



Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300

Release 6.0.x
Issue 2
February 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

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.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The 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.

Third Party Components

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

Service Provider

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

Compliance with Laws

You acknowledge and agree that it is Your responsibility 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 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 LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction	6
Purpose	6
Change history	6
Prerequisites	6
Chapter 2: Overview S8300	8
What's new in Avaya Solutions Platform Release R6.0.x	8
S8300E server specification	8
S8300E topology	9
ASP 6.0.x storage layout for KVM on RHEL 8.10	12
Chapter 3: Registration	16
Overview	16
HealthCheck tool registration process	16
Registering a new device	17
Viewing the status of your registration request	19
Technical Onboarding process	20
Registering device after S8300E migrates from AVP 8.1.x or ASP S8300 R5.x to ASP 6.0.x	20
Chapter 4: Installing Avaya Solutions Platform S8300	22
ASP S8300 R6.0.x shipped from Avaya's integrator	22
Creating USB Flash Media Drives for an ASP R6.0.x Software Installation image	22
Steps for installing the ASP R6.0.x KVM on the S8300	27
Chapter 5: Configuration of ASP S8300 R6.0.x	32
Configuring ASP S8300 R6.0.x	32
Additional configuration options	40
Configuring SNMP on KVM on RHEL 8.10	40
SNMP overview	40
Configuring SNMP v3 on a KVM on RHEL 8.10	40
Configuring SNMP v2 on RHEL 8.10	44
OID information for currently supported alarms	47
TLS protocol configuration for KVM on RHEL 8.10 Environment	50
Viewing TLS settings in KVM on RHEL 8.10 (Cockpit/Port 9090)	51
Chapter 6: Network port verification	55
Purpose	55
Validating network port configuration in Shell and Web	55
Status information commands	56
Chapter 7: Securing Network Configuration (OoBM)	58
Overview	58
No OOBM configured	58
In-band MGMT and OOBM access to Cockpit enabled and VM OOBM enabled	59
In-band MGMT and OOBM access to Cockpit disabled and VM OOBM enabled	60

Chapter 8: Performing server recovery or software remastering.....	62
Chapter 9: Replacing SSL certificates and Keys with Custom Certificates in RHEL	
8.10 - Cockpit Web Service.....	63
Overview.....	63
Replacing SSL certificates and Keys with Custom Certificates in RHEL 8.10 - Cockpit Web Service.....	64
Creating the Certificate configuration file for KVM on RHEL 8.10 host.....	65
Generating the Certificate signing Request in KVM on RHEL 8.10.....	69
Signing the Certificate Signing Request (CSR) by an Organizational CA.....	71
Replacing SSL certificates in Cockpit with a CA signed certificate.....	76
Adding the CA root certificate to Chrome or Microsoft Edge.....	83
Adding the CA root certificate to Firefox.....	85
Chapter 10: ASP R6.0.x update process.....	91
Chapter 11: Troubleshooting.....	92
Verifying the ASP configuration and network topology.....	92
Server inaccessible.....	93
Troubleshooting using CLI commands.....	93
Troubleshooting gateway CLI command in S8300	93
Troubleshooting gateway log messages.....	94
Gateway faults.....	95
Log and file collection to aid in troubleshooting.....	95
Collecting Host level log information.....	95
Collecting a KVM on RHEL 8.10 SOS Report from the CLI.....	95
Collecting a KVM on RHEL 8.10 SOS Report from the Cockpit UI.....	97
Chapter 12: Resources.....	101
Avaya Solutions Platform 130/S8300 documentation.....	101
Finding documents on the Avaya Support website.....	103
Avaya Documentation Center navigation.....	104
Support.....	105
Using the Avaya InSite Knowledge Base.....	105

Chapter 1: Introduction

Purpose

This document provides installation, maintenance, and troubleshooting procedures and information for Avaya Solutions Platform (ASP) S8300 R6.0.x.

The information in this document replaces the *Application Note for Deployment of Avaya Solutions Platform (ASP) S8300 Release 6.0.x (KVM on RHEL 8.10)*.

Examples in this document may reference ASP 130 but will be similar output for ASP S8300.

Change history

Issue	Date	Summary of changes
2	February 2026	• Updated tracking codes used in upgrade process. • Updates for 6.0.0.4.
1	June 2025	Initial Release 6.0.x document.

Prerequisites

Before installing or migrating Avaya Solutions Platform S8300, ensure that you have the following knowledge, skills, and tools.

Knowledge

- KVM on Red Hat Enterprise Linux 8.10 installation and configuration.
- VMware ESXi installation and configuration (not required but helpful for upgrades from ASP 5.1.x and earlier).
- Avaya Virtualization Platform (AVP) administration (not required but helpful for upgrades from AVP).

Skills

- General Linux knowledge.

- General virtualization knowledge and concepts.
- General network and server configuration.
- Simple Network Management Protocol (SNMP).

Tools

- USB drive for KVM on Red Hat Enterprise Linux 8.10 ISO deployment.
- Rufus software on laptop (for remaster).
- Laptop for services port access.

Chapter 2: Overview S8300

What's new in Avaya Solutions Platform Release R6.0.x

The ASP R6.0.x program introduces a new hypervisor and updated server hardware. In June 2024, Broadcom made the strategic decision to discontinue its Embedded OEM program. As Avaya is an Embedded OEM partner of VMware, this decision impacted the ASP 130 and ASP S8300 solutions leading to the necessity of identifying a new hypervisor. The ASP R6.0.x program introduces *KVM on Red Hat Enterprise Linux 8.10 (KVM on RHEL 8.10)*. In addition to the new hypervisor, ASP R6.0.x also introduces an updated server hardware platform with the Dell R660xs. All ASP R6.0.x solutions (ASP 130 and ASP S8300) only ship with the new KVM on RHEL 8.10 hypervisor.

 Important:

ESXi is not supported on ASP R6.0.x.

To ensure a smooth transition, Avaya has developed a migration path from earlier versions of ASP 130 or ASP S8300 running on VMware. For more information, see *PSN020640u – Avaya Solutions Platform R6.0.x Introduction*.

- For existing Installed ASP 130 Release and ASP S8300 Release 5.1 VMware Systems: Broadcom continues to provide critical security patches for currently installed VMware ESXi 7.0 systems on Avaya's ASP 5.1.x platform.
- Existing ASP 130 (Dell R640) have a migration path to ASP R6.0.x KVM on RHEL 8.10 while maintaining investments in the existing Dell R640 hardware platform.
- Existing ASP S8300 5.1.x have a migration path to ASP R6.0.x KVM on RHEL 8.10.

For detailed information about each specific release, see the latest [Avaya Solutions Platform S8300 Release Notes](#).

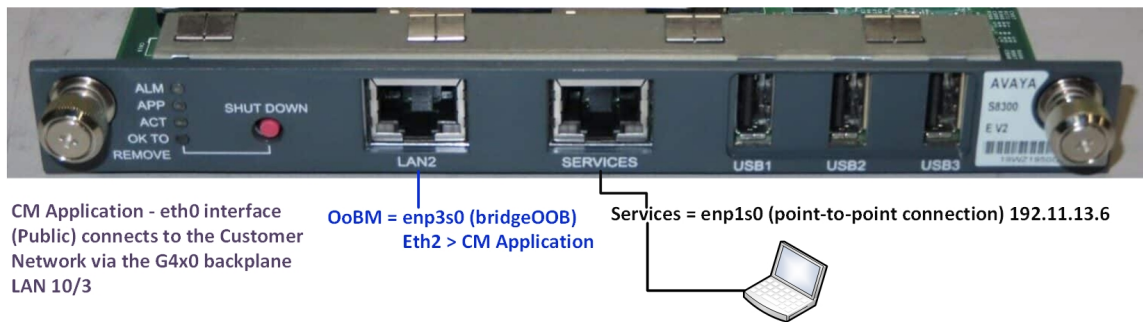
The Avaya Solutions Platform S8300 R6.0.x supports virtualization with a customized image of KVM on Red Hat Enterprise Linux 8.10.

S8300E server specification

The following table lists the S8300E server components and their respective specification:

S8300E components	Specification
CPU	Intel B925C based on Ivy Bridge processor
CPU frequency	2.0
Physical cores	2
Virtual cores	4
Supports HyperThreading	Yes
RAM Type	DDR3
RAM Size	16GB
Maximum RAM Size	16GB
HDD Type	SATA2
Storage	HDD/SSD
Capacity	320GB, 500GB, and 1TB HDD and 480GB SSD
NIC port type	1 GbE (internal connection to Gateway backplane, limited to 100Mbps)
Number of LAN ports	3
USB	2
Number of USB ports	3

S8300E topology



On S8300E, the public network of virtual machines (VM Network) is assigned to `enp2s0` and the `enp2s0` is connected through the G4x0 gateway backplane. The internal connection to the G4X0 backplane is limited to 100Mbps. The LAN port on the G4x0 Gateway is assigned to the public interface of the virtual machines. The management interface of the hypervisor (Management Network) is also assigned to `bridge0/enp2s0` and this is connected through the backplane of the G4x0 similar to the VM network. The services port is assigned to `enp1s0` and is directly associated with the services port on the front of the S8300E.

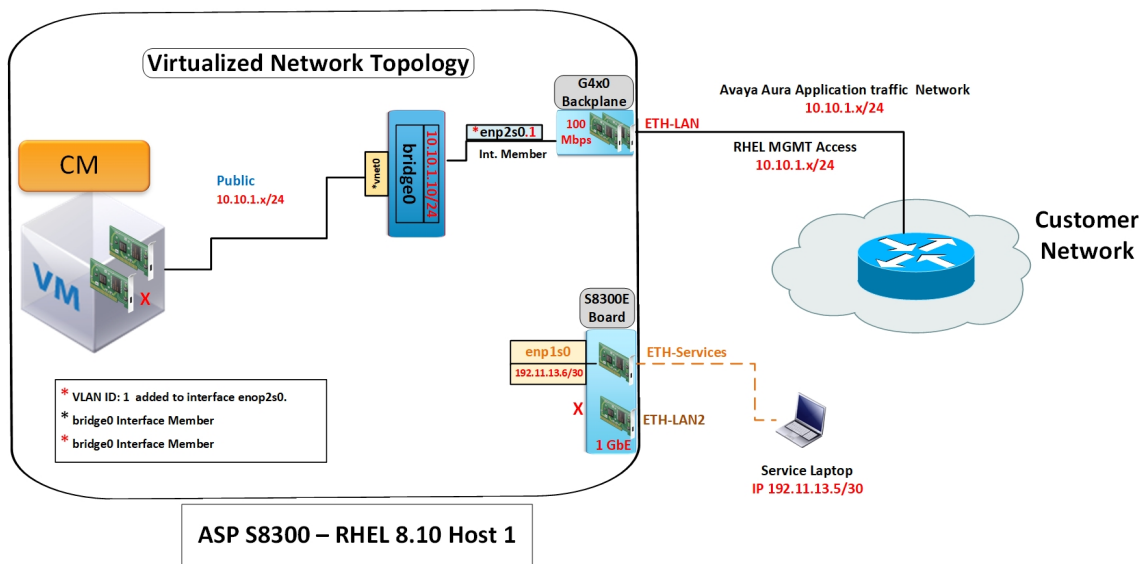
*** Note:**

There will not be any bridge/virtual switch configuration associated with the services port. If OOBM is enabled, the LAN 2 port is utilized and is assigned to `enp3s0`.

The default vlan id is “1” in the bridge0 (`enp2s0.<vlan#>`) in the table below. The vlan ID number on the G4X0 must always match the vlan ID number on the S8300.

The Connection Profile Name is displayed when the `nmcli connection` shell command is executed. The Connection Profile Name does not appear in the Cockpit UI. The Device Name is displayed in the Cockpit UI.

Connection profile name	S8300 device name	Notes
Mgt_VM_Network	bridge0 (<code>enp2s0.<vlan#></code>)	Default without OOBM enabled
VM_Network		If OOBM enabled
Services	<code>enp1s0</code>	192.11.13.6 svc port
OOBM_Network	bridgeOOB (<code>enp3s0</code>)	Optional: Must be enabled during configuration
EMB-VLAN	<code>enp2s0.4093</code>	Internal connection to G4X0



Note: VLAN ID 1 is the default VLAN ID that gets assigned by the network script.

Figure 1: Default network topology

For more information about the network configurations below and enabling OOBM (Out of Band Management), see [Securing Network Configuration \(OoBM\)](#) on page 58.

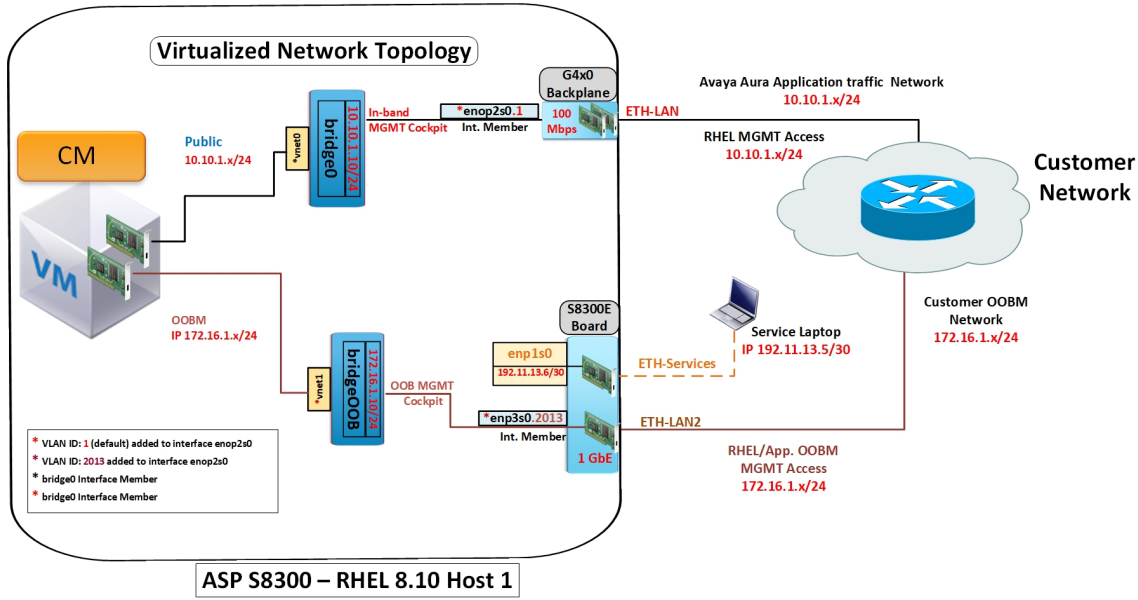


Figure 2: Network topology with OOBM enabled - Option A

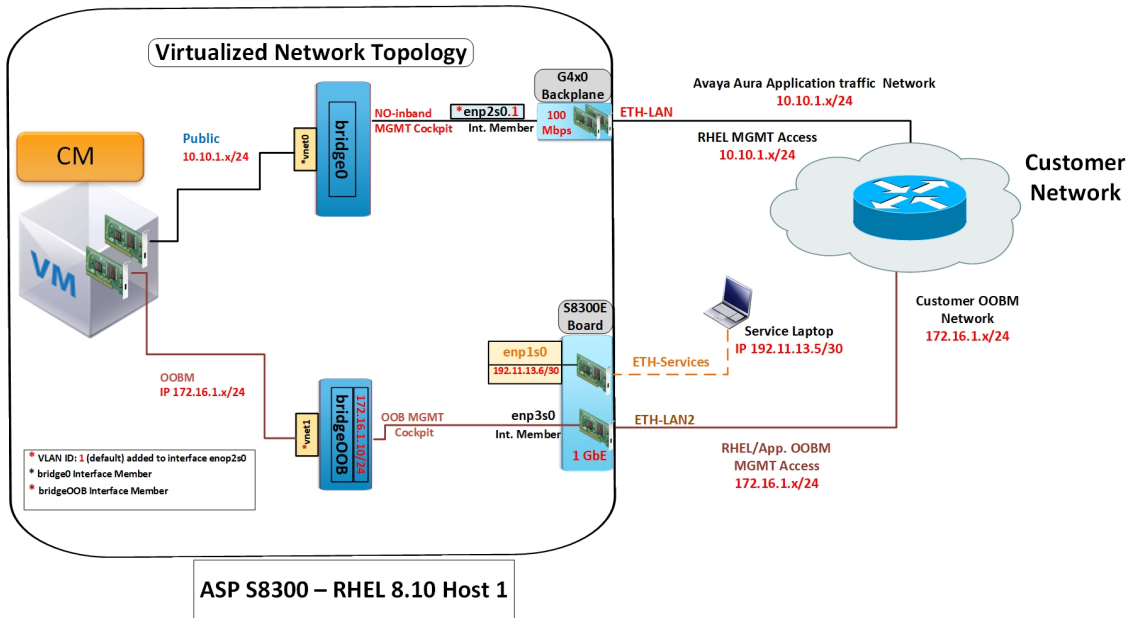
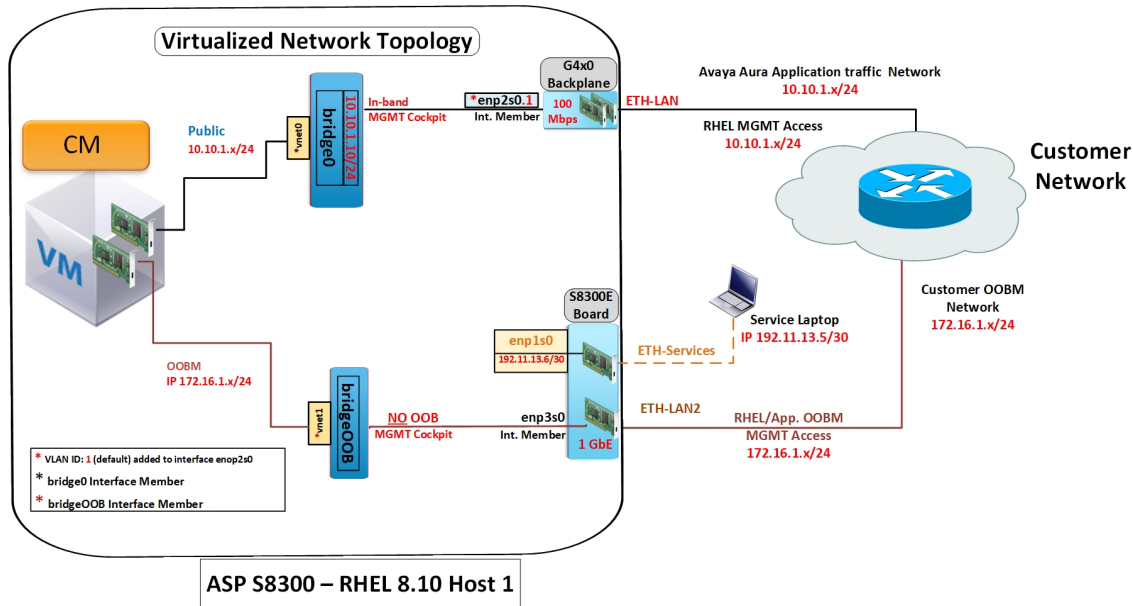


Figure 3: Network topology with OOBM enabled - Option B



Note: In-band MGMT access to cockpit is kept on **bridge0** (IP Address is assigned). **Out of Band Management** (OOBM) access to cockpit is not configured on **bridge008** (No IP Address is assigned).

Figure 4: Network topology with OOBM enabled - Option C

ASP 6.0.x storage layout for KVM on RHEL 8.10

This section outlines the disk partition scheme for the Avaya Solutions Platform (ASP) 6.0 – running on Kernel-based Virtual Machine (KVM) with Red Hat Enterprise Linux (RHEL) 8.10. The defined layout is designed to ensure optimal performance, security, and compatibility across supported hardware platforms (S8300E & Dell R640/R660xs) as well as across the full range of supported Avaya Aura® applications. Each partition is listed with its recommended size and functional role, supporting both the host operating system and the virtualized guest environments for application deployment.

⚠ Caution:

Unless explicitly instructed by Avaya, DO NOT change, modify, expand or delete any of the partitions listed in this table. Doing so may compromise the integrity of the entire solution and will require a full system re-image to restore the system back to a supported configuration.

★ Note:

By default, the Linux shell when using for example `df -h` reports storage in binary units (for example, GiB = 1024³ bytes), unless explicitly specified (for example, `df -H` for decimal).

Cockpit displays storage in decimal units (for example, GB = 1000³ bytes), so values may appear slightly different when using different interfaces.

Partition	Size	Notes
/boot	1 GiB	This partition contains the essential operating system kernel, enabling your system to initiate Red Hat Enterprise Linux, along with necessary files utilized during the bootstrap process.
/boot/efi	600 MiB	This partition uses the EFI System Partition (ESP) filesystem and is required for systems with a UEFI BIOS. For ASP deployments, all server hardware profiles except the S8300E use UEFI BIOS and therefore require this partition.
/	10 GiB	This is the root partition, which contains the root directory (/) of the file system. All files and directories not assigned to a separate partition reside here. For example, it includes the /usr directory, which holds most of the software and system binaries on a Red Hat Enterprise Linux system.
/var	6 GiB	This partition stores variable data used by the system and various applications. It includes files such as spool files, and temporary data that change frequently during normal operation.
/var/log	15 GiB	The system log files as well as application log files are located under this partition.
/var/log/audit	5 GiB	This partition contains the audit log files of the system.
/tmp	3 GiB	This partition contains temporary data used by system and applications.
/var/tmp	4 GiB	This partition contains temporary data used by system and applications.
/var/lib/libvirt	S8300: ~244 – 877.6 GiB	This partition contains the KVM (Hypervisor) data. In particular, the VM disk files are stored in the directory <code>/var/lib/libvirt/images</code>. * Note: The total available storage size may vary depending on the server hardware profile (for example, S8300E, R640/R660xs). The displayed storage for <code>/var/lib/libvirt</code> accounts for a system-reserved allocation of approximately 53.7 GiB, which is used by other system partitions.

Table continues...

Partition	Size	Notes
Swap	6 GiB	Swap partitions support virtual memory: data is written to a swap partition when there is not enough RAM to store the data your system is processing.
/opt/avaya/asp/guestinfo	~32 - 50 MiB	This partition is shared and mounted within guest virtual machines, enabling file-based communication between the host server and its guest VMs. It ranges between 32 and 50 MiB based on hardware profile.
/home	3 GiB	This partition contains the home directories of system users. For example, /home/custadm is the home directory for the custadm user. It is typically used to store user-specific data separately from system files. However, since ASP server functions as a hypervisor appliance with minimally expected user data, this partition is allocated a relatively small size.

Visual diagram: ASP 6.0.x disk partition layout

The following diagram visually represents the partition layout described in this document:

1 GiB	/boot Bootloader & kernel			
600 MiB	/boot/efi EFI for UEFI Bios			
10 GiB	/ (root) Main OS and binaries			
6 GiB	/var Variable system data			
15 GiB	/var/log System & App logs			
5 GiB	/var/log/audit Audit logs			
3 GiB	/tmp Temporary data			
4 GiB	/var/tmp Temporary data			
*3.5 TiB	/var/lib/libvirt VM images & KVM data			
6 GiB	swap Physical RAM supplement			
50 MiB	/opt/avaya/asp/guestinfo Host-guest Communications			
3 GiB	/home User Home Directories			

*Total available storage size minus ~53.7 GiB used for other system partitions. This number varies depending on the ASP R6.0.x hardware server profile.

Chapter 3: Registration

Overview

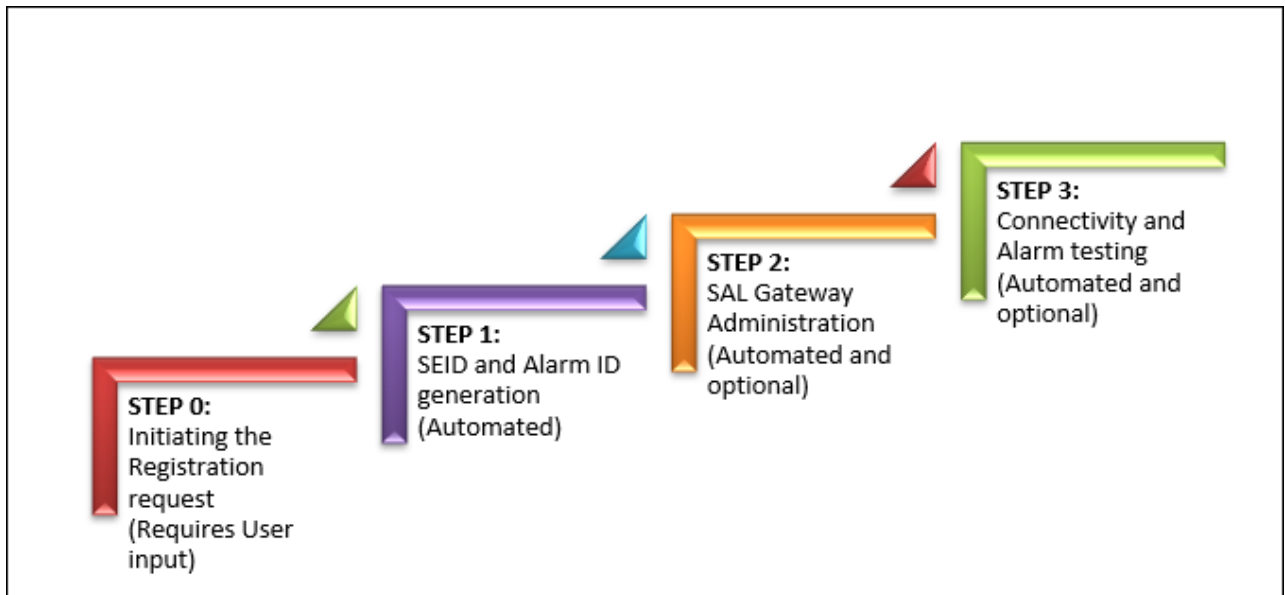
To receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in the HealthCheck tool.

End user product install base is a prerequisite for services support of S8300E. Registration establishes accurate inventory, test SAL connectivity, alarm configuration (if necessary), and ensures proper onboarding of customers into all levels of Avaya support.

For more general information on registration, see <https://support.avaya.com/registration>.

HealthCheck tool registration process

HealthCheck tool registration feature initiates Technical Onboarding that can be divided into four steps. Only the first step has to be completed by the user manually. The other three steps are automated and completed by Avaya backend.



- An Avaya user initiates the product registration request from the HealthCheck Tool.

- HealthCheck submits the registration request to Avaya backend where SEID and Alarm ID for the device is generated.
- HealthCheck portal verifies if the user has opted for SAL Administration and if the provided details are correct. SAL Administration request is then forwarded to SAL Gateway.
- HealthCheck portal verifies if Alarm testing is enabled and forwards the request to Avaya backend.
- HealthCheck Tool sends an email to the user once the request is submitted, and the request is completed with a link of the Status page on the HealthCheck Tool UI.

