Installing the Avaya Solutions Platform 130 Series

Release 6.0.x
Issue 5
February 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

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

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

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

The 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.

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

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users 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

Purpose

This document provides installation procedures and information for the Avaya Solutions Platform 130 Appliance 6.0.x server.

This document is intended for the professional who is involved in installation activities for the Avaya Solutions Platform 130 Appliance 6.0.x server.

Note:

The images and screenshots in this document are for illustration purposes only. The actual user interface may slightly vary due to updates and design changes.

Change history

Issue	Date	Summary of changes
5	February 2026	• Updated for ASP 6.0.0.4.0. • Introduction of support for 10/25GbE NIC.
4	June 2025	• Added ASP 6.0.x storage layout for KVM on RHEL 8.10. • Added NIC assignment mapping. • Updated Chapter 11: ASP R6.0.x update process.
3	April 2025	Updated to include information on configuring SNMP.
2	February 2025	• Updated to include migration from ASP R4.x, R5.x, AVP. • Additional clarification/details provided.
1	October 2024	Initial Release 6.0.x document.

Prerequisites

Before installing or migrating Avaya Solutions Platform 130 Appliance, 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

- Monitor, keyboard, mouse (optional but recommended).
- 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

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.

The ASP 130 R6.0.x server is an Avaya customized Dell R660xs server staged and loaded with KVM on Red Hat Enterprise Linux 8.10 and shipped to an Avaya customer for installation of applications in a virtual environment. The ASP S8300 R6.0.x is a blade server loaded with KVM on Red Hat Enterprise Linux 8.10 and shipped to an Avaya customer for installation of applications in a virtual environment. The R640s are nearing End of Sale and do not ship from Avaya's integrator with KVM on RHEL 8.10. The R640 always requires a migration from ESXi to ASP R6.0.x software KVM on RHEL 8.10.

For detailed information about each specific release, see the latest Avaya Solutions Platform 130 Release Notes.

Summary

- Introduction of Dell R660xs to the ASP 130 product line.
- The ASP 130 R6.0.x R660xs ships with a physical TPM (Trusted Platform Module) that is enabled at the BIOS level. Customer configuration choices with regards to TPM functionality are targeted for a future release.

- Dell R660xs does not support CD/DVD ROM.
- KVM on RHEL 8.10 hypervisor.
- For detailed information about each specific release, see the latest *Avaya Solutions Platform 130 Release Notes* available on https://support.avaya.com.

Avaya Solutions Platform 100 series overview

Avaya Solutions Platform (ASP) is a turnkey hardware solution that is available for many Avaya applications. Avaya Solutions Platform 100 series offers a single virtualized or bare metal server delivering Avaya unified communication and contact center applications. Refer to your product application specific documentation.

The Avaya Solutions Platform 100 series is comprised of three models:

1. ASP 110: This is a bare metal server used by specific Avaya applications. The applications determine which Operating System (OS) is preloaded (application dependent) at Avaya's Integrator. New ASP 110 base servers consist of Dell PowerEdge R660xs and Dell PowerEdge R360xe. Reference application specific documentation for information on ASP 110 servers.
2. ASP 120: This is the Dell R640 shipped from Avaya's Integrator with Avaya Virtualized Platform (AVP) AVP 8.1 preloaded. The ASP 120 is synonymous with Appliance Virtualization Platform (AVP) and required AVP 7.1.3.3 or AVP 8.0.1 or later. ASP 120 shipped with AVP 8.1 preloaded. AVP 8.1 was the final release and ASP 120 is not supported with Avaya Aura® 10.x. Existing ASP 120 can migrate to ASP 130 R6.0.x.
3. ASP 130: This is the Dell R660xs for ASP 6.0.x and ships from Avaya's Integrator with KVM on Red Hat Enterprise Linux 8.10 preloaded. The ASP 130 R4.0 and 5.x versions used the Dell R640 on ESXi 6.5/7.0. Existing ASP 130 R4.0 and 5.x can migrate to ASP 6.0.x KVM on RHEL 8.10.

Note:

This document focuses on Avaya Solutions Platform 130 Appliance (ASP 130) only. Avaya Solutions Platform 130 Appliance R6.0.x utilizes KVM on Red Hat Enterprise Linux 8.10. Avaya does not permit or support the repurposing of servers that deviate from their original integrated configuration.

