.2.1.x on Avaya Solutions Platform 130 Appliance R6.0.0.2 and later (KVM on RHEL 8.10) consists of a single `qcow2` image.

Use a `qcow2` image for the following deployment types:

- Combination Element Management Server (EMS) and SBC
- Standalone EMS
- Standalone SBC

Important:

Deploy the EMS server before you deploy any SBC servers. Ensure the EMS server is online and accessible before you deploy the standalone SBCs.

The same SBC 10.2.1.x `qcow2` file supports both EMS and SBC deployments. When you convert the file from thin to thick, enter a unique filename, such as `EMS1-thick.qcow2` or `SBC1-thick.qcow`, to correctly identify the server type.

Hardware support and requirements

Avaya SBC R10.2.1.x supports the hardware profiles listed in the following table. All Avaya Solutions Platform 130 Appliance and later solutions ship only with the new KVM on RHEL8.10 hypervisor.

Hardware	Unsupported for SBC 10.2.1	Supported for SBC 10.2.1.x
Dell R660xs (Intel Emerald Rapids CPUs)	NA	A1, A2, A3, and A31

All Avaya Solutions Platform 130 Appliance Dell R660xs hardware profiles meet the minimum clock speed requirement of 2.4 GHz.

Existing Dell R640 servers

You can update an existing ASP R5.1.x Dell R640 server to Avaya Solutions Platform 130 Appliance R6.0.x. Application deployment depends on the Dell R640 hardware server profile. Certain profiles do not meet the minimum clock speed requirements (2.4 GHz) and are therefore not supported.

Hardware	Unsupported for SBC 10.2.1	Supported for SBC Server 10.2.1.x
Dell R640 (Intel Skylake CPUs)	Hardware Profiles 2, 3	Profiles 4, 5, and 51
Dell R640 (Intel Cascade Lake CPUs)	Hardware Profiles 2, 3	Hardware Profiles 4, 5, 51

Note:

Hardware Profile 4 requires two additional HDDs for support.

Hardware profile A3 and A31 configurations

If you implement a hardware profile A3 or A31, the following two physical interface configurations are available for SBC deployments:

- With two 10/25 GbE ports: Supports six physical interfaces (2x10/25 GbE NICs and 4x1 GbE NICs).
- Without two 10/25 GbE ports: Supports four physical interfaces (4x1 GbE NICs).

Note:

Avaya Solutions Platform 130 Appliance R6.0 does not support 10/25 GbE Network Interface Cards (NICs). Support for these NICs is planned in the future Avaya Solutions Platform 130 Appliance release. Once available, Avaya Solutions Platform 130 Appliance R6.0.x release notes will be updated accordingly.

Important:

Any mention of 10/25 GbE NICs in this document refers solely to this future functionality.

The number of Virtual Machines (VMs) and servers required for a solution deployment will vary based on multiple factors, such as required sessions or High Availability (HA). You need to deploy additional SBCs to increase the number of sessions available in your solution.

SBC-EMS combo VM resource requirements

The following table outlines the minimum resource requirements for deploying Session Border Controllers (SBCs), Element Management System (EMSs), and Combo Virtual Machines (VMs):

Resource	SBC VM	EMS VM	EMS+SBC Combo VM	Notes
HT supported	Yes	Yes	Yes	Hyper-threading is supported.
vCPU	4	3	4	The combo VM requires SBC sizing.
Minimum CPU Speed	2.4 GHz	2.4 GHz	2.4 GHz	This is the tested baseline speed.
Memory Reservation	16 GB	16 GB	16 GB	Increased from 8 GB.
Storage Reservation	64 GB	64 GB	64 GB	ASP 130 R6.0 requires only thick-provisioned storage.
Virtual Network Interfaces (vNICs)	4 (min) or 6 (max)	1	4 (fixed)	The required number of vNICs depends on your deployment profile.

Table continues…

Resource	SBC VM	EMS VM	EMS+SBC Combo VM	Notes
Standard Deployment	1 SBC instance	1 EMS instance	1 Combo instance	—
High Availability	1 SBC HA Pair (Primary + Secondary)	1 EMS HA Pair (Primary + Secondary)	1 Combo HA Pair	HA pairs must not be sized or installed on the same host.
EMS Scaling	—	Supports 1–12 SBC pairs (maximum of 24 SBCs)	NA	The combo instance couples SBC+EMS tightly. 1- 12 pairs or a combination of pairs with single SBCs means a maximum of 24 SBCs.

For more information about capacity and scalability considerations, see Avaya Session Border Controller Overview and Specification, Chapter 4.

Important:

`t3ch@S1t3` is used as an example password for each login throughout this application note. The password `t3ch@S1t3` is an example only.

Note:

The maximum capacity per SBC VM or EMS+SBC VM using 1GB bandwidth is 5,000 non-encrypted sessions.

SBC qcow2 image

Avaya SBC on Avaya Solutions Platform 130 Appliance R6.0 consists of a single `qcow2` file, for example,`sbce-10.2.1.0-101-24795.qcow2`. This file is initially in the thin format until you convert it to the thick format within the Avaya Solutions Platform 130 Appliance R6.0 hypervisor.

Before converting, decide on a naming convention for the thick-provisioned `qcow2` images.

You can deploy different Virtual Machines (VMs) from the same `qcow2` image. When you convert the file to thick provisioning, you must assign a unique name to each instance that reflects its use.

Example

- EMS: `sbce-10.2.1.0-101-24795-EMS1-thick.qcow2`
- SBC: `sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`

If you deploy multiple SBC instances, replace the number 1 with the next sequential number (for example, `SBC2-thick.qcow2`).

Chapter 4: Planning and preconfiguration

Pre-requisites for Greenfield deployment or migration

To prepare for ASP 130 R6.0.x Greenfield deployment or migration, complete the following system, hardware, and configuration prerequisites to ensure compatibility and data integrity. Ensure you do the following:

#	Description	✔
1	Pre-plan naming conventions for qcow2 files before creating the files.	
2	Process all hardware and software orders through A1SC.	
3	Do not add any VMs that are not certified by Product Management.	
4	Use two additional hard drives when migrating from ASP 130 R5.1.x on Dell R640 with Hardware Profile 4.	
5	Reconfigure the RAID array on existing Dell R640 systems. Use only the Hardware Profile 4, Hardware Profile 5, and Hardware Profile 51 for server configuration. RAID array reconfiguration reformats and erases all hard drives.	
6	Obtain ASP R6.0.0.0 installation media on a USB drive. Also download and install `av-asp-tools-1.5-3.el8.x86_64.rpm` before installing ASP R6.0.0.2 or later. This RPM creates the required directory structure framework for SBCE Server qcow2 image deployment. Future ASP 6.0.x service packs may include updated versions of this RPM.	
7	Connect a monitor and USB keyboard to enable IDRAC and perform BIOS or firmware upgrades.	
8	Perform a backup of the SBCE Server application data currently deployed on ASP 130 R5.1.x. Store the backup off-server for use during ASP 130 R6.0.x deployment.	

Table continues…

#	Description	✔
9	For migrations, capture all host and application IP addresses and naming details, such as hostname, domain name, NTP server, and DNS server from the current ASP 130 ESXi host. **Note:** These details are not automatically migrated and you need to enter these details manually during SBCE Server qcow2 image deployment on ASP 130 R6.0.0.2 or later.	
10	Use Avaya Solutions Platform 130 hardware (Dell PowerEdge R640 or R660xs) with ASP R6.0.0.2 or later installed (KVM on RHEL 8.10). In-place hypervisor upgrades delete all existing data.	
11	Check for newer BIOS or firmware updates. Download and install the latest BIOS/FW for Dell R640 or R660xs. It requires a VGA monitor and USB keyboard.	
12	Verify that you have the `custadmin` username and password or an equivalent for logging into the ASP 6.0 hypervisor running on KVM with RHEL 8.10. These credentials are required for both the Cockpit web UI and the ASP R6.0.x command-line interface (CLI).	

BIOS and firmware update procedures differ between Avaya Dell R640 and Dell R660xs systems. See the latest Product Support Notices (PSNs) on support.avaya.com for model-specific instructions (current as of August 1, 2025).

General rules

Aspect	Guidelines
Bridge interfaces	SBC must be deployed on dedicated Linux bridges mapped to physical NICs in the KVM host for data interfaces (known as A1, A2, B1 and B2).

Table continues…

Aspect	Guidelines
Network bandwidth	• A minimum of 1 GbE connectivity per data interface (A/B sides) must be provisioned. • Bonding in active-backup mode is recommended for resiliency, but a single port may be used if redundancy is not required. • On servers with 10/25 GbE NICs, allocate sufficient bandwidth per SBC instance to meet these capacity requirements, ensuring a minimum guaranteed throughput per interface. • The actual bandwidth requirement is capacity-dependent, based on the number of sessions, encrypted calls, and media handling requirements. • For sizing, refer to the Table 1: SBC capacity and interface sizing guidance on page 23 to determine the correct allocation for your deployment.
Oversubscription	Latency-sensitive SBC traffic (A1, B1, A2, B2) must not share oversubscribed NICs or bridges.
Abstraction	SBC and EMS VMs must never directly bind to physical NICs, only to host-defined bridges.
Consistency	Always maintain the same interface-to-bridge mapping across HA pairs to avoid mismatch.
Isolation	Each latency-sensitive data interface (A1, A2, B1, B2) should have a dedicated bridge backed by a dedicated physical NIC (or bandwidth-guaranteed VF).
Management	• Separate bridges will be required for M1 and M2 to ensure clean HA heartbeat separation. A separate bridge should be created for M2 and M1 will remain on bridge 0. • Given the same physical interface will be shared by M1 and M2, it is necessary to configure a VLAN for each interface. For example, Bridge0 connects to M1 and maps to eno8303 on VLAN 100, while BridgeM2 connects to M2 and maps to eno8303 on VLAN 110. For more information about VLAN and bridge configuration, see Application note for ASP 130 VLAN & VLAN trunking configuration guide-Rev1.

Instance interface order

Within a Virtual Machine (VM), the SBC/EMS application expects the following interface order:

1. M1 (Primary management interface)
2. A1 (Primary access-side data interface)
3. B1 (Primary core-side data interface)
4. M2 (Secondary management/HA heartbeat (SBC only, direct link))
5. A2 (Secondary access-side data interface (SBC only, optional))
6. B2 (Secondary core-side data interface (SBC only, optional))

Note:

For EMS-only deployments, the minimum interface requirement is M1, with M2 available for optional use.

For SBC-only deployments, the minimum interface requirement is M1, A1, B1, and M2, with A2 and B2 for high-capacity six-interface deployments.

For deployments combining EMS and SBC, the minimum interface requirement is M1, A1, B1, and M2.

Deployment options

Following table describes the deployment options available for EMS-only, SCB-only, and combined deployments:

Deployment type	Minimum interfaces	Maximum interfaces	Interface order
EMS-only	1	2	M1, M2 (optional)
SBC-only	4	6	M1, A1, B1, M2 (with A2, B2 if 6-NIC profile)
EMS and SBC (combined)	4	4	M1, A1, B1, M2

SBC interface assignment with capacity guidance

Interface	Function	Typical Usage	Capacity Guidance (Throughout per interface)
M1	Primary Management	EMS ↔ SBC management, CLI/GUI access	Low bandwidth (<100 Mbps). Management traffic only
A1	Primary Access Data	Access-side SIP/media traffic	SBC: ~500 Mbps Medium SBC: ~1 Gbps Large SBC: >1 Gbps (up to NIC line rate; may require 10/25 GbE NICs)
B1	Primary Core Data	Core-side SIP/media traffic	SBC: ~500 Mbps Medium SBC: ~1 Gbps Large SBC: >1 Gbps (up to NIC line rate; may require 10/25 GbE NICs)
M2	Secondary Management / HA Heartbeat	SBC HA sync, state replication	Low bandwidth (<100 Mbps). Critical for HA sync. Must be dedicated.
A2	Secondary Access Data	Redundant/high-capacity access-side traffic	SBC: up to 1 Gbps Large SBC: >1 Gbps (requires 10/25 GbE NICs for scaling)
B2	Secondary Core Data	Redundant/high-capacity core-side traffic	SBC: up to 1 Gbps Large SBC: >1 Gbps (requires 10/25 GbE NICs for scaling)

Note:

- Exact capacity depends on the SBC license, number of sessions, codec usage, and percentage of encrypted calls.
- Capacity Note: The maximum capacity per SBC VM or EMS+SBC VM using 1 Gbps bandwidth is 5,000 non-encrypted sessions. Refer to the Overview and Specification document for additional capacity details.

Note:

- Small SBC Deployment: Uses 4 interfaces (M1, M2, A1, B1). Supports up to ~1 Gbps of aggregate media throughput.
- Medium SBC Deployment: Can extend to 6 interfaces (M1, M2, A1, B1, A2, B2). Supports up to ~2 Gbps of aggregate media throughput.

- Large SBC Deployment: Requires 10/25 GbE NICs (A2, B2) for scaling beyond 2 Gbps of aggregate media throughput.
- Management (M1, M2): Always low bandwidth, but isolation is critical for security and High Availability (HA) stability.

Table 1: SBC capacity and interface sizing guidance

Deployment Tier	Session Capacity	Encryption Profile	Recommended Interfaces	Bandwidth Guidance	Notes
Tier 1 - Small SBC/EMS Combo	~1,000	Encrypted	4 interfaces (M1, M2, A1, B1)	~1 Gbps aggregate (500 Mbps A1 + 500 Mbps B1)	Fits within dual 1 GbE data ports. No 10/25 GbE required.
Tier 2 - Medium	~5,000	Unencrypted	4 interfaces (M1, M2, A1, B1) or 6 (add A2/B2)	~1 Gbps aggregate (500 Mbps A1 + 500 Mbps B1)	NICs and CPU must be correctly sized.
Tier 2 - Medium	~3,000	Mixed (encrypted and unencrypted)	4 interfaces (M1, M2, A1, B1) or 6 (add A2/B2)	~1 Gbps per side (encryption overhead reduces efficiency	Encryption consumes additional CPU. NICs and CPU must be correctly sized. Capacity can be increased by adding more than 4 vCPUs.
Tier 2 - Medium (Secure)	~3,000	Encrypted	4 interfaces (M1, M2, A1, B1) or 6 (add A2/B2)	~1 Gbps per side (encryption overhead reduces efficiency)	Encryption consumes additional CPU. NICs and CPU must be correctly sized. Capacity can be increased by adding more than 4 vCPUs.
Tier 3 - Large	~14,000	Mixed (encrypted and unencrypted)	6 interfaces (M1, M2, A1, A2, B1, B2)	~2–4 Gbps aggregate	Requires bridged VLANs on 10/25 GbE ports for A2/B2. Traffic shaping is recommended if 1G and 10G are mixed. TBD (Not qualified)

Table continues…

Deployment Tier	Session Capacity	Encryption Profile	Recommended Interfaces	Bandwidth Guidance	Notes
Tier 4 - Extra Large	~25,000	Mixed (encrypted and unencrypted)	6 interfaces (M1, M2, A1, A2, B1, B2)	~5–8 Gbps aggregate	Mandatory use of 10/25 GbE NICs with VLAN bridging. Each side (Access/Core) requires a minimum of 2 Gbps guaranteed. TBD (Not qualified)

Note:

- Encrypted sessions require more CPU per call, which may limit throughput before the NIC line rate is reached.
- Bridged VLANs on 10/25 GbE NICs should be used for Tier 3 and Tier 4 deployments.
- Traffic shaping is required when sharing ports across 1G and 10/25G to ensure that latency-sensitive flows (A1, B1, A2, B2) receive guaranteed throughput.

ASP 130 R6.0.x KVM server hardware

The 10/25 GbE Network Interface Cards (NICs) are not supported on Avaya Solutions Platform 130 Appliance R6.0. Support for these NICs is planned in the future Avaya Solutions Platform 130 Appliance release. Once available, Avaya Solutions Platform 130 Appliance R6.0.x release notes will be updated accordingly.

Important:

Any mention of 10/25 GbE NICs in this document refers to this future functionality only.

NIC Configuration	Supported Interfaces	Details
2×10/25 GbE NICs + 4×1 GbE NICs	6 physical interfaces	Use this setup to support high-throughput SBC deployments.
4×1 GbE NICs only	4 physical interfaces	Use this setup for small to medium SBC deployments with moderate bandwidth.

Downloading SBC software from PLDS

Procedure

1. Log in to the PLDS portal using your authorized credentials.
2. Search for the SBC server image files using the following PLDS Download IDs:

PLDS Download ID	File Name	Product Description
SBCE0000376	`sbce-10.2.1.0-101-24795.qcow2`	Avaya SBC deployment options are the following: • All in one Element Management System (EMS) and SBC on same Virtual Machine (VM) • Standalone EMS • Supports up to 24 SBC or 12 pair SBC - HA EMS • Standalone SBC - Up to 24 SBC controlled by 1 EMS • HA SBC - Up to 12 pair SBC controlled by EMS

3. Download the `.tarball.zip` files to your local machine.
4. Extract the downloaded `.zip` files to retrieve the `.ova` files.
5. Convert the `.ova` files to `qcow2` format.

Next steps

- Download the SBC 10.2.1 `qcow2` file from PLDS to your local machine using the provided PLDS Download IDs.
- For new installations or upgrades, download Avaya SBC EMS before downloading Avaya SBC SBCs.

Chapter 5: Deploying EMS on ASP R6.0.x

Verifying the ASP 130 R6.0.x version

About this task

Verifying that ASP 130 is running R6.0.0.2.0 or later ensures the system is up to date.

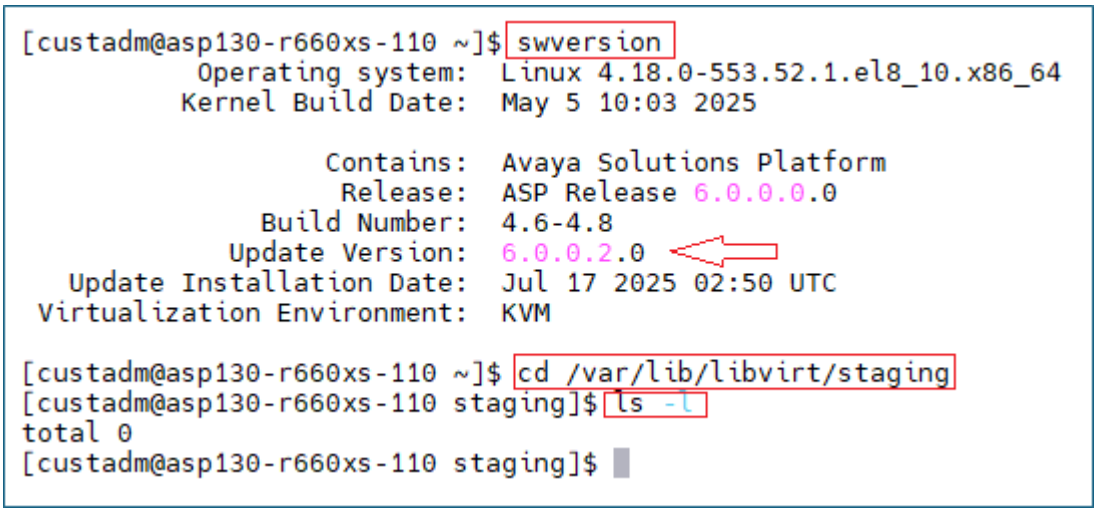
Before you begin

Log in to the ASP R6.0.x CLI using `custadm` credentials.

Verify that ASP 130 is running version R6.0.0.2.0 or later. If not, update before continuing.

Procedure

Run the `swversion` command.