Registering a new device

About this task

Use this task to register and onboard a new Avaya device. For more information, refer to *HealthCheck Tool Registration Feature Description* on <https://support.avaya.com/css/public/documents/101067434>.

Before you begin

Ensure that you have the following:

- An SSO account with a valid user ID and password registered with Avaya to login.
- A Location ID (FL Number) of the device that you want to register.

 Note:

- US Sold To (functional location) location number format: 000XXXXXXX (000 + 7 digits or can be 00 + 8 digits as well).
- Outside of US (Rest of the World) FL# (Ship To) location number: 00XXXXXXX (always 00 + 8 digits).
- The install base of the device that needs to be onboarded must be created in Siebel.

 Note:

Secure Access Link Registration (also called technical onboarding) requires a verified customer install base and FL or Sold to.

- Ensure you have your IP address and host name for the KVM on RHEL host.
- Ensure that you have placed a SAP order with the Avaya Solutions Platform S8300 material codes.

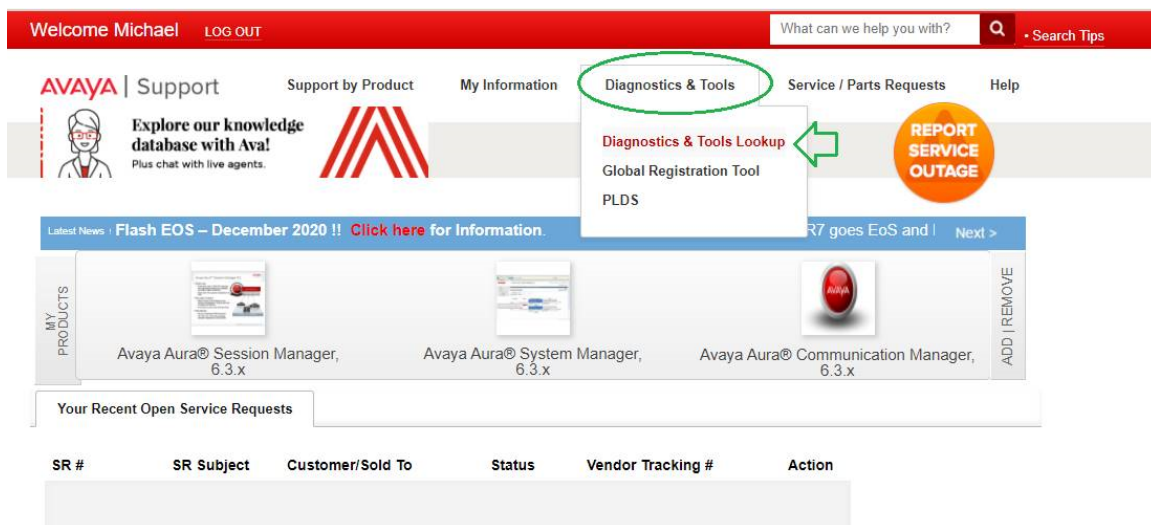
The SAP order will automatically populate Assets under the GRT **Install Base Creation**.

The ASP S8300 R6.0.x new order material codes are the following:

- 700520308 → S8300E R6 PRELOADED TAA
- 700520309 → S8300E R6 PRELOADED
- Login to the GRT install base and verify that the S8300 hardware has been added.

Procedure

1. Log on to <http://support.avaya.com>.
2. On the Home page, click **Diagnostic & Tools**.



3. Click **Diagnostic & Tools Lookup**.
4. Click **Diagnostics and Healthcheck**.
5. Click **Healthcheck**.
6. Click **Load Consolidated Dashboard**.
7. Enter the details in the **Location/Installation ID** field.
8. Click **Unregistered Assets**.
9. Find Avaya Solutions Platform S8300 asset and enter the quantity in the **Location ID** field. Click **Register**.

- Enter the details in the **S8300RHH** and **SAL Gateway** fields for the Avaya Solutions Platform S8300E.

SECODE "S8300RHH" = Redhat Host

- The RHH IP Address and Host name will need to be entered in the Healthcheck tool.
- Choose the SAL Gateway the RHH Host will be Registering to.
- When you check the "**SAL ADMIN**" box, the best practice is to also check the "**TEST CONN**" box. This will test the connectivity to the SAL Gateway you choose.

Device IP and Hostname required for both ACP and ACPEH

- Click **Submit**.
- Click **Submit** again to confirm.

You will receive an email with the Registration status.

Viewing the status of your registration request

About this task

HealthCheck portal sends email notifications to the user when the request is submitted and again when the request is completed. This email also contains the current progress of the registration request, details of the devices, and a link to the Registration Summary page of HealthCheck Tool UI.

For more information, see *HealthCheck Tool Registration Feature Description* on <https://support.avaya.com/css/public/documents/101067434>.

Procedure

To view the registration details, click **View** from the **Detailed Status** field provided in the email.

This link navigates the user to the Registration Summary page on the portal.

Technical Onboarding process

Technical Onboarding comprises of the following:

- **SAL Gateway Administration:** After you register a new device with valid SEID and Alarm ID, you must add it to a SAL Gateway as a Managed element. If there are errors or issues, Avaya Service engineers receive the alarm and can request remote access to your device to troubleshoot them.
- **Connectivity and Alarm Testing:** If there is a failure or issue with your device and device connectivity, an alarm is generated and sent to Avaya backend. Connectivity and Alarm Testing ensures that the alarm generated by the device reaches the Avaya service team for troubleshooting.

These steps are optional while you register a new device, but Avaya recommends you complete these steps at the earliest opportunity.

If you do not complete these steps while registering the device, you can still come back and complete the TOB process with the HealthCheck tool.

To administer an already registered device or to complete the Connectivity and Alarm Test, see [Using HealthCheck Tool KB article](#).

Registering device after S8300E migrates from AVP 8.1.x or ASP S8300 R5.x to ASP 6.0.x

About this task

Existing customers migrating from ASP S8300 (AVP 8.1.x or ASP R5.x) to KVM on RHEL 8.10 must use the new tracking code for SAL/Alarming connectivity but can keep the existing material codes in their Install base record.

Before you begin

Keep ASP S8300 Hardware Material code in install base.

ASP S8300 software migration to ASP S8300 R6.0.x requires ordering appropriate material codes:

- 434559 ASPS8300 AVP UPG ASP8300 R6 RHEL LIC
- 434560 ASPS8300 R5 UPG ASP8300 R6 RHEL LIC

Ordering either of the above codes triggers the following *434561 ASPS8300 R6 RHEL LIC* (not orderable, this is an entitlement) which will be present in the customer record.

Procedure

1. Offboard AVP/System Platform or S8300ESX Solution Element ID (SEID) from ASP S8300 SAL Gateway (SALGW).
2. To set S8300RHH as the Solution Element (SE) code (for KVM on RHEL Host), Technical Onboard ASP S8300 in SALGW with new tracking code:
434533 S8300 UPG to RHEL TRK
 - The new tracking code is used for SAL/Alarming after migration from AVP or from ESXi to RHEL in GRT & HealthCheck.
 - For more information on Technical Onboarding, see [Technical Onboarding process](#) on page 20.
3. Retain ASP S8300 Hardware Material codes in Install base. See codes below:
 - 700508924 S8300E Server
 - 700508955 S8300E – NON GSA

Chapter 4: Installing Avaya Solutions Platform S8300

ASP S8300 R6.0.x shipped from Avaya's integrator

ASP S8300 R6.0.x ships from Avaya's integrator pre-loaded with ASP S8300 R6.0.x (KVM on RHEL 8.10) to an Avaya customer for installation of applications.

Always refer to *PCN2174S* and *Release Notes* for any software updates.

When an ASP S8300 R6.0.x is received from Avaya's integrator, the first time it is powered on, the steps described in this document in section Steps for Installing the ASP R6.0.x KVM on the S8300 at Step 7 and 8 are similar.

Instructions for configuration of ASP S8300 R6.0.x, whether a new install or ASP S8300 received from Avaya's integrator, are the same beginning in Chapter 5.

Creating USB Flash Media Drives for an ASP R6.0.x Software Installation image

Before you begin

- Obtain 1 USB Flash drive (installation USB drive must be minimum 4 GB).
- Download latest [Rufus](#) tool onto a local Windows PC if not already installed. Do not use the Portable version of Rufus.

Latest releases:				
Link	Type	Platform	Size	Date
rufus-4.5.exe	Standard	Windows x64	1.4 MB	2024.05.22
rufus-4.5p.exe	Portable	Windows x64	1.4 MB	2024.05.22
rufus-4.5_x86.exe	Standard	Windows x86	1.5 MB	2024.05.22
rufus-4.5_arm64.exe	Standard	Windows ARM64	4.8 MB	2024.05.22

- If doing a fresh install, obtain the ASP S8300 R6.0.x Customized KVM on RHEL 8.10 ISO File `ASP_R6_all_4.6-4.8.iso`, PLDS ID: ASP000000130 and download to the local Windows PC.

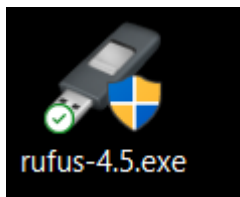
 Note:

The same image is applicable for R640, R660xs and S8300. There is a unique PLDS ID for ASP S8300 and ASP 130 which is required for tracking purposes. Always download the image from the appropriate solution.

- Always Reference *PCN2174S* and *Release Notes* for any software updates.

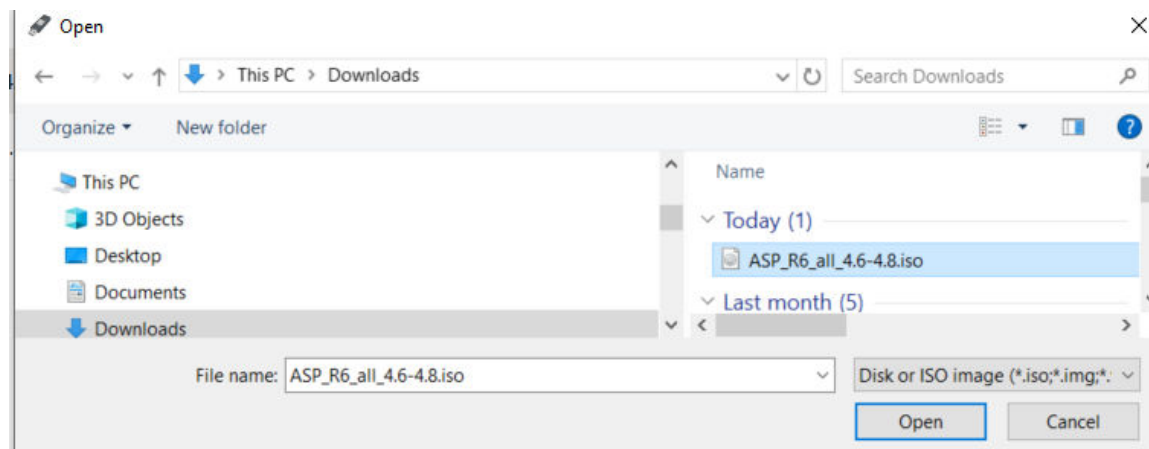
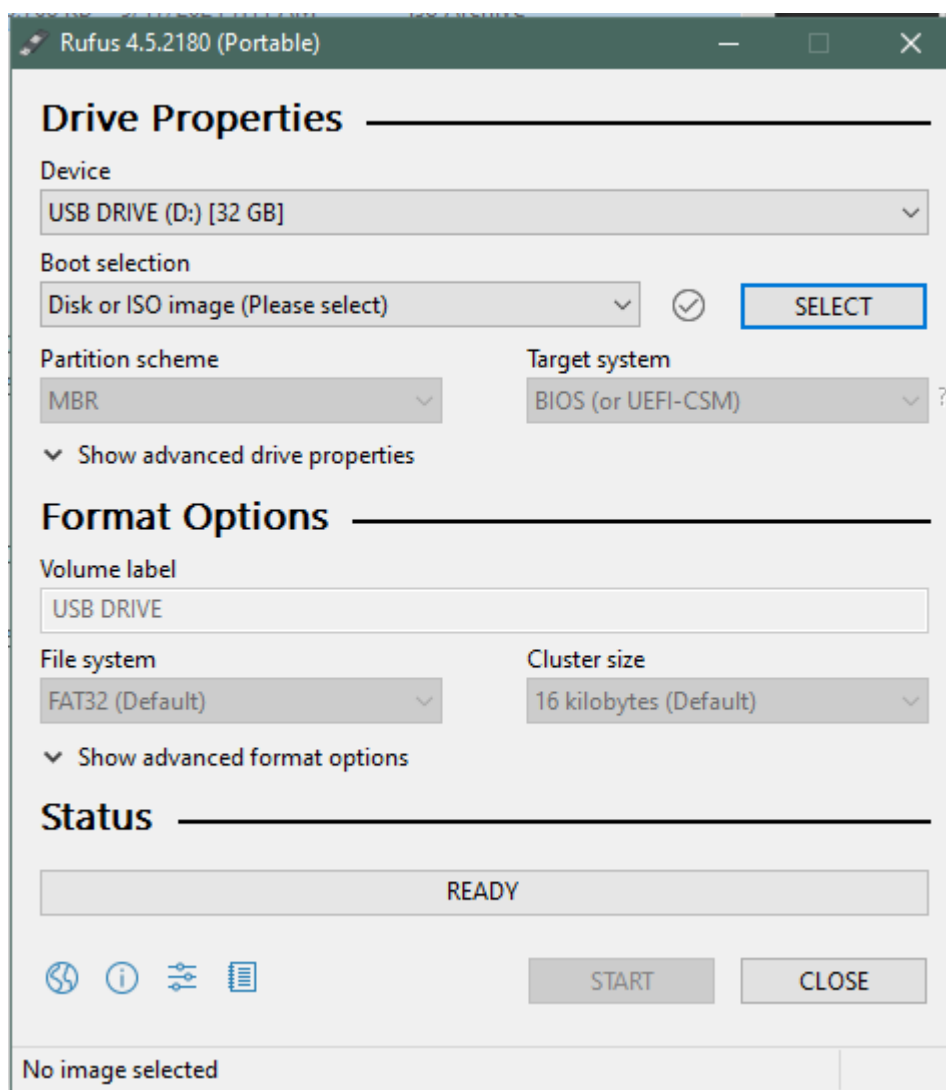
Procedure

1. Insert the 4GB or larger USB flash drive into your Windows PC where the ISO installer file was downloaded.
2. Open Rufus.



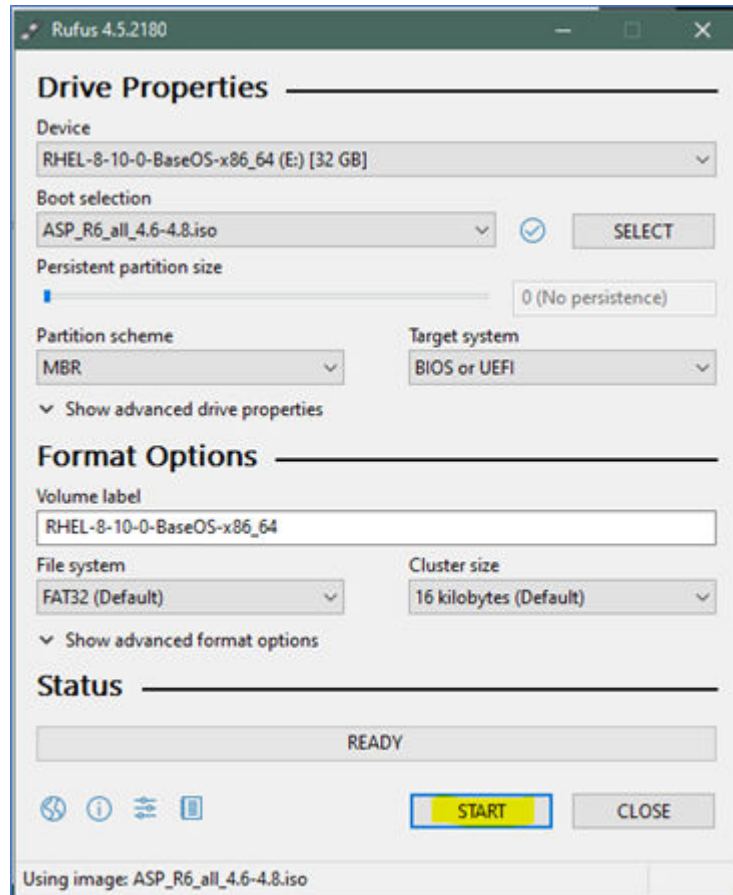
3. Select your flash drive as **Device** if not already selected.
4. Press **SELECT** and browse to the location of the ASP R6.0.x S8300 ISO installer file (reference file previously downloaded (see prerequisites above)).

5. Select that ISO file and select **Open**.



6. Rufus screen should look similar to screen shot below dependent on USB drive size. Press **START** to initiate the process. If the message box below appears after **START** selection, keep the default (Write in ISO Image mode) and press **OK**. Allow to overwrite USB jump drive if prompted.

If a message (see below) is displayed that Rufus is going to download files (`ldlinux.sys` and `ldlinux.bss`) from the internet, the user should update their version of Rufus to 4.5 or newer. If the message is still displayed, the files referenced must be downloaded. The picture below is an example showing a USB device that previously was utilized to create an image.



ISOHybrid image detected



The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode. Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it. However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

☒ Write in ISO Image mode (Recommended)

☐ Write in DD Image mode

OK

Cancel

Download required



This image uses Syslinux 6.04 but this application only includes the installation files for Syslinux 6.04/pre1.

As new versions of Syslinux are not compatible with one another, and it wouldn't be possible for Rufus to include them all, two additional files must be downloaded from the Internet ('ldlinux.sys' and 'ldlinux.bss'):

- Select 'Yes' to connect to the Internet and download these files
- Select 'No' to cancel the operation

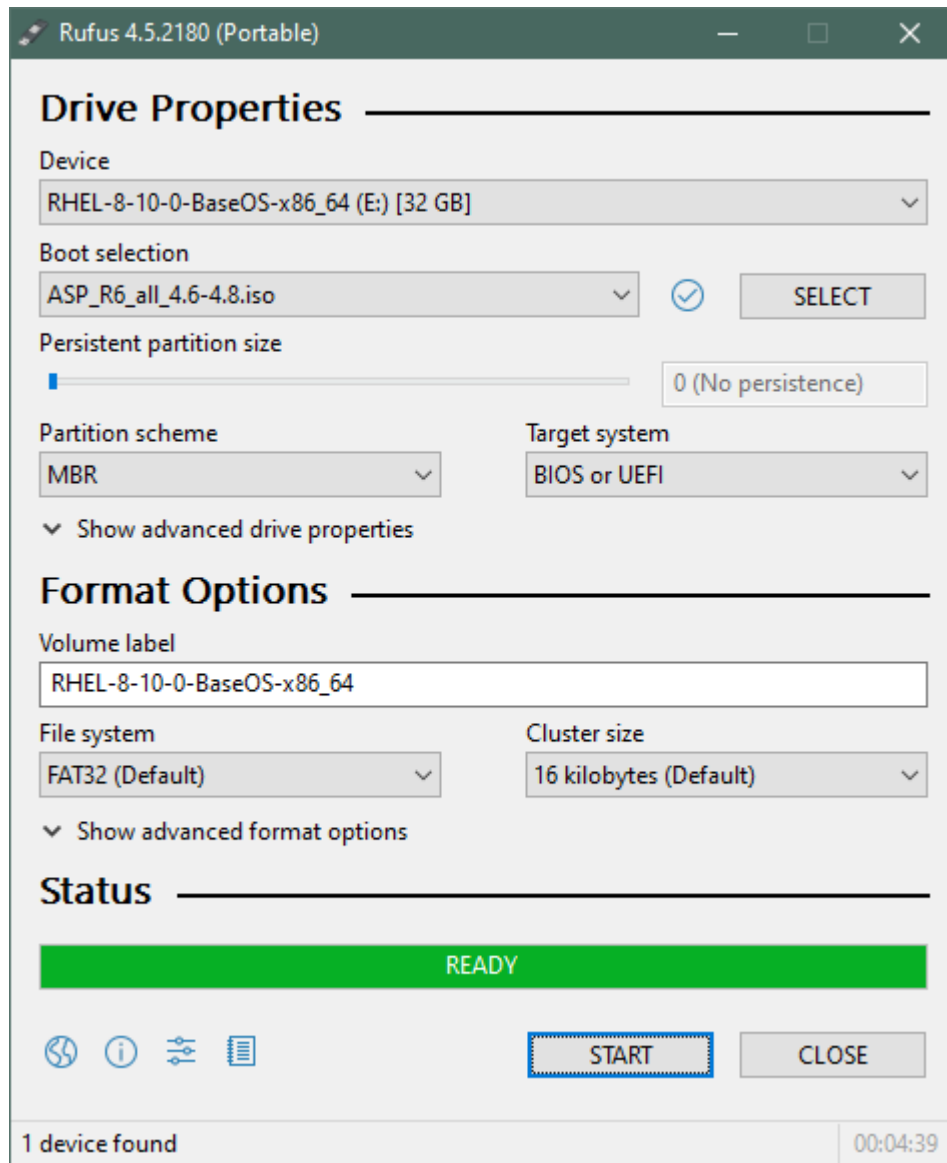
Note: The files will be downloaded in the current application directory and will be reused automatically if present.

Yes

No

7. When the process has completed and Status shows READY, Rufus should be closed, and the Flash drive ejected from the computer. This jump drive now has the ASP R6

Software installation media copied to it. Place a label on the drive designating it as ASP R6 Software Installation Media.



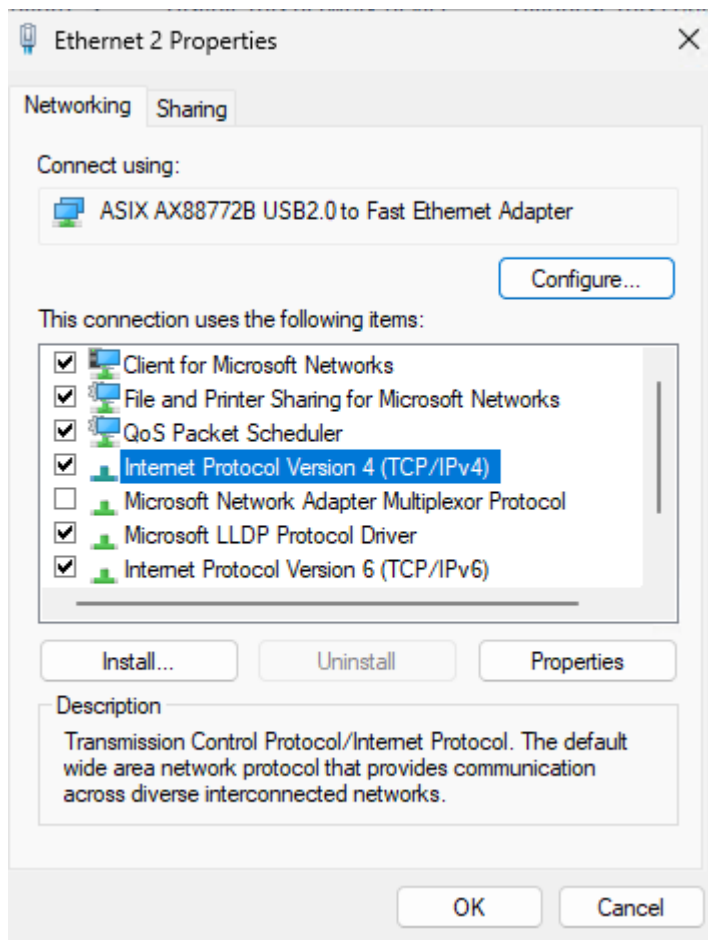
Steps for installing the ASP R6.0.x KVM on the S8300

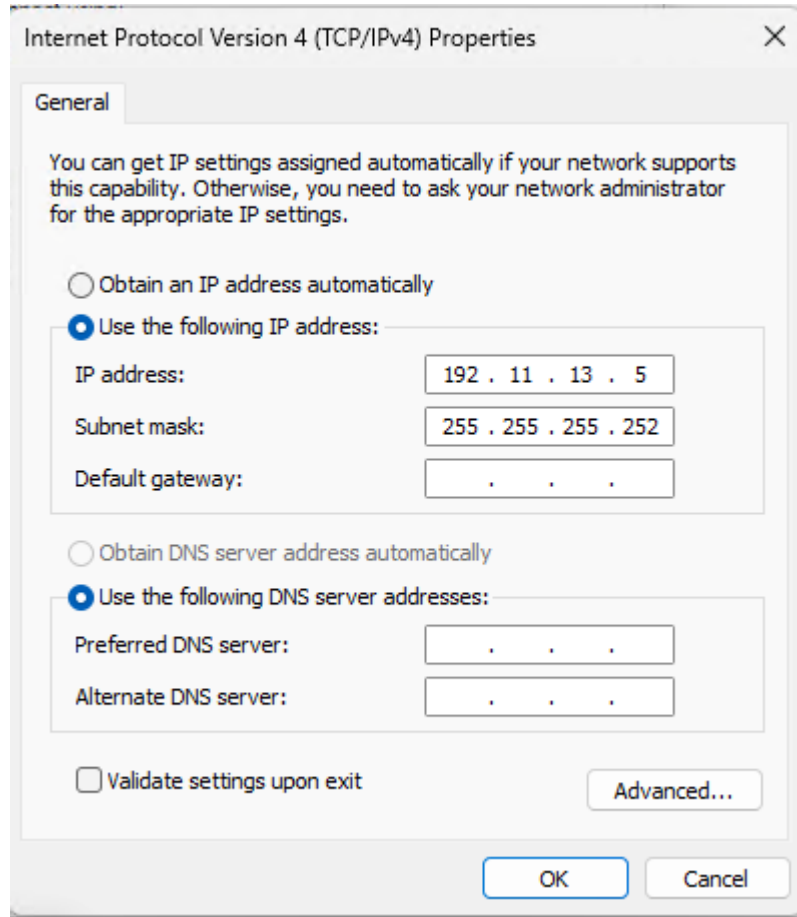
Before you begin

- A PC or a laptop with an available Ethernet port.
- One available routable IP address. This is the same IP address that you use later in the installation.

Procedure

1. Configure a PC network connection to be used for the Services port with the IP address 192.11.13.5 and netmask 255.255.255.252 using the Ethernet port properties menu for IPv4.





2. Unseat (remove) the S8300 board from the gateway.
3. Refer to the image below. Insert the USB ASP R6 KVM Installation Media in the USB1 port on the S8300 front panel. Connect the S8300 Ethernet Services port to the PC. During the installation process do not disconnect the Ethernet cable.