Key features

The Dell PowerEdge R640 and R660xs are the underlying server hardware used for the Avaya Solutions Platform 130.

The Dell PowerEdge R640 is the original server hardware used for the Avaya Solutions Platform 130. The PowerEdge R640 is a 1U single/dual socket CPU platform designed for Avaya's portfolio

of applications. The R640 updates the CPU(s) and other server technologies over previous Avaya Common Server releases. It is used as the base platform for Avaya offers. The architecture of the R640 is designed to maximize performance and provide flexibility to optimize Avaya's applications and customer use cases.

The Dell PowerEdge R660xs is the new, updated hardware platform for ASP 130. The PowerEdge R660xs is a 1U single/dual socket CPU platform designed for Avaya's portfolio of applications. The R660xs updates the CPU(s) and other server technologies over the previous R640 release. It is used as the going forward base platform for Avaya offers. The architecture of the R660xs is designed to maximize performance and provide flexibility to optimize Avaya's applications and customer use cases.

Supported software

The Avaya Solutions Platform 130 Appliance supports virtualization with a customized image of KVM on Red Hat Enterprise Linux 8.10.

Avaya Solutions Platform 130 Dell® R640 and R660xs servers are supplied under an OEM relationship and managed differently than commercially available servers from the vendor. Support, warranty and repair are through Avaya's processes, not through the OEM vendor's support process.

In addition, ASP 100 Series Server configurations are engineered for specific application needs. No hardware substitutions or additions are allowed. Servers cannot be repurposed.

Only use Avaya provided updates. Updating BIOS, FW, or RHEL/KVM directly from the vendors' web sites results in an unsupported configuration.

For further information concerning use and support of the ASP 130, refer to Policies for technical support of the Avaya Solutions Platform (ASP) 130 R6.0.x.

Dell server overview

The Avaya Solutions Platform servers category includes Dell servers that support Avaya software solutions, some requiring additional hardware and memory requirements beyond the standard configuration. This document covers the standard configuration only. Consult specific Avaya product documentation for application-specific or solution-specific server configurations.

- Avaya Solutions Platform servers are supplied under an OEM relationship, and Avaya servers are treated differently than commercially available servers from the vendors.
- Support, warranty and repair are through Avaya's processes, not through the OEM vendor's support process.
- Lifecycle Hardware and BIOS and firmware updates are managed by the Avaya Common Server team in conjunction with application R&D teams. These servers must *not* be updated

with BIOS or firmware updates from the vendor's web site. You can only use Avaya-provided updates. Updating directly from the vendor's web site results in an unsupported configuration.

- All BIOS or firmware updates are provided through Avaya. Go to the Avaya Support website at http://support.avaya.com for additional information.
- BIOS/Firmware updates are available on http://plds.avaya.com and are customer installable.
- Only use Avaya-provided downloads, information, and support. Send questions to the Server Product Management mailbox at aspsales@avaya.com.
- Avaya Solutions Platform servers are turnkey appliances. No servers designed for a particular application can be repurposed for use with another application. The only exception is when an application provides an upgrade or migration path from an existing server state to a different server state with the appropriate kits, tools, documentation, and training materials.
- Avaya Solutions Platform 130 KVM on RHEL updates should only be obtained from Avaya. Updating directly from the vendors' websites results in an unsupported configuration. Avaya creates a customized image to ensure that any updates are compatible with the underlying hardware, drivers, etc. When Avaya has an update from the vendor, the new image is fully vetted with the Avaya solutions to assess any potential performance or capacity impacts. This image is then made available on http://plds.avaya.com and is customer installable.
- Do not contact Dell or Red Hat for Service; all support, warranty, repair, and maintenance are through the Avaya processes.
- Avaya strongly recommends that all servers are protected with an Uninterrupted Power Supply for power surge and interruption protection. Avaya is not responsible for servers damaged by power surges, brownouts, blackouts etc. when the server is connected to standard power mains and has no protection.
- The Dell R640 H730 RAID battery is a consumable item and therefore is considered a customer replaceable unit (CRU). The RAID battery is not covered under the maintenance agreement. Customers are responsible for installing them, the procedure for which is in the *Maintaining and Troubleshooting Avaya Solutions Platform 130 Series* document. The Dell R640 H750 RAID battery and Dell R660xs H755 RAID batteries are not separate orderable entities. In the event of a failure of the RAID battery in the Dell R640 H750 RAID controller or Dell R660xs H755 RAID controller, the RAID controller itself will need to be replaced. The RAID controller includes a battery.
- Quality assurance - product integrity testing or international environmental restrictions have been completed by Dell and verified with Avaya through the use of Design for Environmental Checklists. These lists include: batteries, printed wiring boards, plastic parts, product packaging, RoHS, green requirements, and energy efficiency.
- It is imperative that only ASP certified applications be deployed on ASP servers. A1SC is required to be utilized for ordering for new installs, migrations, additions of applications. If A1SC output results in multiple servers, applications must be deployed based on configurator output.
- Until an Avaya application is listed as compatible with ASP R6.0.x in the Product Compatibility Matrix on support.avaya.com, and the application has published detailed instructions for deployment on ASP R6.0.x, the application is not considered certified and therefore is not supported.