If the version is R6.0.0.2.0 or later, you may continue. If the version is earlier than R6.0.0.2.0, stop and update ASP 130 to R6.0.0.2.0 or later before proceeding.

Copying the qcow2 files to the ASP R6.0.x host server

About this task

Copy the SBC `qcow2` image file from a local machine to the ASP 130 R6.0.x host server for deployment.

Note:

The directory is created automatically with proper ownership and permissions when the `av-asp-tools-1.5-3.el8.x86_64.rpm` is installed, and the server is updated to ASP R6.0.0.2.0. If the directory does not exist, the server has not been correctly updated and must be upgraded before proceeding.

Procedure

From the local machine, copy the qcow2 file to the `/var/lib/libvirt/` staging directory on the ASP 130 R6.0.x host server (KVM on RHEL 8.10).

Converting the qcow2 image to thick-provisioned

About this task

Convert the thin-provisioned `qcow2` image downloaded from PLDS to a thick-provisioned format with a unique name for deployment.

Before you begin

- Ensure you are in the `/var/lib/libvirt/staging` directory.
- Before converting files, determine the naming conventions for the thick-provisioned `qcow2` images to deploy multiple VMs from the same `qcow2` image. Each image must have a unique name. For recommended naming examples, see Supported footprints of Avaya SBC server on Avaya Solutions Platform 130 Appliance R6.0.x on page 15.

  For example, when converting to a thick-provisioned `qcow2` image, you must label it as EMS or SBC:

  - sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
  - sbce-10.2.1.0-101-24795-SBC1-thick.qcow2

  In this example, one image is labeled as EMS and the other as the first SBC. For subsequent EMS or SBC images, replace the number "1" with the following sequential number.
- Ensure that you convert the thin-provisioned `qcow2` image downloaded from PLDS to a thick-provisioned format.
- Ensure that the thick image includes a `-thick` identifier and role label (for example, EMS or SBC) when running the commands.

Procedure

1. Run the conversion command to create the thick-provisioned image using the thick-provisioned image name.

   For example, run the following command:

   ```
   sudo qemu-img convert -O qcow2 -o preallocation=full
   sbce-10.2.1.0-101-24795.qcow2 sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
   ```

2. Verify both the thin and thick `qcow2` files are present in the staging directory.

   For example, run the following command:

   ```
   ls -l
   ```

   The thin and thick-provisioned image files are listed as follows:

   ```
   -rw-r-----. 1 custadm custadm 3417178112 Nov 25 2024
   sbce-10.2.1.0-101-24795.qcow2

   -rw-r-----. 1 root root 68730224640 Oct 3 19:54
   sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
   ```

3. Check the disk size of the thick image to confirm the conversion was successful.

   For example, run the following command:

   ```
   qemu-img info sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
   ```

   The disk size shows as 64 GiB for EMS or SBC VMs.

   Note:

   Check the disk size, not the virtual size. In a thin-provisioned `qcow2` image, the virtual size also displays as 64 GiB, but the disk size is approximately 3.18 GiB.

   A sample output from the `qemu-img info sbce-10.2.1.0-101-24795-EMS1-thick.qcow2` is as follows:

   ```
   [custadm@aasp130clv staging]$ qemu-img info
   sbce-10.2.1.0-101-24795-EMS1-thick.qcow2

   image: sbce-10.2.1.0-101-24795-EMS1-thick.qcow2

   file format: qcow2

   virtual size: 64 GiB (68719476736 bytes)

   disk size: 64 GiB

   cluster_size: 65536

   Format specific information:

   compat: 1.1

   compression type: zlib

   lazy refcounts: false
   ```

```
refcount bits: 16
corrupt: false
extended l2: false
[custadm@aasp130clv staging]$
```

4. Move the thick image to the `/var/lib/libvirt/images` directory:

   For example, run the following command:

   ```
   sudo mv sbce-10.2.1.0-101-24795-EMS1-thick.qcow2 /var/lib/libvirt/images
   ```

   You must enter the custadm password before proceeding.

5. Verify that the image is present in the new directory.

   For example, run the following command:

   ```
   cd /var/lib/libvirt/images
   sudo ls -l
   ```

6. Change the owner and permissions of the thick image to 640.

   For example, run the following command:

   ```
   sudo chown qemu:qemu sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
   sudo chmod 640 sbce-10.2.1.0-101-24795-EMS1-thick.qcow2
   ```

7. Confirm the changes.

   For example, run the following command:

   ```
   sudo ls -l
   ```

8. Clean up the staging directory to free space for future deployments.

   For example, run the following command:

   ```
   cd /var/lib/libvirt/staging
   sudo rm *.qcow2
   ```

   Note:

   Do not remove any files from the image directory. The cleanup must be completed before deploying additional VMs.

Importing EMS VM on ASP R6.0.x using the cockpit web console

About this task

Import and configure EMS Virtual Machine (VM) on Avaya Solutions Platform 130 Appliance R6.0.x using the cockpit web console. This ensures the EMS VM is correctly configured with the required resources, firmware, and network settings, enabling successful deployment and management of SBC instances.

Before you begin

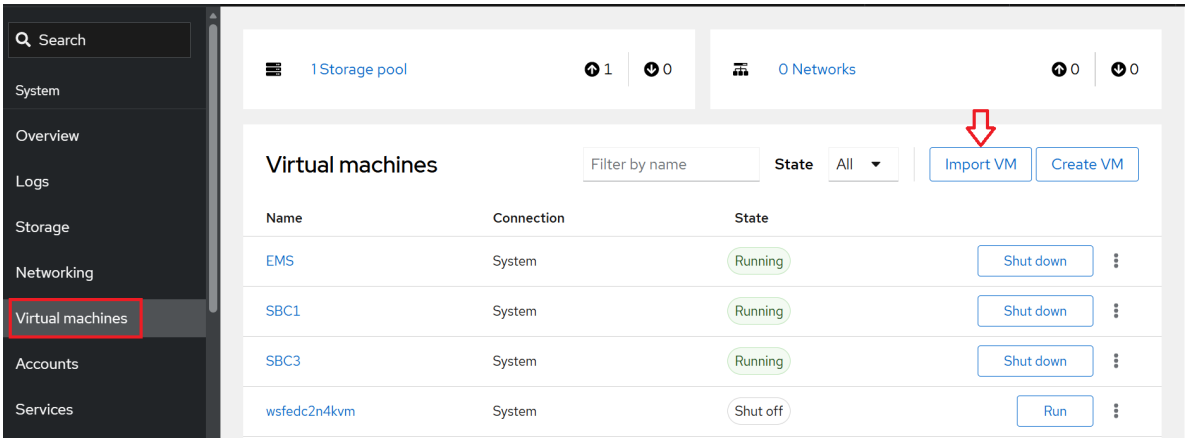
- Ensure that you have the `custadm` credentials for the ASP130 R6.0.x cockpit web console.
- If your access is limited, switch to Administrative access before continuing.
- The SBC disk image (`sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`) is available at `/var/lib/libvirt/images/`.

Procedure

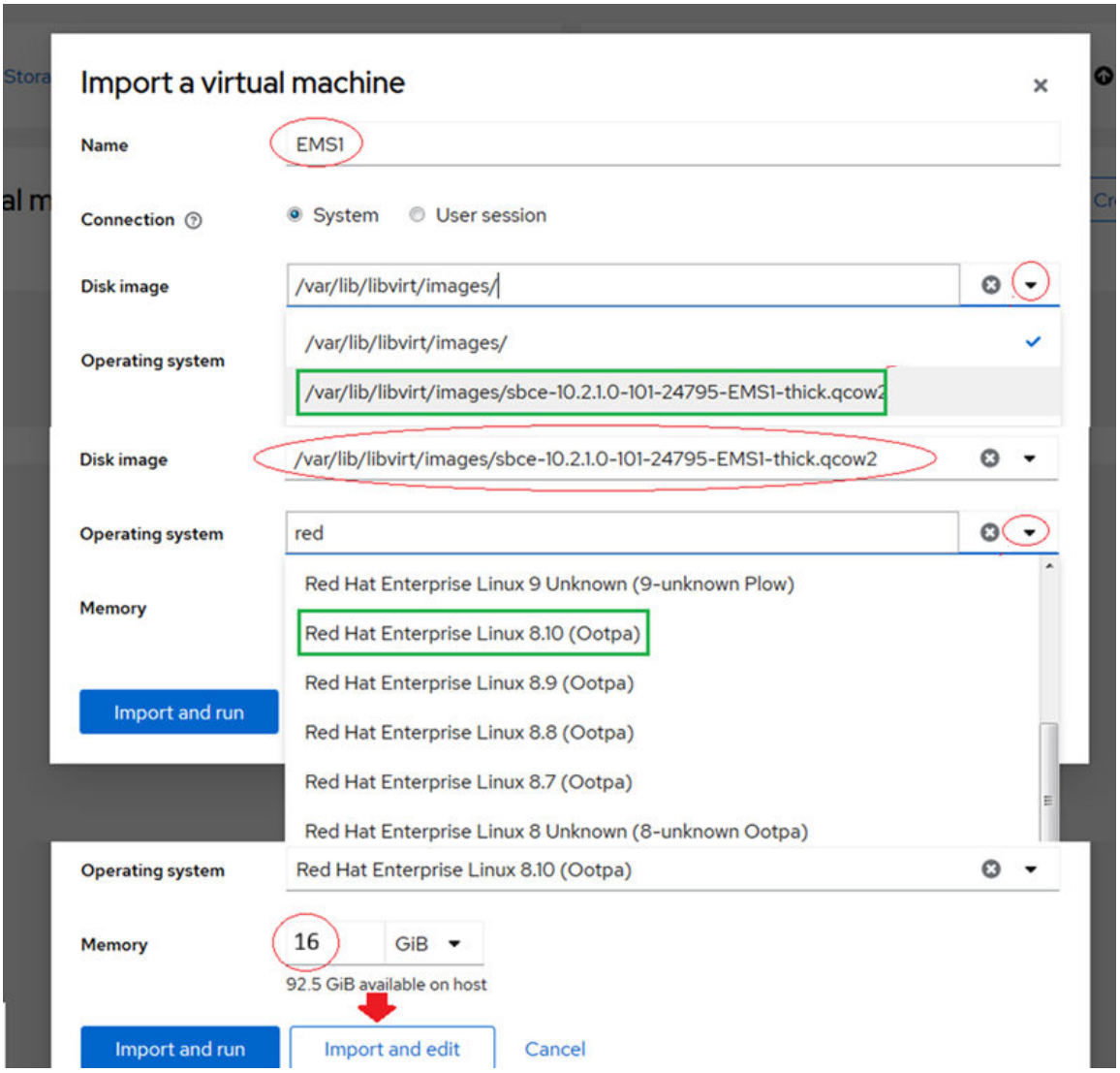
1. Log in to the ASP 130 R6.0.x cockpit web console in one of the following ways:

- External access: `https://<IP address or FQDN of the ASP 130 R6 KVM host>:9090`
- Services port access: https://192.11.13.6:9090

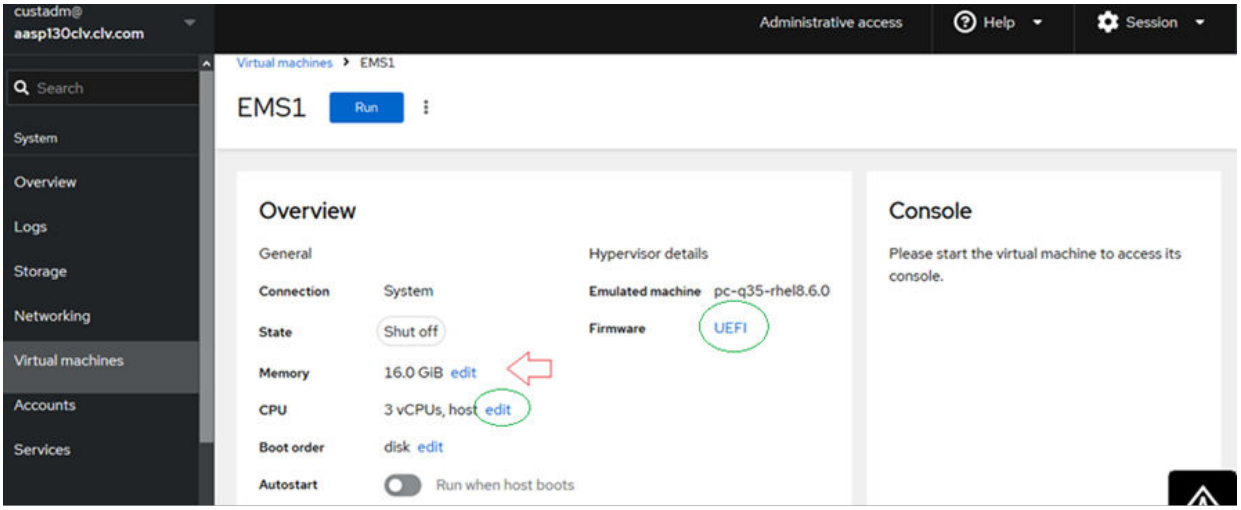
2. Use the `custadm` credentials to log in.
3. Navigate to **System** > **Virtual machines** > **Import VM**.



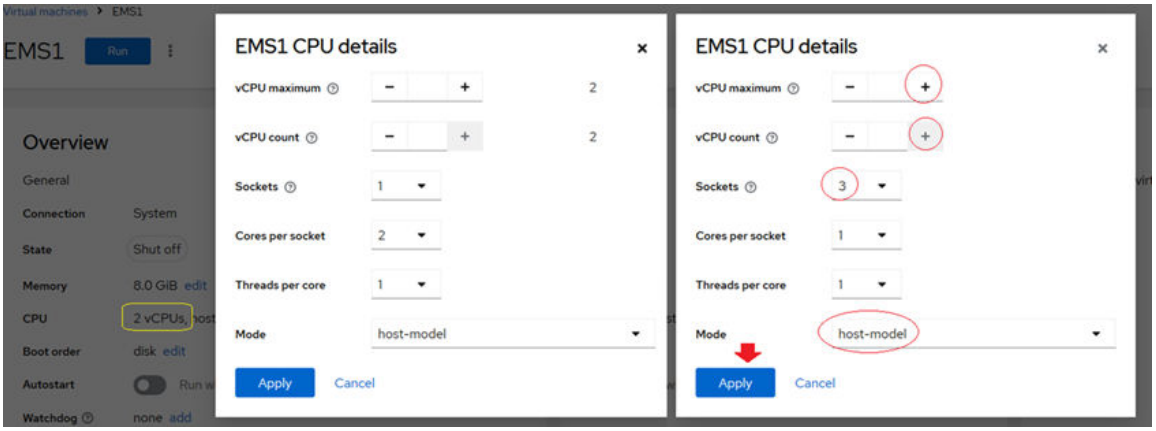
4. In the Import VM window, enter a name and the required details for the SBC EMS VM as follows:
   - Enter the VM **Name**.
   - Set **Disk image** to `/var/lib/libvirt/images/sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`.
   - Set **Operating system** to `Red Hat Enterprise Linux 8.10 (Ootpa)`.
   - Set **Memory** to `16 GiB` as defined by the selected deployment profile.
   - Click **Import and edit**.



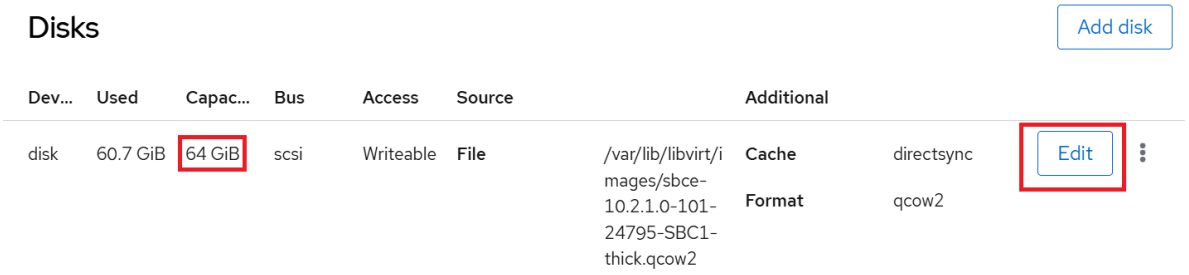
5. In the EMS1 Overview window, verify that memory is set to **16 GiB**.



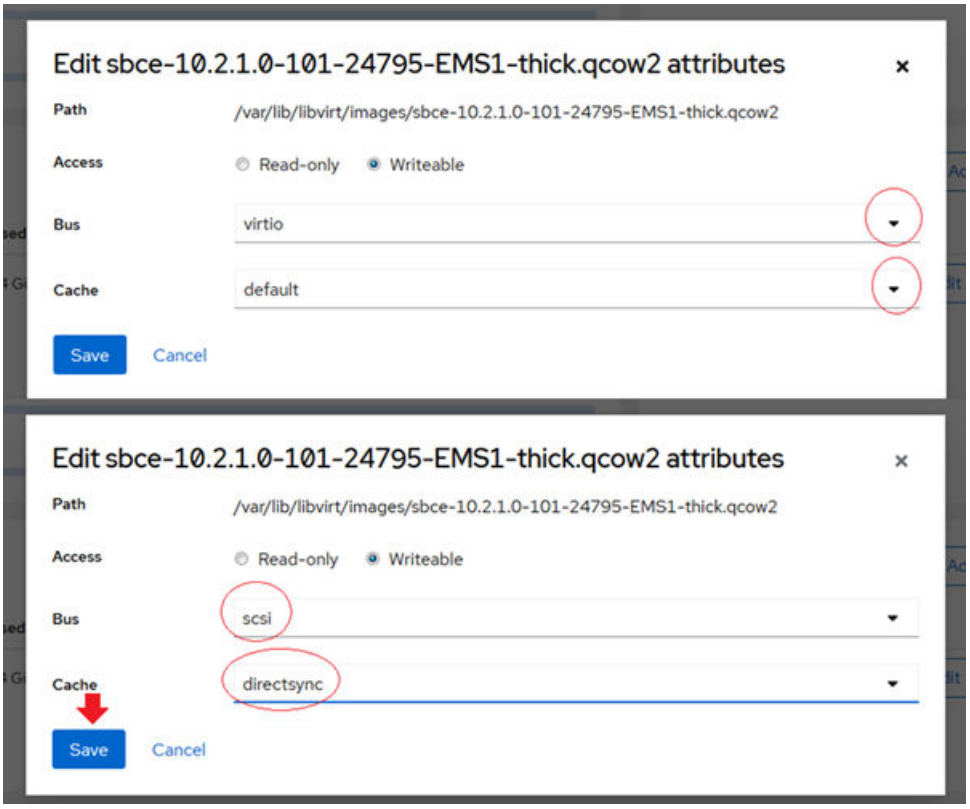
6. Click **Edit** next to CPU, enter the following details:
   - In the CPU details window, increase both **vCPU maximum** and **vCPU count** to `3`.
   - Set **Mode** to `host-model`.
   - Click **Apply**.