4. On the PC, start a Command Window (search for `cmd`) and run the command: `ping -n 1000 192.11.13.6`.
5. Insert the S8300 board in the gateway. Ensure that the board is properly seated. The ALARM LED becomes solid and then in approximately 30 seconds it starts to flash. Initially, the **ping** fails and after 2-3 minutes it starts to respond while the software is installing:

```
C:\Users\admin>ping -n 1000 192.11.13.6

Pinging 192.11.13.6 with 32 bytes of data:
Reply from 192.11.13.5: Destination host unreachable
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
```

6. After approximately 8 minutes, the LED lights turn on and off sequentially in the following order: ALM LED → APP LED → ACT LED → 'OK TO REMOVE' LED. Each LED turns on and off within 1 second, and the process takes approximately 4 to 5 seconds to complete. However, ALM LED turns on and off within 1 second and ALM LED continues to blink for a few more seconds. After the LED sequence turns on and off in the above order, all LEDs are off. After a few seconds, the 'OK TO REMOVE' LED turns on to indicate that the software was copied into the internal disk of the S8300 and the S8300 was powered off. At the same time, the **ping** fails again.

```
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Request timed out.
Reply from 192.11.13.5: Destination host unreachable
Request timed out.
Request timed out.
Request timed out.
```

7. Now you can pull the S8300 board, extract the USB drive and reinsert the board, keep the ethernet cable connected. Restart the **ping** command on the PC. When S8300 boots, the ALARM LED becomes solid and then flashes. After approximately 30 seconds, the LED lights turn on and off sequentially in the following order - ALM LED -> APP LED -> ACT LED -> OK TO REMOVE LED. Each LED turns on and off within 1 second, and the process takes approximately 4 to 5 seconds to complete. However, ALM LED turns on and off within 1 second and ALM LED continues to blink for a few more seconds. After the LED sequence turns on and off in the above order, all LED are now off.
8. You will notice the **ping** starts again. Do not login now since the S8300 will perform a second reboot to complete the setup. The **ping** then fails and restarts as the S8300 reboots.
9. On the second boot, the LEDs behavior is the same as the first boot in step 7.

 Note:

Step 7 above is the same LED behavior seen on a pre-loaded ASP S8300 R6.0.x when it is inserted into the G4X0 and powered on at the customer site for the first time.

Follow the same instructions for accessing the services port as described on a new installation.

```
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Reply from 192.11.13.5: Destination host unreachable
Request timed out.
Request timed out.
Request timed out.
Request timed out
Request timed out
Request timed out
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
Reply from 192.11.13.6: bytes=32 time<1ms TTL=64
```

10. You can stop the **ping** command.

Chapter 5: Configuration of ASP S8300 R6.0.x

Configuring ASP S8300 R6.0.x

Procedure

1. Start an **SSH** session to 192.11.13.6. Login using the credentials: `custadm/ACP130_pw`. At your first login, you are prompted to change the default password and when successful the connection drops, and you need to connect and login again with the new password.

```
C:\Users\admin>ssh -l custadm 192.11.13.6
```

```
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.
```

```
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.
```

```
All users must comply with all corporate instructions regarding the protection of information assets.
```

```
custadm@192.11.13.6's password:
```

```
You are required to change your password immediately (administrator enforced)
```

```
Activate the web console with: systemctl enable --now cockpit.socket
```

```
WARNING: Your password has expired.
```

```
You must change your password now and login again!
```

```
Changing password for user custadm.
```

```
Current password:
```

```
New password:
```

```
Retype new password: |
```

2. After the new login as `custadm` with the new password, read and accept the EULA. (After the EULA is accepted, the Red Hat cockpit Web UI is accessible from the PC connected to the services port using the URL `https://192.11.13.6:9090`). After the EULA is

accepted, you are asked if you want to enable EASG. Avaya highly recommends that EASG be enabled to facilitate expedient troubleshooting.

```
*****
Do you accept the agreement (Y or N)?
*****
> y
Avaya EULA accepted.

===== Enhanced Access Security Gateway (EASG) =====

Enable: (Recommended)
  By enabling Avaya Logins you are granting Avaya access to your system.
  This is necessary to maximize the performance and value of your Avaya
  support entitlements, allowing Avaya to resolve product issues in a
  timely manner.

  In addition to enabling the Avaya Logins, this product should be
  registered with Avaya and technically onboarded for remote connectivity
  and alarming. Please see the Avaya support site
  (support.avaya.com/registration) for additional information for
  registering products and establishing remote access and alarming.

Disable:
  By disabling Avaya Logins you are preventing Avaya access to your system.
  This is not recommended, as it impacts Avaya's ability to provide support
  for the product. Unless the customer is well versed in managing the
  product themselves, Avaya Logins should not be disabled.

Do you want to Enable EASG? (yes/no) |
```

3. Configure a new password for the root account, followed by time zone.

```
==== You must configure a new root password ====
The prompt below will ask you to enter new password for the root account.
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Make sure to remember the new password for root account that you have configured.

Time zone: America/New_York (EDT, -0400)
Keep this timezone (y/n) |
```

If the wrong time zone is selected, answer `n` to the question to keep this time zone and follow the prompts again.

4. Next you will be prompted to configure a hostname, IP address, default gateway, and DNS server. Later you can use the `configNetwork` command to change values. After an IP address is configured, the Cockpit Web UI is accessible from any other machine on the

network using the IP address configured and port 9090. For example, `https://<KVM host IP Address>:9090`

*** Note:**

The default VLAN (1) is usually correct, but it can be configured on the gateway to any other value by entering a different vlan interface and issuing the `icc-vlan` or `server-blade-vlan` command on the Media Gateway (G4X0). Make sure the VLAN matches the gateway configuration by running `show icc-vlan` on the G430 or `show server-blade-vlan` on the G450.

```
===== Server Network Configuration =====
Note: you should run this command from the console or services port
      After making configuration changes running VMs should be restarted.

Do you want to continue (y/n) y

The configured or default value is displayed in parentheses ().
Press 'enter' to accept it, enter 'd' to delete it or type a new value.

Connect this server to an Out Of Band Management network (OOBM)? y/n (n)
Create an OOBM bridge for VMs use? y/n (n) y
Enter VLAN ID for the Management/VM's network (1):
Do you want to configure a OOB VLAN? y/n (n)
Enter Server hostname (asp-s8300): asp-s8300-43.dr.avaya.com
Enter Server IPv4 (169.254.181.67): 135.0.0.43
Enter Server netmask or /prefix (/16): /24
Enter the IPv4 default gateway (): 135.0.0.254
Do you want to configure IPv6? y/n (n)
Enter comma separated DNS servers (): 108.100.8.11
Enter comma separated IPv4 domain search (): dr.avaya.com
Continue with these values? y=continue/n=retry/q=quit (n) y

Bridge bridge0: initialization successful
Bridge slave port enp2s0.1 on bridge0: initialization successful
Bridge bridge00B: initialization successful
Bridge slave port enp3s0 on bridge00B: initialization successful
Bridge bridge0: IP initialization successful.
Bridge bridge00B: IP initialization successful.
[custadm@asp-s8300 ~]$ |
```

5. Run the command `ip addr` and verify your network information is correct. An active network link needs to be connected for IP information to display.

```

root@asp130-s8300-156b:~#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 90:fb:5b:88:23:98 brd ff:ff:ff:ff:ff:ff
    inet 192.11.13.6/30 brd 192.11.13.7 scope global noprefixroute enp1s0
        valid_lft forever preferred_lft forever
    inet6 fe80::92fb:5bff:fe88:2398/64 scope link
        valid_lft forever preferred_lft forever
3: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 90:fb:5b:88:23:99 brd ff:ff:ff:ff:ff:ff
4: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 90:fb:5b:88:23:9a brd ff:ff:ff:ff:ff:ff
5: enp2s0.4093@enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 90:fb:5b:88:23:99 brd ff:ff:ff:ff:ff:ff
    inet 169.254.1.31/24 brd 169.254.1.255 scope link noprefixroute enp2s0.4093
        valid_lft forever preferred_lft forever
    inet6 fe80::943a:45fe:7942:7a32/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
6: bridge0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 90:fb:5b:88:23:99 brd ff:ff:ff:ff:ff:ff
    inet [REDACTED] brd 10.133.100.255 scope global noprefixroute bridge0
        valid_lft forever preferred_lft forever
7: enp2s0.1@enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master bridge0 state UP group default qlen 1000
    link/ether 90:fb:5b:88:23:99 brd ff:ff:ff:ff:ff:ff
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#
[root@asp130-s8300-156b ~]#

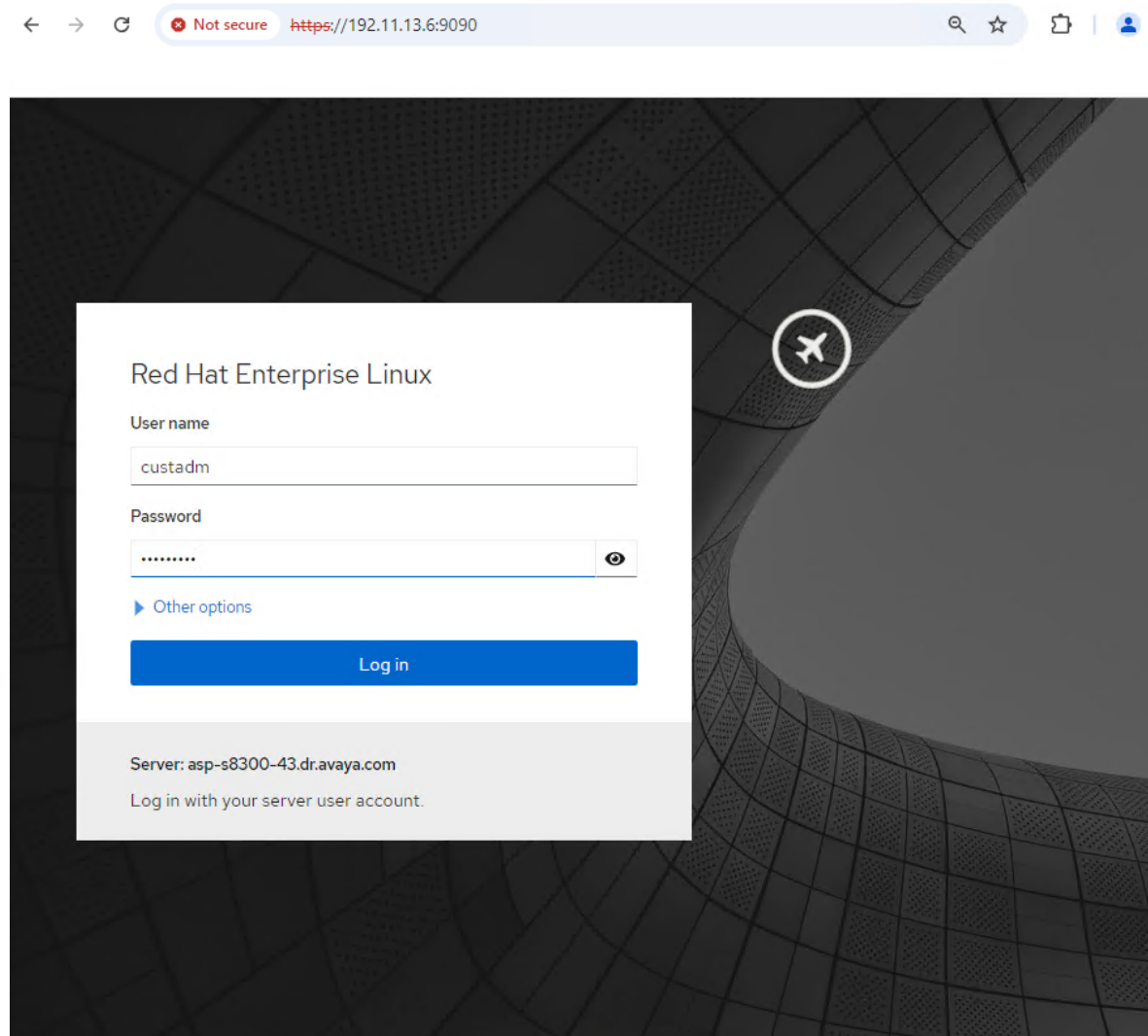
```

*** Note:**

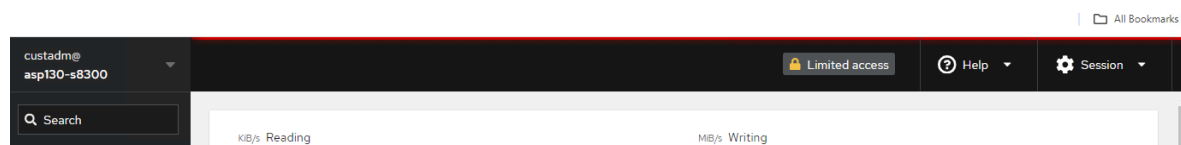
Other CLI verification commands can be executed such as `swversion`, `ifconfig`, or `netstat -nr`.

6. Login to the Cockpit Web UI by opening a browser and enter the IP address you assigned to as Server IPv4 and append port 9090 to it (`https://<KVM host IP Address>:9090`). Login and verify system parameters. Login using credentials: `custadm`

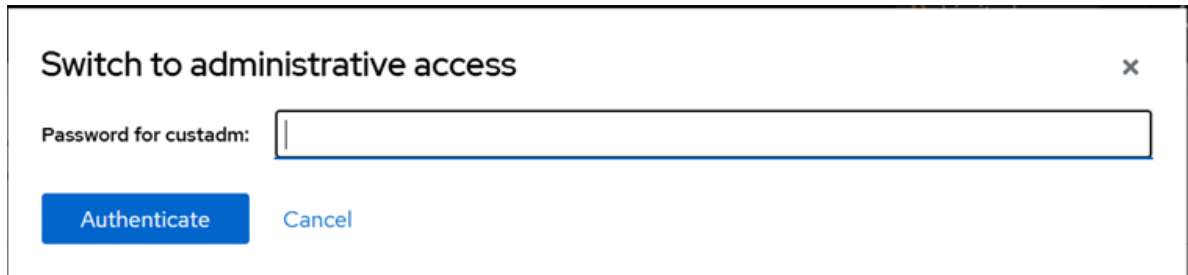
and your chosen password. The picture below is accessing the Cockpit Web UI using the services port (192.11.13.6:9090).



7. Once logged in, view the Overview page and additional tabs for configuration verification. Additional configuration can be performed from this interface.
8. For administration actions you need to click on the button labeled **Limited access**.



9. Enter the password for `custadm` at the message box and click **Authenticate**.

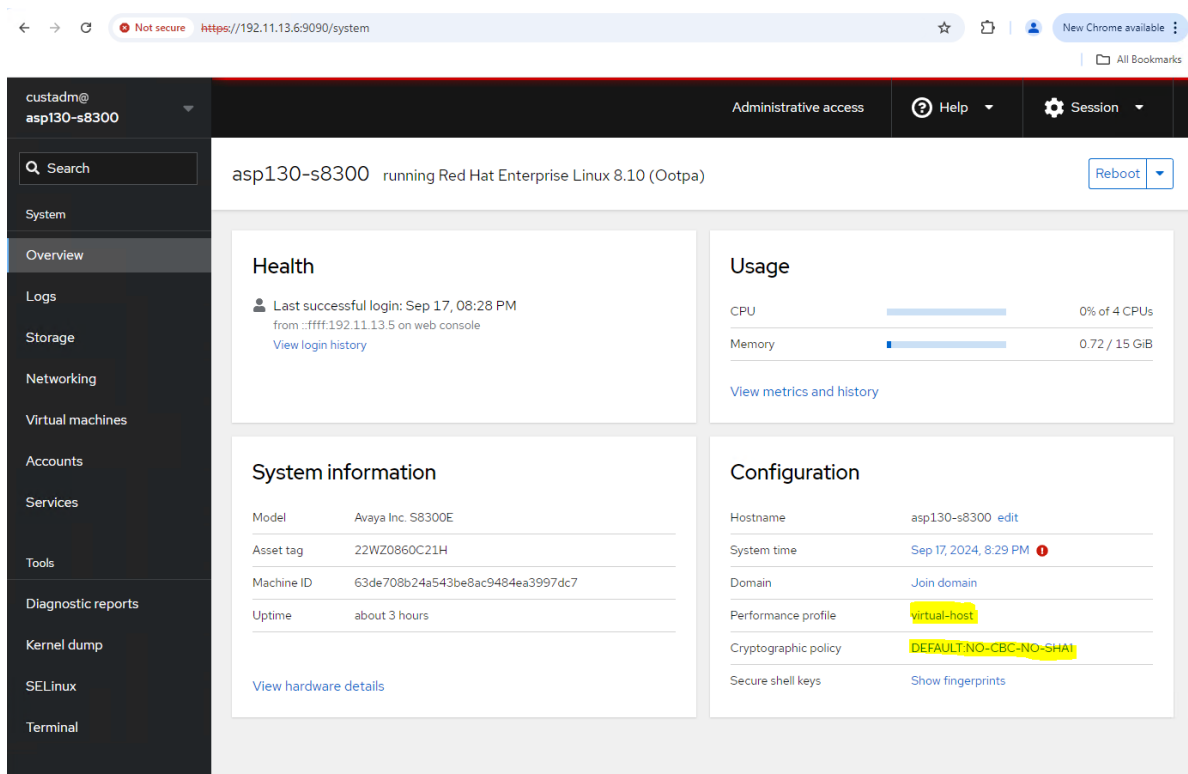


A dialog box titled "Switch to administrative access" with a close button (X) in the top right corner. It contains a label "Password for custadm:" followed by a text input field. Below the input field are two buttons: "Authenticate" (blue) and "Cancel" (light blue).

Note:

Administrative access means root equivalent access. Be careful with what you do.

10. Verify that the Performance profile and the Cryptographic policy matches the image below. This indicates that the installation completed successfully.



A screenshot of the Cockpit web interface for a system named `asp130-s8300` running Red Hat Enterprise Linux 8.10 (Ootpa). The interface shows administrative access and includes a sidebar with navigation options like System, Overview, Logs, Storage, Networking, Virtual machines, Accounts, Services, Tools, Diagnostic reports, Kernel dump, SELinux, and Terminal. The main content area displays system health, usage, and configuration details.

Health	
Last successful login:	Sep 17, 08:28 PM
from:	ffff:192.11.13.5 on web console
View login history	

Usage	
CPU	0% of 4 CPUs
Memory	0.72 / 15 GiB
View metrics and history	

System information	
Model	Avaya Inc. S8300E
Asset tag	22WZ0860C21H
Machine ID	63de708b24a543be8ac9484ea3997dc7
Uptime	about 3 hours
View hardware details	

Configuration	
Hostname	asp130-s8300 edit
System time	Sep 17, 2024, 8:29 PM ⚠
Domain	Join domain
Performance profile	virtual-host
Cryptographic policy	DEFAULT:NO-CBC:NO-SHA1
Secure shell keys	Show fingerprints

Cockpit is now available for additional configuration and deployment of VMs.

11. Configure NTP server by clicking on the value of the **System time** field (Turn on administrative access). In the **Set time** field, change the combo box to “Automatically using additional NTP servers”. A new field for NTP server is shown.

The system defaults to the RHEL 8 default NTP pool configuration. But those often do not work from within customers’ networks and it is considered a best practice to have the hosts configured to an authoritative time (NTP) server. For security reasons, Avaya recommends

synchronizing the clock with a time server that is located on the management network (Customer private network) rather than directly with a time server on a public network.

Change system time

Time zone: America/Denver

Set time: Automatically using additional NTP servers

NTP server: [+] [×]

[Change] [Cancel]

12. Enter either the IP Address or FQDN (DNS required) of the NTP server (example: `time.abc.com`) and click **Change**. The system time should get synchronized after a few minutes.
13. The hostname (along with domain) can be also changed by clicking on **Edit** beside the **Hostname** field in the Overview page. Enter the hostname (along with domain) in the **Real host name** field and click **Change**. The **Pretty host name** field can be left blank.

Change host name [×]

Pretty host name: []

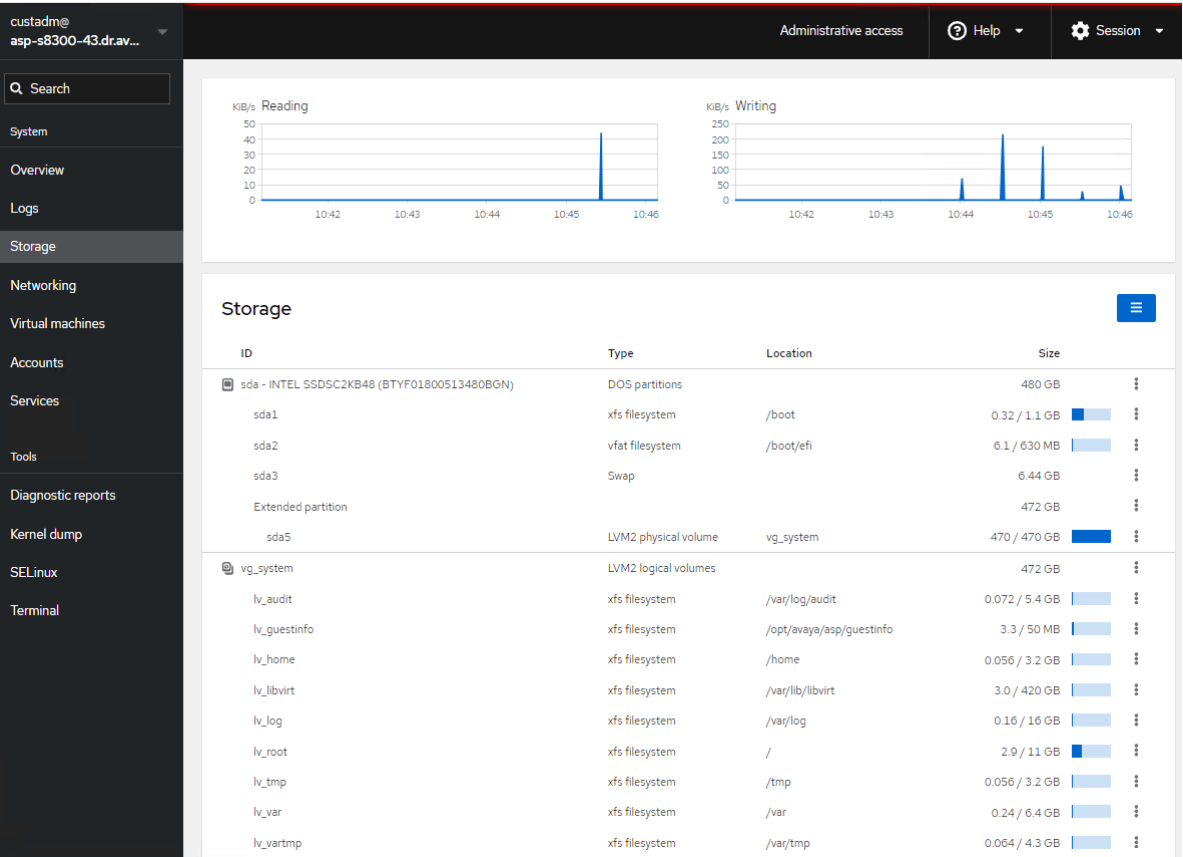
Real host name: asp-s8300.dr.avaya.com

[Change] [Cancel]

14. The screen shot below shows the partition where virtual machines should be deployed (`/var/lib/libvirt`). Within this partition a directory, `/var/lib/libvirt/images` is created and is intended to store the VM disk images that will be used for VM deployment.

*** Note:**

The sda5 LVM2 physical volume is fully allocated for volumes, the cockpit shows the allocated and not the used space so it is normal that it appears to be full.



15. The following sda2 warning (yellow triangle) can be ignored if it matches the message shown below. Any other warnings MUST be investigated. Reach out to Avaya Services if necessary.

Storage > sda - DELL PERC H755 Front (00262070a5a862f42d00118b6f80e04e) > sda2

Partition

This partition is not completely used by its content.
Partition size is 1.07 GB. Content size is 1.07 GB.

[Shrink partition](#) [Grow content](#)

Name -

UUID befcc3b-9640-439b-834a-b1f98f7c14cd

Type Linux filesystem data [edit](#)

xfs filesystem [Unmount](#)

Name - [edit](#)

Mount point /boot (stop boot on failure, nodev, nosuid, noexec) [edit](#)

Usage 0.32 / 1.1 GB

 Note:

Do not attempt to shrink or grow the disk volumes.

Additional configuration options

The following commands can be executed as `custadm` or `root` from the CLI after the initial configuration to modify default KVM on RHEL settings:

- `setMaxLoginSessions` – set max number of login sessions for any user (default 5).
- `setSessionsTimeout` – set the idle timeout on bash and cockpit (default 10 minutes).
- `setTimezone` – to change timezone.

Configuring SNMP on KVM on RHEL 8.10

SNMP overview

Configuring SNMP allows monitoring of system performance and resources by enabling network devices to send management data to SNMP-enabled servers.

ASP S8300 must be on R6.0.0.1.1 or later for SNMP configuration.

This section provides steps to configure the supported SNMP versions for the Avaya Solutions Platform KVM on RHEL 8.10 hypervisor.

 Caution:

The RHEL OS provides a default script for configuring SNMP, named `snmpconf`. However, this script does not include all the customizations applied by the Avaya `configSnmp` script. Therefore, the RHEL `snmpconf` script *must not* be used when configuring SNMP on KVM on RHEL 8.10.

Using the default RHEL `snmpconf` script could potentially overwrite or remove the custom configurations applied by the Avaya `configSnmp` script, preventing future usage of it. To ensure proper SNMP configuration, only the Avaya `configSnmp` script must be used.

Configuring SNMP v3 on a KVM on RHEL 8.10

About this task

The SNMP v3 feature is available on KVM on RHEL 8.10. This section provides steps for configuring the more secure SNMP version.

Examples below may reference ASP 130 but you see similar output for ASP S8300.

*** Note:**

The SAL GW does not support Engine ID info exchange, configuring that function has been omitted from this section. For details on creating/supporting Engine ID with other NMS devices, please refer to the following Red Hat KB article:

[24.6.3. Configuring Net-SNMP | Red Hat Product Documentation](#)

*** Note:**

Although KVM on RHEL 8.10 supports MD5 and DES for authentication protocol and privacy protocol, these are considered weak, thus vulnerable. Avaya strongly recommends using SHA-224 (or higher when possible) & AES instead.

Before you begin

Ensure that the SSH functionality is enabled on KVM on RHEL 8.10.

ASP S8300 must be on R6.0.0.1.1 for SNMP configuration.

Procedure

1. From a Putty session, using SSH, access the KVM on RHEL host. Authenticate using the custadm credentials.
2. Execute the Avaya `configSnmp` script and follow the prompt to complete the following fields:
 - System Location (optional): For example, Thornton (could be a site location name, city name, etc.)
 - System contact and email: For example, John Kennedy
jkennedy@yourdomain.com
 - System description (optional): For example, Avaya ASP 130 R6.0.x - (host FQDN)
 - Do you want to enable SNMPv1/SNMPv2c access? y/n: n
 - Do you want to enable SNMPv3 access? y/n: y
 - Do you want to add/change an SNMPv3 user y/n: y
 - Enter the SNMPv3 username, for example: Test1v3
 - Enter the index of the authentication hash type: (0=SHA, 1=SHA-224, etc...) e.g. 1

*** Note:**

SHA/SHA1 is considered deprecated and, therefore, vulnerable to security scanners.