Note:

This document focuses on the Dell R660xs server constructs. For additional information on the Dell R640, please reference Installing the Avaya Solutions Platform 130 Series R5.1.x.

Avaya Solutions Platform Appliance profiles

In the Avaya Solutions Platform 100 Series, server constructs are shared among Avaya Solutions Platform 110 Appliance and Avaya Solutions Platform 130 Appliance.

Hardware configurations for each profile are locked. The addition of memory, storage, or changing out the NICs is not permitted and results in an unsupported configuration.

Note:

A1SC configurator algorithms reserve capacity/resources for the hypervisor, migrations, upgrades.

Dell R660XS XL

Table 1: Intel Emerald Rapids CPUs

Appliance Constructs	A1 (replaces P2)	A2 (replaces P3)	A3 (replaces P5)	A31 (replaces P51)
Rack Mount Unit (RMU)	1U	1U	1U	1U
Intel CPU	4510	4510	6526Y	6526Y
Number of CPUs	1	2	2	2
Number of Cores/Server	12	24	32	32
Core Frequency (GHz)	2.4	2.4	2.8	2.8
Number of Fans	5	7	7	7
Number of 8GB RDIMMs	-	-	-	-
Number of 16 GB RDIMMs	4	8	16	16
Memory/Server in GB	64	128	256	256
10K 2.5” SAS HDD Size GB	600	600	600	600
Number of HDDs 2.5” 10K SAS	5	6	6	8
RAID Options	5	6	6	6
Usable Virtual Disk Capacity	1726GiB/ 1853GB	1726GiB/ 1853GB	1726GiB/ 1853GB	2619GiB/ 2812GB
Network 1 Gb ports (Base-T)	2 (onboard)	2 (onboard)	2 (onboard)	2 (onboard)
Network 1 Gb ports (Base T-OCP3)	4	4	4	4

Table continues…

Appliance Constructs	A1 (replaces P2)	A2 (replaces P3)	A3 (replaces P5)	A31 (replaces P51)
Network 10/25 Gb ports (BCM57414)	0	0	2*	2*
TPM	Yes	Yes	Yes	Yes
Power Supplies (800 W)	2	2	2	2
Rail Kit	Y	Y	Y	Y
DVD-ROM Drive	N	N	N	N

* Must be at ASP R6.0.0.4 or later for ASP 130 to recognize 10/25GB card. The R660xs must be at BIOS FW v2 or later.

Note:

Usable Virtual Disk Capacity has been reduced by 20% to allow for upgrades and storage overhead.

Note:

Usable Virtual Disk Capacity is also reduced by 60GiB for Avaya RHEL 8.10 OS.