7. Change the firmware from **BIOS** to **UEFI**.
8. Scroll to Disks, verify that disk capacity is **64 GiB**.

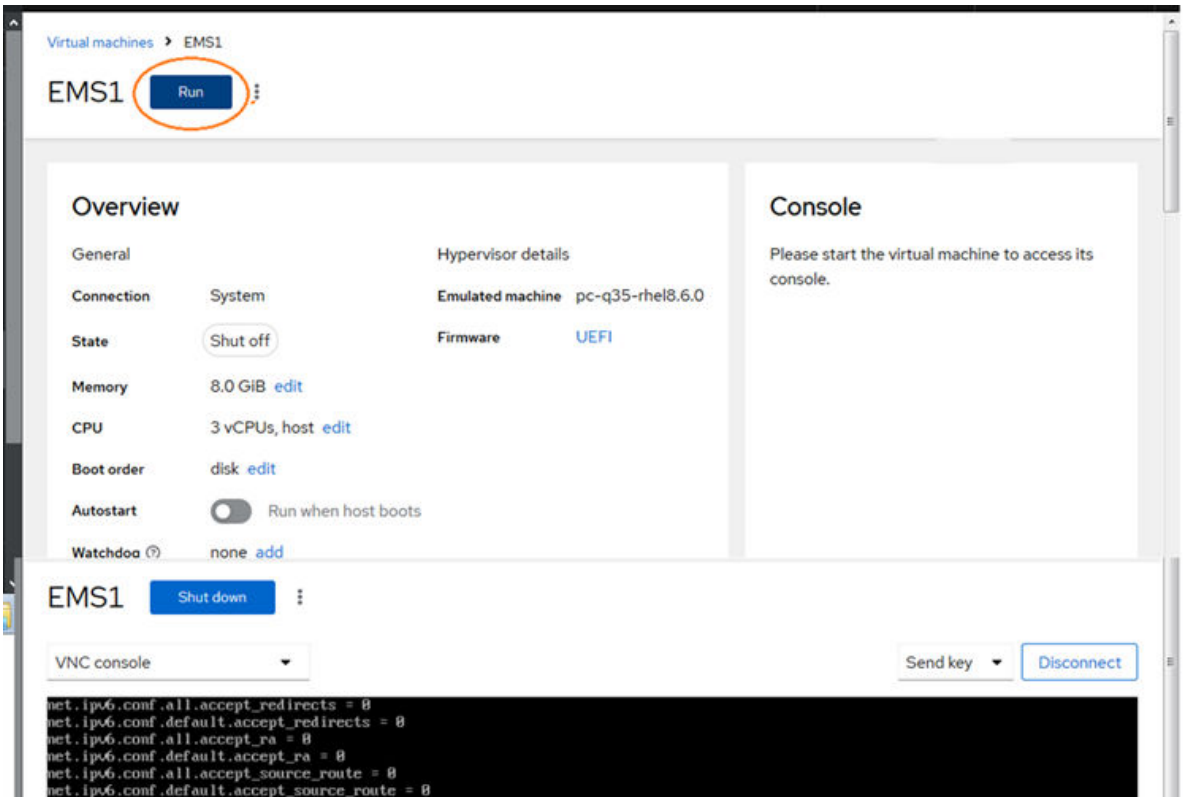


9. Click **Edit**, enter the following details:
   - In the Edit attributes window, set **Bus** to `scsi`.
   - Set **Cache** to `directsync`.
   - Click **Save**.



10. In Network interfaces, verify that the source for the network interface is **bridge0**.

11. To start the EMS VM, scroll to EMS1 Overview and click **Run**.



Configuring EMS using CLI

About this task

Use the CLI to establish essential network settings, secure initial access, and prepare the EMS system for operation.

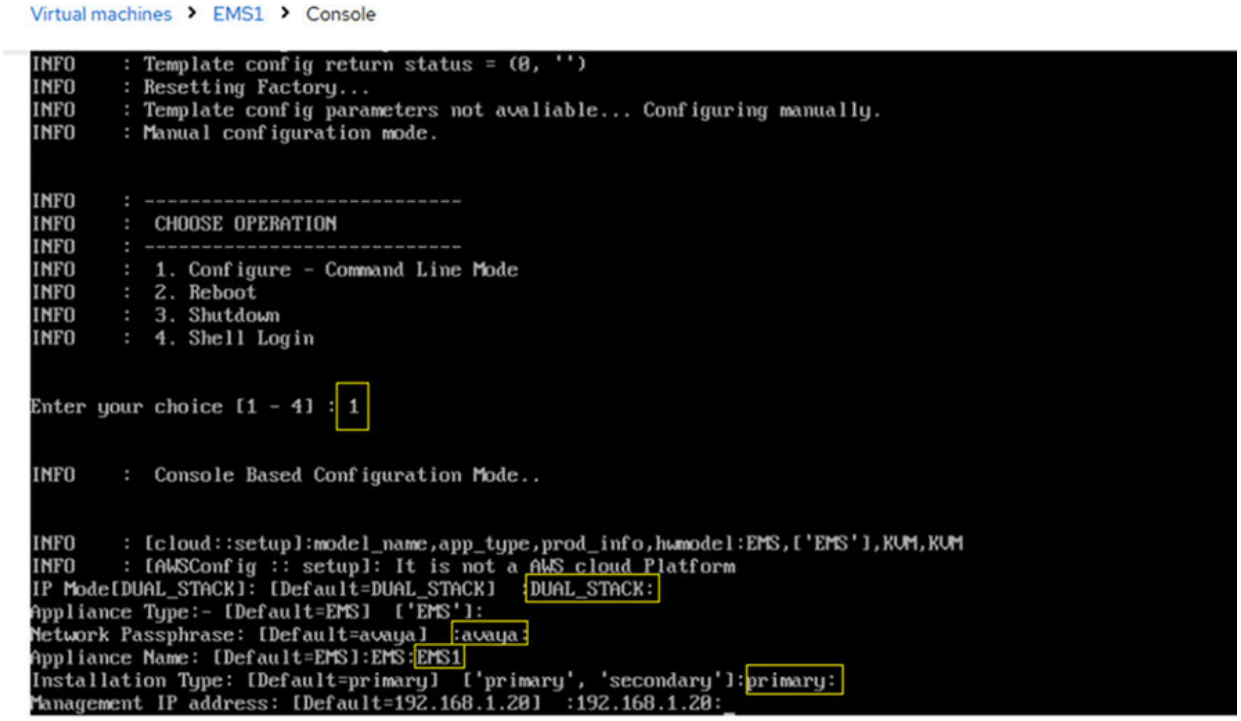
Before you begin

Procedure

1. In the console section, click **Expand** to enlarge the VNC console.
2. Under CHOOSE OPERATION, enter `1` to select **Configure - Command Line Mode**.
3. When prompted, enter the following values:

- At the **IP Mode** prompt, press **Enter** to accept the default value **DUAL_STACK**.
- At the **Appliance Type** prompt, press **Enter** to accept the default value **EMS**.
- At the **Network Passphrase** prompt, press **Enter** to accept the default value **avaya**.
- At the **Appliance Name** prompt, enter the name of the SBC EMS VM.
- At the **Installation Type** prompt, select the required installation type and press **Enter**.
- At the **Management IP address** prompt, enter `192.168.10.20`.

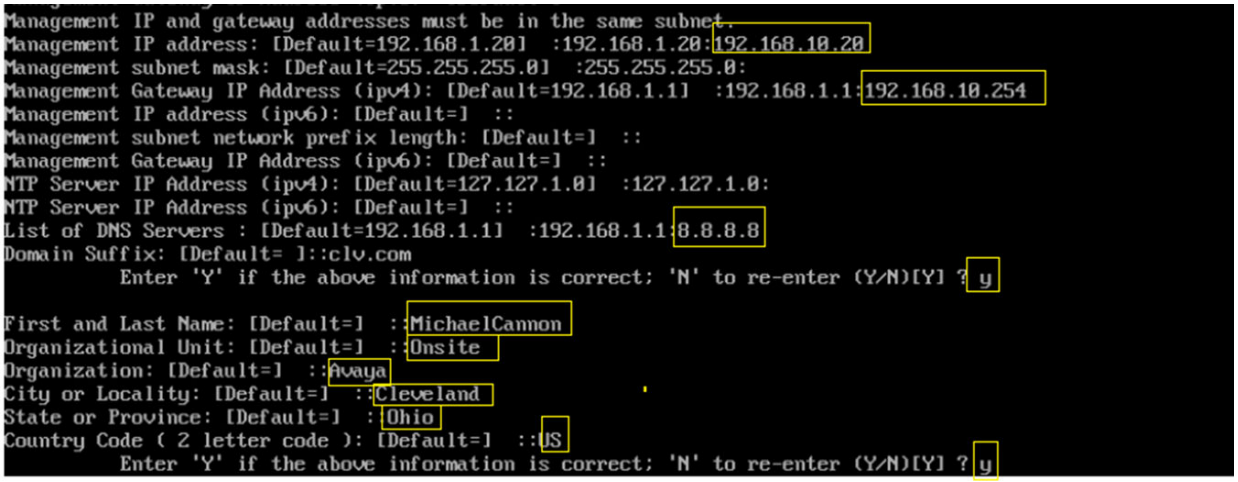
- At the **Management Gateway IP Address (ipv4)** prompt, enter `192.168.10.254`.
- At the **List of DNS Servers** prompt, enter `8.8.8.8`.
- At the confirmation prompt, enter `Y` to confirm the information.



4. Enter the required information at the following prompts:

- **First and Last Name**
- **Organizational Unit**
- **Organization**
- **City or Locality**
- **State or Province**
- **Country Code (2 letter code)**

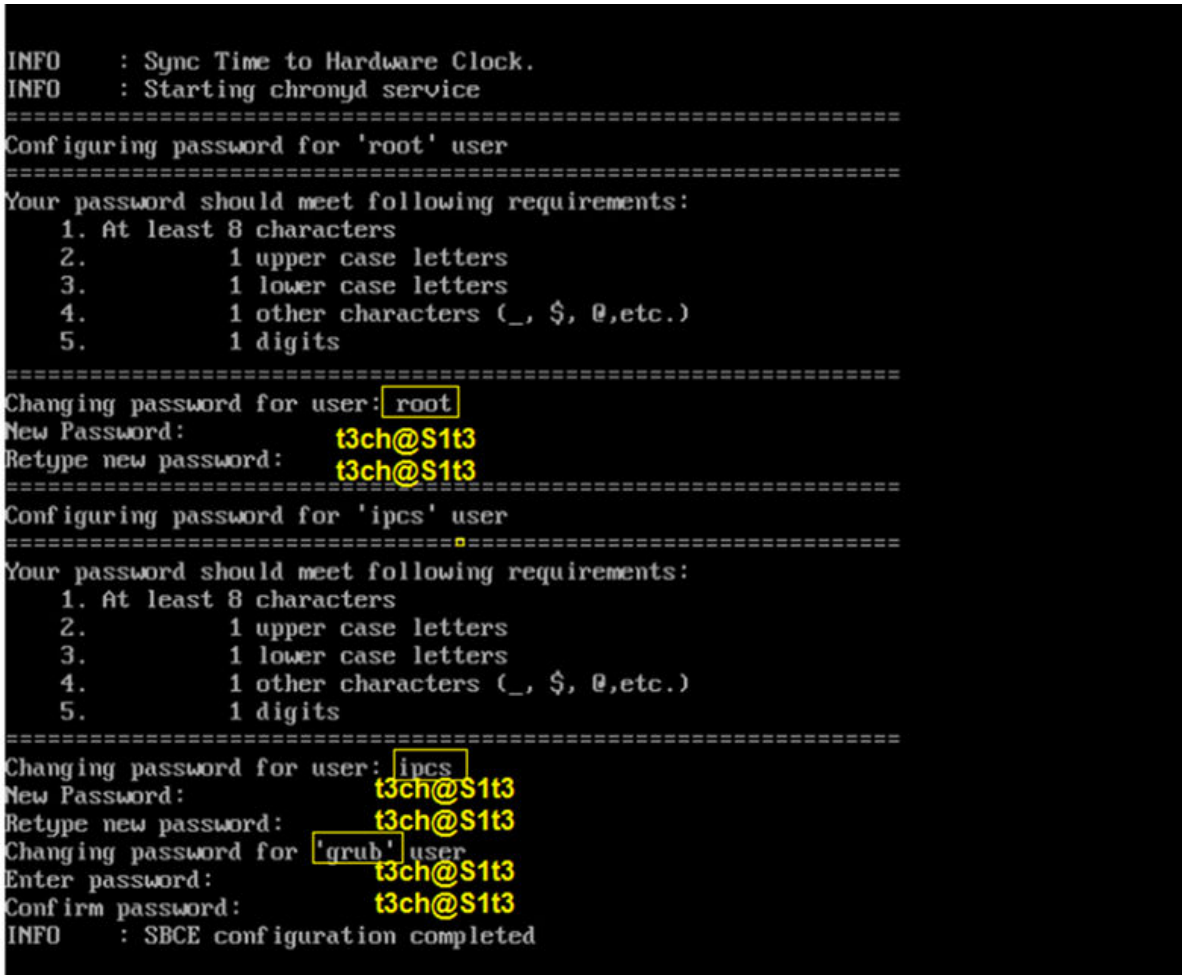
5. At the confirmation prompt, enter `Y` to confirm the information.



6. Configure passwords for `root` and `ipsec` users.

   Note:

   Use a unique, secure password that complies with the your organization's security policies. The displayed password is for illustration only.



Next steps

After the initial EMS deployment for R10.2.1 is complete, you can deploy the first SBC instance using the same `qcow2` thin image file. You can deploy up to 24 single or 12 paired instances of SBC VMs.

Chapter 6: Deploying SBC on ASP R6.0.x

Network planning for SBC VM

Avaya SBC requires a minimum of four Virtual Network Interface Cards (vNICs), and depending on the deployment scenario, it use up to six vNICs.

Each vNIC serves a specific role:

- M1: Management interface
- M2: High Availability (HA) interface
- A1: Intranet interface
- B1: Internet interface
- A2/B2: Optional secondary interfaces for intranet and internet, respectively

In the example configuration below, the SBC will use M1, A1, and B1 interfaces.

For Avaya Solutions Platform 130 Appliance server utilizing 1GB NICs, assign VLANs to ports only on the customer's data switch when possible.

You must configure the network using the following procedure:

- Create a new bridge on the hypervisor.
- Assign the SBC Virtual Machine (VM) vNIC to the new bridge.
- Disable both IPv4 and IPv6 on the bridge interface.

Disabling automatic IP configuration prevents the bridge from attempting to assign an IP address, which could otherwise result in the bridge disabling its port members.

Note:

The R660xs Profile A3/A31 currently does not support dual 10/25GB NICs. Support for these interfaces is targeted for Avaya Solutions Platform 130 Appliance future release. Once available, VLAN tagging within the hypervisor will become more common for these high-speed interfaces. In such cases, VLANs must be explicitly associated with the appropriate bridge.

KVM networking configuration

On Avaya Solutions Platform 130 Appliance R6.0.x (Dell R660xs profile A3/A31) KVM servers, physical Network Interface Cards (NICs) are not directly visible to SBC or EMS Virtual Machines (VMs). Instead, these NICs are mapped into Linux bridge interfaces on the host. The mapping follows the structure: Physical NIC → Linux Bridge → VM NIC.

Creating bridges for ASP 130 R640 ports

Before you begin

Determine if the Avaya Solutions Platform 130 Appliance server configured for Out Of Band Management (OOBM) traffic (bridgeOOB). If so, you can map M1 to bridgeOOB instead of bridge0. Do not modify the bridge0 or bridgeOOB labels.

Procedure

1. Integrate 1GbE ports on bridge0 for KVM host management and application management.
   - For 1GB 4 × 1GbE card, create the following bridges:
     - Consolidate M1 and M2 interfaces onto a single connection through bridge0 on the eno1 interface.
     - Connect A1 interface through bridge-A1 on the eno3 interface.
     - Connect B1 interface through bridge-B1 on the ens1f0 or ens2f0 or enp216s0f0 interface.
2. Integrate 1GbE NICs on bridge0 for KVM host management and application management.
   - For model with 6 physical 1GB Ethernet ports, map the following bridges:
     - Map bridge0 to the physical port M1 (eno1) with unique VLAN ID
     - Map bridge0 to the physical port M2 (eno1) with either a unique VLAN ID or a private, non-routable network segment (for example, 192.11.13.12-13).
   - For 1GB 4 × 1GbE card, map the following bridges:
     - Map bridge-A1 to the physical port A1 (eno3)
     - Map bridge-B1 to the physical port B1 (eno4)
     - Map bridge-A2 to the physical port A2 (ens1f0 or ens2f0 or enp216s0f0)
     - Map bridge-B2 to the physical port for B2 (ens1f1 or ens2f1 or enp216s0f1)

Creating bridges for R660xs ports

Before you begin

Determine if the Avaya Solutions Platform 130 Appliance server configured for OOBM traffic (bridgeOOB). If so, you can map M1 to bridgeOOB instead of bridge0. Do not modify the bridge0 or bridgeOOB labels.

Procedure

1. Integrate 1GbE ports on bridge0 for KVM host management and application management.
   - For 1GB 4 × 1GbE card, map the following bridges:
     - Map bridge0 to the physical port M1 (eno8303)
     - Map bridge0 to the physical port M2 (eno8303)
     - Map bridge-A1 to the physical port A1 (eno12399)

Note:

If the hypervisor is using OOBM (bridgeOOB), do not use eno12399, use the next available NIC.

- Map bridge-B1 to physical port B1 (eno12419)

- **Note:**

  The 10/25 GbE NICs available are not supported on Avaya Solutions Platform 130 Appliance R6.0. Support is planned for the future release.

For 10/25GbE 2 × NIC card (if present), map the following bridges:

- Map bridge-A2 to physical port A2 (ens1f0np0)
- Map bridge-B2 to physical port B2 (ens1f0np1)

2. Integrate 1GbE NICs on bridge0 for KVM host management and application management.
   - For model with 6 physical 1GB Ethernet ports, map the following bridges:
     - Map bridge0 to physical port M1 (eno8303) with unique VLAN ID
     - Map bridge0 to physical port M2 (eno8303) with either a unique VLAN ID or a private, non-routable network segment
   - For 1GB 4 × 1GbE card, create the following bridges:
     - Map bridge-A1 to physical port A1 (eno12399)
     - Map bridge-B1 to physical port B1 (eno12419)
     - Map bridge-A2 to physical port A2 (eno12409)
     - Map bridge-B2 to physical port B2 (eno12429)
   - **Note:**

     The 10/25 GbE NICs available are not supported on Avaya Solutions Platform 130 Appliance R6.0. Support is planned for the future release.
   - For model with 6 physical 1GB Ethernet ports + 2 10/25 GbE Ethernet ports, map the following bridges:
     - Map bridge0 to physical port M1 (eno8303) with unique VLAN ID
     - Map bridge0 to physical port for M2 (eno8303) with either a VLAN ID or a private, non-routable network segment
     - Map bridge-A1 to physical port A1 (eno12399)
     - Map bridge-B1 to physical port for B1 (eno12419)
     - Map bridge-A2 to physical port for A2 (ens1f0np0)
     - Map bridge-B2 to physical port for B2 (ens1f0np1)

Virtual network interface ordering

After you create the network bridges, the system ensures that the corresponding virtual Network Interfaces (vNICs) present the operating system of the SBC Virtual Machines (VMs) in a fixed sequence.

The SBC VM then sees them as virtio NICs in the following sequence:

Functional Interface	Attached Bridge
M1	bridge0
A1	bridge-A1
B1	bridge-B1
M2	bridge0
A2	bridge-A2 (if available)
B2	bridge-B2 (if available)

Network bridge configuration: Dell R640 vs. R660xs

Before deploying Avaya SBC, you must configure the network bridging using the cockpit management interface. The configuration varies based on the server model (Dell R640 or Dell R660xs) due to differences in physical port mapping and numbering.

Both configurations rely on specific physical Network Interface Cards (NICs):

- 1GbE Ports: A card providing four 1GbE ports.
- High-Speed Ports: An expansion card providing two 10/25GbE ports.