- Enter the Authentication PassPhrase, for example: avaya123

*** Note:**

This field is mandatory and requires a minimum of 8 characters.

- Re-enter the Authentication PassPhrase, for example: avaya123

- Enter the index of the Encryption algorithm: (0=AES, 1= AES-192, etc...) e.g. 0
- Enter the Encryption PassPhrase, for example: avaya123

*** Note:**

This field is mandatory and requires a minimum of 8 characters.

- Re-enter the Encryption PassPhrase, for example: avaya123
- Do you want to add/change an SNMPv3 user y/n (optional): n

*** Note:**

In this example, a single SNMPv3 will be configured but multiple users can be configured at the same time.

- Do you want to add SNMPv1 trap receivers? y/n: (n) n
- Do you want to add SNMPv2c trap2 receivers? y/n: (n) n
- Do you want to add SNMPv2c inform receivers? y/n: (n) n
- Do you want to add SNMPv3 trap receivers? y/n: (n) y

System will display Existing SNMPv3 users previously created e.g: Test1v3

- Enter the IP/FQDN of the host receiving the traps: e.g. 192.168.10.254
- Enter the optional host port where to send the traps: 162 is the default value and will be used in this example.
- Do you want to add another SNMPv3 trap receiver? y/n (optional): n

*** Note:**

In this example a single trap receiver will be configured, however, multiple trap receivers can be configured at the same time.

- Do you want to add SNMPv3 inform receivers? y/n: (n) (optional)

*** Note:**

In this example inform receivers are not configured. SNMP inform traps require the SNMP manager (NMS Tool) to send an acknowledgment that it received the inform trap (get-response), therefore providing more reliability. If the manager does not acknowledge the inform trap, the agent will retry sending the inform trap a certain number of times. Both inform trap and snmp trap carry the same information.

ASP130 output example:

```
[root@asp130-r660xs-a31-8HHD ~]# configSnmp
Note: The configured or default value is displayed in parentheses ().
Press 'Enter' to accept it, or type a new value.
Enter the system location: () Thornton
Enter the system contact and email: () John Kennedy jkennedy@yourdomain.com
Enter the system description: (Avaya ASP 130 R6) Avaya ASP 130 R6.0.x - asp130-
r660xs-a31-8HHD.acp.avaya.com
Do you want to enable SNMPv1/SNMPv2c access? y/n: (n) n
Do you want to enable SNMPv3 access? y/n: y
```

```

Do you want to add/change an SNMPv3 user y/n: (n) y
Enter the SNMPv3 username: ( ) Testlv3
  0) SHA
  1) SHA-224
  2) SHA-256
  3) SHA-384
  4) SHA-512
  5) MD5
Enter the index of the authentication hash type: (0=SHA) 1
Enter the Authentication PassPhrase:
Re-Enter the Authentication PassPhrase:
  0) AES
  1) AES-192
  2) AES-256
  3) DES
Enter the index of the Encryption algorithm: (0=AES) 0
Enter the Encryption PassPhrase:
Re-Enter the Encryption PassPhrase:
Do you want to add/change an SNMPv3 user y/n: (n) n
Do you want to add SNMPv1 trap receivers? y/n: (n) n
Do you want to add another SNMPv2c trap2 receiver? y/n: (n) n
Do you want to add SNMPv2c inform receivers? y/n: (n) n
Do you want to add SNMPv3 trap receivers? y/n: (n) y
Existing SNMPv3 users: Testlv3
Enter the IP/FQDN of the host receiving the traps: 192.168.10.254
Enter the optional host port where to send the traps: (162)
Do you want to add another SNMPv3 trap receiver? y/n: (n) n
Do you want to add SNMPv3 inform receivers? y/n: (n) n
[root@asp130-r660xs-a31-8HHD ~]#

```

3. (Optional) Verify snmpd service status:

- `systemctl status snmpd`

ASP130 Output Example:

```

[root@asp130-r660xs-a31-8HHD ~]# systemctl status snmpd
• snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2025-03-21 14:10:44 MDT; 18min ago
     Process: 142066 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
    Main PID: 141140 (snmpd)
       Tasks: 1 (limit: 1643572)
      Memory: 7.2M
      CGroup: /system.slice/snmpd.service
              └─141140 /usr/sbin/snmpd -LS0-6d -f
Mar 21 14:10:44 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
Mar 21 14:10:44 asp130-r660xs-a31-8HHD.acp.avaya.com snmpd[141140]: NET-SNMP version 5.8
Mar 21 14:10:44 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
Mar 21 14:19:19 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Reloading Simple Network Management Protocol (SNMP) Daemon..
Mar 21 14:19:19 asp130-r660xs-a31-8HHD.acp.avaya.com snmpd[141140]: Reconfiguring daemon
Mar 21 14:19:19 asp130-r660xs-a31-8HHD.acp.avaya.com snmpd[141140]: NET-SNMP version 5.8 restarted
Mar 21 14:19:19 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Reloaded Simple Network Management Protocol (SNMP) Daemon..

```

4. Retrieve SNMP Engine ID:

- `sudo cat /var/lib/net-snmp/snmpd.conf | grep EngineID`

ASP130 Output Example:

```
[custadm@asp130-r660xs-a31-8HHD ~]$ sudo cat /var/lib/net-snmp/snmpd.conf | grep EngineID
[sudo] password for custadm:
oldEngineID 0x80001f8880c589fb4c72f08f6700000000
```

5. Generate a SNMPv3 test trap:

```
snmptrap -v3 -u <SNMPv3_user_created> -l authPriv -a SHA -A <authpassphrase> -x AES -X <privpassphrase> 192.168.10.254 ' ' SNMPv2-MIB::sysName sysName.0 s "SNMPv3 test trap from RHEL 8.10"
```

Example:

```
snmptrap -v3 -u testlv3 -l authPriv -a SHA -A avaya123 -x AES -X avaya123 10.129.209.21 ' ' SNMPv2-MIB::sysName sysName.0 s "SNMPv3 test trap from RHEL 8.10"
```

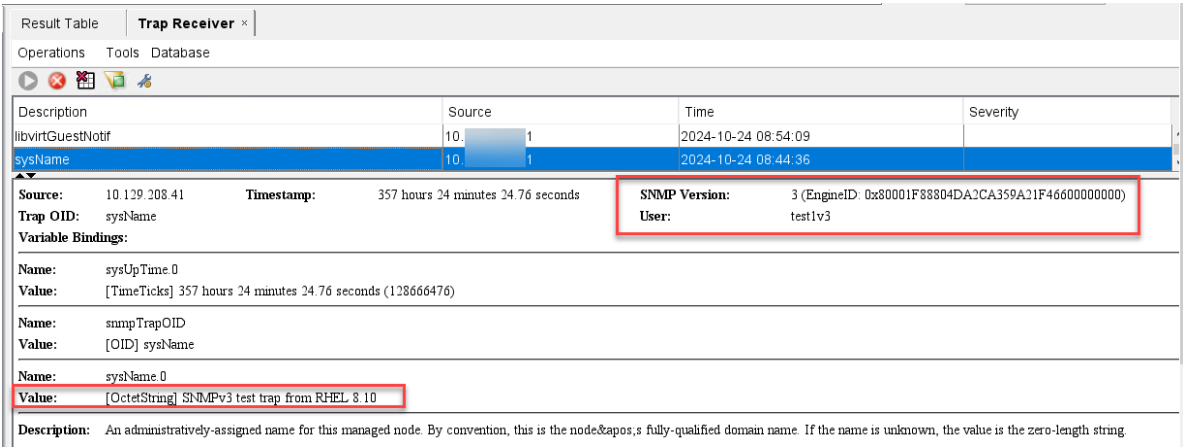


Figure 5: Trap View from NMS Tool – Use for Example Only

Configuring SNMP v2 on RHEL 8.10

About this task

The SNMP v2 feature is available on KVM on RHEL 8.10. This section provides steps for configuring the less secure SNMP version.

Examples below may reference ASP 130 but you see similar output for ASP S8300.

* Note:

To align with security best practices, when possible, Avaya strongly recommends configuring SNMPv3 instead of SNMPv2/v1.

Before you begin

Ensure that the SSH functionality is enabled on KVM on RHEL 8.10.

ASP S8300 must be on R6.0.0.1.1 for SNMP configuration.

Procedure

1. From a Putty session, using SSH, access the KVM on RHEL host. Authenticate using the custadm credentials.

2. Execute the Avaya `configSnmp` script and follow the prompt to complete the following fields:

- System Location (optional): For example, `Thornton` (could be a site location name, city name, etc.)
- System contact and email: For example, `John Kennedy`
`jkennedy@yourdomain.com`
- System description (optional): For example, `Avaya ASP 130 R6.0.x - (host FQDN)`
- Do you want to enable SNMPv1/SNMPv2c access? y/n: `y`
- Enter the Read-Only community string: (): For example, `avaya123`
- Do you want to enable SNMPv3 access? y/n: `n`

*** Note:**

In this example, only SNMPv2 will be configured, however SNMPv3 can be configured at the same time if required.

- Do you want to add SNMPv1 trap receivers? y/n: (n) `n`

*** Note:**

In this example, only SNMPv2 will be configured, however SNMPv1 can be configured at the same time if required.

- Do you want to add SNMPv2c trap2 receivers? y/n: (n) `y`
- Enter the IP/FQDN of the host receiving the trap2s: `192.168.10.254`
- Enter the optional community to be included: `avaya123`
- Enter the optional host port where to send the trap2s: (162) `162`
- Do you want to add another SNMPv2c trap2 receiver? y/n: (n) `n`

*** Note:**

In this example a single trap receiver will be configured, however, multiple trap receivers can be configured at the same time.

- Do you want to add SNMPv2c inform receivers? y/n: (n) `n`

*** Note:**

In this example inform receivers are not configured. SNMP inform traps require the SNMP manager (NMS Tool) to send an acknowledgment that it received the inform trap (get-response), therefore providing more reliability. If the manager does not acknowledge the inform trap, the agent will retry sending the inform trap a certain number of times. Both inform traps and snmp traps carry over the same information.

- Do you want to add SNMPv3 trap receivers? y/n: (n) `n`

- Do you want to add SNMPv3 inform receivers? y/n: (n) **n**

Output example:

```
[root@asp130-r660xs-a31-8HHD ~]# configSnmp
Note: The configured or default value is displayed in parentheses ().
Press 'Enter' to accept it, or type a new value.
Enter the system location: ( ) Thornton
Enter the system contact and email: ( ) John Kennedy jkennedy@yourdomain.com
Enter the system description: (Avaya ASP 130 R6) Avaya ASP 130 R6.0.x - asp130-r660xs-a31-8HHD.acp.avaya.com
Do you want to enable SNMPv1/SNMPv2c access? y/n: (n) y
Enter the Read-Only community string: ( ) avaya123
Do you want to enable SNMPv3 access? y/n: n
Do you want to add SNMPv1 trap receivers? y/n: (n) n
Do you want to add SNMPv2c trap2 receivers? y/n: (n) y
Enter the IP/FQDN of the host receiving the trap2s: 192.168.10.254
Enter the optional community to be included: avaya123
Enter the optional host port where to send the trap2s: (162) 162
Do you want to add another SNMPv2c trap2 receiver? y/n: (n) n
Do you want to add SNMPv2c inform receivers? y/n: (n) n
Do you want to add SNMPv3 trap receivers? y/n: (n) n
Do you want to add SNMPv3 inform receivers? y/n: (n) n
```

3. (Optional) Verify snmpd service status:

- `systemctl status snmpd`

ASP130 Output Example:

```
[custadm@asp130-r660xs-a31-8HHD ~]$ systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2025-03-22 06:30:47 MDT; 2min 45s ago
     Main PID: 222051 (snmpd)
        Tasks: 1 (limit: 1643572)
       Memory: 6.8M
      CGroup: /system.slice/snmpd.service
              └─222051 /usr/sbin/snmpd -LS0-6d -f
Mar 22 06:30:47 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
Mar 22 06:30:47 asp130-r660xs-a31-8HHD.acp.avaya.com snmpd[222051]: NET-SNMP version 5.8
Mar 22 06:30:47 asp130-r660xs-a31-8HHD.acp.avaya.com systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
```

4. Generate a SNMPv2 test trap:

```
snmptrap -v 2c -c <community-string> <SALGW-IP> '' SNMPv2-MIB::sysName sysName.0 s "test trap from RHEL 8.10"
```

Example:

```
snmptrap -v 2c -c private123 192.168.0.50 '' SNMPv2-MIB::sysName sysName.0 s "test trap from RHEL 8.10"
```

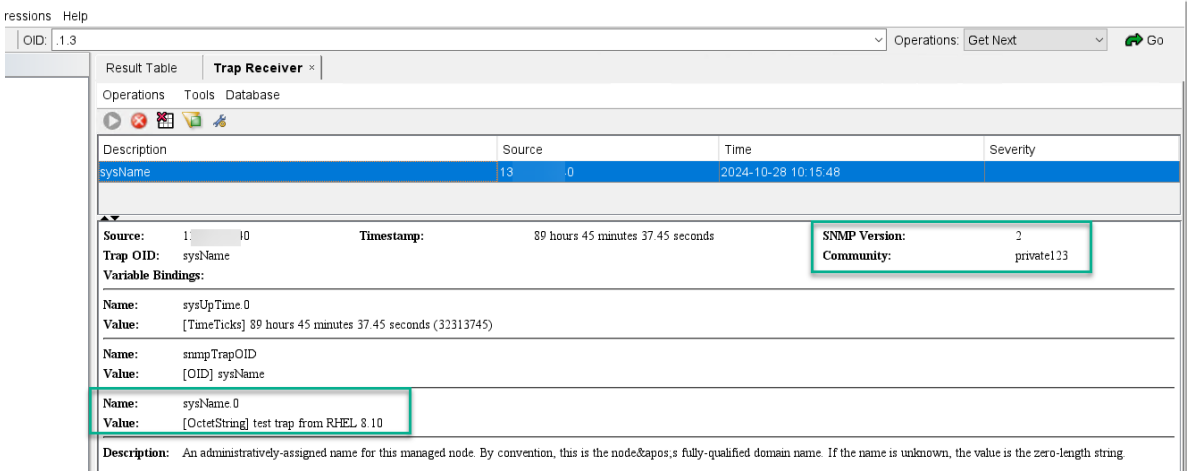


Figure 6: Trap View from NMS Tool – Use for Example Only

OID information for currently supported alarms

*** Note:**

All RHEL MIB modules can be found under the `/usr/share/snmp/mibs/` directory. For the ASP R6.x solution, Avaya has not implemented any proprietary MIBs.

Alarm Description	SNMP OID Information	Alarm Name
Generic Interface Down Event: A physical network interface in the server has gone down. This requires investigation. If network redundancy has not been configured, services will get impacted. Also, when a virtual machine gets shutdown a link down event gets triggered with the VM virtual interface info e.g. vnet0.	1.3.6.1.6.3.1.1.5.3	linkDown
Generic Interface Up Event: A physical network interface in the server has gone UP. Also, when a virtual machine gets powered on a link UP event gets triggered with the VM virtual interface info e.g. vnet0. This event can be used to clear alarm generated by "Link Down" event.	1.3.6.1.6.3.1.1.5.4	linkUp

Table continues...

Alarm Description	SNMP OID Information	Alarm Name
A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered. Trap gets generated when the SNMP agent on the host gets restarted.	1.3.6.1.6.3.1.1.5.1	coldStart
An error message describing the load-average and its surpassed watch-point value. For ASP 130 snmpd.conf file has been set to: %90 CPU utilization to represent Load Average in 1 minute.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.1 [laErrorFlag.1] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.1 [laNames.1]	laErrorMessage.1
The 1-minute CPU load average is below the established, watch-point value. High CPU Usage flag has cleared.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.1 [laErrorFlag.1] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.1 [laNames.1]	laErrorMessage.1
An error message describing the load-average and its surpassed watch-point value. For ASP 130 snmpd.conf file has been set to: %85 CPU utilization to represent Load Average in 5 minutes.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.2 [laErrorFlag.2] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.2 [laNames.2]	laErrorMessage.2

Table continues...

Alarm Description	SNMP OID Information	Alarm Name
The 5-minute CPU load average is below the established, watch-point value. High CPU Usage flag has cleared.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.2 [laErrorFlag.2] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.2 [laNames.2]	laErrorMessage.2
An error message describing the load-average and its surpassed watch-point value. For ASP 130 snmpd.conf file has been set to: %80 CPU utilization to represent Load Average in 15 minutes.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.3 [laErrorFlag.3] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.3 [laNames.3]	laErrorMessage.3
The 15-minute CPU load average is below the established, watch-point value. High CPU Usage flag has cleared.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.4.1.2021.10.1.100.3 [laErrorFlag.3] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0] 1.3.6.1.4.1.2021.10.1.2.3 [laNames.3]	laErrorMessage.3
A text description providing a warning, and the space left on the disk. For ASP 130 snmpd.conf file has been set to: disk /var/lib/libvirt 10%	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 Object Name: 1.3.6.1.4.1.2021.9.1.101.1	dskErrorMsg
High Disk Usage flag has cleared. Total system disk usage is below the established, watch-point value.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 Object Name: 1.3.6.1.4.1.2021.9.1.101.1	dskErrorMsg

Table continues...

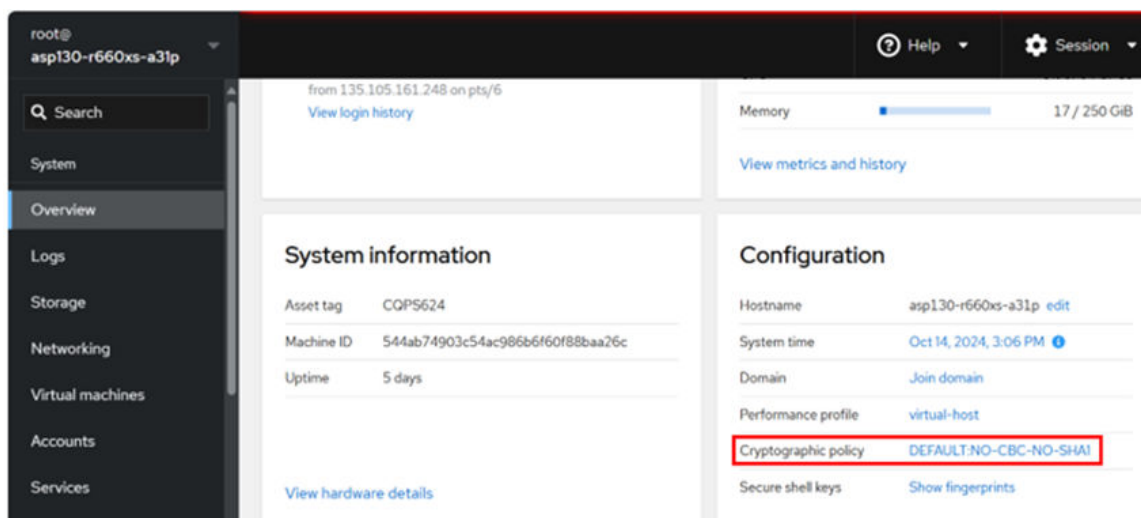
Alarm Description	SNMP OID Information	Alarm Name
Available memory in Host below threshold. For ASP S8300 snmpd.conf file has been set to: memSysAvail <=1500000 (1.5GB)	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.2.1.25.2.3.1.5.11 [hrStorageSize.11] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0]	mteHotTrigger
High Memory Usage flag has cleared. Available memory is above the established, watch-point value.	Variable Binding OID: 1.3.6.1.2.1.88.2.0.1 [mteTriggerFired] OID: 1.3.6.1.2.1.25.2.3.1.5.11 [hrStorageSize.11] Object Name: 1.3.6.1.2.1.88.2.1.1.0 [mteHotTrigger.0] 1.3.6.1.2.1.88.2.1.5.0 [mteHotValue.0]	mteHotTrigger
An indication that the SNMP agent is in the process of being shut down.	OID: 1.3.6.1.4.1.8072.4.0.2	nsNotifyShutdown

TLS protocol configuration for KVM on RHEL 8.10 Environment

Examples below may reference ASP 130 but will be similar output for ASP S8300.

ASP S8300 R6.0.x KVM on RHEL 8.10 comes with the system-wide cryptographic policy profile set to customized `DEFAULT:NO-CBC-NO-SHA1`, enabling TLS v1.2 and TLS v1.3 only. TLS v1.0 and TLS v1.1 are disabled by default. Weak and deprecated CBC and SHA-1 encryption ciphers are disabled.

Cryptographic policy profile shown in Cockpit:



Viewing TLS settings in KVM on RHEL 8.10 (Cockpit/Port 9090)

About this task

Use the following procedure to view the TLS versions enabled on a KVM on RHEL 8.10 Host (Cockpit/Port 9090).

Procedure

1. Open an SSH session to the KVM on RHEL host using PuTTY. Log in with the `custadm` or `root` credentials.
2. Use the **OpenSSL** command to view the TLS versions enabled or disabled:
 - a. For TLS 1.0: `openssl s_client -connect localhost:9090 -tls1`
 - b. For TLS 1.1: `openssl s_client -connect localhost:9090 -tls1_1`
 - c. For TLS 1.2: `openssl s_client -connect localhost:9090 -tls1_2`
 - d. For TLS 1.3: `openssl s_client -connect localhost:9090 -tls1_3`

3. If the TLS version is disabled (TLS v1.0/v1.1), the Cipher will be set to 0000 as shown below:

```

---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1
  Cipher    : 0000
  Session-ID:
  Session-ID-ctx:
  Master-Key:
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1728994228
  Timeout    : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: no
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.1
  Cipher    : 0000
  Session-ID:
  Session-ID-ctx:
  Master-Key:
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1728994439
  Timeout    : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: no

```

4. If the TLS version is enabled (TLS v1.2/v1.3), the Cipher will display a unique identifier as shown below:

*** Note:**

The system will not be able to verify server's identity and certificate unless the installed SSL certificate has been signed by a trusted Certificate Authority. Verify return code: 21 (unable to verify the first certificate) will be displayed. With an SSL certificate Verify return code: 18 (self signed certificate) will be displayed. If the root CA is installed in a ca-trusted location (/etc/pki/ca-trust/source/anchors) the Verify return code: 0 (ok) will be displayed. Refer to [Replacing SSL certificates and Keys with Custom Certificates in RHEL 8.10 - Cockpit Web Service](#) on page 64 for more details.

TLS v1.2:

```

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher    : ECDHE-RSA-AES256-GCM-SHA384
  Session-ID: D304C41EB7032D2C90C78BEAC7C9C3F48E5D616A98999C6CB30BA77CC0F80680
  Session-ID-ctx:
  Master-Key: 5EE00038053ECD154CBB214F1960E8B763D6509B675312D01BF27D507CE6F15D7619306792861CAE3A540C438AD733B4
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1729001462
  Timeout    : 7200 (sec)
  Verify return code: 21 (unable to verify the first certificate)
  Extended master secret: yes

```

```

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES256-GCM-SHA384
  Session-ID: D3326E0E861330CE38E22C2C62C19FA9BBAA435E155BC061EF797B43EAF8A1
  Session-ID-ctx:
  Master-Key: 9E1427336B6CA4A7A030879AC191E10D72349391E3FBD2ECF06929E45777DB6D51479D110BE16FA6FF9C1E096D707CE1
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1729083913
  Timeout : 7200 (sec)
  Verify return code: 18 (self signed certificate)
  Extended master secret: yes

```

```

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES256-GCM-SHA384
  Session-ID: 396175A39788BD7D467672FE82D9090A7840D7376FB01C83F55BC7233DD5A196
  Session-ID-ctx:
  Master-Key: 7FC423BD35FD43816368367D2DEA568BE42BC231E9D3E47DAAAF1247A5F8AEF1E6D410F69BAD7F0C4B90D69F57FABAEAE
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1729547503
  Timeout : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: yes

```

TLS v1.3:

```

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 21 (unable to verify the first certificate)

```

```

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self signed certificate)

```

```
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```



Chapter 6: Network port verification

Purpose

Note:

Unless otherwise stated by Avaya, DO NOT change the default network labels as this may impact integration with other Avaya applications and scripts.

This section is utilized to verify the Services Port configuration and the Management Port configuration. Other ports are displayed as well.

Services port configuration is included in the R6 ISO deployment. Port eno8403 is assigned to the services port. The services port IP address is 192.11.13.6/30. To access the host from your laptop, the laptop IP address must be 192.11.3.5/30.

Validating network port configuration in Shell and Web

About this task

Use this procedure to verify network port configuration.

The following commands can be used for status information. These are examples only, and actual output will vary as some screen shots may be from an ASP S8300, others from an ASP 130.

Procedure

1. From the CLI, execute `nmcli conn` to display network interfaces.

For example:

```
[custadm@asp130-s8300 ~]$ nmcli con
NAME                                UUID                                TYPE      DEVICE
Mgmt_VM_Network                    31ba8c18-899c-4e57-91b8-9d93fe4844f1 bridge    bridge0
EMB_VLAN                            cf810e80-bfec-45eb-aed5-934fe5b5b733 vlan      enp2s0.4093
System enp1s0                       055d252e-a442-49e1-a91c-7a554dc54faa ethernet  enp1s0
bridge0-port                        ebfe3c7f-7745-44bb-bcb5-bd77ba057920 vlan      enp2s0.1
bridgeOOB-port                      8b287bd8-0d7c-46a6-aec1-8d35a426bd89 ethernet  enp3s0
OOBM_Network                        961eaa4f-ac2c-4adc-bd6b-2c992587075a bridge    bridgeOOB
enp2s0                              33fb60d4-d934-4727-9433-66fa6aa94f1e ethernet  --
enp3s0                              d12f488d-01e8-455f-91bf-1bee23614953 ethernet  --
Services                            46ad7013-d17f-469e-9516-6418c7dec831 ethernet  --
```

2. Cockpit can also be used to display network interfaces.

Note that the Connection Profile name does not appear in Cockpit, but the “Device Name” is displayed.

*** Note:**

There will not be any bridge/virtual switch configuration associated with the services port. If OOBM is enabled, the LAN 2 port is utilized and is assigned to enp3s0.

The default vlan id is “1” in the bridge0 (enp2s0.<vlan#>) in the table below. The vlan id number on the G4X0 must always match the vlan id number on the S8300.

Connection Profile Name	S8300 Device Name	Notes
Mgt_VM_Network	bridge0 (enp2s0.<vlan#>)	Default without OOBM enabled
VM_Network		If OOBM enabled
Services	enp1s0	192.11.13.6 svc port
OOBM_Network	bridgeOOB (enp3s0)	Optional: Must be enabled during configuration
EMB-VLAN	enp2s0.4093	Internal connection to G4X0

ASP R6.0.x S8300

Connection Profile Name	S8300 Device Name	Notes
Mgt_VM_Network	bridge0 (enp2s0.vlan)	Default w/out OOBM enabled
VM_Network		With OOBM enabled
Services	enp1s0	192.11.13.6 services port
OBOM_Network	bridgeOOB (enp3s0)	Optional: Must be enabled during configuration

The “Connection Profile Name” is what is seen when the **nmcli connection** shell command is executed. The Connection Profile Name does not appear in the Cockpit UI. The “Device Name” is what is seen in the Cockpit UI.

Status information commands

nmcli device - to list all network devices

```
[custadm@asp130-r660xs ~]$ nmcli device
DEVICE    TYPE      STATE      CONNECTION
bridge0   bridge    connected  Mgmt_VM_Network
eno8303    ethernet  connected  bridge0-port
eno12399   ethernet  unavailable --
eno12409   ethernet  unavailable --
eno12419   ethernet  unavailable --
eno12429   ethernet  unavailable --
eno8403    ethernet  unavailable --
lo         loopback  unmanaged  --
```

showConfig – provides detailed information about the existing configuration including hardware and filesystem information. Recommendation is to redirect to a file for viewing. *Example below shows only the beginning of the output.*

```
[custadm@asp-s8300-43 ~]$ showConfig
===== System =====
Server type: Avaya S8300

System Information
  Manufacturer: Avaya Inc.
  Product Name: S8300E
  Version: -1A
  Serial Number: 22WZ0860C21H
  UUID: 03000200-0400-0500-0006-000700080009
  Wake-up Type: Power Switch

Chassis Information
  Manufacturer: Avaya Inc.
  Type: Other
  Lock: Not Present
  Version: -1A
  Boot-up State: Safe
  Power Supply State: Safe
  Thermal State: Safe
  Security Status: None
  OEM Information: 0x00000000
  Height: Unspecified
  Number Of Power Cords: 1
  Contained Elements: 0
```

configNetwork – Server Network Configuration. Allows one to reconfigure the Network settings that were previously established. Should be run from the services port or console as changing network information may disconnect the session. After making any configuration changes, VMs on the host should be restarted.

swversion - displays the full software version output.