Dell R640 XL

Table 2: Intel Skylake CPUs

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Rack Mount Unit (RMU)	1U	1U	1U	1U	1U
Intel Skylake CPU	S-4114	S-4114	G-6132	G-6132	G-6132
Number of CPUs	1	2	1	2	2
Number of Cores/Server	10	20	14	28	28
Core Frequency (GHz)	2.2	2.2	2.6	2.6	2.6
Number of Fans	5	8	5	8	8
Number of 8GB RDIMMs	3	6	-	-	-
Number of 16 GB RDIMMs	-	-	6	12	12
Memory/Server in GB	24	48	96	192	192
10K 2.5” SAS HDD Size GB	600	600	600	600	600
Number of HDDs 2.5” 10K SAS	3 (+2 for migration to ASP R6.0.x)	4 (+2 for migration to ASP R6.0.x)	4 (+2 for migration to ASP R6.0.x)	6	8
RAID Options	5	6	6	6	6
Usable Virtual Disk Capacity	1726GiB/ 1853GB	1726GiB/ 1853GB	1726GiB/ 1853GB	1726GiB/ 1853GB	2619GiB/ 2812GB

Table continues…

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Network 1 Gb ports (Base-T)	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe
Network 1 Gb ports (Base T-OCP3)	-	-	-	-	-
Network 10/25 Gb (BCM57414)	-	-	-	ASP 110 for SBCE only	-
TPM	-	-	-	-	-
Power Supplies (750 W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

Note:

Usable Virtual Disk Capacity has been reduced by 20% to allow for upgrades and storage overhead.

Note:

Usable Virtual Disk Capacity is also reduced by 60GiB for Avaya RHEL 8.10 OS.

Table 3: Intel Cascade Lake CPUs

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Rack Mount Unit (RMU)	1U	1U	1U	1U	1U
Intel Cascade Lake CPU	S-4210	S-4210	G-6226R	G-6226R	G-6226R
Number of CPUs	1	2	1	2	2
Number of Cores/Server	10	20	16	32	32
Core Frequency (GHz)	2.2	2.2	2.9	2.9	2.9
Number of Fans	5	8	5	8	8
Number of 8GB RDIMMs	3	6	-	-	-
Number of 16 GB RDIMMs	-	-	6	12	12
Memory/Server in GB	24	48	96	192	192
10K 2.5” SAS HDD Size GB	600	600	600	600	600
Number of HDDs 2.5” 10K SAS	3 (+2 for migration to ASP R6.0.x)	4 (+2 for migration to ASP R6.0.x)	4 (+2 for migration to ASP R6.0.x)	6	8
RAID Options	5	6	6	6	6

Table continues…

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Usable Virtual Disk Capacity	1726GiB/ 1853GB	1726GiB/ 1853GB	1726GiB/ 1853GB	1726GiB/ 1853GB	2619GiB/ 2812GB
Network 1 Gb ports (Base-T)	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe	6 (4LOM, 2 PCIe
Network 1 Gb ports (Base T-OCP3)	-	-	-	-	-
Network 10/25 Gb (BCM57414)	-	-	-	ASP 110 for SBCE only	-
TPM	-	-	-	-	-
Power Supplies (750 W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

Note:

Usable Virtual Disk Capacity has been reduced by 20% to allow for upgrades and storage overhead.

Note:

Usable Virtual Disk Capacity is also reduced by 60GiB for Avaya RHEL 8.10 OS.

Dell R660xs specifications

Front view of Dell™ PowerEdge™ R660xs Server

Note:

The Dell R660xs does not contain a CD-ROM drive. All media installation is done using USB.