Note:

The 10/25 GbE Network Interface Cards (NICs) currently available are not supported on Avaya Solutions Platform 130 Appliance R6.0. Support for these NICs will be introduced in future Avaya Solutions Platform 130 Appliance release.

The following table details the mapping of the logical bridge names to the physical interfaces:

Table 2: Logical bridge names to the physical interfaces

Bridge interface	Dell R640 interface (4 × 1GbE ports)	Dell R640 interface (6 physical 1GB ports)	Dell R660xs interface (6 physical 1GB ports)	Dell R660xs interface (6 physical 1GB ports + 2 × 10/25GbE NIC Card)
M1/M2	bridge0 on eno1	bridge0 on eno1	bridge0 on eno8303	bridge0 on eno8303
A1	bridge-A1 on eno3	bridge-A1 on eno3	bridge-A1 on eno12399	bridge-A1 on eno12399

Table continues…

Bridge interface	Dell R640 interface (4 × 1GbE ports)	Dell R640 interface (6 physical 1GB ports)	Dell R660xs interface (6 physical 1GB ports)	Dell R660xs interface (6 physical 1GB ports + 2 × 10/25GbE NIC Card)
B1	bridge-B1 on ens1f0 or ens2f0 or enp216s0f0	bridge-B1 on eno4	bridge-B1 on eno12419	bridge-B1 on eno12419
A2	NA	bridge-A2 on ens1f0 or ens2f0 or enp216s0f0	bridge-A2 on eno12409	bridge-A2 on ens1f0np0
B2	NA	bridge-B2 on ens1f1 or ens2f1 or enp216s0f1	bridge-B2 on eno12429	bridge-B2 on ens1f1np1

Regardless of the server model, you must complete the following mandatory steps using the Cockpit management interface:

- Assign the required VLAN ID to each respective bridge.
- To ensure proper control over network addressing, the automatic assignment of IPv4 and IPv6 settings must be disabled for each bridge.
- After validation of the network settings, the SBC system files (`qcow2`) are ready for deployment through the shell.

Management interface configuration

The management interface M1 is always VLAN tagged. You can create the necessary VLANs on the bridge0 parent interface for M1 using eno8303 or eno1.

Note:

- You must use the `configNetwork` script provided with the ASP 130 R6.0.x software to add, modify, or remove VLAN configurations on bridge0 or other bridge interfaces.
- Any changes made directly using the Linux shell or the ASP 130 Cockpit web interface will result in a loss of integration with the network configuration script.

For specific configuration steps regarding M1 tagging, refer to the Management Interface Configuration in the Host for VLAN Tagging section (starting on page 77) of the latest Installing the Avaya Solutions Platform 130 Series - Release 6.0.x guide.

Configuring the HA interface M2

About this task

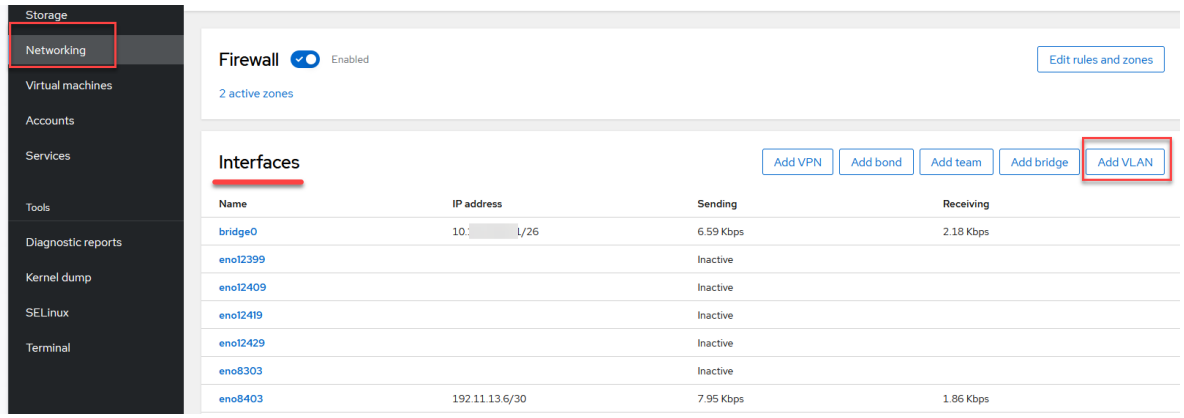
Configure the High Availability (HA) management interface M2 using eno8303 or eno1.

Note:

The VLANs are created on the Parent eno8303 or eno1. If bridge0 is configured with a bonded interface, then the VLAN is created on the parent bon0 instead.

Procedure

1. Log in to the Cockpit web console.
2. In the left pane, go to the **Networking** tab.
3. In the Interfaces section, click **Add VLAN**.



4. From the Parent drop-down menu, select `eno8303` or `eno1`.

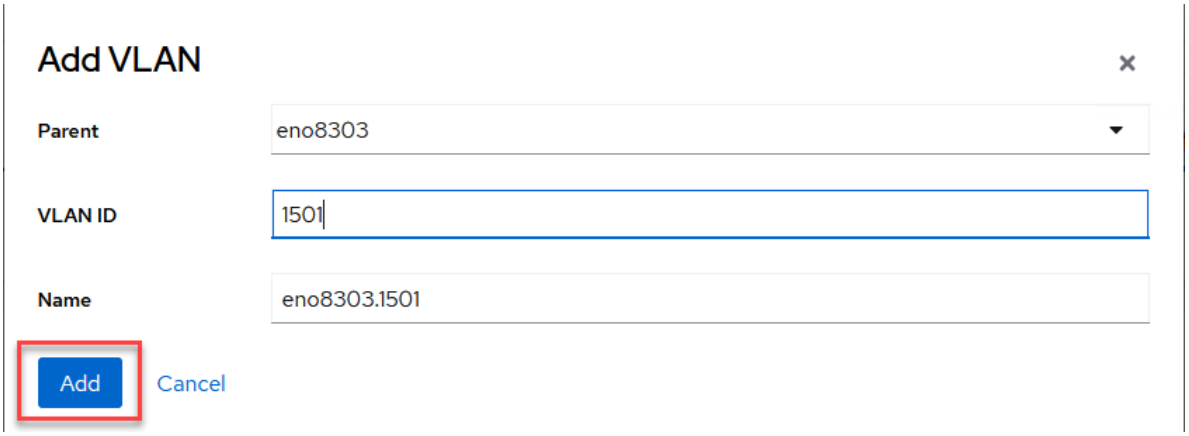
Note:

If bridge0 is configured with a bonded interface, then select bond0.

5. Enter the appropriate VLAN ID for M2.
6. Leave the default **Name** field. Click **Add**.

Note:

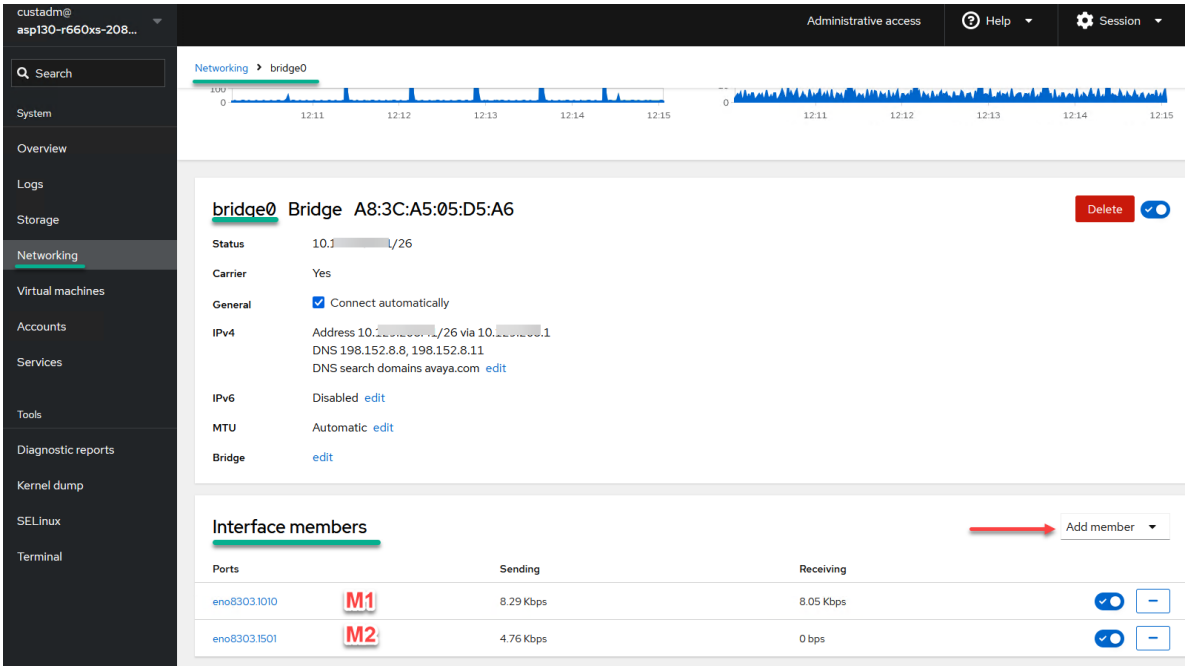
In the following example VLAN 1501 has been configured on the Host physical adapter eno8303.



7. From the **Networking** > **Interfaces** view, select `bridge0`.
8. Scroll to Interface members, select the newly created VLAN for M2, for example: eno8303.1501.

Note:

You configured bridge0 with 2 different VLAN tags, one for the M1 interface and one for the M2 interface as shown in the example below.



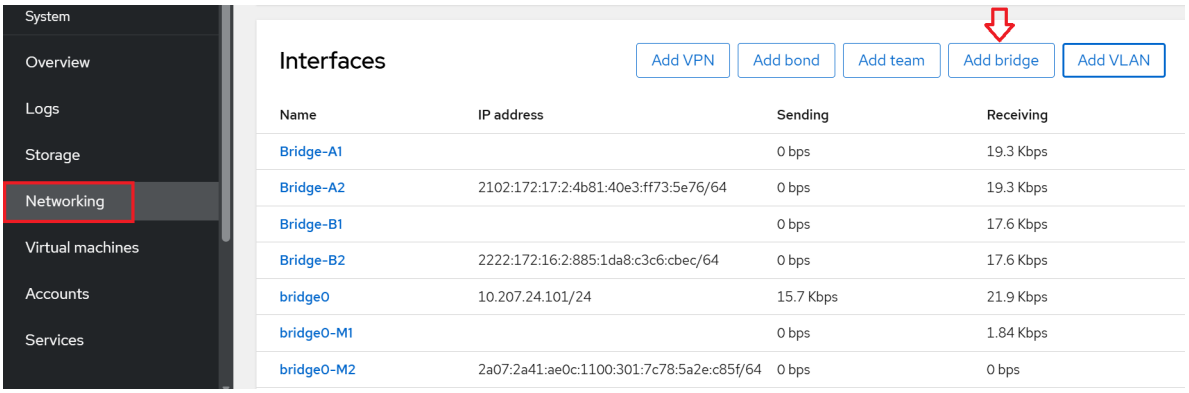
Configuring the intranet interface bridge A1

About this task

You can configure the intranet interface bridge A1, ensuring the physical interface is used and IP addressing is disabled.

Procedure

1. Log in to the Cockpit web console.
2. In the left pane, go to the **Networking** tab.
3. In the Interfaces section, click **Add Bridge**.

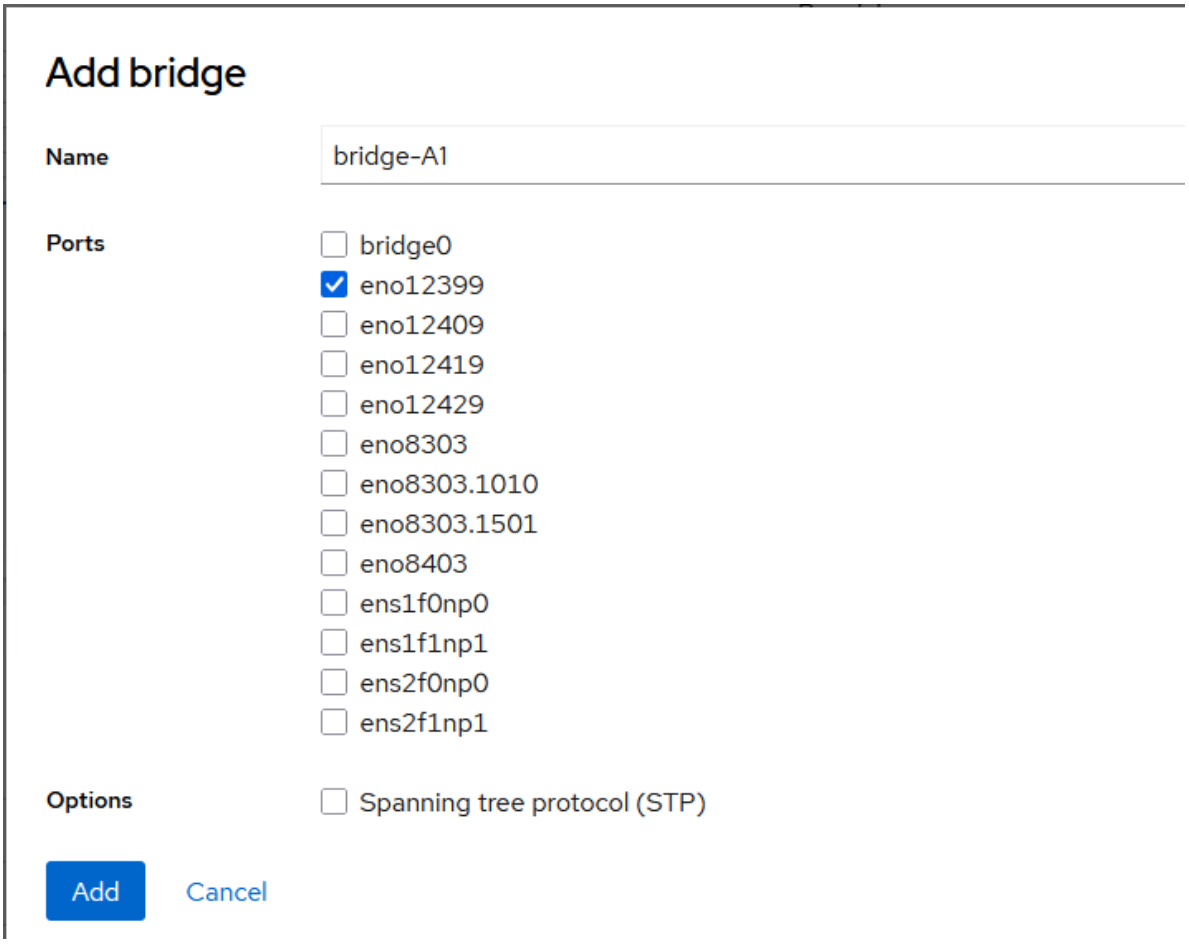


4. In the Add bridge window, in the **Name** field, type the new bridge name.
5. In the Add bridge window, from the **Ports** list, select the correct physical port. For example, `eno12399` or `eno3`.

   Note:

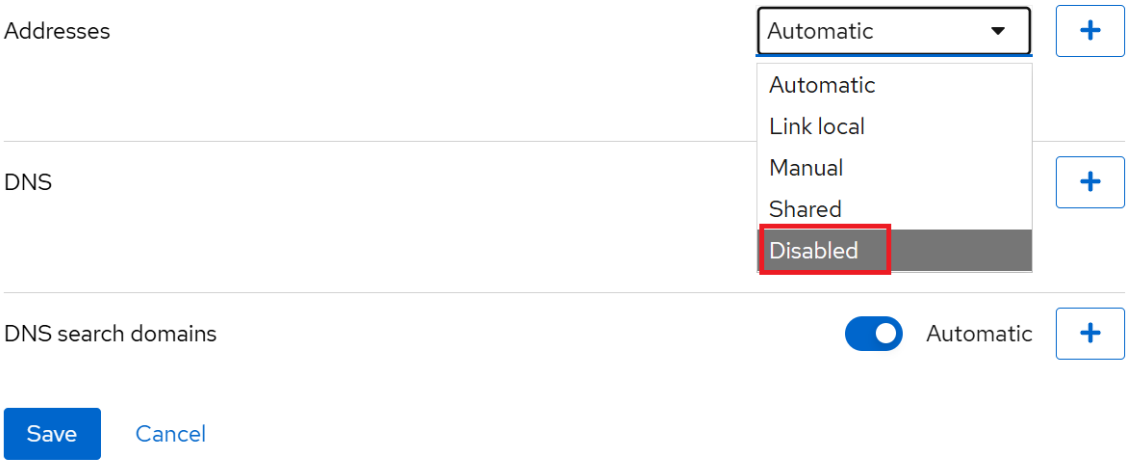
   You can refer to the Table 2: Logical bridge names to the physical interfaces on page 41 to select the correct physical port and determine if you require either 4 or 6 ports.

6. Click **Add**.

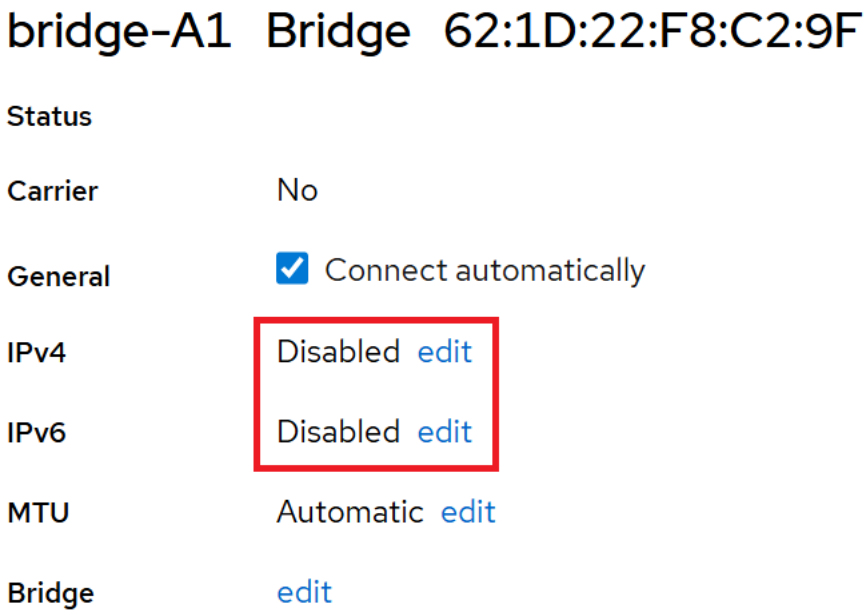


7. Select the newly created bridge-A1. In the bridge-A1 window, next to IPv4, click **edit**.

8. In the IPv4 settings window, in the **Addresses** list, select **Disabled**.
9. Click **Save**.
10. In the bridge-A1 window, next to IPv6, click **edit**.
11. In the IPv6 settings window, in the **Addresses** list, select **Disabled**.
12. Click **Save**.