```
[custadm@asp130-r660xs ~]$ swversion
  Operating system: Linux 4.18.0-553.22.1.el8_10.x86_64
    Built: Sep 11 18:02 2024

    Contains: Avaya Solutions Platform
      Release: ASP Release 6.0.0.0.0
    Build Number: 4.6-4.8
    VM Environment: KVM
```

The Build Number is of the format X.Y-A.B where X.Y is the ASP R6.0.x build number and A.B is the ASP R6.0.x Kickstart build number.

Chapter 7: Securing Network Configuration (OoBM)

This chapter describes secure network configuration details on Avaya Solutions Platform S8300 R6.0.x.

Overview

The Out of Band Management (OOBM) network configuration separates management traffic of the hypervisor and virtual machines through a secure private network, separated from the rest of the customer network. The OOBM network configuration permits restricted access only to System Administrators.

 Note:

Default gateway address is on the Public Network interface. All devices accessing OOBM Network interface should be on the same subnet as the OOBM interface or have static routes created for those devices.

OOBM can be administered during initial configuration of ASP 6.0.x (Reference Chapter 5: Configuration) or at a later time by executing the `configNetwork` script.

No OOBM configured

When performing initial configuration of the server or when running the `configNetwork` script, answering `n` to the following two questions will ensure that OOBM access to Cockpit and OOBM access for VMs is disabled.

 Note:

On ASP host with OOBM enabled, if the in-band MGMT access is disabled by `setNonOobAccess disable` command, it is required to enable in-band MGMT access by `setNonOobAccess enable` command before disabling OOBM with `n` option using above description to avoid both OOBM and in-band MGMT access being disabled.

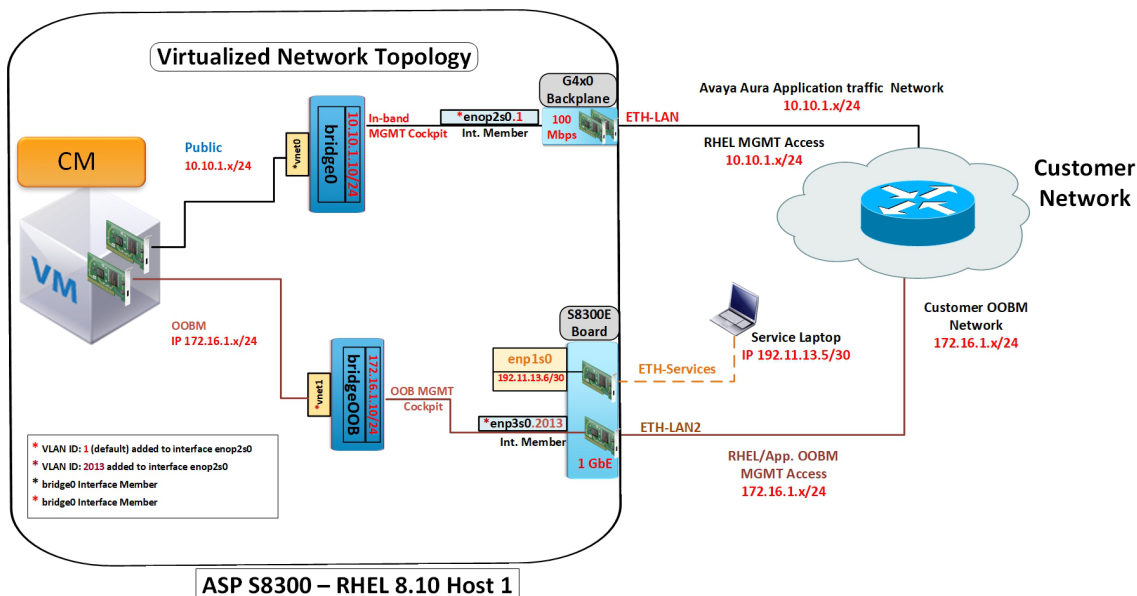
```
Connect this server to an Out of Band Management network (OOBM)? y/n
(n) n
```

Create an OOBM bridge for VMs to use? y/n (n)n

In-band MGMT and OOBM access to Cockpit enabled and VM OOBM enabled

When performing initial configuration of the server or when running the `configNetwork` script, answering `y` to the first question will ensure that OOBM access to Cockpit and OOBM access for VMs are both enabled and no additional prompts for OOBM configuration are presented.

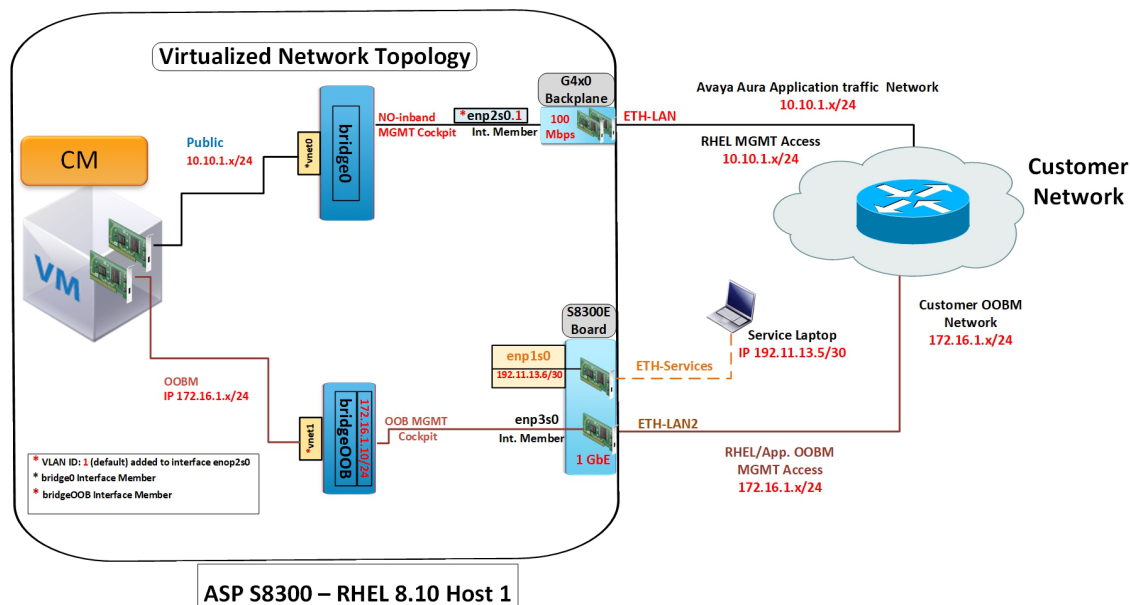
Connect this server to an Out of Band Management network (OOBM)? y/n (n) y



Note: In-band MGMT access to cockpit is kept on `bridge0` (IP Address is assigned). Out of Band Management (OOBM) access to cockpit is configured on `bridge0OB` by assigning an IP Address within the customer OOBM Network segment.

* Note:

You can disable in-band MGMT access to Cockpit after the above configuration is completed by removing the IP configuration from `bridge0` after initial configuration is completed. This is accomplished using the command: `setNonOobAccess <disable|enable>` (disable ssh/cockpit access from public/VM network).

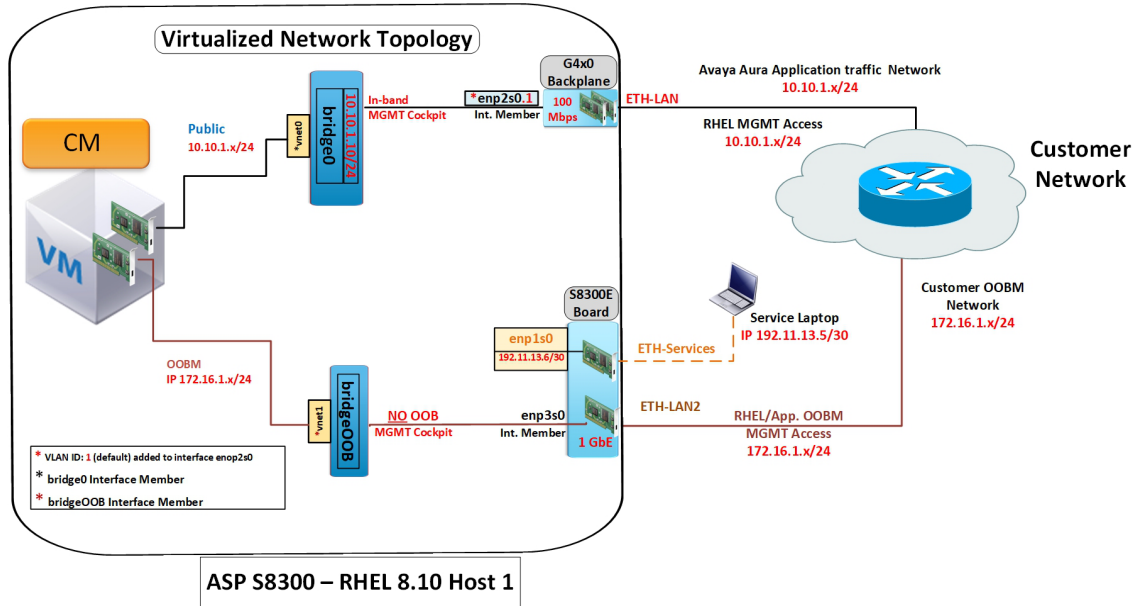


In-band MGMT and OOBM access to Cockpit disabled and VM OOBM enabled

When performing initial configuration of the server or when running the `configNetwork` script, answering `n` to the first question and `y` to the second question ensures that OOBM access to Cockpit is disabled but OOBM access for VMs is both enabled.

```
Connect this server to an Out of Band Management network (OOBM)? y/n
(n) n
```

Create an OOBM bridge for VMs to use? y/n (n)y



Chapter 8: Performing server recovery or software remastering

In the event of server failure, a user needs to determine which of the following is necessary:

- Server has a hardware failure and requires replacement.
- Software reinstallation is required on the existing server.

If possible, all application data should be backed up to a remote storage device. This data is required for a seamless recovery. All IP naming conventions should be captured from the failed server.

The installation instructions documented in *Chapter 4: Installing Avaya Solutions Platform S8300* and *Chapter 5: Configuration of ASP S8300 R6.0.x* are the same for recovery/remastering.

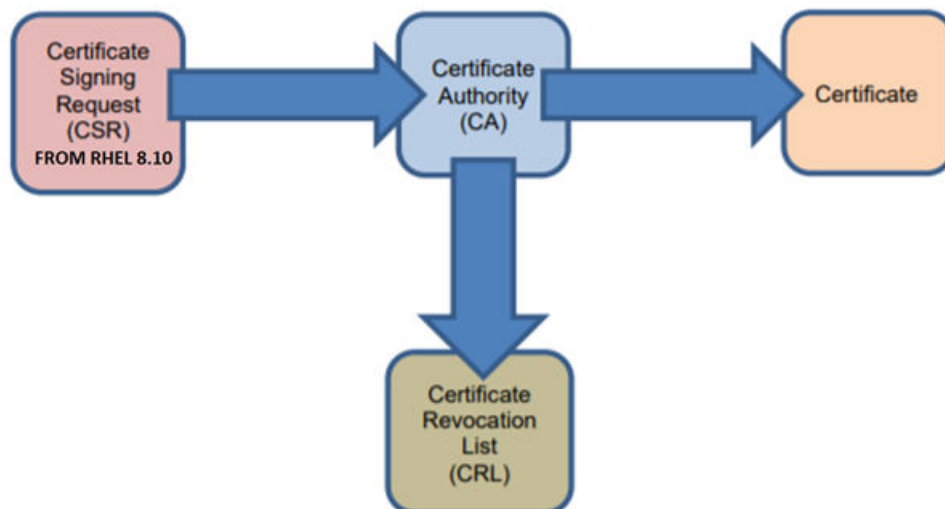
Chapter 9: Replacing SSL certificates and Keys with Custom Certificates in RHEL 8.10 - Cockpit Web Service

Overview

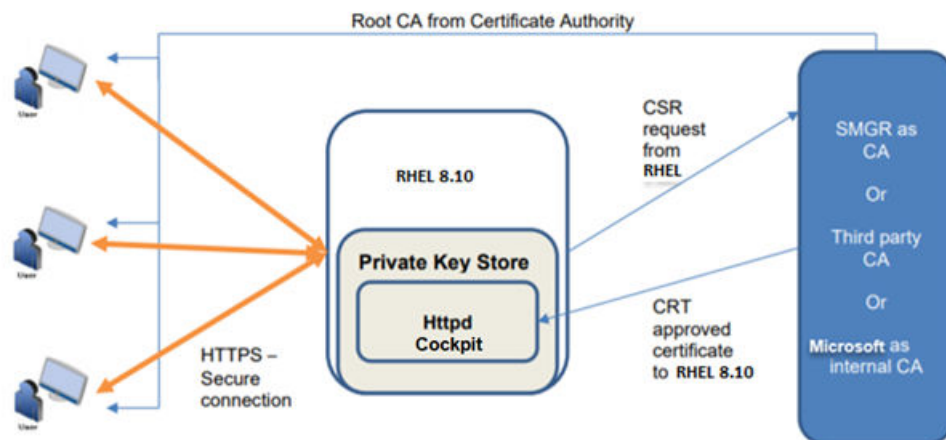
Secure Sockets Layer (SSL) with CA Signed Certificates

Secure Sockets Layer (Transport Layer Security (TLS) more accurately) is the technology that you can use for a secure connection. The root certificate, often called a trusted root, is at the center of the trust model that provides support for the Public Key Infrastructure issued by trusted Certificate Authority. In the SSL ecosystem, you can generate a signing key and sign a new certificate with that signature. The certificate is considered valid only when it gets directly signed by a trusted Certificate Authority (CA). To validate the certificate, the device compares the certificate issuer with the list of trusted CAs. If there is no match, the client checks to see if the certificate of the issuing CA was issued by a trusted CA, and this continues until the end of the certificate chain where the root certificate issued by a trusted Certificate Authority is found.

The following image shows the HTTPS communication from Root CA and KVM on RHEL 8.10:



The following figure shows the Certificate Authority in RHEL 8.10:



Replacing SSL certificates and Keys with Custom Certificates in RHEL 8.10 - Cockpit Web Service

About this task

Company's security policies might require replacing default KVM on RHEL 8.10 SSL certificates with a third-party CA-signed certificate on each KVM on RHEL 8.10 host.

Self-signed certificates can be replaced on KVM on RHEL 8.10 with certificates from a trusted CA, either a commercial Certificate Authority (CA) or an organizational CA, when company policy requires it.

* Note:

This activity can be conducted 100% remotely and it is NOT a service affecting procedure for the virtual machines running on the KVM on RHEL 8.10 host. Nonetheless Avaya strongly recommends conducting this activity in a customer approved maintenance window during off business hours when possible or low traffic hours.

* Note:

To eliminate misconfigurations and avoid errors during the implementation of customs certificates, Avaya strongly recommends conducting this activity with one server at a time, when having multiple ASP 130 compute servers. Hence, do not attempt to replace SSL certificates and Keys on multiple servers at the same time.

* Note:

This procedure consists of multiple sub-sections and steps that must be followed and completed in the order documented to ensure the successful implementation of custom certificates in KVM on RHEL 8.10.

**Warning:**

Avoid any administrative tasks such as making configuration changes to the host when conducting this procedure.

Before you begin

- Ensure you have access to the ASP 130 R640/R660xs server management network either through a SAL Gateway connection (remotely) or direct service port connection (onsite).
- SSH tool such as Putty (not provided by Avaya).
- SFTP / SCP client such as WinSCP (not provided by Avaya).
- **custadm** password.
- Customer DNS records should be updated with each KVM on RHEL 8.10 FQDN (Hostname + Domain).

Creating the Certificate configuration file for KVM on RHEL 8.10 host

Procedure

1. In a text editor of choice (for example Notepad, WordPad, etc.), copy the following content as is:

```
[ req ]

days = 365

default_md = sha256  ###change to SHA512 or higher/different as required by
customer###

default_bits = 2048      ### change to higher RSA key as required by customer###
default_keyfile = server-fqdn.company.com.key
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req

[ v3_req ]

basicConstraints = CA:FALSE

keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth

subjectAltName = DNS:"ServerName.domain.com", DNS:"ServerShortName",
IP:"ServerIPAddress"
```

```
[ req_distinguished_name ]
countryName = "Country (two-letter code alpha-2)"
stateOrProvinceName = "State (two-letter code)"
localityName = "City"
0.organizationName = "Company Name"
organizationalUnitName = "Company Unit Name"
commonName = "serverhostname.domain.com"
emailAddress= "email Address"

[ alt_names ]
DNS.1 = "ServerHostname.domain.com"
DNS.2 = "ServerShortName"
IP.1 = "ServerIPAddress"
```

2. Edit the content in the following fields as follows:

- **Days** = Enter the number in days for certificate expiry. For example: 365 if certificate should expire in 1 year, 730 for 2 years and so forth.
- **default_keyfile**: Update with the KVM on RHEL 8.10 host FQDN. For example:
asp130-r660xs.acp.avaya.com.key
- **subjectAltName**: Enter the KVM on RHEL 8.10 host FQDN, hostname, IP. For example: DNS:asp130-r660xs-01.acp.avaya.com, DNS:asp130-r660xs-01, IP:192.168.220.57
- **countryName**: Type the two-letter country code without the punctuation. For example, US.
- **stateOrProvinceName**: Type the two-letter code of the state or province. For example, CO for the USA state of Colorado.
- **localityName**: Type the name of the city. For example, Denver.
- **organizationName**: Type the name of the organization. For example: Avaya LLC.
- **OrganizationalUnitName**: Type the name of the of the department or organization unit making the request. For example: IT, Engineering, etc.
- **commonName**: Type the KVM on RHEL 8.10 host Fully Qualified Domain Name. For example: asp130-r660xs-01.acp.avaya.com
- **emailAddress** (Optional): Type the email address of the contact person responsible for the ASP 130 infrastructure at the customer site or customer IT department. For example, support@company.com
- **DNS.1**: Type the Fully Qualified Domain Name of the KVM on RHEL 8.10 host. For example: asp130-r660xs-01.acp.avaya.com
- **DNS.2**: Type the short, hostname for the KVM on RHEL 8.10 host. For example: asp130-r660xs-01

- **IP.1:** Type the KVM on RHEL 8.10 host IP Address. For example: 192.168.200.57.

The following image is an example of an edited configuration file:

```

1  [ req ]
2
3  days = 365
4
5  default_md = sha512
6
7  default_bits = 2048
8
9  default_keyfile = aspl30-r660xs.acp.avaya.com.key
10
11 distinguished_name = req_distinguished_name
12
13 encrypt_key = no
14
15 prompt = no
16
17 string_mask = nombstr
18
19 req_extensions = v3_req
20
21 [ v3_req ]
22
23 basicConstraints = CA:FALSE
24
25 keyUsage = digitalSignature, keyEncipherment, dataEncipherment
26
27 extendedKeyUsage = serverAuth, clientAuth
28
29 subjectAltName = DNS:aspl30-r660xs.acp.avaya.com, DNS:aspl30-r660xs, IP:192.168.200.57
30
31 [ req_distinguished_name ]
32
33 countryName = US
34
35 stateOrProvinceName = CO
36
37 localityName = Denver
38

```

```

38
39 0.organizationName = Avaya LLC
40
41 organizationalUnitName = ASP-Engineering
42
43 commonName = aspl30-r660xs.acp.avaya.com
44
45 emailAddress = support@company.com
46
47 [ alt_names ]
48
49 DNS.1 = aspl30-r660xs.acp.avaya.com
50
51 DNS.2 = aspl30-r660xs
52
53 IP.1 = 192.168.200.57
54

```

3. Save the configuration file with a file extension of `cfg`. For example: `aspl30-R660xs-1.cfg`.

*** Note:**

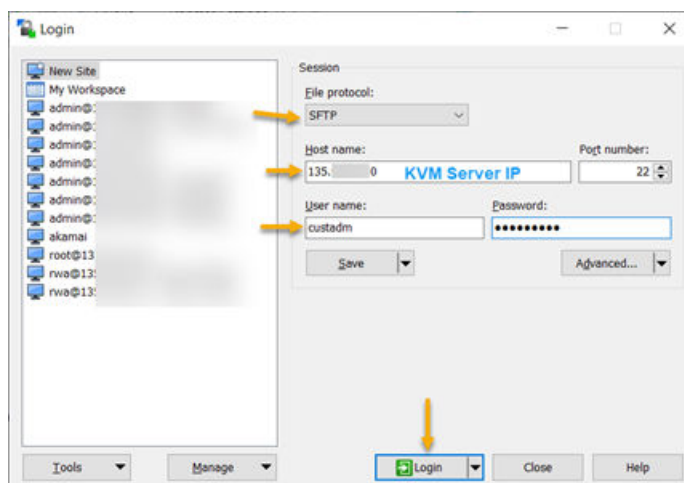
Depending on the used text editor, the configuration file may have to be saved as a text file first, therefore this will be saved with a `.txt` extension. The newly saved configuration file can then be “renamed” along with changing the extension from `.txt` to `.cfg`

Name	Status	Date modified	Type	Size
asp130-r660xs-1.cfg		10/10/2024 12:18 PM	CFG File	1 KB

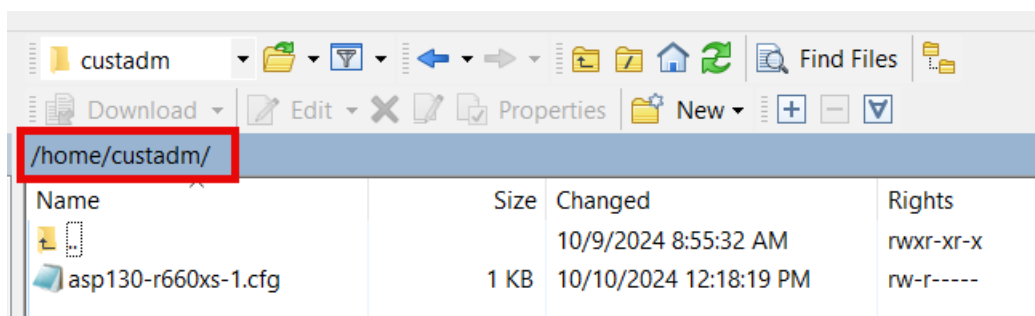
*** Note:**

Configuration files are unique per each KVM on RHEL 8.10 host (ASP 130 server). If replacing SSL certificates in multiple hosts, it is strongly recommended to save these using a descriptive name that could easily help the user to differentiate each server configuration file when transferring these, for example: `asp130-r660xs-1.cfg` for the 1st ASP 130 server, `asp130-r660xs-2.cfg` for the 2nd ASP 130 server, `asp130-KVM on RHEL 8.10-N.cfg`, etc. This will help or prevent users from using configuration files and replacing SSL certificates in the erroneous ASP 130 server.

- Starting with the first, desired KVM on RHEL 8.10 host, open a WinSCP session using the root credentials.



- Using WinSCP transfer the configuration file created in previous steps e.g. "`asp130-r660xs-1.cfg`" to the same "`/home/custadm/`" directory.



- WinSCP session can now be closed.

Generating the Certificate signing Request in KVM on RHEL 8.10

Before you begin

[Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65 must be completed before continuing with the following procedure.

Procedure

1. Using Putty or any other desired SSH tool, open a new SSH session to the selected KVM on RHEL 8.10 host during the certificate configuration file creation steps. Login using the existing `custadm` credentials.
2. Run the following commands:
 - a. `sudo mv /home/custadm/<server-config-file>.cfg /etc/cockpit/ws-certs.d/` [sudo] password for custadm:
 - b. `cd /etc/cockpit/ws-certs.d/`
 - c. `ls -lrt` (to validate configuration file has been properly moved)

```
[custadm@asp130-r660xs ~]$ sudo mv /home/custadm/asp130-r660xs-1.cfg /etc/cockpit/ws-certs.d/
[sudo] password for custadm:
[custadm@asp130-r660xs ~]$ cd /etc/cockpit/ws-certs.d/
[custadm@asp130-r660xs ws-certs.d]$ ls -lrt
total 24
-rw-----. 1 root    root    1704 Oct  9 09:51 0-self-signed.key
-rw-r--r--. 1 root    root    1708 Oct  9 09:51 0-self-signed.cert
-rw-r--r--. 1 root    root    2126 Oct  9 09:51 0-self-signed-ca.pem
-rw-----. 1 root    root    1704 Oct 10 15:47 user-generated-cockpit-selfsigned.key
-rw-r--r--. 1 root    root    1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert
-rw-r--r--. 1 custadm custadm  921 Oct 11 06:41 asp130-r660xs-1.cfg
[custadm@asp130-r660xs ws-certs.d]$
```

- d. `hostname` (to display current system hostname)

* Note:

Hostname for both Key and CSR must be exactly as displayed in previous step.

- e. `sudo openssl req -new -sha256 -nodes -out <HOSTNAME>.csr -newkey rsa:2048 -keyout <HOSTNAME>.key -config <server-config-file>.cfg`

Example:

```
sudo openssl req -new -sha256 -nodes -out asp130-r660xs.acp.avaya.com.csr -newkey rsa:2048 -keyout asp130-r660xs.acp.avaya.com.key -config <server-config-file>.cfg
```

- f. `ls -lrt`

* Note:

Two new files `<HOSTNAME>.key` and `<HOSTNAME>.csr` will be listed.

Note:

The following figure shows an out example using the configuration file previously created and transferred during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65 `asp130-r660xs-1.cfg`. Contemplate that configuration files will change per each KVM on RHEL 8.10 host when generating the certificate signing request (CSR).