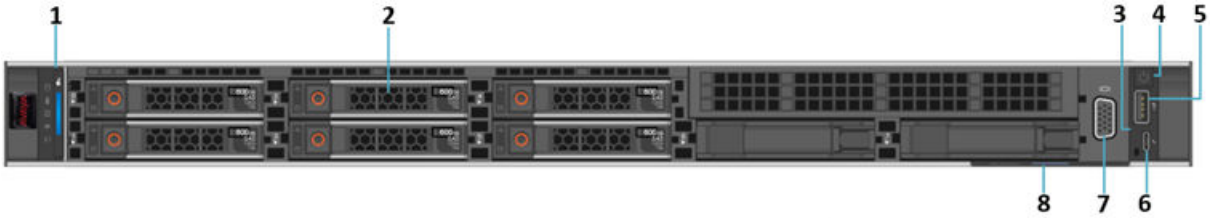


Figure 1: Front View of Dell PowerEdge R660xs – Single/Dual CPU Server

No.	Item	Icon	Description
1	Left control panel	NA	Displays the system health, system ID, and status LED indicators. • Status LED: Enables you to identify failed hardware components. There are up to five status LEDs and an overall system health LED (chassis health and system ID) bar.
2	Drive slots	N/A	Enables installation of hard disk drives (HDDs) that are supported on your system.
3	Right control panel	NA	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
4	Power button		Indicates if the system is powered on or off. Press the power button to manually power on or off the system. **Note:** Press the power button to gracefully shut down an ACPI-compliant operating system.
5	USB 2.0 port		The USB is a 4-pin connector and 2.0-compliant. This port enables you to connect USB devices to the system.
6	iDRAC Direct micro port		The iDRAC Direct port (Micro-AB USB) enables you to access the iDRAC direct features.
7	VGA port		Enables connection to the display device (console) of the system. If the user connects to the front VGA port, the rear VGA port does not function.
8	Express service tag	NA	The Express Service Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag will also contain the iDRAC secure default password.

Rear view of Dell™ PowerEdge™ R660xs Server

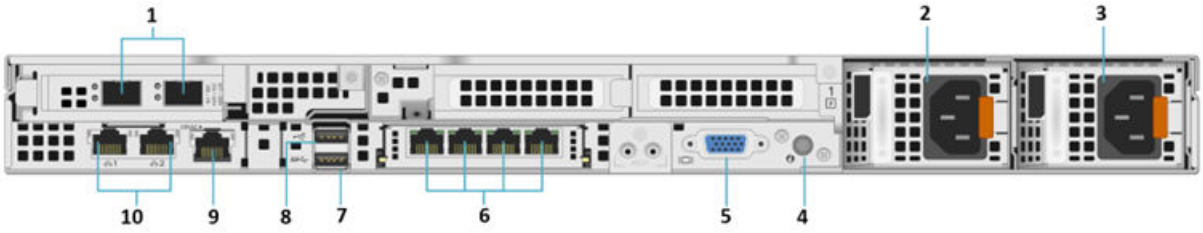


Figure 1: Rear View of Dell PowerEdge R660xs – Single/Dual CPU Server Profiles A3-A31