13. In the bridge-A1 window, verify that both the IPv4 status and the IPv6 status are displayed as **Disabled**.



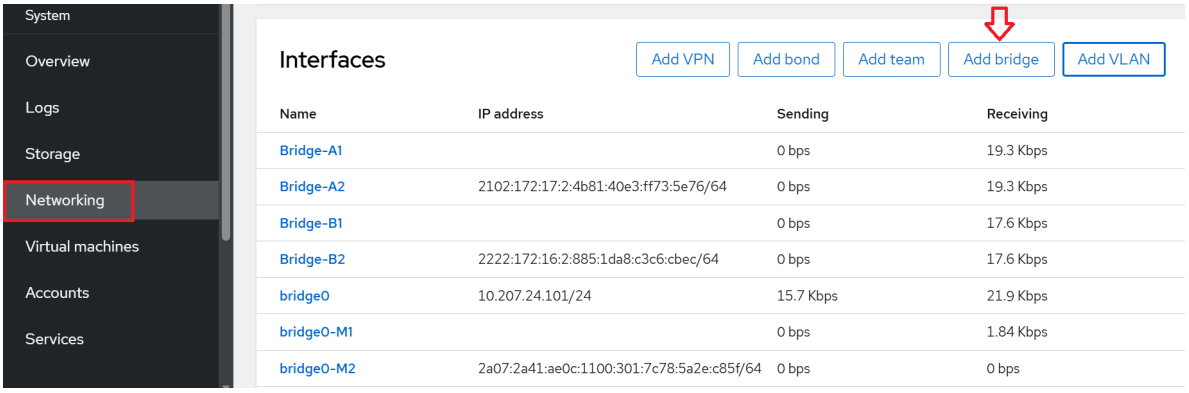
Configuring the internet interface bridge B1

About this task

You can configure the internet interface bridge B1, ensuring the physical interface is used and IP addressing is disabled.

Procedure

1. Log in to the Cockpit web console.
2. In the left pane, go to the **Networking** tab.
3. In the Interfaces section, click **Add Bridge**.

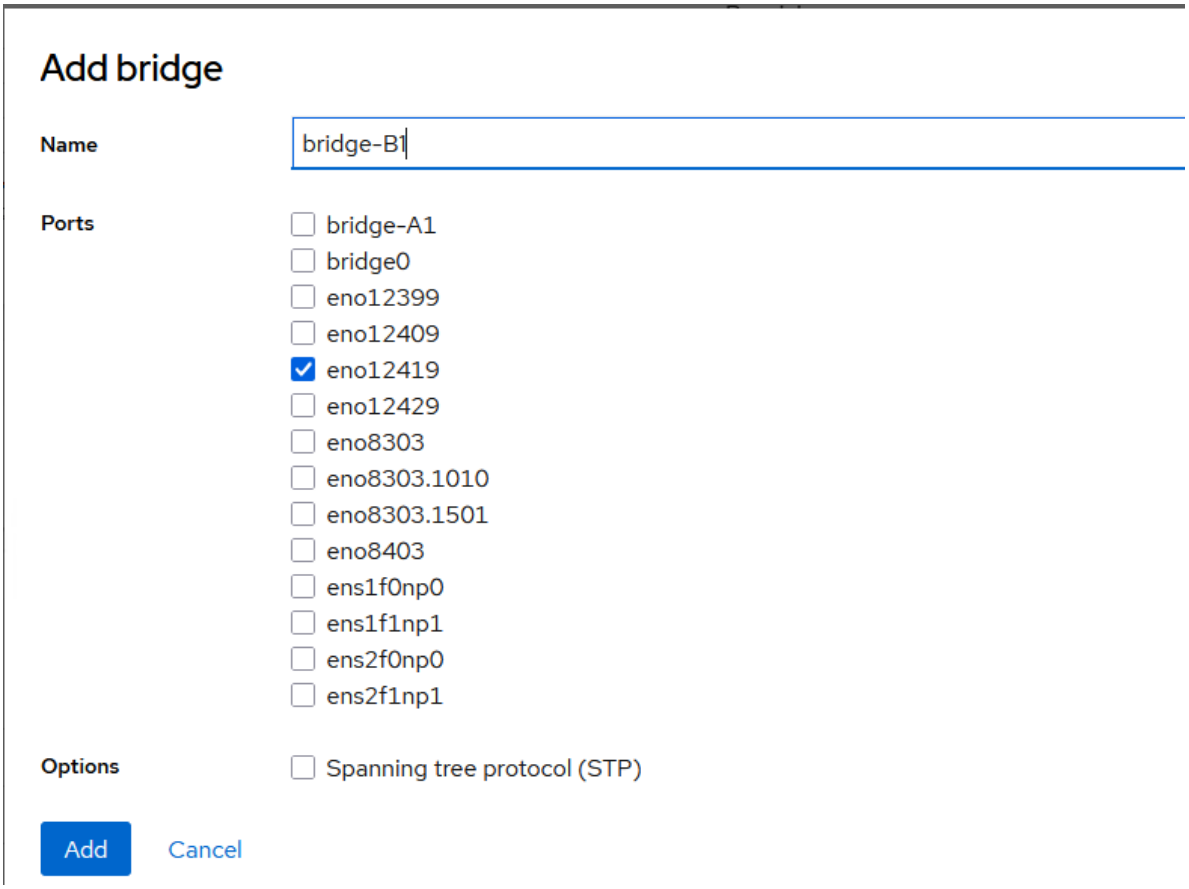


4. In the Add bridge window, in the **Name** field, type the new bridge name.

5. In the Add bridge window, from the **Ports** list, select the correct physical port. For example, `eno12419`.

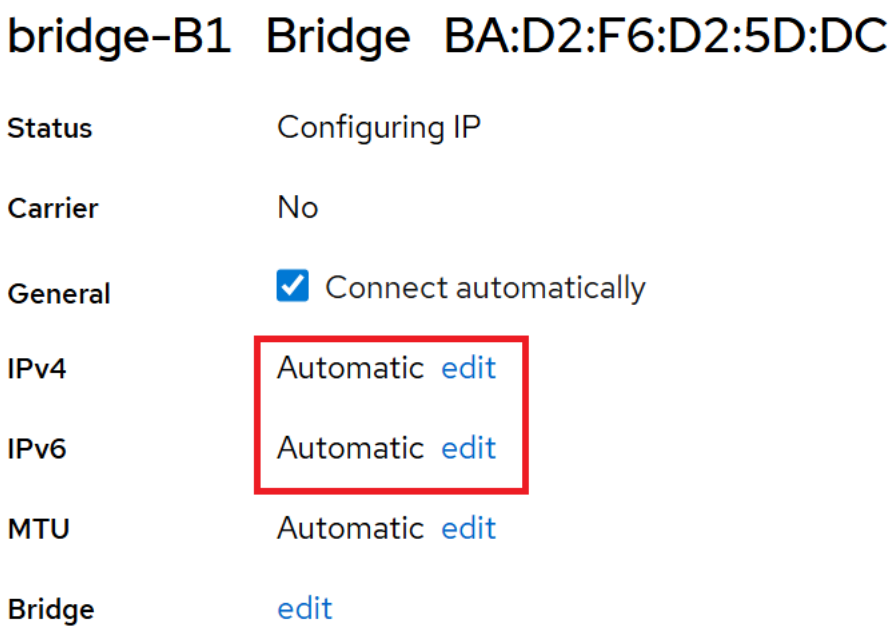
Note:

You can refer to the Table 2: Logical bridge names to the physical interfaces on page 41 to select the correct physical port and determine if you require either 4 or 6 ports.

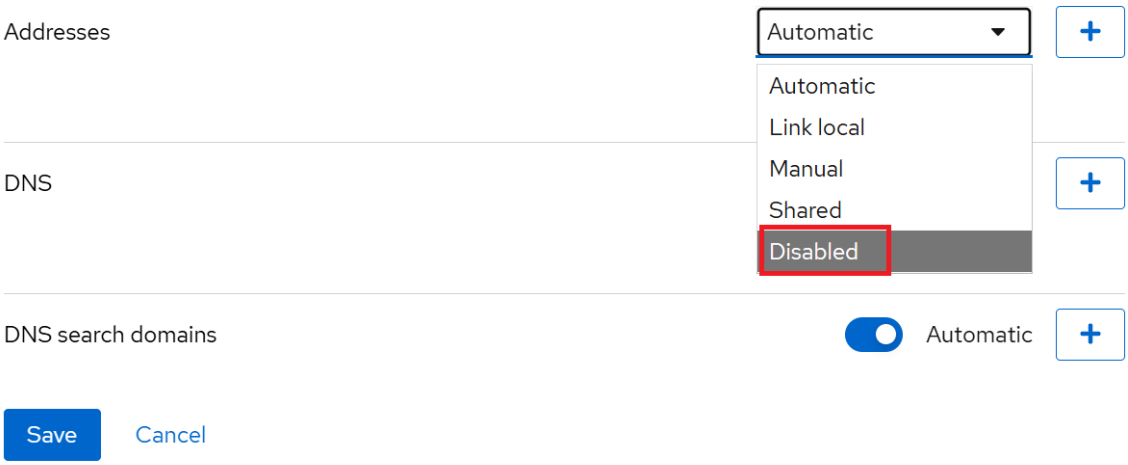


6. Click **Add**.

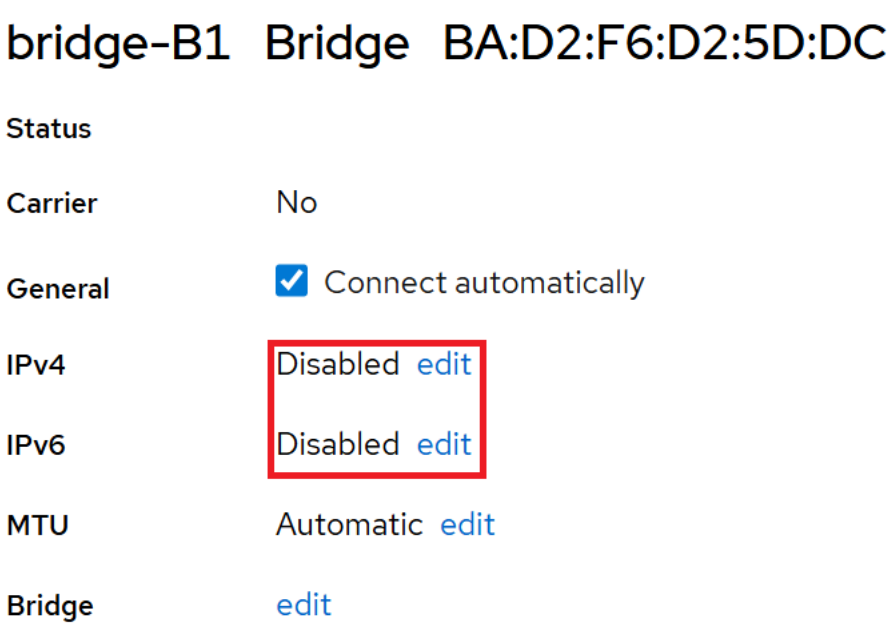
7. Select the newly created bridge-B1. In the bridge-B1 window, next to IPv4, click **edit**.



8. In the IPv4 settings window, in the **Addresses** list, select **Disabled**.
9. Click **Save**.
10. In the bridge-B1 window, next to IPv6, click **edit**.
11. In the IPv6 settings window, in the **Addresses** list, select **Disabled**.
12. Click **Save**.



13. In the bridge-B1 window, verify that both the IPv4 status and the IPv6 status are displayed as **Disabled**.



14. Deploy SBC `qcow2` files in the shell.

Next steps

The physical interface is determined by the server model to ensure the use of its highest supported port speed for interfaces A2 and B2.

For 6 physical 1GbE ports deployments:

- Configure A2 interface bridge-A2 using ens1f0 or ens2f0 or enp216s0f0 or eno12409
- Configure B2 interface bridge-B2 using ens1f1 or ens2f1 or enp216s0f1 or eno12429

For 6 physical 10/25GbE ports deployments:

- Configure A2 interface bridge-A2 using ens1f0np0
- Configure B2 interface bridge-B2 using ens1f0np1

Verifying the correct ASP 130 R6.0.x version

About this task

Verify that ASP 130 is running version R6.0.0.2.0 or later. If not, update before continuing.

Before you begin

Log in to the ASP R6.0.x CLI using `custadm` credentials.

Procedure

Run the `swversion` command.

If the version is R6.0.0.2.0 or later, you can continue. If the version is earlier than R6.0.0.2.0, stop and update ASP 130 to R6.0.0.2.0 or later before proceeding.

Converting a qcow2 image to a thick-provisioned format

About this task

The qcow2 image extracted during EMS installation is thin-provisioned by default. Use this procedure to convert the qcow2 image to a thick-provisioned format before deploying SBC instances.

Before you begin

Ensure that you are in the `var/lib/libvirt/staging` directory.

If the `/var/lib/libvirt/staging` directory does not exist, update ASP 130 to ASP R6.0.0.2.

Ensure that you use the same `sbce-10.2.1.0-101-24795.qcow2` file you copied from the local machine to `/var/lib/libvirt/staging` of ASP 130 R6.0.x (KVM ON RHEL 8.10) hypervisor server.

Procedure

1. Run `ls-l` to verify that the thin and thick qcow2 files are present in the `var/lib/libvirt/staging` directory.

   The command produces output similar to the following:

   ```
   -rw-r-----. 1 custadm custadm 3417178112 Nov 25 2024 sbce-10.2.1.0-101-24795.qcow2
   ```

   ```
   -rw-r-----. 1 root root 68730224640 Oct 3 19:54 sbce-10.2.1.0-101-24795-SBC1-thick.qcow2
   ```

2. To change the permission, run the following: `sudo chmod 755 sbce-10.2.1.0-101-24795-SBC11-thick.qcow2`
3. To verify that the conversion is successful, run the following: `[custadm@aasp130clv staging]$ qemu-img info sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`
4. Check that the disk size is 64GiB.
5. Run `[custadm@aasp130clv staging]$ sudo mv sbce-10.2.1.0-101-24795-SBC1-thick.qcow2 /var/lib/libvirt/images` to move the thick qcow2 image to the `/var/lib/libvirt/images` directory.
6. When prompted, enter the `custadm` password to complete the operation.
7. Run the following commands to verify the image is present in the `lib/libvirt/images` directory:

```
cd/var/lib/libvirt/images
sudo ls -l
```

8. While in the `/var/lib/libvirt/images` directory, run the following commands to change **Owner** to `qemu` and permissions to `640`:

```
sudo chown qemu:qemu sbce-10.2.1.0-101-24795-SBC1-thick.qcow2
sudo chmod 640 sbce-10.2.1.0-101-24795-SBC1-thick.qcow2
```

9. Run `sudo ls -l` and verify the owner and permissions.

Next steps

Remove all extracted and converted images from the `/var/lib/libvirt/staging` directory before deploying additional VMs.

Importing SBC VM on ASP R6.0.x using the cockpit web console

About this task

Import and configure SBC Virtual Machine (VM) on Avaya Solutions Platform 130 Appliance R6.0.x using the cockpit web console. This procedure includes steps for VM setup, network interface configuration, initial CLI-based setup, and Secure Boot key registration.

Before you begin

- Ensure that you have the `custadm` credentials for the ASP130 R6.0.x cockpit web console.
- If your access is limited, switch to Administrative access before continuing.
- The SBC disk image (`sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`) is available at`/var/lib/libvirt/images/`.
- Navigate to **System** > **Networking** > **Networking Interfaces** and confirm that bridges (bridge0 (M1 and M2), bridge-A1, and bridge-B1) are created.

Note:

Each bridge must have an assigned interface, and both IPv4 and IPv6 must be disabled (The default setting is automatic).

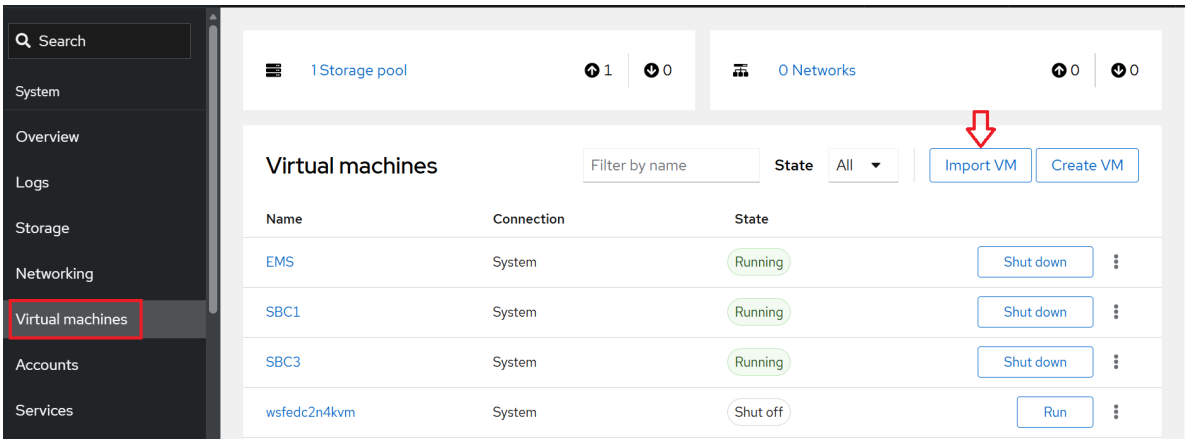
Procedure

1. Log in to the ASP 130 R6.0.x cockpit web console in one of the following ways:

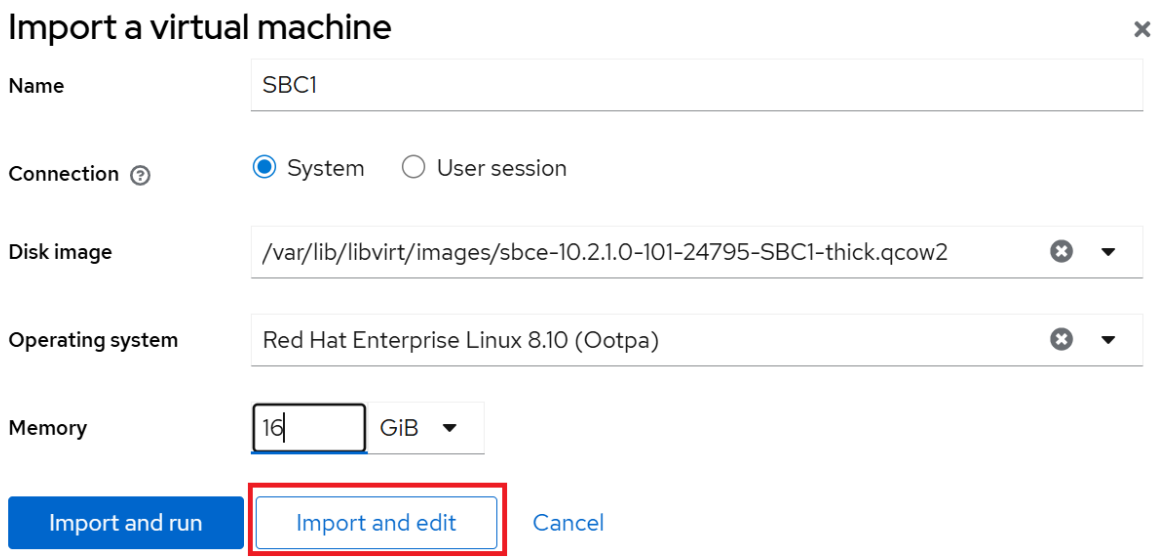
- External access: `https://<IP address or FQDN of the ASP 130 R6 KVM host>:9090`
- Services port access: https://192.11.13.6:9090

2. Use the `custadm` credentials to log in.

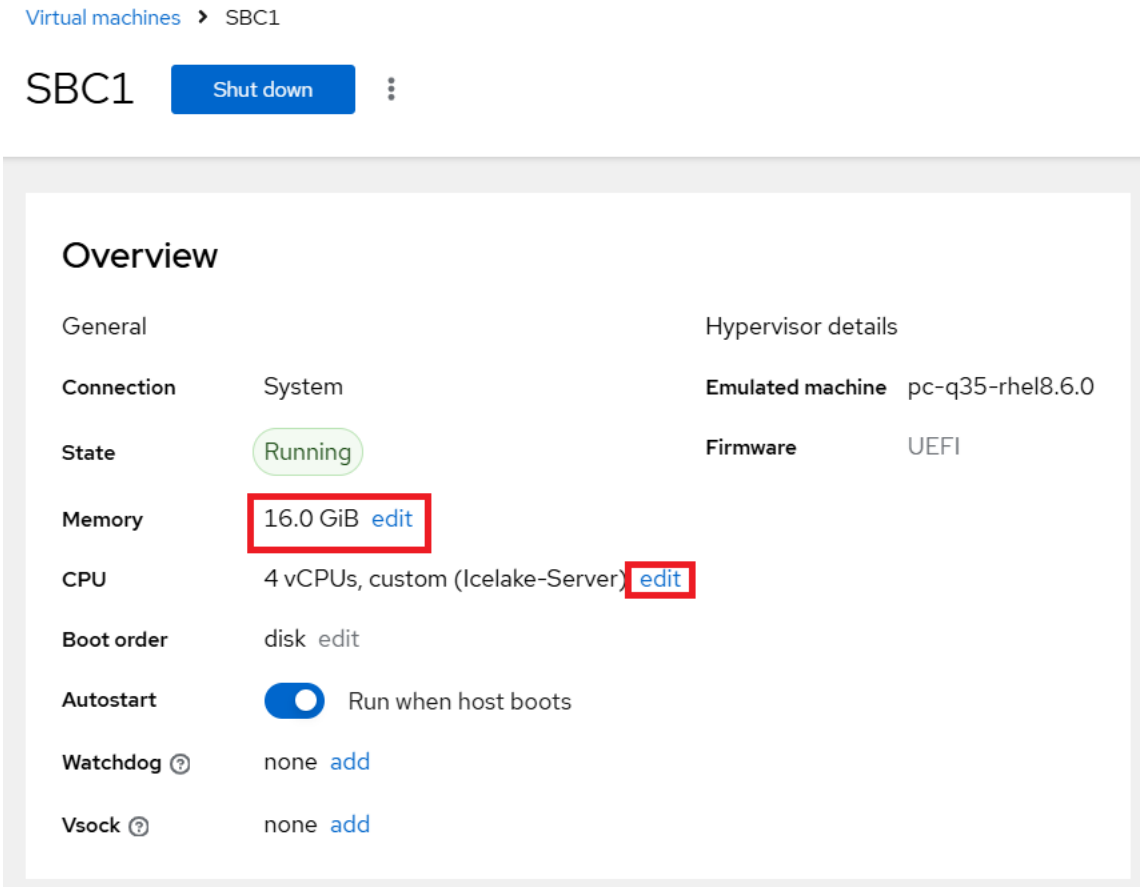
3. Navigate to **System** > **Virtual machines** > **Import VM**.