```
[custadm@asp130-r660xs ws-certs.d]# hostname
asp130-r660xs.acp.avaya.com
[custadm@asp130-r660xs ws-certs.d]# sudo openssl req -new -sha256 -nodes -out asp130-r660xs.acp.avaya.com.csr -newkey rsa:2048 -keyout asp130-r660xs.acp.avaya.com.key -config asp130-r660xs-l.cfg
[sudo] password for custadm:
Generating a RSA private key
.....+++++
...+++++
Writing new private key to 'asp130-r660xs.acp.avaya.com.key'
-----
[custadm@asp130-r660xs ws-certs.d]# ls -lft
total 32
-rw-r--r--. 1 root root 1704 Oct 9 09:51 0-self-signed.key
-rw-r--r--. 1 root root 1708 Oct 9 09:51 0-self-signed.cert
-rw-r--r--. 1 root root 2128 Oct 9 09:51 0-self-signed-ca.pem
-rw-r--r--. 1 root root 1704 Oct 10 15:47 user-generated-cockpit-selfsigned.key
-rw-r--r--. 1 root root 1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert
-rw-r--r--. 1 custadm custadm 921 Oct 11 06:41 asp130-r660xs-l.cfg
-rw-r--r--. 1 root root 1704 Oct 11 07:36 asp130-r660xs.acp.avaya.com.key
-rw-r--r--. 1 root root 1269 Oct 11 07:36 asp130-r660xs.acp.avaya.com.csr
[custadm@asp130-r660xs ws-certs.d]#
```

```
g. sudo openssl req -in <HOSTNAME>.csr -noout -text
```

 Note:

This will help user to validate certificate entries prior to submitting the certificate signing request file to the Certificate Authority (CA).

```
[custadm@aspl30-r660xs ws-certs.d]$ sudo openssl req -in aspl30-r660xs.acp.avaya.com.csr -noout -text
[sudo] password for custadm: 
Certificate Request:
    Data:
      Version: 1 (0x0)
      Subject: C = US, ST = CO, L = Denver, O = Avaya LLC, OU = ASP-Engineering, CN = aspl30-r660xs.acp.avaya.com, emailAddress = support@company.com
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
          RSA Public-Key: (2048 bit)
          Modulus:
            00:b1:f8:53:e6:4c:cb:fc:99:5a:9b:59:c2:68:4c:
            ca:83:52:b7:a3:2b:f1:ff:92:fd:11:96:2e:10:31:
            37:d8:ab:ce:5d:be:36:96:ac:b9:9b:a6:1f:84:ef:
            b4:34:43:ec:87:0f:d6:d1:98:88:65:11:b2:3e:8d:
```

```
Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  X509v3 Key Usage:
    Digital Signature, Key Encipherment, Data Encipherment
  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Subject Alternative Name:
    DNS:aspl30-r660xs.acp.avaya.com, DNS:aspl30-r660xs, IP Address:135.149.1.10
Signature Algorithm: sha256WithRSABEncryption
93:e0:7e:dd:37:23:f1:81:f3:aa:1b:ee:e4:9c:b8:03:e1:a6:
d7:cc:bb:09:ae:77:57:5b:9e:dc:ec:50:55:d9:f5:c7:43:d7:
f1:04:df:72:25:aa:c4:f9:32:74:15:9a:0a:d1:59:1a:cb:2c:
```

h. `sudo cp <HOSTNAME>.csr /home/custadm/`

Example:

```
sudo cp asp130-r660xs.acp.avaya.com.csr /home/custadm/ [sudo]
password for custadm:
```

```
i. cd /home/custadm
```

```
j. sudo chmod 644 <HOSTNAME>.csr
```

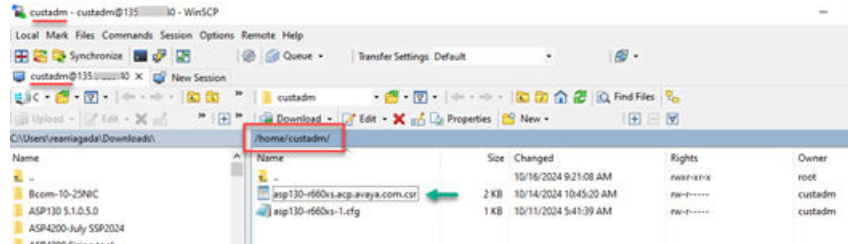
Example:

```
sudo chmod 644 asp130-r660xs.acp.avaya.com.csr
```

- Using WinSCP, re-connect to the RHEL 8.10 host and transfer the Certificate Signing Request file e.g. `asp130-r660xs.acp.avaya.com.csr` previously created to a local PC and submit it to the Certificate Authority of choice to have it signed.

*** Note:**

The CSR file will be stored under `/home/custadm/`



Signing the Certificate Signing Request (CSR) by an Organizational CA

About this task

In this example, the Avaya Aura® System Manager application will be used to sign the CSR file generated in KVM during [Generating the Certificate signing Request in KVM on RHEL 8.10](#) on page 69.

Alternatively, customers can sign certificate signing request (CSR) with a Microsoft Windows server when configured to act as a Certificate Authority (not included by Avaya). Reference to Microsoft documentation for installing and configuring CA as well as signing requests.

*** Note:**

Customers using an external, trusted CA to sign CSR i.e. VeriSign, DigiCert, Symantec can skip and proceed with the next section [Replacing SSL certificates in Cockpit with a CA signed certificate](#) on page 76.

*** Note:**

Depending on the Avaya Aura® System Manager version, steps and screens may slightly vary. Always refer to the latest, available Avaya Aura® System Manager documentation available at <https://support.avaya.com>.

Before you begin

- [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65 and [Generating the Certificate signing Request in KVM on RHEL 8.10](#) on page 69 must be completed prior to continuing.

- Access to an Avaya Aura® System Manager server.
- Transfer the CSR file `asp130-r660xs.acp.avaya.com.csr` file to a local computer that has access to the Avaya Aura® System Manager acting as CA.
- User account with administrative privileges in Avaya Aura® System Manager e.g., `admin` account.

Procedure

1. Using a Web browser, enter the Avaya Aura® System Manager IP address or FQDN.
2. Login with administrative credentials. For example, `admin`
3. Navigate to **Services > Security > Certificates > Authority**.
4. Under **RA Functions**, select **Add End Entity**.
5. Enter the following information in the respective fields for the following fields:

Username:

- a. **End Entity Profile:** `EXTERNAL_CSR_PROFILE`
- b. **Username:** Enter any desired username. For example, `avaya`
- c. **Password (or Enrollment code):** Enter any desired password. For example, `avaya123`
- d. **Confirm Password:** `avaya123`
- e. **E-mail address (optional):** Same value used if configured in the certificate configuration file `asp130-r660xs-1.cfg` during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.

Subject DN Attributes

- a. **CN, Common name:** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
- b. **O, Organization:** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
- c. **C, Country (ISO 3166):** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
- d. **OU, Organizational Unit:** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
- e. **L, Locality:** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during step [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.

- f. **ST, State or Province:** Same value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.

Subject Alternative Name

- a. **DNS Name:** Enter the DNS.1 value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
 - b. **DNS Name:** Enter the DNS.2 value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
 - c. **IP Address:** Enter the KVM on RHEL 8.10 host IP value set in the `asp130-r660xs-1.cfg` (for example) configuration file during [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65.
6. Review and save:
- a. Review and compare the values typed with the ones in the configuration file created during steps in the [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65 `asp130-r660xs-1.cfg`.
 - b. When ready, click the **Add** button to save the changes and create the new Entity.

New entity will be displayed.

[Reload](#)

Previously added end entities

Username	CN	OU	O (organization)	Actions
avaya	asp130-r660xs.acp.avaya.com	ASP Engineering	AVAYA LLC	View Edit

© 2002–2020 PrimeKey Solutions AB. EJBCA® is a registered trademark of PrimeKey Solutions AB.

7. From the middle column menu, under **CA Functions**, select **CA Structure & CRLs**.
8. Click on **Download PEM file**.

AVAYA Aura® System Manager 10.2

Users Elements Services Widgets Shortcuts

Home Security

Security Certificates Authority Enrollment Password Manage Certificate ... Manage Entity Clas... Configuration

EJBCA PKI by PrimeKey

Home

CA Functions

- CA Activation
- CA Structure & CRLs**
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers
- Validators

RA Functions

CA Structure & CRLs

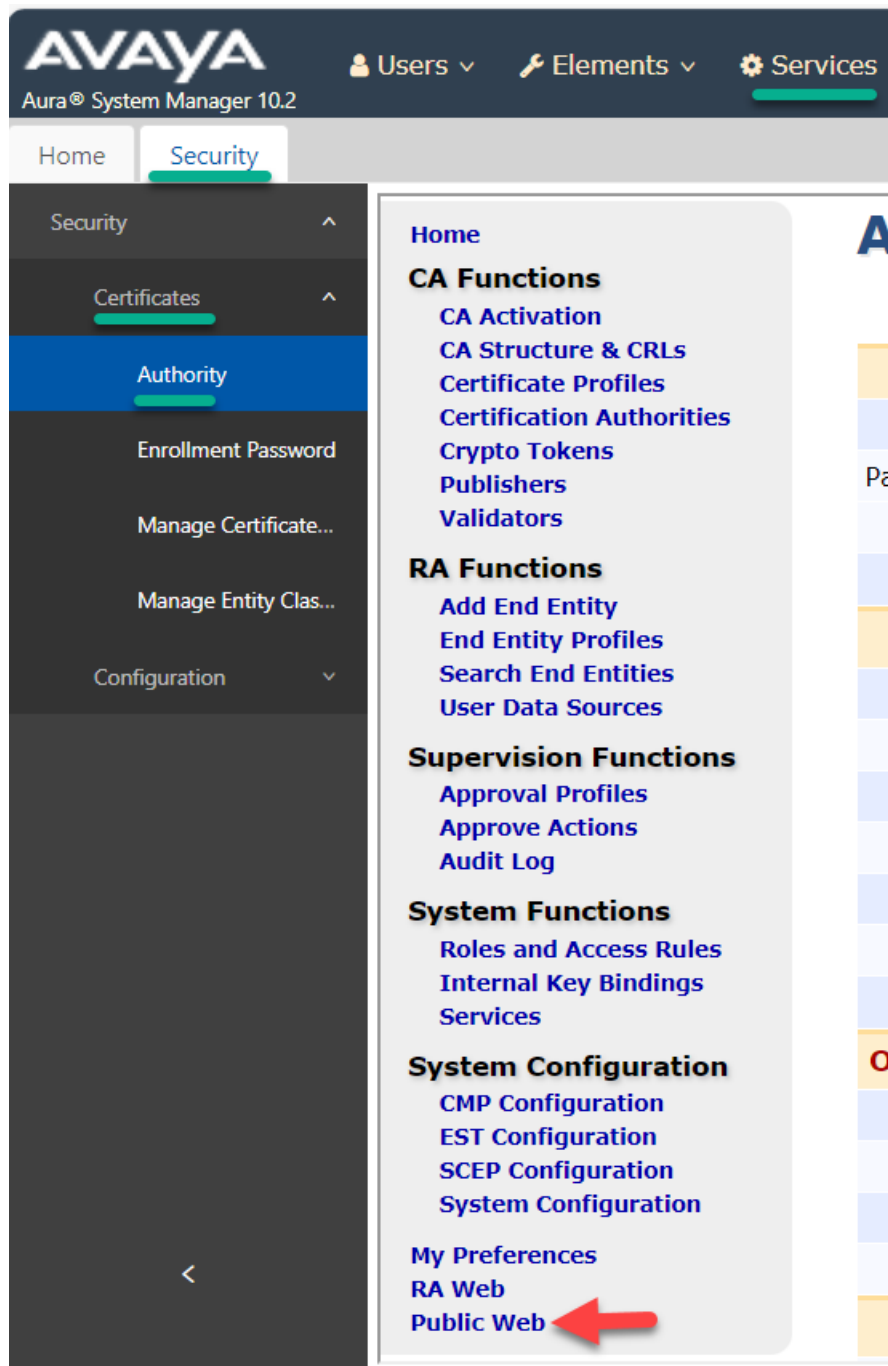
Basic Functions

Basic Functions for CA : tmdefaultca [View Certificate](#) [View Information](#)

Root CA: CN=System Manager CA,OU=MGMT,O=AVAYA

[Download binary/to IE](#) [Download to Firefox](#) **[Download PEM file](#)** [Download JKS file](#)

9. From the middle column menu, under **System Configuration**, select **Public Web**.
A new tab opens.



10. From the **EJBCA** webpage, select **Create Certificate from CSR** under **Enroll**.

11. Enter the following information:

- a. **Username:** The one configured when creating the entity during step 5 e.g. `avaya`
- b. **Enrollment Code:** The one configured when creating the entity during step 5 i.e. `avaya123`

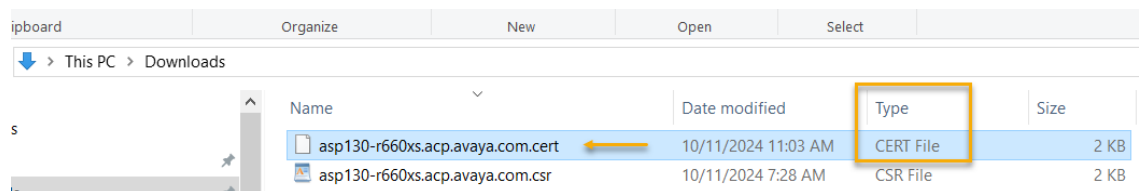
- c. **Request file:** Select **Choose File** to import the CSR file created during [Generating the Certificate signing Request in KVM on RHEL 8.10](#) on page 69 e.g. `asp130-r660xs.acp.avaya.com.csr`
 - d. **Result type:** From drop-down menu, select **PEM-full certificate chain**.
Full certificate chain is required for validation.
 - e. Select **OK** to generate the certificate.
12. A certificate with a PEM format is created and automatically downloaded to the computer used to issue the sign request.



13. Navigate to the location where the certificate is downloaded.
14. Rename and change the extension to `.cert` of the PEM certificate generated by Avaya Aura® System Manager to match exactly the KVM on RHEL 8.10 host e.g. `asp130-r660xs.acp.avaya.com.cert`.

*** Note:**

Changing the file extension from `.pem` to `.cert` (or vice versa) does not alter the actual content of the file because both file formats essentially contain the same type of data: encoded X.509 certificates.



Replacing SSL certificates in Cockpit with a CA signed certificate

Before you begin

- Steps in [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65, [Generating the Certificate signing Request in KVM on RHEL 8.10](#) on page 69, and [Signing the Certificate Signing Request \(CSR\) by an Organizational CA](#) on page 71 if using Avaya Aura® System Manager must be completed prior to continuing.

- Customers using an external CA or any other organizational CA such as Microsoft CA should have by now the signed certificate in a CERT format and renamed to match the KVM on RHEL 8.10 hostname e.g. `asp130-r660xs.acp.avaya.com.cert` and CA root certificate.
- The `.cert` file should contain two OpenSSL style PEM blocks. First one BEGIN CERTIFICATE block for the server certificate and appended by the intermediate certificate chain authority.

Example:

```
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIJAPXW+CuNYS6QMA0GCSqGSIb3DQEBCwUAMD8xKTAnBgNV
BAoMIGI0OGE2NGNkNmMwNTQ1YThhZTgxOTEzZDE5YmJjMmRjMRIwEAYDVQQDDAIs
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIJAPXW+CuNYS6QMA0GCSqGSIb3DQEBCwUAMD8xKTAnBgNV
BAoMIGI0OGE2NGNkNmMwNTQ1YThhZTgxOTEzZDE5YmJjMmRjMRIwEAYDVQQDDAIs
...
-----END CERTIFICATE-----
```

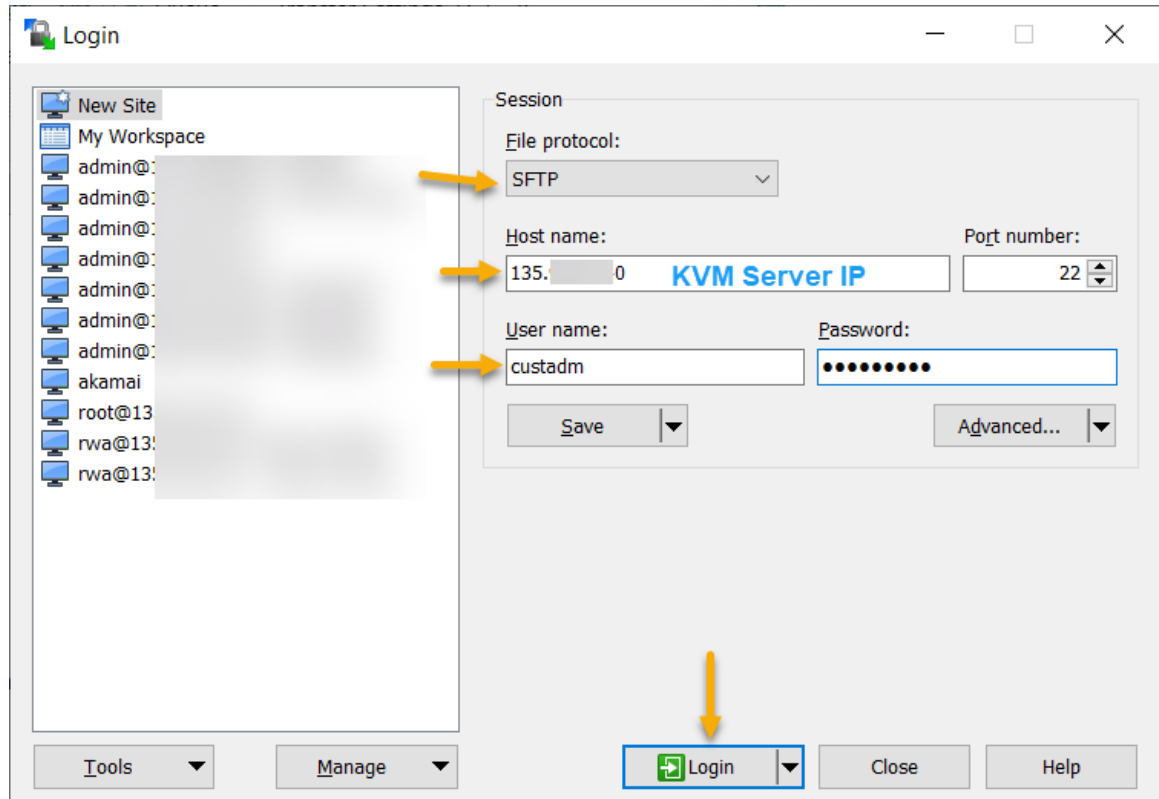


Note:

Desirably, the CA ROOT certificate should be in a `pem` format. However, certificates can be converted by leveraging `openssl` once they get transferred to the KVM on RHEL 8.10 host.

Procedure

1. Open a WinSCP session using the `custadm` credentials to the KVM on RHEL 8.10 host selected in the [Creating the Certificate configuration file for KVM on RHEL 8.10 host](#) on page 65 procedure.



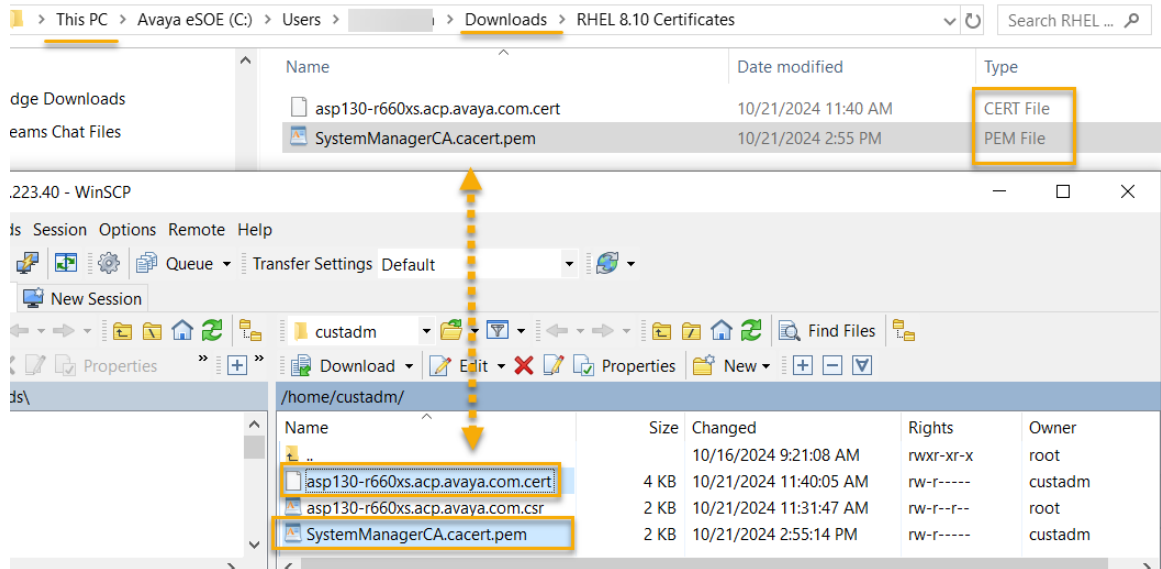
2. Transfer the returned signed certificate by the Certificate Authority (CA) with `cert` extension to the `custadm` home directory.

*** Note:**

In this example, the `asp130r660xs.acp.avaya.com.cert` certificate has been signed and generated by Avaya Aura® System Manager. When using an external CA such as: VeriSign, DigiCert, Symantec, etc. ensure to rename the generated signed certificate with the corresponding name and format: `<HOSTNAME>.cert`.

3. Transfer the Root CA certificate provided by the Certificate Authority (CA) to the `custadm` home directory.

In the following example the Root CA certificate downloaded from Avaya Aura® System Manager will be used.



4. Log in to the corresponding KVM on RHEL 8.10 host using a Secure Shell (SSH) client such as Putty (not provided by Avaya).
5. Authenticate using the existing `custadm` credentials.
6. Run the following commands:

- a. `sudo cp <HOSTNAME>.cert /etc/cockpit/ws-certs.d/ [sudo]`
password for custadm:

Example:

```
sudo cp asp130r660xs.acp.avaya.com.cert /etc/cockpit/ws-certs.d/
```

- b. `cd /etc/cockpit/ws-certs.d/`

- c. `ls -lrt`

*** Note:**

At this point, it is expected to have a key file and a CA signed certificate under the `/etc/cockpit/ws-certs.d/` directory.

*** Note:**

If there is a user generated self-signed certificate and a key present as displayed in the example below, these must be renamed prior to restarting cockpit services. System auto-generated certificates and key do not require renaming (`0-self-signed.key`, `0-self-signed.cert`, `0-self-signed-ca.pem`).

```

[cert:adm@aspl30-r660xs ~]$ sudo cp aspl30r660xs.acp.avaya.com.pem /etc/cockpit/ws-certs.d/
[sudo] password for custadm:
[custadm@aspl30-r660xs ~]$ cd /etc/cockpit/ws-certs.d/
[custadm@aspl30-r660xs ws-certs.d]$ ls -lrt
total 36
-rw-----. 1 root    root    1704 Oct  9 09:51 0-self-signed.key
-rw-r--r--. 1 root    root    1708 Oct  9 09:51 0-self-signed.cert
-rw-r--r--. 1 root    root    2126 Oct  9 09:51 0-self-signed-ca.pem
-rw-----. 1 root    root    1704 Oct 10 15:47 user-generated-cockpit-selfsigned.key
-rw-r--r--. 1 root    root    1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert
-rw-r--r--. 1 custadm custadm  921 Oct 11 06:41 aspl30-r660xs-1.cfg
-rw-----. 1 root    root    1704 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.key
-rw-r--r--. 1 root    root    1269 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.csr
-rw-r--r--. 1 root    root    1850 Oct 11 12:56 aspl30-r660xs.acp.avaya.com.cert
[custadm@aspl30-r660xs ws-certs.d]$

```

7. Following steps are required only if user has generated self-signed certificates apart from the ones that comes with the system by default.

- a. `sudo mv <user-generated-self-signed>.cert <user-generated-self-signed>.cert.bak` [sudo] password for custadm:

Example:

```
mv user-generated-cockpit-selfsigned.cert user-generated-cockpit-selfsigned.cert.bak
```

- b. `sudo mv <user-generated-self-signed>.cert <user-generated-self-signed>.key.bak`

Example:

```
mv user-generated-cockpit-selfsigned.key user-generated-cockpit-selfsigned.key.bak
```

- c. `ls -lrt`

```

[custadm@aspl30-r660xs ws-certs.d]$ ls -lrt
total 36
-rw-----. 1 root    root    1704 Oct 10 15:47 user-generated-cockpit-selfsigned.key.bak
-rw-r--r--. 1 root    root    1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert.bak
-rw-r--r--. 1 custadm custadm  921 Oct 11 06:41 aspl30-r660xs-1.cfg
-rw-----. 1 root    root    1704 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.key
-rw-r--r--. 1 root    root    1269 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.csr
-rw-r--r--. 1 root    root    1850 Oct 11 12:56 aspl30-r660xs.acp.avaya.com.cert
-rw-----. 1 root    root    1704 Oct 11 13:49 0-self-signed.key
-rw-r--r--. 1 root    root    1769 Oct 11 13:49 0-self-signed.cert
-rw-r--r--. 1 root    root    2204 Oct 11 13:49 0-self-signed-ca.pem
[custadm@aspl30-r660xs ws-certs.d]$

```

8. Restart cockpit services executing the following commands:

- a. `sudo systemctl daemon-reload` Enter custadm password
- b. `sudo systemctl restart cockpit`
- c. `sudo systemctl status cockpit`

*** Note:**

Validate cockpit service is active “(running)”. If system failed to start, ensure proper certificate, key file has been transferred with the corresponding format and labels (must match system hostname). If problem persists, reach out to Avaya support.