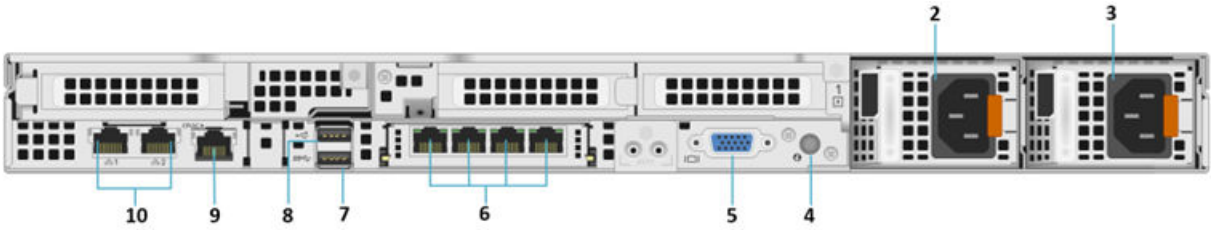


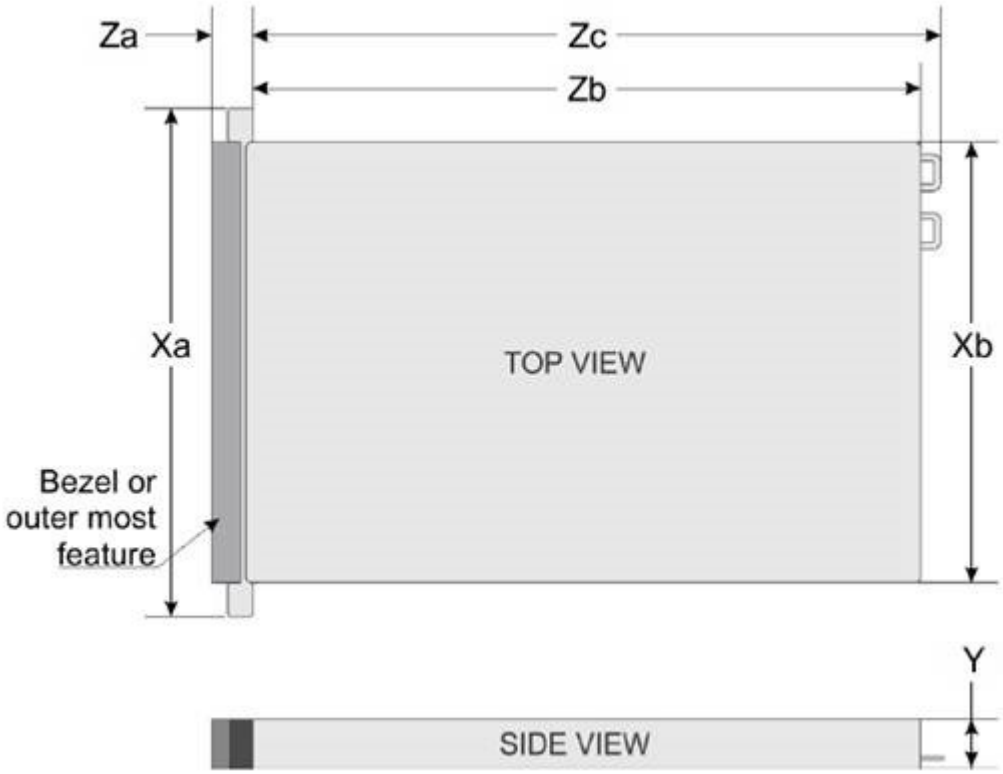
Figure 2: Rear View of Dell PowerEdge R660xs – Single/Dual CPU Server Profiles A1-A2

Table 4: Back View of Dell PowerEdge R660xs Server

No.	Item	Icon	Description
1	PCIe expansion riser card 1 slot(1)	N/A	Avaya Solutions Platform 1XX systems with R660xs server have a 2x10/25 GbE Broadcom NIC installed (BCM57414) in PCIe slot 1. In KVM on RHEL 8.10 these network interfaces will be displayed as: ens1f0np0, ens1f0np1. (Right-to-left assignment if viewing from rear of the server). Available for use beginning with ASP R6.0.0.4.0 and with BIOS FW v2 or later. This Network Card is only populated in Profiles: A3-A31.
2	Power supply unit (2)		PSU1 is the primary PSU of the system. Can accept voltages from 100-240VAC.
3	Power supply unit (2)		PSU2 is the secondary PSU of the system. Can accept voltages from 100-240VAC.
4	System identification button (ID)		Press the system ID button: • To locate a particular system within a rack. • To turn the system ID on or off. To reset iDRAC, press and hold the button for 16 seconds.
5	VGA port		Enables connection to the display device (console) of the system. If the user is connected to the front VGA port, the rear VGA port will not function.
6	OCP NIC ports (4)	N/A	4x1 GbE OCP NIC card. (eno12399, eno12409, eno12419 and eno12429 – Left to right viewing from rear of the server).
7	USB 3.0 port		This USB port is a 9 pin connector and 3.0-compliant. This port enables you to connect USB devices to the system (use for bootable ISO).
8	USB 2.0 port		This USB port is a 4 pin connector and 2.0-compliant. This port enables you to connect USB devices to the system.
9	iDRAC9 dedicated port		If enabled and cabled allows you to remotely access iDRAC.
10	NIC ports (2)		2 x 1 GbE NIC ports integrated on the system mother board. (eno8303 {Management} and eno8403 {Services} ports)

Dell PowerEdge R660xs server dimensions

R660xs Server	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
8x2.5 inch HDDs	482.0 mm (18.97 inches)	434.0 mm (17.08 inches)	42.8 mm (1.68 inches)	35.84 mm (1.41 inches)	22.0 mm (0.86 inches	626.42 mm (24.66 inches) Ear to rear wall	661.37 (26.03 inches) Ear to PSU handle



Weight

System	Maximum Weight
Avaya Solutions Platform 100 series Dell PowerEdge R660xs	18.25 kilogram (40.23 lbs)

Dell PowerEdge R660xs Environmental requirements

The tables in this section list the environmental requirements for the server.

Table 5: Temperature

Temperature	Specifications
Storage	–40°C to 65°C (–40°F to 149°F)
Continuous operation (for altitude <= 900 m or 2953 ft)	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.
Fresh air	For information about fresh air, see Expanded Operating Temperature at https://www.dell.com.
Maximum temperature gradient (operating and storage)	20°C in an hour (36°F in a hour) and 5°C in 15 minutes (9°F in 15 minutes).