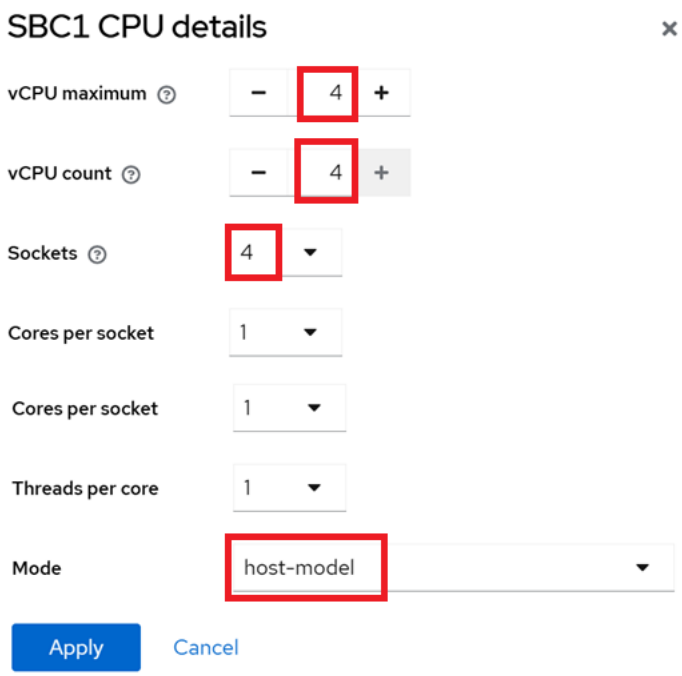
4. In the Import a virtual machine window, enter the appropriate details based on the specifications below:
   - Enter the VM **Name**.
   - Set **Disk image** to `/var/lib/libvirt/images/sbce-10.2.1.0-101-24795-SBC1-thick.qcow2`.
   - Set **Operating system** to `Red Hat Enterprise Linux 8.10 (Ootpa)`.
   - Set **Memory** to `16 GiB` as defined by the selected deployment profile..
   - Click **Import and edit**.



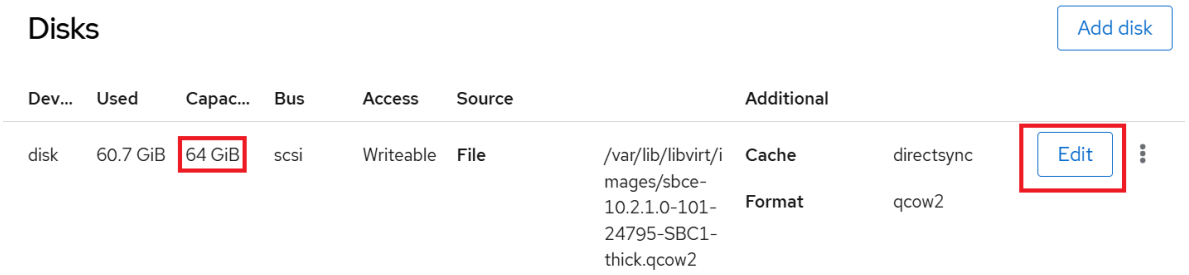
5. In the SBC1 Overview window, verify that memory is set to **16 GiB**.



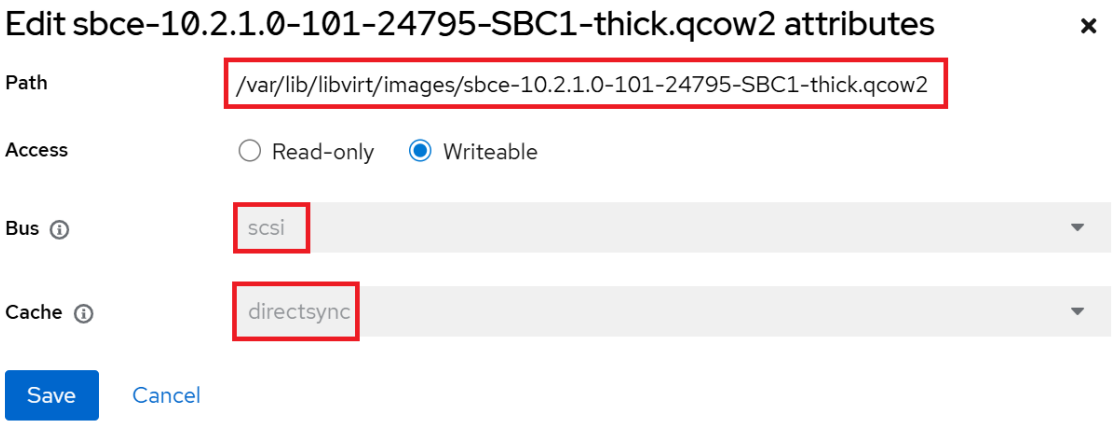
6. Click **Edit** next to CPU, enter the following details:
   - In the CPU details window, increase both **vCPU maximum** and **vCPU count** to `4`.
   - Confirm that the number of sockets matches the vCPU maximum.
   - Set **Mode** to `host-model`.
   - Click **Apply**.



7. Change the firmware from **BIOS** to **UEFI**.
8. Scroll to the Disks section, verify that disk capacity is **64 GiB**.



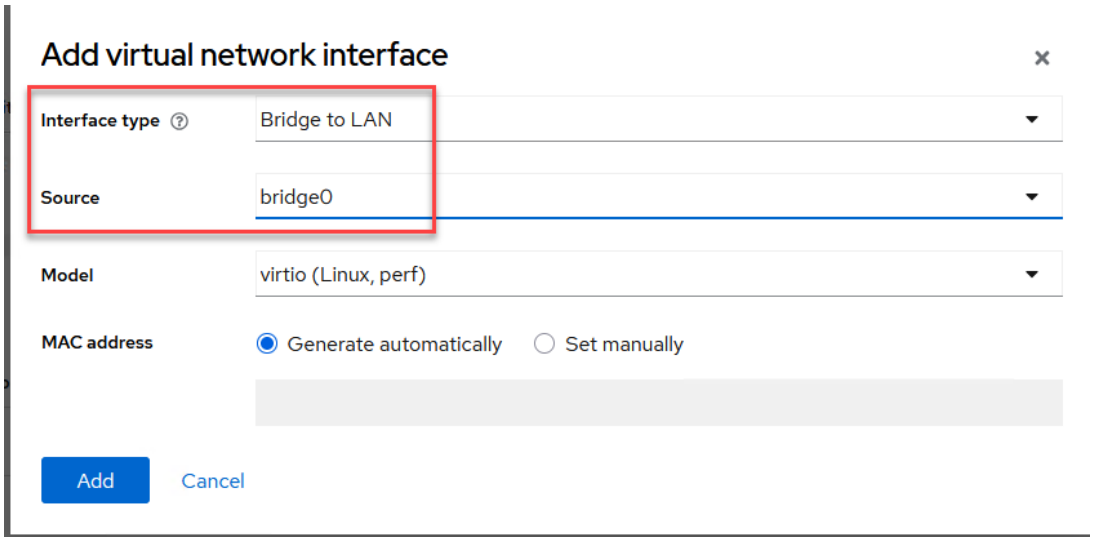
9. Click **Edit**, enter the following details:
   - In the Edit attributes window, set **Bus** to `scsi`.
   - Set **Cache** to `directsync`.
   - Click **Save**.



10. Scroll to the Network interfaces section.
11. To add interfaces, click on **Add network interface**.

    Note:

    By default, the SBC VM imports single network interface which uses the host default bridge0. For SBC deployment, you require atleast a minimum of 4 interfaces.
12. In the Add network interface window, do the following:
    - For M1 and M2 interfaces:
      a. Set **Interface type** to `Bridge to LAN`.
      b. Set **Source** to `bridge0`.
      c. Set **Model** to `virtio (Linux, perf)`.
      d. Click **Add**.



Note:

M2 interface also uses bridge0.

- Repeat the above process for M2 interface.
- For A1, B1 (if required, A2 and B2 interfaces), do the following:

Note:

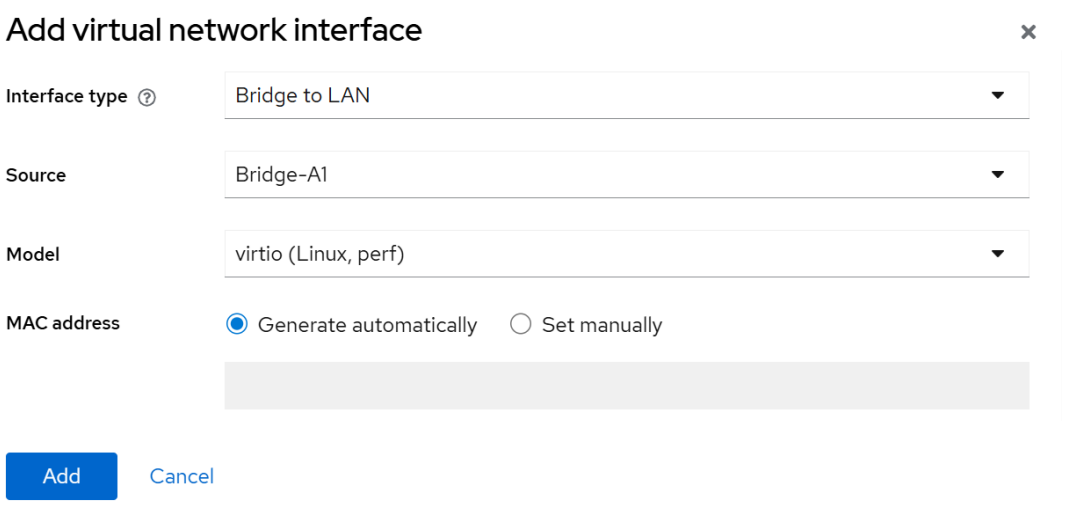
A new bridge for A1, B1 interfaces is required. Ensure these have been created prior to continuing.

a. Set **Interface type** to `Bridge to LAN`.

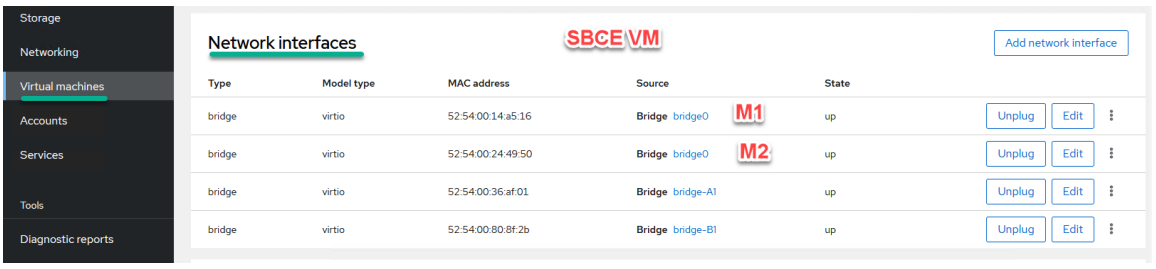
b. Set **Source** to `bridge-A1`.

c. Set **Model** to `virtio (Linux, perf)`.

d. Click **Add**.



- Repeat the process for bridge-B1 (if required, bridge-A2 and bridge-B2).



Note:

For SBC and EMS+SBC, add interfaces: A1, B1, M2 (and optionally A2, B2 for six interfaces).

13. Scroll back to the SBC1 Overview section, click **Run** to start the SBC1 VM.

Configuring SBC using the CLI

About this task

Use the CLI to establish essential network settings, secure initial access, and prepare the SBC system for operation.

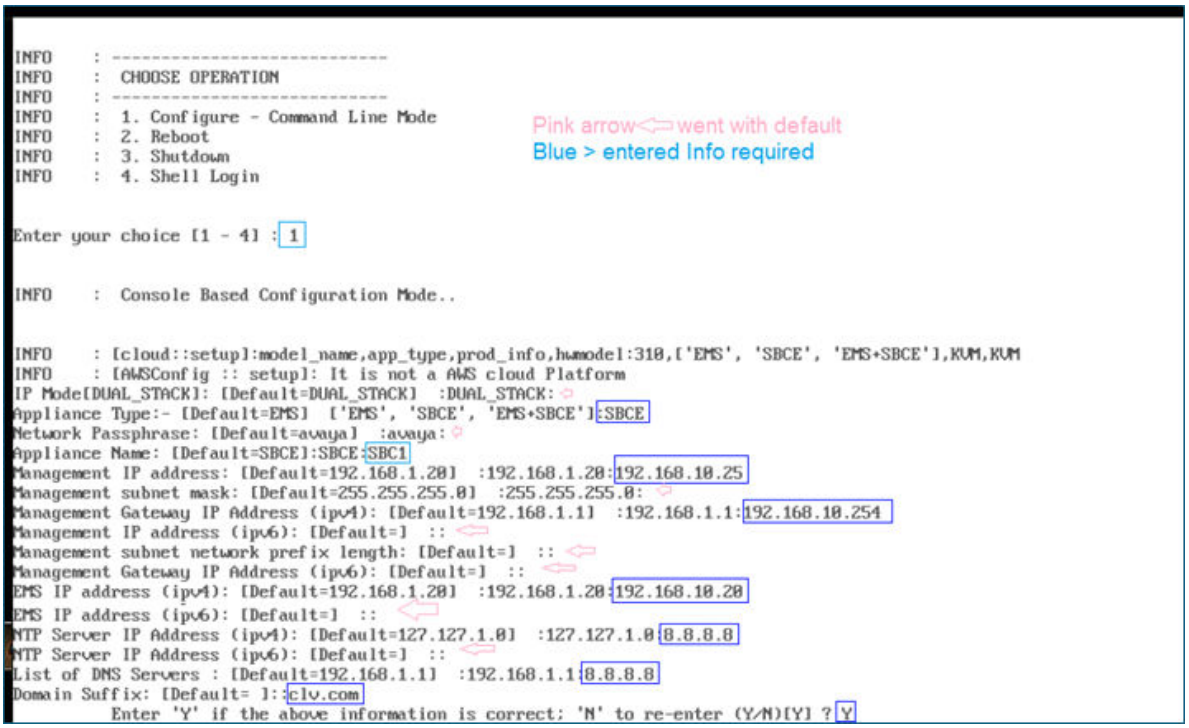
Procedure

1. In the console section, click **Expand** to enlarge the VNC console.
2. Ensure your cursor is active inside the console window.

   Login is not required for the initial base configuration.
3. Under CHOOSE OPERATION, enter `1` to select **Configure - Command Line Mode**.
4. When prompted, enter the following values:

- At the **IP Mode** prompt, press **Enter** to accept the default value **DUAL_STACK**.
- At the **Appliance Type** prompt, press **Enter** to accept the default value **EMS**.
- At the **Network Passphrase** prompt, press **Enter** to accept the default value **avaya**.
- At the **Appliance Name** prompt, enter the name of the SBC VM.
- At the **Installation Type** prompt, select the required installation type and press **Enter**.
- At the **Management IP address** prompt, enter `192.168.10.25`.
- At the **Management Gateway IP Address (ipv4)** prompt, enter `192.168.10.254`.
- At the **List of DNS Servers** prompt, enter `8.8.8.8`.
- At the confirmation prompt, enter `Y` to confirm the information.