```
[custadm@aspl30-r660xs ws-certs.d]$ sudo systemctl daemon-reload
[sudo] password for custadm:
[custadm@aspl30-r660xs ws-certs.d]$
[custadm@aspl30-r660xs ws-certs.d]$
[custadm@aspl30-r660xs ws-certs.d]$ sudo systemctl restart cockpit
[custadm@aspl30-r660xs ws-certs.d]$ sudo systemctl status cockpit
● cockpit.service - Cockpit Web Service
   Loaded: loaded (/usr/lib/systemd/system/cockpit.service; static; vendor preset: disabled)
   Active: active (running) since Fri 2024-10-11 13:05:48 MDT; 8s ago
     Docs: man:cockpit-ws(8)
   Process: 6514 ExecStartPre=/usr/libexec/cockpit-certificate-ensure --for=cockpit-tls (code=exited, status=0/SUCCESS)
  Main PID: 6516 (cockpit-tls)
    Tasks: 1 (limit: 406662)
   Memory: 916.0K
   CGroup: /system.slice/cockpit.service
           └─6516 /usr/libexec/cockpit-tls

Oct 11 13:05:48 aspl30-r660xs.acp.avaya.com systemd[1]: Starting Cockpit Web Service...
Oct 11 13:05:48 aspl30-r660xs.acp.avaya.com systemd[1]: Started Cockpit Web Service.
[custadm@aspl30-r660xs ws-certs.d]$
```

Following example displays a discrepancy between the key file name and current system short hostname `aspl30r660xs` vs `aspl30-r660xs`, thus preventing cockpit service to start.

```
● cockpit.service - Cockpit Web Service
   Loaded: loaded (/usr/lib/systemd/system/cockpit.service; static; vendor preset: disabled)
   Active: failed (Result: exit-code) since Fri 2024-10-11 13:52:03 MDT; 1min 20s ago
     Docs: man:cockpit-ws(8)
   Process: 7169 ExecStartPre=/usr/libexec/cockpit-tls (code=killed, signal=TERM)
   Process: 7237 ExecStartPre=/usr/libexec/cockpit-certificate-ensure --for=cockpit-tls (code=exited, status=1/FAILURE)
  Main PID: 7169 (code=killed, signal=TERM)

Oct 11 13:52:03 aspl30-r660xs.acp.avaya.com systemd[1]: Starting Cockpit Web Service...
Oct 11 13:52:03 aspl30-r660xs.acp.avaya.com cockpit-certificate-ensure[7237]: cockpit-certificate-ensure: open: /etc/cockpit/ws-certs.d/aspl30r660xs.acp.avaya.com.key: No such file or directory
Oct 11 13:52:03 aspl30-r660xs.acp.avaya.com systemd[1]: cockpit.service: Control process exited, code=exited status=1
Oct 11 13:52:03 aspl30-r660xs.acp.avaya.com systemd[1]: cockpit.service: Failed with result 'exit-code'.
Oct 11 13:52:03 aspl30-r660xs.acp.avaya.com systemd[1]: Failed to start Cockpit Web Service.
~
```

9. Proceed with the following commands to install the CA root certificate in the CA trust store location:

- a. `cd /home/custadm`
- b. `ls -lrt`

*** Note:**

It is expected to have the CA root certificate transferred as described in STEP 3.

Example:

```
[custadm@aspl30-r660xs ~]$ ls -lrt
total 12
-rw-r--r--. 1 root    root    1269 Oct 21 12:31 aspl30-r660xs.acp.avaya.com.csr
-rw-r-----. 1 custadm custadm 3335 Oct 21 12:40 aspl30-r660xs.acp.avaya.com.cert
-rw-r-----. 1 custadm custadm 1241 Oct 21 15:55 SystemManagerCA.cacert.pem
[custadm@aspl30-r660xs ~]$
```

- c. If the Root CA certificate is not in a `pem` format e.g. `crt` or other, it must be converted to a `pem` format prior to continuing. If the certificate has been transferred

in the expected format, you may skip to the next step, otherwise use the following commands to convert certificates to PEM:

- From CRT to PEM

```
sudo openssl x509 -inform DER -in <ROOT_CA_Certificate>.cert
-out
<ROOT_CA_Certificate>.pem
```

Example:

```
sudo openssl x509 -inform DER -in SystemManagerCA.cacert.crt
-out
SystemManagerCA.cacert.pem
```

- From DER to PEM

```
sudo openssl x509 -inform DER -in <ROOT_CA_Certificate>.der
-out
<ROOT_CA_Certificate>.pem
```

Example:

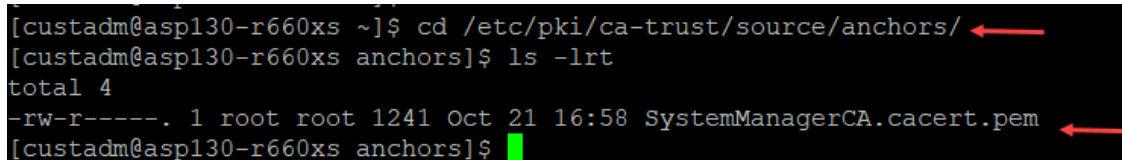
```
sudo openssl x509 -inform DER -in SystemManagerCA.cacert.der
-out
SystemManagerCA.cacert.pem
```

d. `sudo cp <ROOT_CA_Certificate>.pem /etc/pki/ca-trust/source/anchors/`

[sudo] password for custadm:

e. `cd /etc/pki/ca-trust/source/anchors/`

f. `ls -lrt`



```
[custadm@asp130-r660xs ~]$ cd /etc/pki/ca-trust/source/anchors/
[custadm@asp130-r660xs anchors]$ ls -lrt
total 4
-rw-r-----. 1 root root 1241 Oct 21 16:58 SystemManagerCA.cacert.pem
[custadm@asp130-r660xs anchors]$
```

g. `sudo update-ca-trust enable`

h. `sudo update-ca-trust extract`

i. `sudo openssl verify <ROOT_CA_Certificate>.pem`

Example:

```
sudo openssl verify SystemManagerCA.cacert.pem
```

```
[custadm@asp130-r660xs anchors]$ sudo update-ca-trust enable
[custadm@asp130-r660xs anchors]$ sudo update-ca-trust extract
[custadm@asp130-r660xs anchors]$
[custadm@asp130-r660xs anchors]$
[custadm@asp130-r660xs anchors]$ sudo openssl verify SystemManagerCA.cacert.pem
SystemManagerCA.cacert.pem: OK
```

j. Verify installed SSL certificate in Cockpit:

- openssl s_client -connect localhost:9090 -tls1_3
- openssl s_client -connect localhost:9090 -tls1_2

Example:

```
330/121KPNWJc2pc3N1X190495312dGVtJ1W1W5U1W1C1UYRENBLE9VFO1H
TVQsTz1BVkFZQTAdBgNVHQ4EFgQUHUIIpVLFJxARtr60lqkpEo7WNLgwdQYXKZoi
hvcNAQELBOADggEBAGek0PDYNjSt/DXNeWMNg+J7W3CtToKhRDeAFDRRMj8nDfIS
ceZ/i123soZ/AgNjJlDhBNWf0atz/SUVsUDhKz48XbF10vH4kOAh1Kg4M15zYlrc
FfsEGdOptaSk83HOjg/e+uJTbcHf9F6qhu0IFzmqjovRteYiyidqr060FUCU4SkY
CNuDLJusa/8IP5YoDiGhCHLM06lLbwgaWcbu7naxuLYICRXU0YfUUAi81710XRPbY
6QBWvbtYrfFulldl8Bwyu//cBPJe7YmqjFhFlA70MQIBmA4U9d9GeBuoctExuR9DC
bnSL4RsVg/ArG/1z9zVLMf5sYhPIGVw1jF9EWXY=
-----END CERTIFICATE-----
subject=CN = aspl30-r660xs.acp.avaya.com, CN = aspl30-r660xs, OU = ASP-Engineering, O = Avaya LLC, L = Denver, ST = CO, C
= US

issuer=CN = System Manager CA, OU = MGMT, O = AVAYA

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2761 bytes and written 297 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS not supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
closed
```

Adding the CA root certificate to Chrome or Microsoft Edge

About this task

Use this procedure to install on every client PC the CA root certificate provided by an organizational or external CA.

In this procedure the Avaya Aura® System Manager root certificate is used. Customers using an external CA or a Microsoft CA can skip steps 1 through 5 and proceed with the root certificate installation.

*** Note:**

Certificates signed by a trusted, reputable Certificate Authority may not require installing root certificate on every client (PC) web browser. Consult with CA vendor.

For browsers not listed in this section, refer to the browser vendor documentation to import CRT certificates.

Users (Client PC) with other OS apart from Windows such as Mac OS, RedHat, or CentOS, should refer to each vendor OS documentation to properly install CA root certificates.

Before you begin

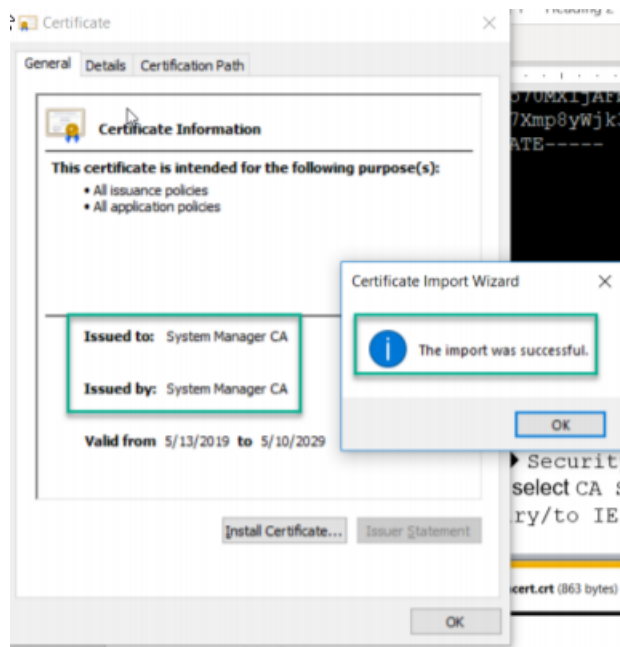
Customers using an External CA or Microsoft CA, should have by now the root certificate provided by the CA in CRT format.

Procedure

1. Open *Microsoft Edge* or *Chrome* and access Avaya Aura® System Manager.
2. Login with administrative credentials. For example, `admin`.
3. Navigate to **Services > Security > Certificates > Authority**.
4. Under **CA Functions**, select **CA Structure & CRLs**.
5. Select **Download binary/to IE**.



6. Select **Open**.
7. Select **Install Certificate**.
8. Select **Local Machine**.
9. Select **Next**.
10. Select **Place all certificates in the following store** and click **Browse**.
11. Select **Trusted Root Certification Authorities** and click **OK**.
12. Select **Next**.

13. Select **Finish**.

Adding the CA root certificate to Firefox

About this task

Use this procedure to install on every client PC the CA root certificate provided by an organizational or external CA.

In this procedure the Avaya Aura® System Manager root certificate is used. Customers using an external CA or a Microsoft CA can skip steps 1 through 5 and proceed with the root certificate installation.

* Note:

Certificates signed by a trusted, reputable Certificate Authority may not require installing root certificate on every client (PC) web browser. Consult with CA vendor.

For browsers not listed in this section, refer to each browser vendor documentation to import CRT certificates.

Users (Client PC) with other OS apart from Windows such as Mac OS, RedHat, or CentOS, should refer to each vendor OS documentation to properly install CA root certificates.

Before you begin

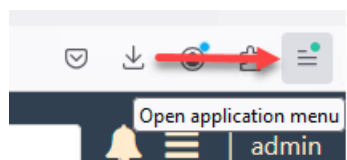
Customers using an External CA or Microsoft CA, should have by now the root certificate provided by the CA in CRT format.

Procedure

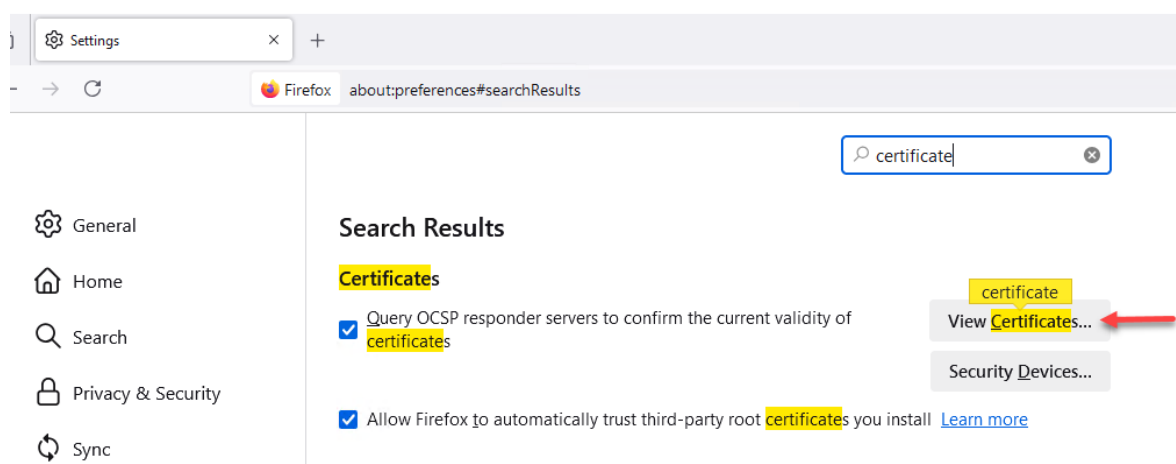
1. Open a web browser using Firefox and access Avaya Aura® System Manager.
2. Login with administrative credentials: For example, `admin`.
3. Navigate to **Services > Security > Certificates > Authority**.
4. Under **CA Functions**, select **CA Structure & CRLs**.
5. Select **Download to Firefox**.

A file with a name `cacert` downloads automatically.

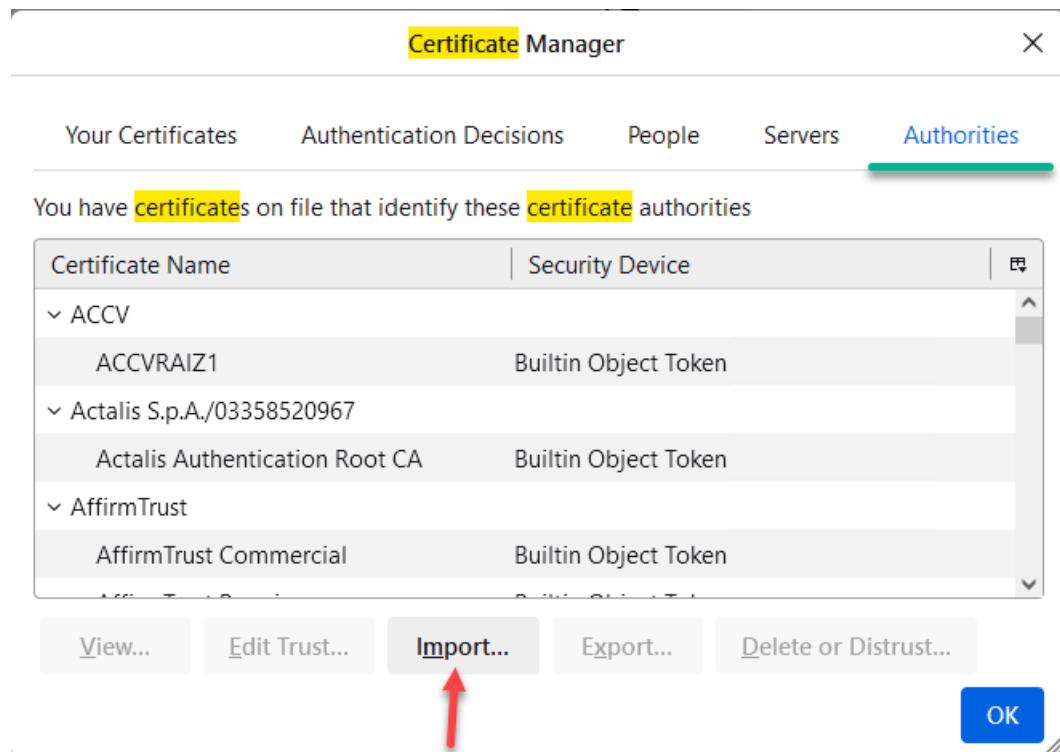
6. Click on the 3 lines icon in the browser upper-right corner and select **Settings**.



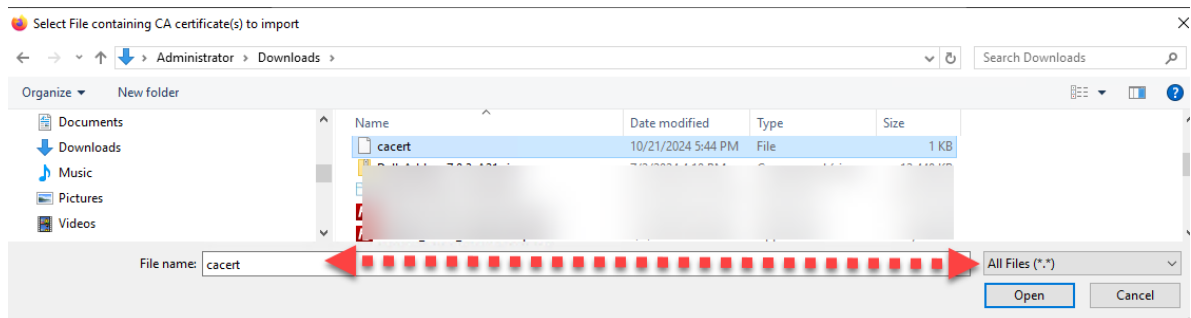
7. In the **Find in Settings** field type in Certificate and click on **View Certificates...**



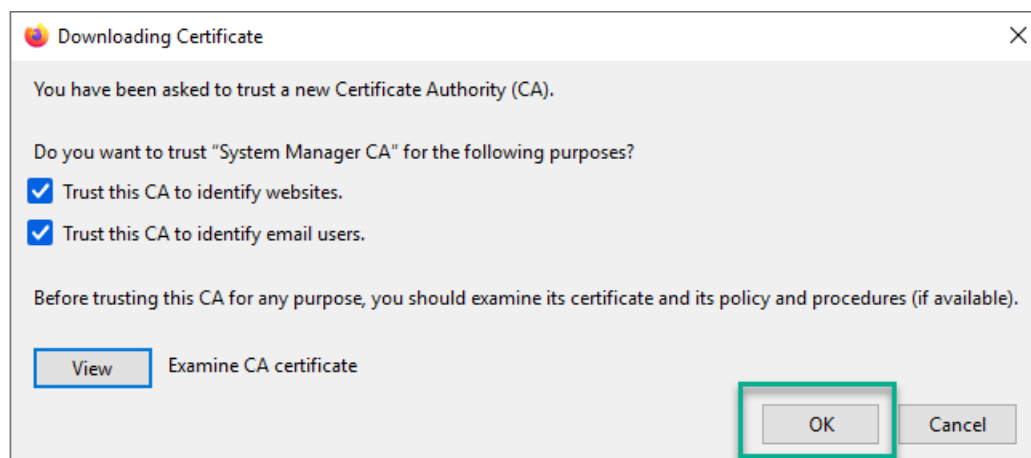
8. Under the Authorities tab, click on **Import...**



9. Browse to the location where the `cacert` file was previously downloaded, for example `downloads` on the local PC, and change from the drop-down menu the file type to **All Files (*.*)**. Select the `cacert` file and click **Open**.



10. Check both selections and click **OK**.

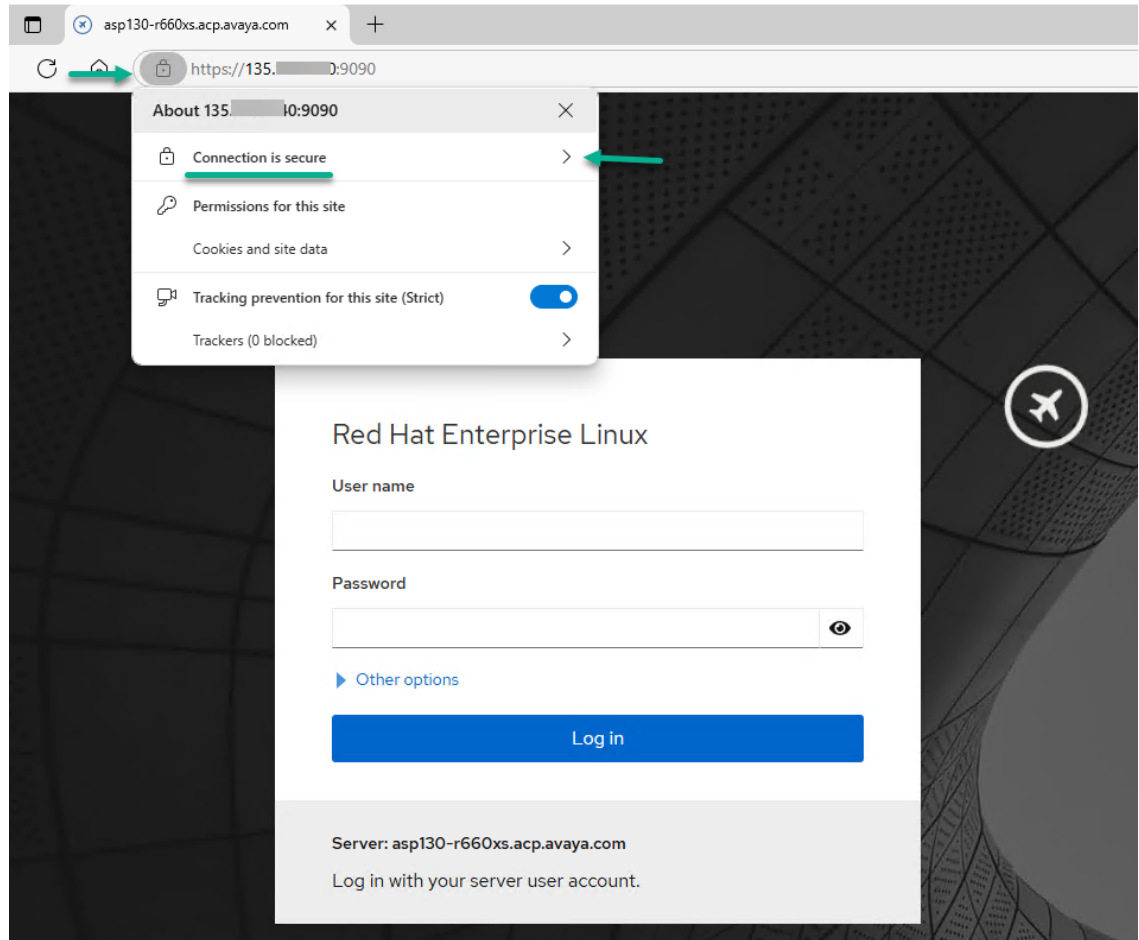


11. Clear the history, cache, and cookies from all previously used browsers. Reference to each browser documentation if needed when doing so.
12. Open a new Web browser to the corresponding KVM on RHEL 8.10 cockpit by either using the FQDN or IP Address, for example `https://<cockpit-ip>:9090`.

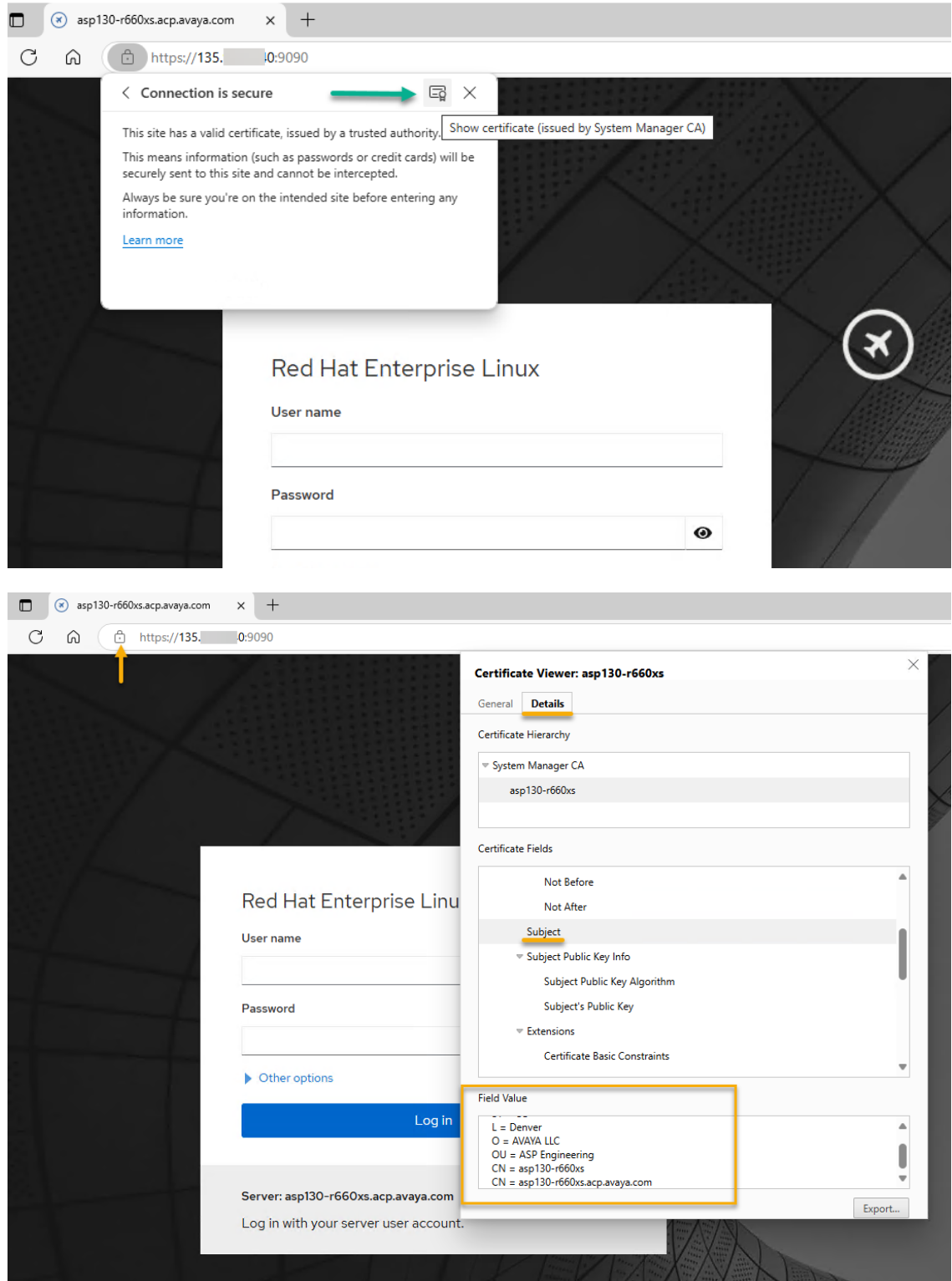
*** Note:**

Connection at this point will show as secure. You can also click on **Certificate** to review the certificate information.

The example screens below may vary depending on the browser. Use as reference only.



Replacing SSL certificates and Keys with Custom Certificates in RHEL 8.10 - Cockpit Web Service



Chapter 10: ASP R6.0.x update process

The ASP R6.0.x update process for security updates and bug fixes was introduced with ASP R6.0.0.1 in 1Q2025. Reference ASP 130 Release Notes for documented upgrade paths and appropriate upgrade documentation based on what release is being updated.

 Note:

As documented in the upgrade documentation listed below, you must install `av-asp-tools-1.5-3.el8.x86_64.rpm` prior to the first ASP 6.0.x service pack.

As of February 2026:

[ASP 130 & S8300 Updating to R6.0.0.4.0 from R6.0.x-rev5](#)

[ASP 130 & S8300 Updating to R6.0.0.3.0 from R6.0.x-rev4](#)

[ASP 130 and S8300 Updating to R6.0.0.2.0 from R6.0.x-rev3](#)

[ASP 130 and S8300 Updating to R6.0.0.1.1 from R6.0.x-rev2](#)

[ASP 130 and S8300 Updating to R6.0.0.1.0 from R6.0-rev1](#)

Always check support.avaya.com for the latest Update documentation for ASP R6.0.x.

Chapter 11: Troubleshooting

Verifying the ASP configuration and network topology

Executing `showConfig` will provide detailed information on the following:

- System (server type, BIOS version)
- CPU
- Memory
- Disk
- Raid controller
- Power supply
- Network interfaces
- USB devices
- Software
- Updates installed in the system
- Network topology
- Network bridge topology
- Other network connections
- Virtual Machine IP addresses
- NTP configuration
- Performance profile
- Failed SystemD units
- Error message
- Crypto policy
- OS hardening
- Virtual Machines
- Virtual Machines without autostart
- Virtual Machines Storage Pools

Server inaccessible

Condition

In some cases, an S8300E may become inaccessible. This can be identified with the **OK-to-Remove** LED blinking continuously.

Typically recovery requires a server reboot (reseat the S8300E). Within the following 8 to 10 minutes, the **OK-to-Remove** LED stops blinking and server undergoes a reboot automatically. After a further 5 to 6 mins if all LEDs are off, then the server is stabilized.

Cause

S8300 card has been reseated without performing the graceful shutdown.

Solution

1. Before removing or reseating the S8300 card in the Branch Gateway, shut down the S8300 card by pressing the **Shut Down** button for 3 to 4 seconds.
2. Once **OK TO REMOVE** LED stops blinking and becomes stable, then reseal the S8300 into the Branch Gateway.

Troubleshooting using CLI commands

Troubleshooting gateway CLI command in S8300

The G450 and G430 gateway monitor the presence and sanity of the S8300 using a heartbeat on an internal Ethernet connection through the gateway backplane.

When you use the **show mg list** CLI command, one of the following messages or values are displayed when you check the status of the S8300 in slot v1 :

• Not Installed