Table 6: Relative humidity

Relative humidity	Specifications
Storage	58% RH with -12°C (10.4°F) minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point. Atmosphere must be non-condensing at all times.
Operating	8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point. Atmosphere must be non-condensing at all times.

Table 7: Maximum vibration

Maximum vibration	Specifications
Operating	0.21 G_{rms} at 5 Hz to 500 Hz for 10 minutes (all operation orientations).
Storage	1.88 G_{rms} at 10 Hz to 500 Hz for 15 min (all six sides tested).

Table 8: Maximum shock

Maximum shock	Specifications
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms.
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms.

Table 9: Maximum altitude

Maximum altitude	Specifications
Operating	3048 m (10000 ft)
Storage	12000 m (39370 ft)

Table 10: Operating temperature de-rating

Operating temperature de-rating	Specifications
Up to 35°C (95°F)	Maximum temperature is reduced by 1°C/300 m (1.8°F/984 ft) above 900 m (2953 ft).

Dell PowerEdge R660xs Power requirements

The ASP 130 R660xs are provided with two AC power supply units (PSU) and support them.

Table 11: PSU specifications

PSU	Class	Heat dissipation (maximum)	Frequency	Voltage
800 W AC	Platinum	3000 BTU/hr	50/60 Hz	100–240 V AC, autoranging

Table 12: ASP 130 Series - Dell R660xs Power Requirements

ASP 130 Dell R660xs	System VA rating	Heat Output (BTU/hr)	Peak Power Max. (Watts)
Profile A1	237	808	280
Profile A2	433	1477	470
Profile A3	585	1721	670
Profile A31	597	1802	700

Dell R640 specifications

Front view of Dell™ PowerEdge™ R640 Server

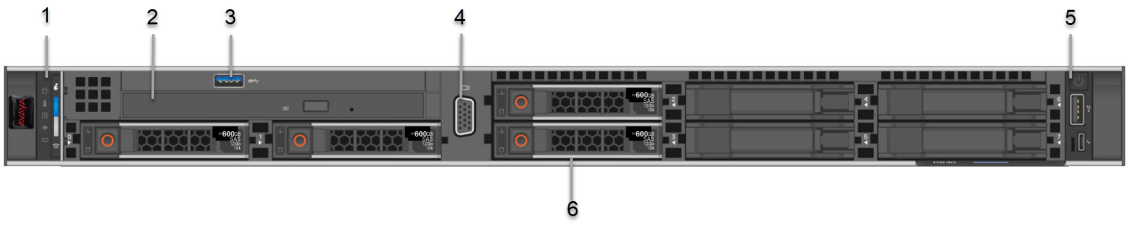


Figure 1: Front view of Dell PowerEdge R640 server

No.	Item	Icon	Description
1	Left control panel	NA	Displays the system health, system ID, and status LED indicators. • Status LED: Enables you to identify failed hardware components. There are up to five status LEDs and an overall system health LED (Chassis health and system ID) bar.
2	Optical drive	N/A	One slim SATA DVD-ROM drive. **Note:** DVD devices are data only.
3	USB port		The USB port is USB 3.0 compliant.
4	VGA port		Enables connection to the display device (console) of the system.
5	Right control panel	NA	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
6	Drive slots	NA	Enables installation of hard disk drives (HDDs) that are supported on your system.

Rear view of Dell™ PowerEdge™ R640 Server

Due to supply constraints the Avaya ASP 1XX Server will ship with an H750 RAID Controller Adapter in place of the H730P Mini RAID Controller, and also the 4x1GbE Intel NIC daughter card (NDC) will be replaced by a 4x1GbE Broadcom NIC daughter card. These changes occurred in 4QCY2022. The Broadcom 2x1GbE NIC card will now be installed in PCIe slot 2 to accommodate the H750 RAID Controller installed in PCIe Slot 1.