5. Type `Y` to confirm the information is correct.

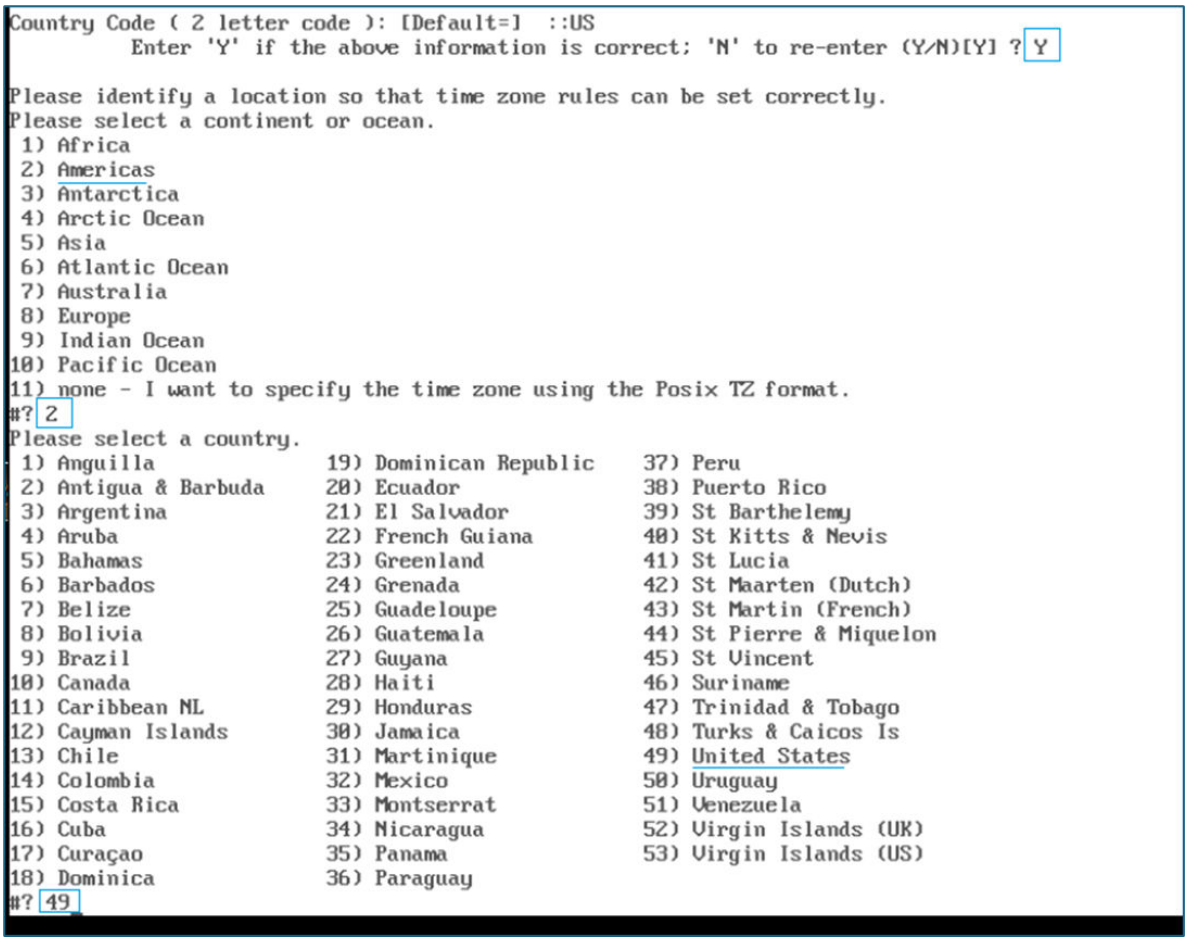



```
INFO    : ----------------------------
INFO    :  CHOOSE OPERATION
INFO    : ----------------------------
INFO    :  1. Configure - Command Line Mode
INFO    :  2. Reboot
INFO    :  3. Shutdown
INFO    :  4. Shell Login

Enter your choice [1 - 4] : 1

INFO    :  Console Based Configuration Mode..

INFO    : [cloud::setup]:model_name,app_type,prod_info,hwmodel:310,['EMS', 'SBCE', 'EMS+SBCE'],KVM,KVM
INFO    : [AWSConfig :: setup]: It is not a AWS cloud Platform
IP Mode[DUAL_STACK]: [Default=DUAL_STACK]  :DUAL_STACK:
Appliance Type:- [Default=EMS]  ['EMS', 'SBCE', 'EMS+SBCE']:SBCE
Network Passphrase: [Default=avaya]  :avaya:
Appliance Name: [Default=SBCE]:SBCE:SBC1
Management IP address: [Default=192.168.1.20]  :192.168.1.20:192.168.10.25
Management subnet mask: [Default=255.255.255.0]  :255.255.255.0:
Management Gateway IP Address (ipv4): [Default=192.168.1.1]  :192.168.1.1:192.168.10.254
Management IP address (ipv6): [Default=]  ::
Management subnet network prefix length: [Default=]  ::
Management Gateway IP Address (ipv6): [Default=]  ::
EMS IP address (ipv4): [Default=192.168.1.20]  :192.168.1.20:192.168.10.20
EMS IP address (ipv6): [Default=]  ::
NTP Server IP Address (ipv4): [Default=127.127.1.0]  :127.127.1.0:8.8.8.8
NTP Server IP Address (ipv6): [Default=]  ::
List of DNS Servers : [Default=192.168.1.1]  :192.168.1.1:8.8.8.8
Domain Suffix: [Default= ]::clv.com
         Enter 'Y' if the above information is correct; 'N' to re-enter (Y/N)[Y] ? Y
```

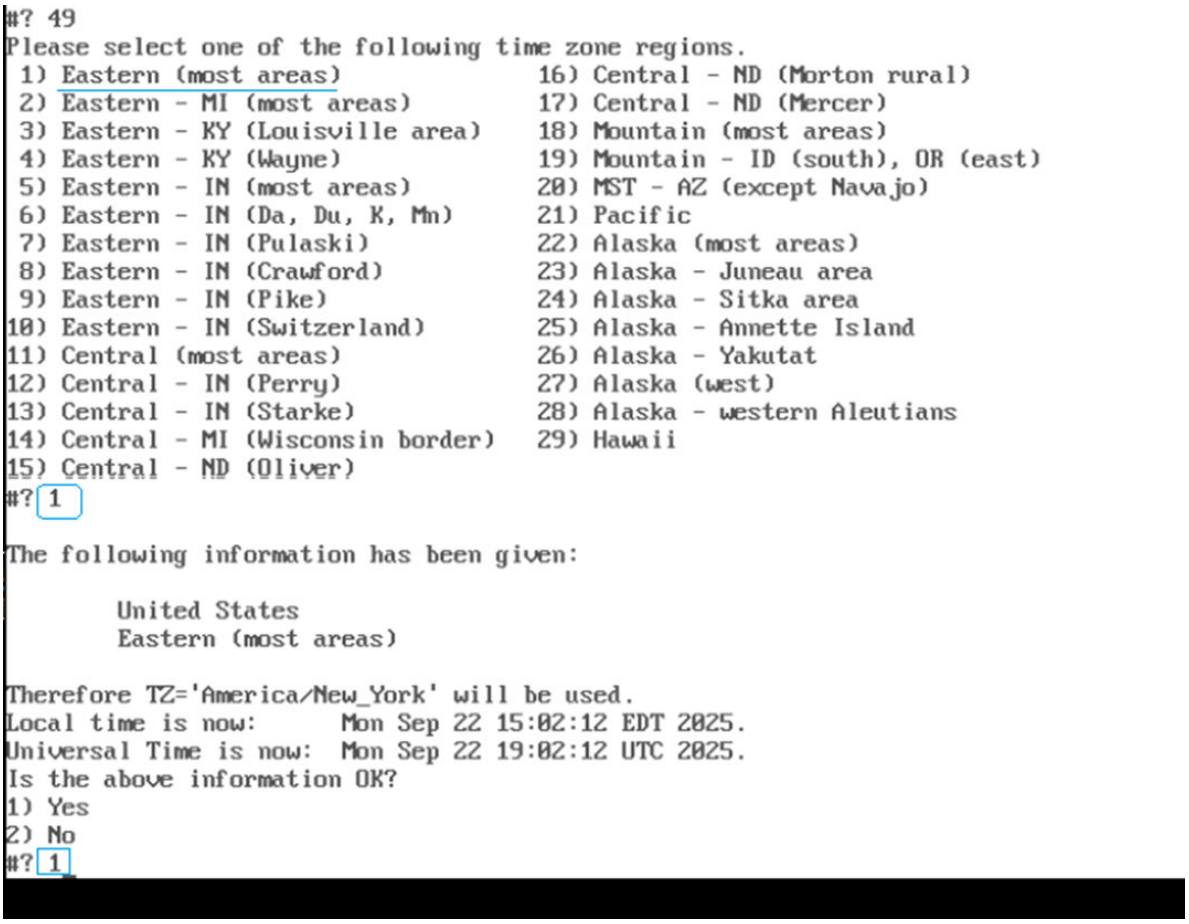
6. Enter contact and organization information when prompted.
7. Type `Y` to confirm the information is correct.

```
Domain Suffix: [Default= ]::clv.com
         Enter 'Y' if the above information is correct; 'N' to re-enter (Y/N)[Y] ? Y

First and Last Name: [Default=]  ::Michael Cannon
Organizational Unit: [Default=]  ::Avaya
Organization: [Default=]  ::AvaYA Services
City or Locality: [Default=]  ::Cleveland
State or Province: [Default=]  ::OH
Country Code ( 2 letter code ): [Default=]  ::US
         Enter 'Y' if the above information is correct; 'N' to re-enter (Y/N)[Y] ? Y
```

8. Select continent/ocean and country.

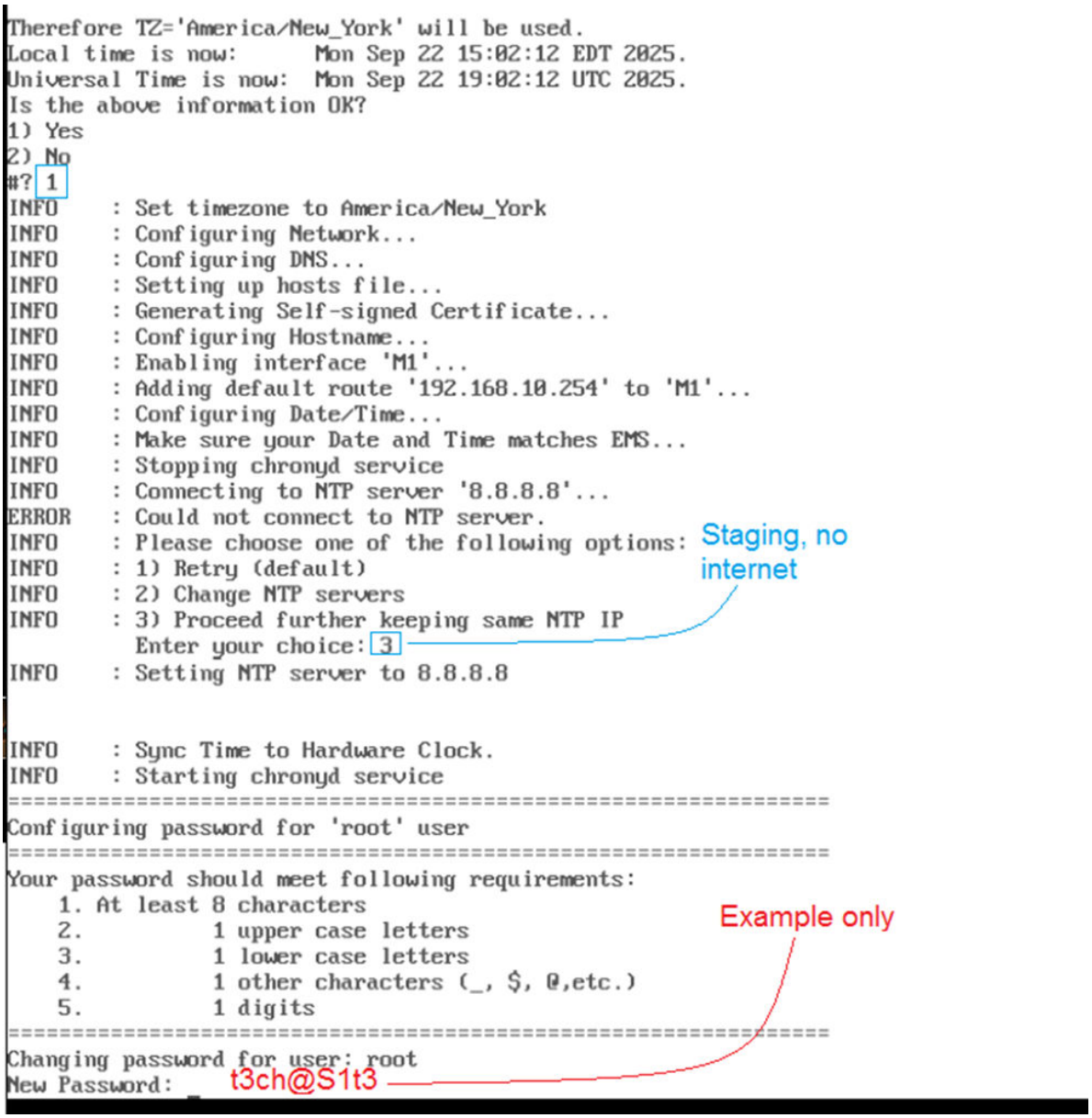


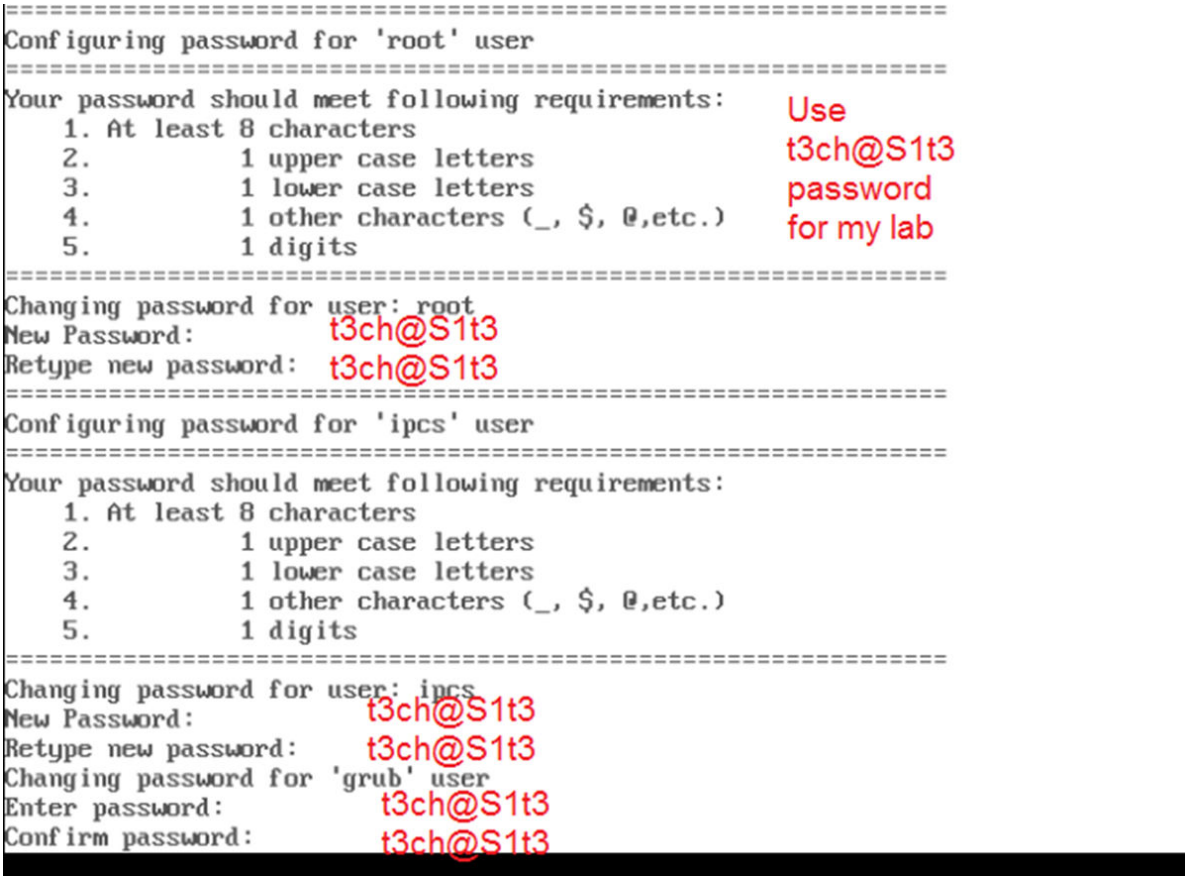
9. Select the region and confirm the time zone.



The system starts the base configuration of SBC1 immediately.

10. Create passwords for root, ipcs, and grub.



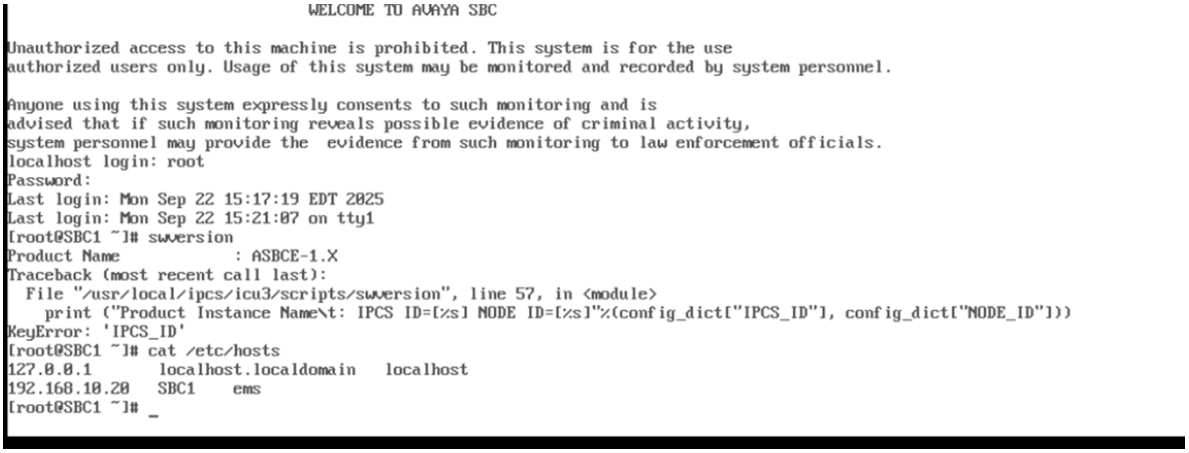


11. After you complete the base configuration, create secure passwords for the following accounts:

    - `root`
    - `ipcs`
    - `grub`

    Note:

    Do not use the password displayed in the illustrations. Assign a unique and secure password that complies with your organization's security policies.

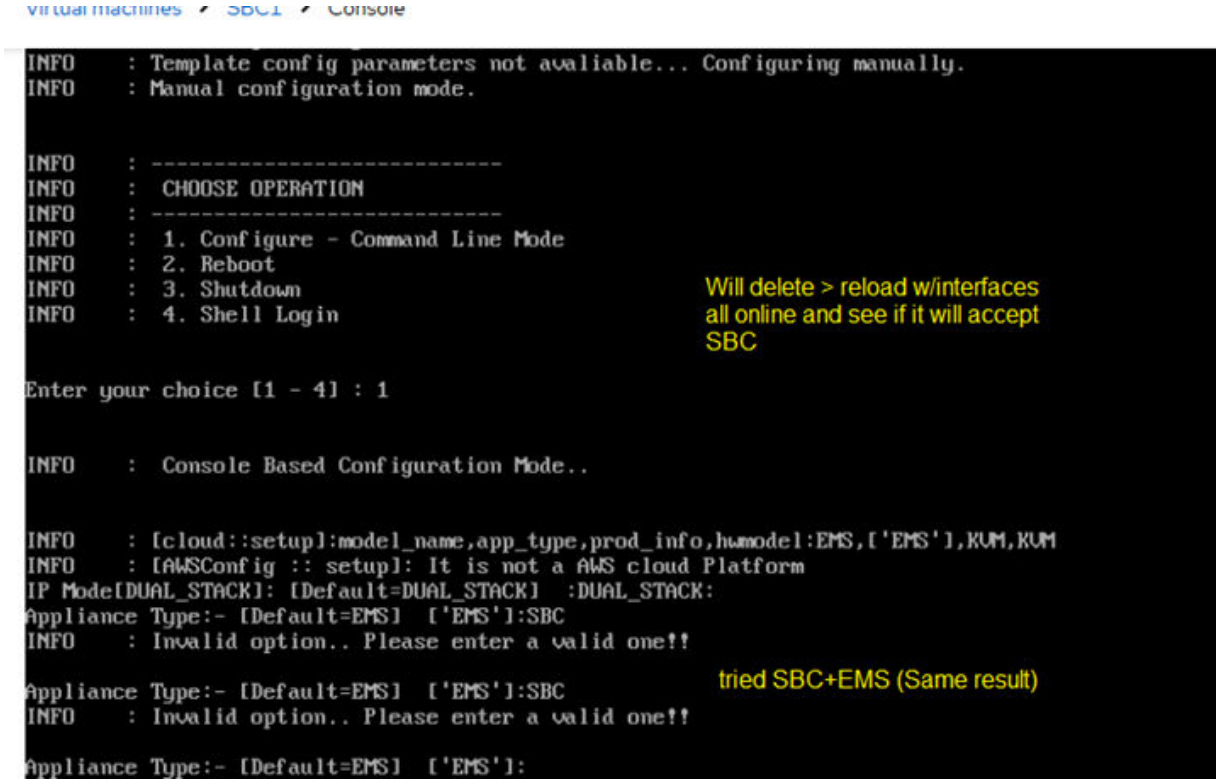


Use the secure access to connect to the shell. Then, verify your passwords by logging into root and ipcs to confirm system access.