```
G450-001(super)# show mg list
SLOT    TYPE          CODE          SUFFIX    HW VINTAGE    FW VINTAGE
----    -
v1      -- Not Installed --
v2
```

S8300 displays **Not Installed**, when the gateway does not detect a board. Possible causes are empty slot, S8300 not fully inserted, or faulty connectors.

• Initializing/Faulted

```
G450-001(super)# show mg list
SLOT    TYPE          CODE          SUFFIX    HW VINTAGE    FW VINTAGE
----    -
v1      -- Initializing --
v2
```

S8300 displays **Initializing/Faulted**, when the gateway detects a board, but it does not respond to ping. Possible causes are faulted board, vSwitch not setup correctly, software not loaded or not running.

- Board **SUFFIX** is **X** and **HW VINTAGE** is **0**

```
G450-001(super)# show mg list
SLOT      TYPE      CODE      SUFFIX  HW VINTAGE  FW VINTAGE
-----
v1         S8300      ICC       X        0           0
v2
```

S8300 displays values for SUFFIX and HW VINTAGE as X and 0 respectively. This implies that the gateway can ping the S8300 on the internal VLAN, but the heartbeat is not present and the gateway did not receive the board suffix and Vintages. Possible causes are the S8300 is not fully initialized or the Avaya heartbeat software is not operational, but the ESXi vSwitch is setup correctly.

- Board **SUFFIX** is correct

```
G450-001(super)# show mg list
SLOT      TYPE      CODE      SUFFIX  HW VINTAGE  FW VINTAGE
-----
v1         S8300      ICC       E        1           1
v2
```

S8300 displays correct suffix. This implies that the S8300 heartbeat is present and no issues are detected by the gateway.

Troubleshooting gateway log messages

You can view the syslog stored locally on the gateway using the **show logging file content** CLI command.

If the S8300 heartbeat stops, the gateway will reset the S8300 and log a message indicating that a **HARD RESET** and then a **SOFT RESET** was performed. There could also be **Unsupported Media Module** messages when the gateway has not identified the type of board in the slot.

```
<187>Dec 29 15:25:04 g450graf -NoTag: -NoUTC(0 0 0:14:20) 2021 350 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 carries out HARD RESET,
ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:24:11 g450graf -NoTag: -NoUTC(0 0 0:13:27) 2021 690 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
insertion 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:24:11 g450graf -NoTag: -NoUTC(0 0 0:13:27) 2021 690 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
extraction 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:22:05 g450graf -NoTag: -NoUTC(0 0 0:11:21) 2021 420 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
insertion 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:19:43 g450graf -NoTag: -NoUTC(0 0 0:08:59) 2021 650 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 carries out SOFT RESET,
ID=e2a214cc8919d0e4ebf0620beb381a53
```

Gateway faults

You can generate and display faults or alarms when S8300 is not inserted into v1, using the **set icc-monitoring enable** CLI command and by setting the S8300 Monitoring status to **Enabled**. Set status to **Disabled** when you are not using the **show faults** feature.

```
g450graf-019(develop)# show icc-monitoring
Slot v1 S8300 Monitoring Status: Enabled
Done!
g450graf-019(develop)# show faults
```

```
CURRENTLY ACTIVE FAULTS
```

```
-----
+ Expected S8300 in v1 not present, 01/13-16:14:24.00
```

When monitoring status is set to enabled, a log message is displayed similar to the following example, if the S8300 is not in service in the show logging file content output.

```
<187>Jan 21 16:14:24 g450graf -NoTag: -NoUTC(0 0 0:01:32) 2022 105 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 in slot v1 is NOT
INSERVICE, ID=e2a214cc8919d0e4ebf0620beb381a53
```

Log and file collection to aid in troubleshooting

Collecting Host level log information

When there is an issue with Avaya Aura® applications, or solution behaviors that require troubleshooting or further investigation by Avaya services teams, you should immediately gather the following logs so that the information related to the incident timeframe is not lost in log rotation.

- SOS reports
- Libvirt debug logs for individual VMs – reference application specific documentation
- All /var/log/asp update logs
- .bash_history for both root and custadm users

Collecting a KVM on RHEL 8.10 SOS Report from the CLI

About this task

When there is an issue with the KVM on RHEL host or Avaya Aura® applications, or solution behaviors that require troubleshooting or further investigation by the Avaya support teams, it is required to collect the KVM on RHEL SOS report from the host.

Examples below may reference ASP 130 but will be similar output for ASP S8300.

Procedure

1. Open an SSH session to the KVM on RHEL host using PuTTY.
2. Log in with the custadm credentials.

 Note:

User will be prompted to re-enter the `custadm` password throughout this procedure to use `sudo`.

3. Run the following command to generate the SOS report: **`sudo sos report`**

4. Press **Enter** to continue.

```
[custadm@asp-s8300-43 ~]$ sudo sos report
[sudo] password for custadm:

sosreport (version 4.7.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.47wlv83 and may be provided to a Red Hat support
representative.

Any information provided to Red Hat will be treated in accordance with
the published support policies at:

    Distribution Website : https://www.redhat.com/
    Commercial Support   : https://access.redhat.com/

The generated archive may contain data considered sensitive and its
content should be reviewed by the originating organization before being
passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.
```

5. It prompts to enter the case id that you are generating the report for, but this is optional, leave blank and press **Enter** to continue.

```
Optionally, please enter the case id that you are generating this report for []:

Setting up archive ...
Setting up plugins ...
[plugin:fwupd] skipped command 'fwupdmgr get-approved-firmware': required
services missing: fwupd.
[plugin:fwupd] skipped command 'fwupdmgr get-devices --no-unreported-check':
required services missing: fwupd.
[plugin:fwupd] skipped command 'fwupdmgr get-history': required services missing:
fwupd.
[plugin:fwupd] skipped command 'fwupdmgr get-remotes': required services missing:
fwupd.
[plugin:fwupd] skipped command '/usr/libexec/fwupd/fwupdagent get-devices':
required services missing: fwupd.
[plugin:fwupd] skipped command '/usr/libexec/fwupd/fwupdagent get-updates':
required services missing: fwupd.
[plugin:networking] skipped command 'ip -s macsec show': required kmods missing:
macsec. Use '--allow-system-changes' to enable collection.
[plugin:sssd] skipped command 'sssdctl config-check': required services missing:
sssd.
[plugin:sssd] skipped command 'sssdctl domain-list': required services missing:
sssd.
[plugin:systemd] skipped command 'resolvectl status': required services missing:
systemd-resolved.
[plugin:systemd] skipped command 'resolvectl statistics': required services
missing: systemd-resolved.
```

```
Running plugins. Please wait ...

Finishing plugins
Finished running
plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
    /var/tmp/sosreport-asp-s8300-43-2025-04-24-uipubds.tar.xz

Size      17.04MiB
Owner     root
sha256    8fc96dd5485f49c77b380228e9bd0ece436905e8c26ceb2030287a1a1c82c296

Please send this file to your support representative.
```

The SOS report will be saved in the `/var/tmp/` directory.

6. Change directory to `/var/tmp/` and list the contents.
7. Copy the sos report `tar.xz` file and `tar.xz.sha256` file to `/home/custadm/` directory:
 - a. `sudo cp <sosreport_name.tar.xz> /home/custadm/`
 - b. `sudo cp <sosreport_name.tar.xz.sha256> /home/custadm/`
8. Change directory to `/home/custadm/` and list the contents. The SOS report files will be displayed.

```
(custadm@asp130-r660xs-a31p ~)$ ls
asp130-r660xs-a31p.acp.avaya.com.cert  sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz
asp130-r660xs-a31p.acp.avaya.com.csr  sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz.sha256
```

9. Modify the permissions on both files:
 - a. `sudo chmod 775 <sosreport_name.tar.xz>`
 Example: `sudo chmod 775 sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz`
 - b. `sudo chmod 775 <sosreport_name.tar.xz.sha256>`
 Example: `sudo chmod 775 sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz.sha256`
10. WinSCP to the KVM on RHEL host and log in with the `custadm` credentials.
11. Go to `/home/custadm/` and download the SOS report files to a local machine.

/home/custadm/				
Name	Size	Changed	Rights	Owner
		9/19/2024 10:30:23 AM	rw-r-xr-x	root
sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz.sha256	1 KB	10/17/2024 9:53:02 AM	rw-rw-r-x	root
sosreport-asp130-r660xs-a31p-2024-10-17-wrtdvkq.tar.xz	20,760 KB	10/17/2024 9:44:55 AM	rw-rw-r-x	root

Collecting a KVM on RHEL 8.10 SOS Report from the Cockpit UI

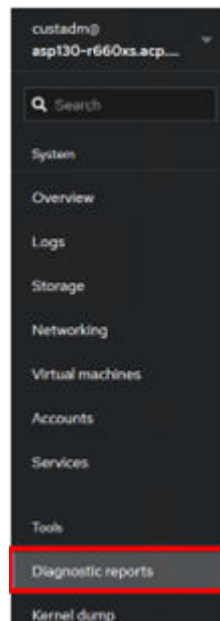
About this task

Examples below may reference ASP 130 but will be similar output for ASP S8300.

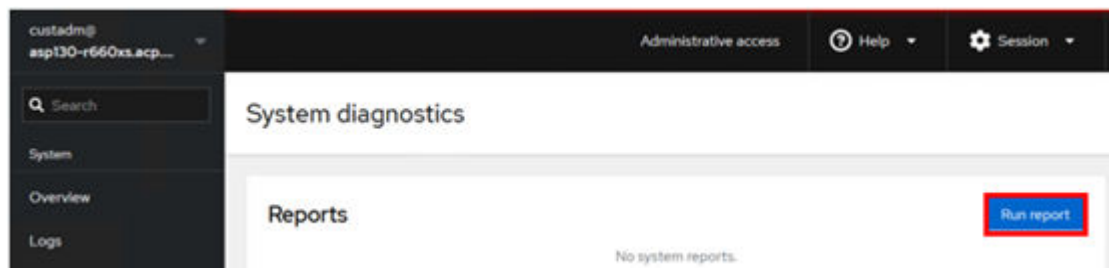
When there is an issue with Avaya Aura® applications, or solution behaviors that require troubleshooting or further investigation by Avaya support teams, it is required to collect the KVM on RHEL SOS report from the host.

Procedure

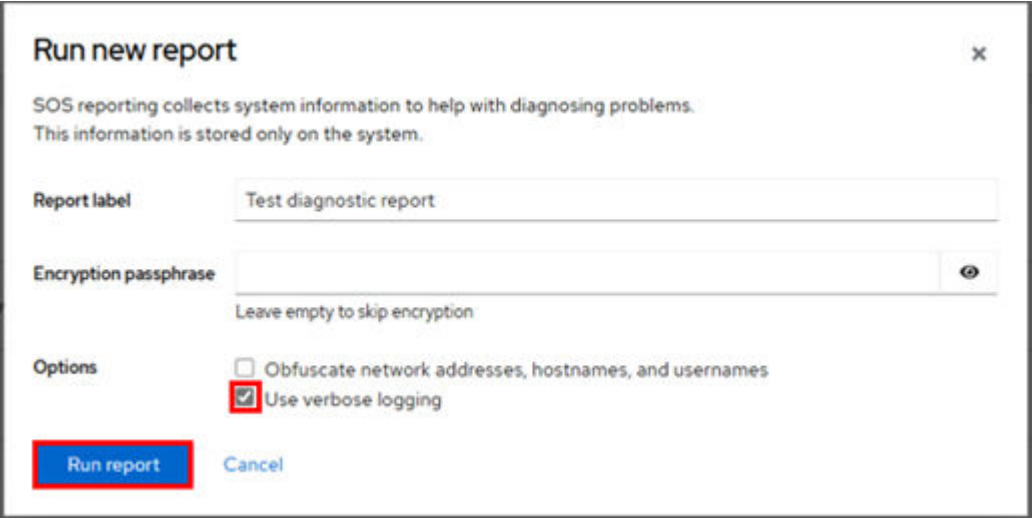
1. Open a web browser to the Cockpit UI `https://server_ip_fqdn:9090/` and log in with the `custadm` or `root` credentials.
2. From the left pane, go to **Diagnostic reports**.



3. Click **Run report**.



4. Enter the report label and in Options, check **Use verbose logging**. Click **Run report**.



Run new report [X]

SOS reporting collects system information to help with diagnosing problems.
This information is stored only on the system.

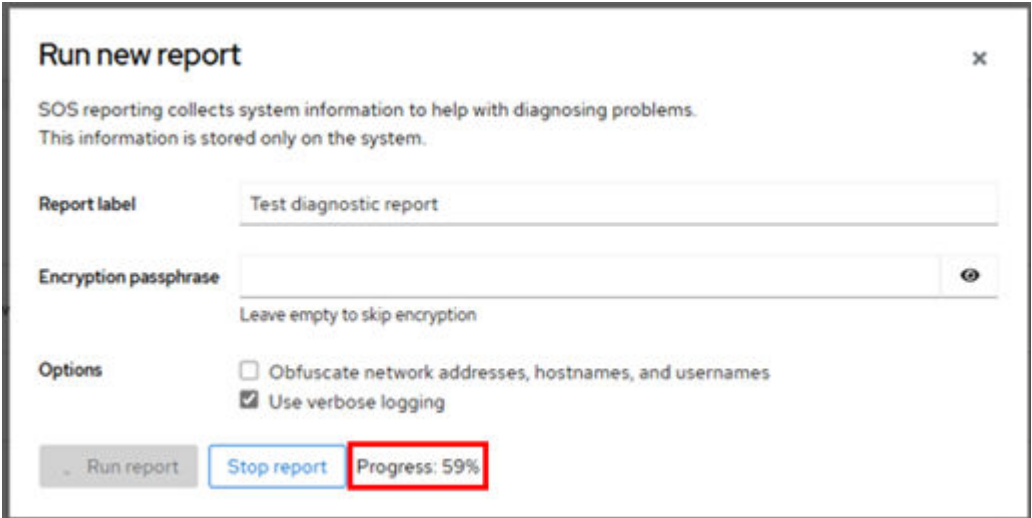
Report label: Test diagnostic report

Encryption passphrase: [Empty] [Eye icon]
Leave empty to skip encryption

Options:
☐ Obfuscate network addresses, hostnames, and usernames
☒ Use verbose logging

[Run report] [Cancel]

Progress is displayed at the bottom.



Run new report [X]

SOS reporting collects system information to help with diagnosing problems.
This information is stored only on the system.

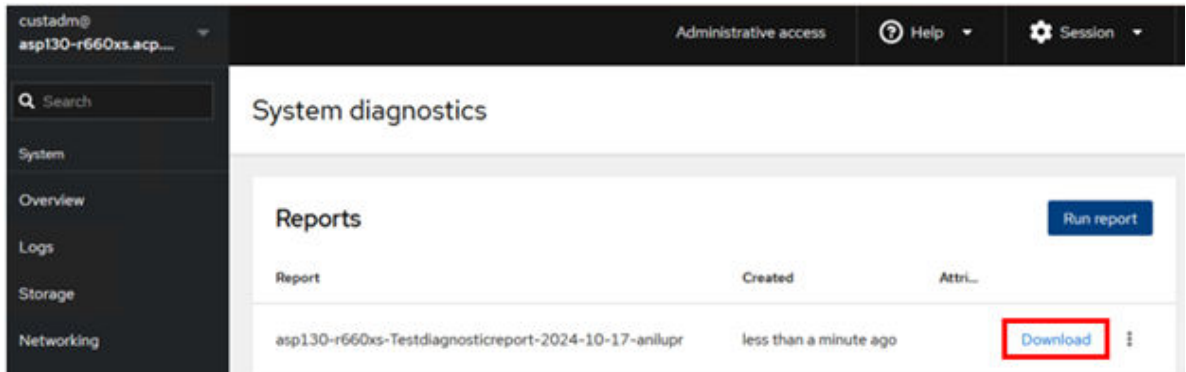
Report label: Test diagnostic report

Encryption passphrase: [Empty] [Eye icon]
Leave empty to skip encryption

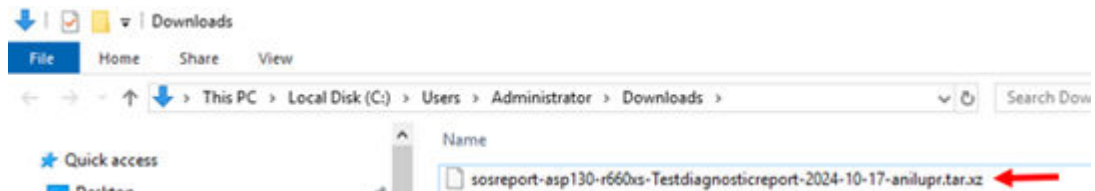
Options:
☐ Obfuscate network addresses, hostnames, and usernames
☒ Use verbose logging

[Run report] [Stop report] [Progress: 59%]

- Once the report completes, click **Download** to download/save the SOS report files to a local machine.



A tar.xz file is downloaded.



Chapter 12: Resources

Avaya Solutions Platform 130/S8300 documentation

The following documents are available on Avaya support site at <https://support.avaya.com/>:

Title	Description
<i>Avaya Solutions Platform 130/S8300 Overview and Specification</i>	Describes the key features of Avaya Solutions Platform
<i>Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300</i>	Describes how to install, maintain, and troubleshoot Avaya Solutions Platform S8300.
<i>Installing the Avaya Solutions Platform 130 Series</i>	Describes how to install Avaya Solutions Platform 130 Series 6.0.x.
<i>Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series 6.0.x</i>	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series 6.0.x.
<i>Avaya Solutions Platform S8300 6.0.x Release Notes</i>	Release Notes.
<i>Avaya Solutions Platform 130 6.0.x Release Notes</i>	Release Notes.
<i>PCN2174Su – Avaya Solutions Platform S8300 6.0.x</i>	Product Correction Notice (PCN) introducing the ASP S8300 R6.0.x software and subsequent Service Packs.
<i>PCN2180Su – Avaya Solutions Platform S8300 6.0 SSP</i>	Product Correction Notice (PCN) introducing the ASP S8300 R6.0.x Security Service Packs (SSPs) available beginning with ASP R6.0.0.3.0 and later.
<i>PCN2173Su – Avaya Solutions Platform 130 6.0.x</i>	Product Correction Notice (PCN) introducing the ASP 130 R6.0.x software and subsequent Service Packs.
<i>PCN2179Su – Avaya Solutions Platform 130 6.0 SSP</i>	Product Correction Notice (PCN) introducing the ASP 130 R6.0.x Security Service Packs (SSPs) available beginning with ASP R6.0.0.3.0 and later.
<i>Avaya Solutions Platform R6.0.x Security Service Pack Installation Application Note</i>	Instructions for installing ASP Security Service Packs (SSPs).

Table continues...

Title	Description
<i>ASP 130 R6.0.0.4.0 and Later VLAN & VLAN TRUNKING CONFIGURATION GUIDE</i>	This application note provides guidance for configuring VLANs and enabling VLAN trunking on ASP R6.0.0.4.0 (KVM on RHEL 8.10) or later release. It is intended for system administrators and technical users responsible for deploying and managing virtual infrastructure on Avaya Solutions Platform (ASP) compute servers.
<i>ASP 130 R6.0.0.3.0 and Earlier VLAN & VLAN TRUNKING CONFIGURATION GUIDE</i>	This application note provides guidance for configuring VLANs and enabling VLAN trunking on ASP R6.0.0.3.0 (KVM on RHEL 8.10) or earlier release. It is intended for system administrators and technical users responsible for deploying and managing virtual infrastructure on Avaya Solutions Platform (ASP) compute servers.
<i>Port Matrix for ASP S8300</i>	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices.
<i>Port Matrix for ASP 130</i>	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices.
<i>Policies for technical support of the Avaya Solutions Platform (ASP) 130 and S8300E R6.0.x</i>	This document and statements related to support are only with respect to Avaya Services support of the software and hardware of the Avaya Solutions Platform (ASP) 130 server and S8300E server based on supported and tested configurations.
<i>Avaya Solutions Platform 130 Series iDRAC9 Best Practices</i>	Describes the best practices of using the Integrated Dell Remote Access Controller (iDRAC).
<i>PSN027113u - Avaya Solutions Platform 100 Series Dell® R660xs Avaya Certified BIOS/Firmware Update, Version 2</i>	Always check for a newer version of Avaya certified BIOS/Firmware. New PSNs are published for each new release.

Table continues...

Title	Description
<i>PSN027112u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 16</i>	Always check for a newer version of Avaya certified BIOS/Firmware. New PSNs are published for each new release.
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.x.0 documents listed below	Follow the steps outlined in the appropriate document(s) when planning and conducting updates to ASP R6.0.x KVM on RHEL 8.10 hosts running on ASP 130 & S8300E servers using the Avaya certified and approved files. Always check support.avaya.com for new documents as new Service Packs are released.
<i>Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.4.0 (RHEL 8.10) from R6.0.0.3.0 (RHEL 8.10)</i>	 Note: Upgrades to R6.0.0.4.0 and later R6.0.0.x.0 service packs require a step upgrade to R6.0.0.3.0 first.
<i>Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.3.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)</i>	
<i>Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.2.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)</i>	
<i>Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)</i>	
<i>Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)</i>	

 Note:

Documents for migrating from AVP and older ASP R5.x EOMS releases can be found on support.avaya.com.

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.

5. In **Select Release**, select the appropriate release number.

This field is not available if there is only one release for the product.

6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

You can select multiple items in each filter category. For example, you can select a product and multiple user roles.

- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.

- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite 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 collections that others have shared with you.
- Click **Watch** () to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

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.

Using the Avaya InSite Knowledge Base

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

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

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

A

adding the CA root certificate to a Web browser	83 , 85
ASP	
R6.0.x	8
R6.0.x update process	91
verifying configuration	92
verifying network topology	92
Avaya InSite Knowledge Base	105
Avaya Solutions Platform	8
Avaya Solutions Platform S8300	
purpose	6
Avaya support website	105

C

certificate	
creating configuration file	65
certificate administration	
overview	63
certificate signing request in KVM	69
Cockpit	
OOBM access	59 , 60
collection	
delete	104
edit	104
generating PDF	104
sharing content	104
configNetwork	56
configNetwork script	58
configuration	
additional options	40
configuring	
SNMP on RHEL 8.10 host	40
SNMP v2 on RHEL 8.10 host	44
SNMP v3 on RHEL 8.10 host	40
content	
publishing PDF output	104
searching	104
sharing	104
sort by last updated	104
watching for updates	104

D

device registration	20
document changes	6
documentation	101
documentation center	104
finding content	104
navigation	104
documentation portal	104

F

finding content on documentation center	104
---	---------------------

G

gateway CLI command	93
Gateway faults	95
Gateway log messages	94

H

HealthCheck tool registration	16
-------------------------------------	--------------------

I

iDRAC Support Assist file	95
installation	
overview	22

K

KB	
Support site	105
knowledge required	6

L

Libvirt debug logs	95
--------------------------	--------------------

M

migration to ASP 6.0.x	20
------------------------------	--------------------

N

network port verification purpose	55
network settings	
configuration	32
nmcli connection	56
nmcli device	56

O

OOBM	
configuration	58
Overview	58

P

purpose	
---------	--

purpose (<i>continued</i>)		TLS (<i>continued</i>)	
Avaya Solutions Platform S8300	6	viewing settings	51
R		tools required	6
registering new device	17	troubleshooting	
registration		server inaccessible	93
overview	16	V	
status	19	validating	
Release R6.0.x	8	network port configuration	55
replacing		VM	
SSL certificates and keys	64	OOBM access	59 , 60
replacing host server	22	W	
replacing SSL certificates	69	watchlist	104
replacing SSL certificates in Cockpit with a CA signed			
certificate	76		
S			
S8300			
installation	27		
S8300E			
server specification	8		
topology	9		
searching for content	104		
securing network configuration	58		
server inaccessible	93		
server recovery	22 , 62		
setBootPassword	40		
setMaxLoginSessions	40		
setSessionsTimeout	40		
setTimezone	40		
sharing content	104		
show mg list	93		
showConfig	56		
signing the Certificate Signing Request (CSR)	71		
skills required	6		
SNMP			
OID information	47		
SNMP v3 configuration	40		
software remastering	22 , 62		
sort documents	104		
SOS report			
collecting	95 , 97		
SOS reports	95		
SSL certificate			
replacing	76		
storage layout	12		
support	105		
swversion	56		
T			
Technical Onboarding process	20		
TLS			
protocol configuration	50		