Next steps

The base configuration options available depend on the number of virtual Network Interface Cards (vNICs) assigned to the SBC VM:

- If fewer than four interfaces are assigned to the SBC VM, only EMS displays as a configuration option.
- SBC or EMS+SBC modes are not available.



Post-configuration

After the initial boot configuration is complete, Avaya Session Border Controller returns to the login screen. Perform the following post-configuration tasks:

- Enable Secure Boot by registering the SBC Secure Boot key.
- Apply optional hardening or management configurations based on your deployment requirements.

Secure Boot configuration

Apply Secure Boot only to SBCs or EMS+SBCs. By default, VMs created with UEFI firmware have Secure Boot enabled. The SBC bootloader/kernel must be signed with a key that the firmware of VM recognizes.

Authorizing the certificate

About this task

Authorize a custom Secure Boot certificate on Avaya SBC to ensure trusted startup.

Procedure

1. Log in to Avaya SBC with root credentials.
2. Navigate to the following certificate signatures directory:

   ```
   cd /usr/local/ipcs/etc/cert/signatures/
   ```

3. Run the following command to import the certificate:

   ```
   mokutil --import asbc_custom_secure_boot_cert.cer
   ```

4. When prompted, enter a password.

   You need this password later in the UEFI key management console.

5. Reboot the system through the Virtual Machine (VM) console.

Registering the key

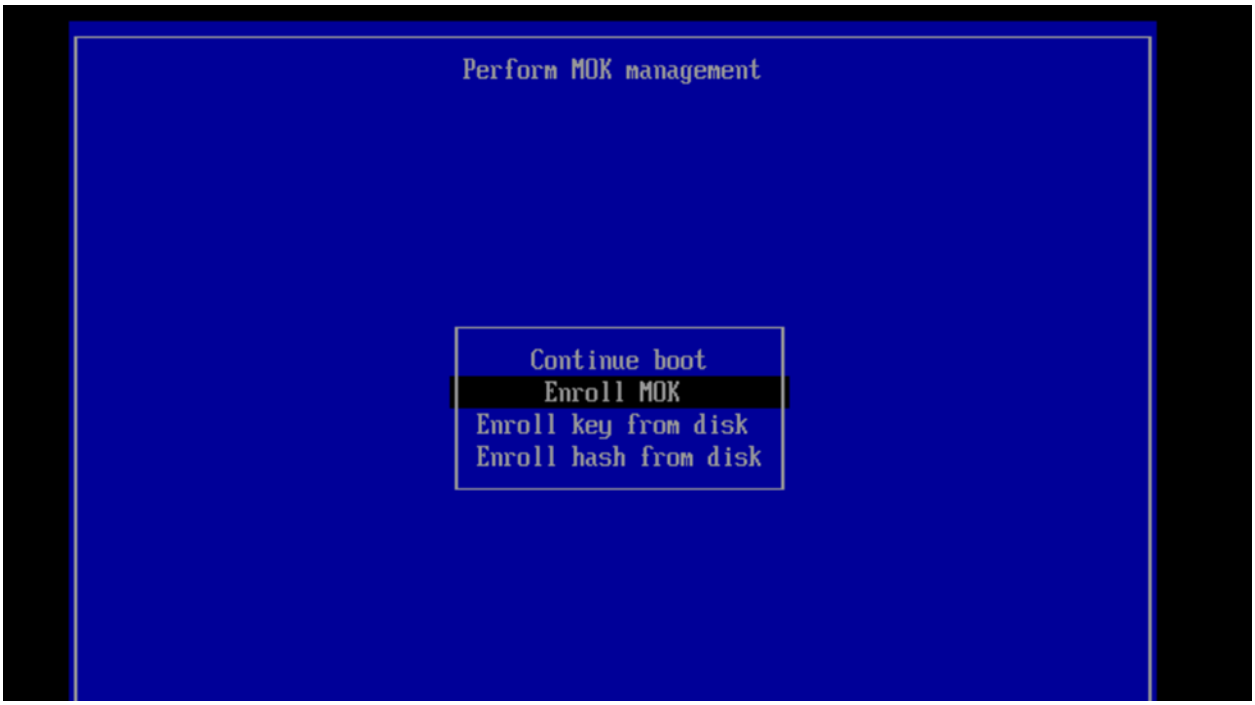
About this task

Register the custom key in the Shim UEFI key management console, completing the Secure Boot setup. By enrolling the key and confirming with the previously set password, Avaya Session Border Controller is prepared to run securely under UEFI BIOS settings.

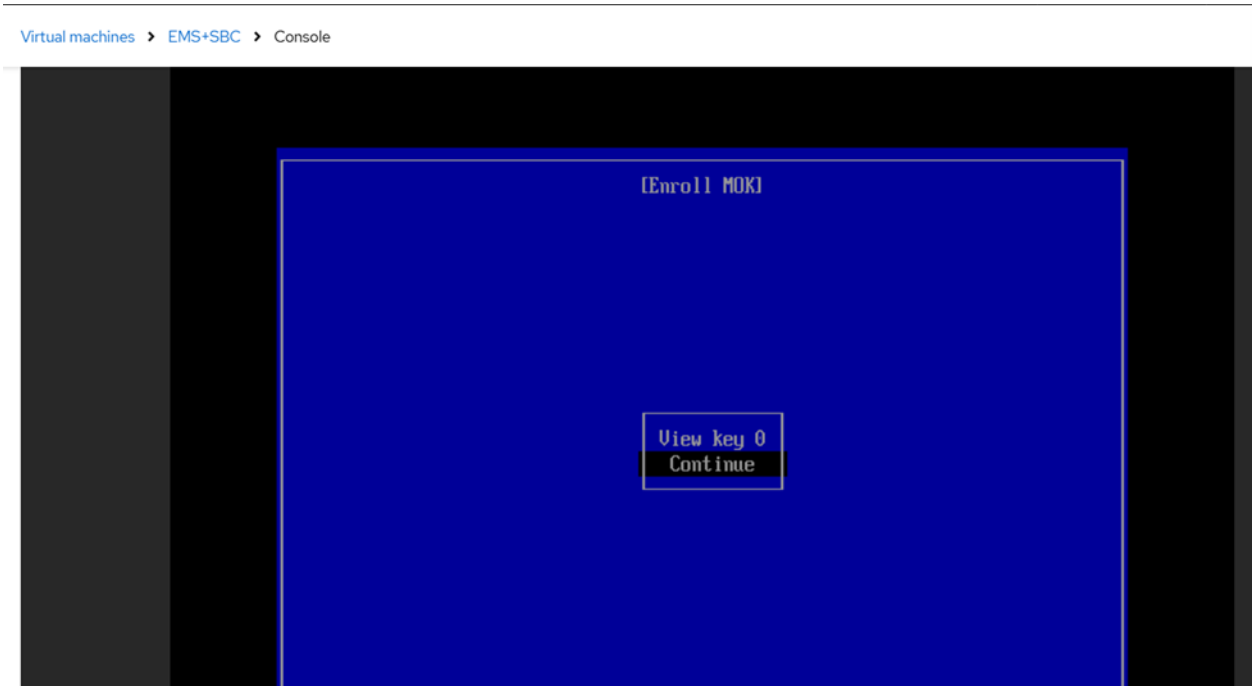
Procedure

1. After reboot, the Shim UEFI key management console opens.
2. Press any key to start (within 8 seconds).

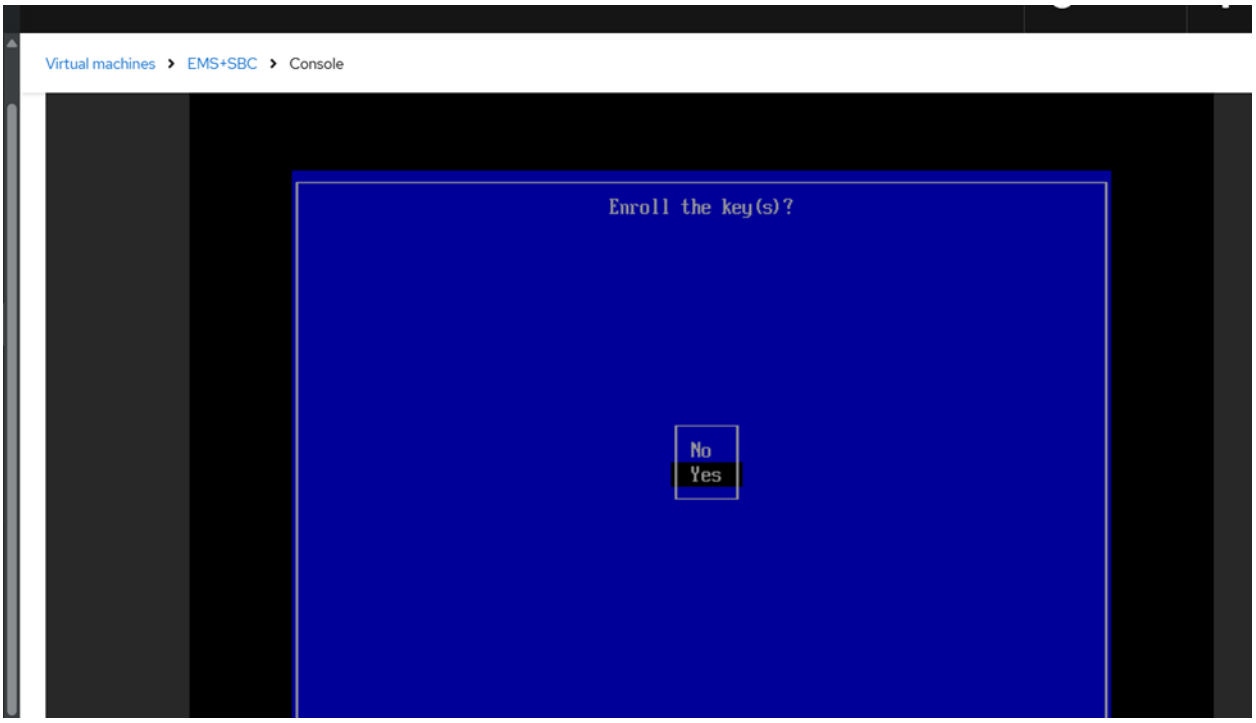
3. On the MOK management screen, select **Enroll MOK**.



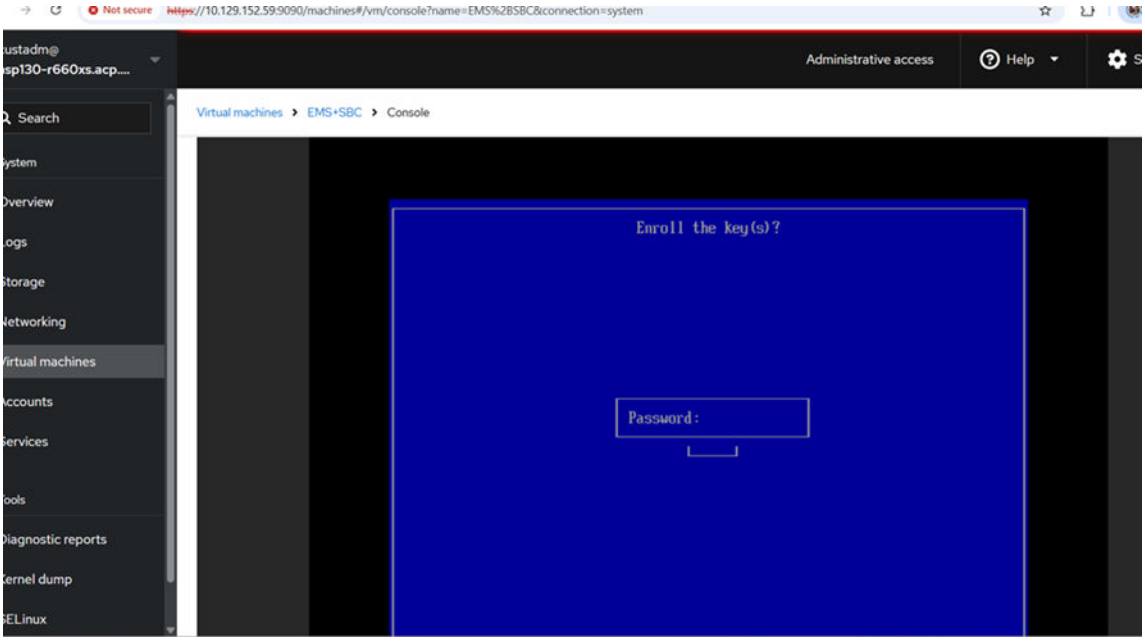
4. Select **Continue**.



5. Select **Yes** to enroll the key.

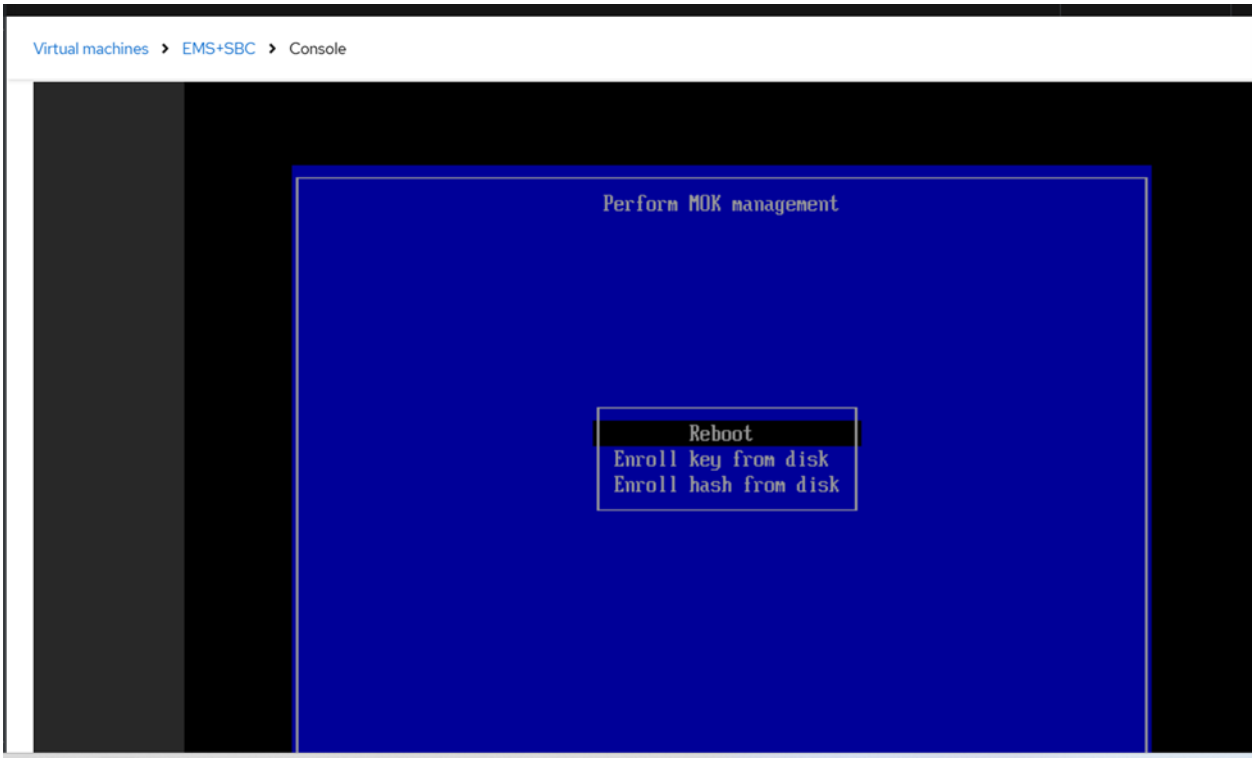


6. Enter the password you set earlier.



7. Confirm changes and reboot the system.

   The system is now configured for Secure Boot with UEFI BIOS settings.


Virtual machines
EMS+SBC
Console
Perform MOK management
Reboot
Enroll key from disk
Enroll hash from disk

Chapter 7: Deploying SBC2 and SBC3 using the EMS web interface

About this task

This task outlines the steps required to enable A1 and B1 interfaces (and optionally A2 and B2) in the Element Management System (EMS) web interface.

Before you begin

Before enabling the interfaces, ensure that you have configured WebLM and installed a live license.

Procedure

1. Log on to the EMS web interface from https://EMSip/login.

   Use the following credentials:

   - **Username**: `ucsec`
   - **Password**: `ucsec`

2. Update the default password to a strong, secure one (for example, `t3ch@S1t3`).

   After updating the password, the screen displays the EMS dashboard.

3. Navigate to **Network Flows** > **Network Management** > **Interfaces**.

   Enable interfaces A1 and B1. If required, enable A2 and B2.

4. Click the **Networks** tab next to the interface settings.

   Assign the required IP configuration details to interfaces A1 and B1. If required, assign IPs to A2 and B2 interfaces, if you have enabled interfaces in the step 3.

Chapter 8: Resources

Documentation

Avaya Solutions Platform (ASP) 100/130 Series and related R6.0.x systems customer documentation is available in HTML and PDF format on the Avaya Support website.

Title	Use this document to:
Installing the Avaya Solutions Platform 130 Series	Perform installation procedures for the Avaya Solutions Platform 130 Appliance 6.0.x server.
Policies for technical support of the Avaya Solutions Platform (ASP) 130 and ASP S8300 R6.0.x	Verify which software and hardware features of the Avaya Solutions Platform (ASP) 130 and S8300 R6.0.x servers are supported by Avaya Services. It outlines the tested configurations, identifies supported and unsupported features, and clarifies the boundaries of technical support responsibility in the event of issues
Avaya Converged Platform 130 Series iDRAC9 Best Practices	Securely manage and maintain the iDRAC9 interface for Avaya Solutions Platform 130 servers (Dell R640 and Dell R660xs).
Avaya Solutions Platform 130/S8300 Overview and Specification	Review technical specifications of the Avaya Solutions Platform 130 products, including key features, hardware details, and system capabilities.
Application Note for Avaya Solutions Platform (ASP) 130 Release 6.0.x (KVM on RHEL 8.10)	Implement VLAN configurations on ASP R6.0 KVM systems running Red Hat Enterprise Linux (RHEL) 8.10.
Avaya Solutions Platform 130 Release Notes	Review release notes, important notices, and known issues related to Avaya Solutions Platform (ASP) 130 R6.0.x.
PCN2173Su	Access details about the Avaya Solutions Platform R6.0.0.3.0 customized zip bundle, including updated RPM packages listed in the Security Information section.
PSN027113u	Update BIOS or firmware for Avaya Solutions Platform 100 Series Dell® R660xs, Version 2.
PSN027112u	Update BIOS or firmware for Avaya Solutions Platform 100 Series Dell® R640, Version 16.
PSN020640u	Review Avaya Solutions Platform R6.0.x general specifications.

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.