Original Configuration of Single CPU R640 server (H730P and Intel 4x1GbE NDC)

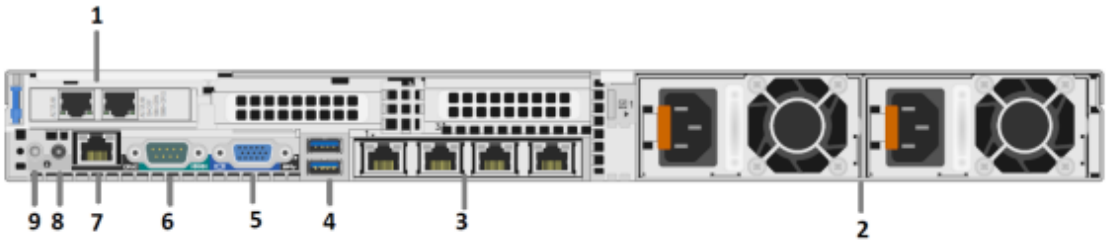


Figure 2: Back View of Dell PowerEdge R640 Single CPU Server with H730P Mini RAID Controller

New Configuration of Single CPU R640 server (H750 and Broadcom 4x1GbE NDC)

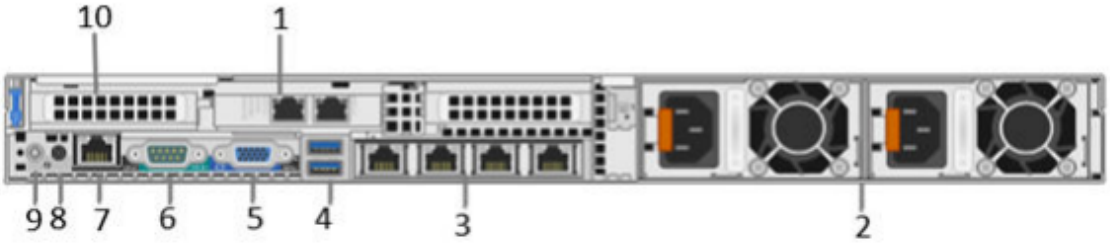


Figure 3: Back View of Dell PowerEdge R640 Single CPU Server with H750 RAID Controller Adapter

Original Configuration of Dual CPU R640 server (H730P and Intel 4x1GbE NDC)

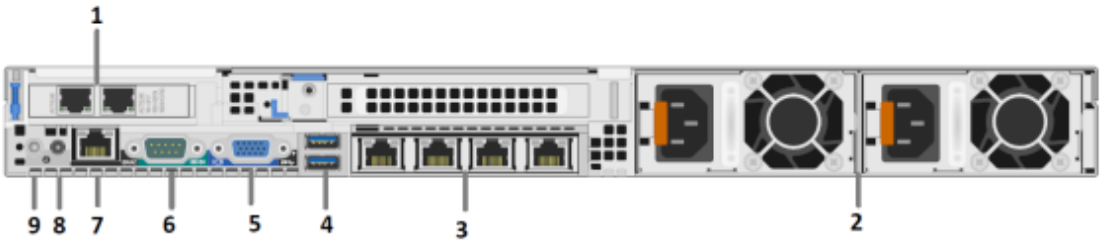


Figure 4: Back View of Dell PowerEdge R640 dual CPU Server with H730P Mini RAID Controller

New Configuration of Dual CPU R640 server (H750 and Broadcom 4x1GbE NDC)

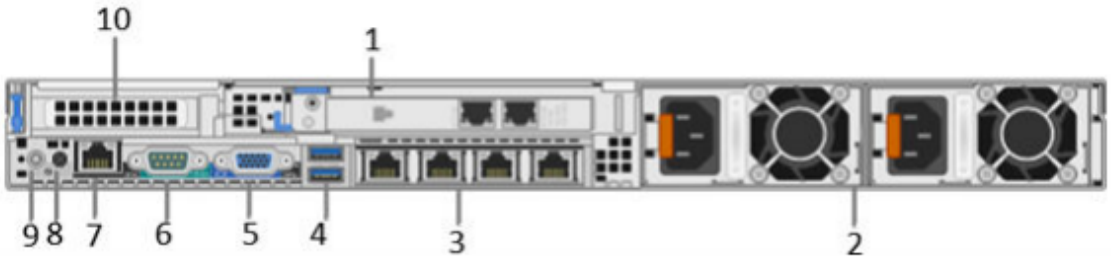


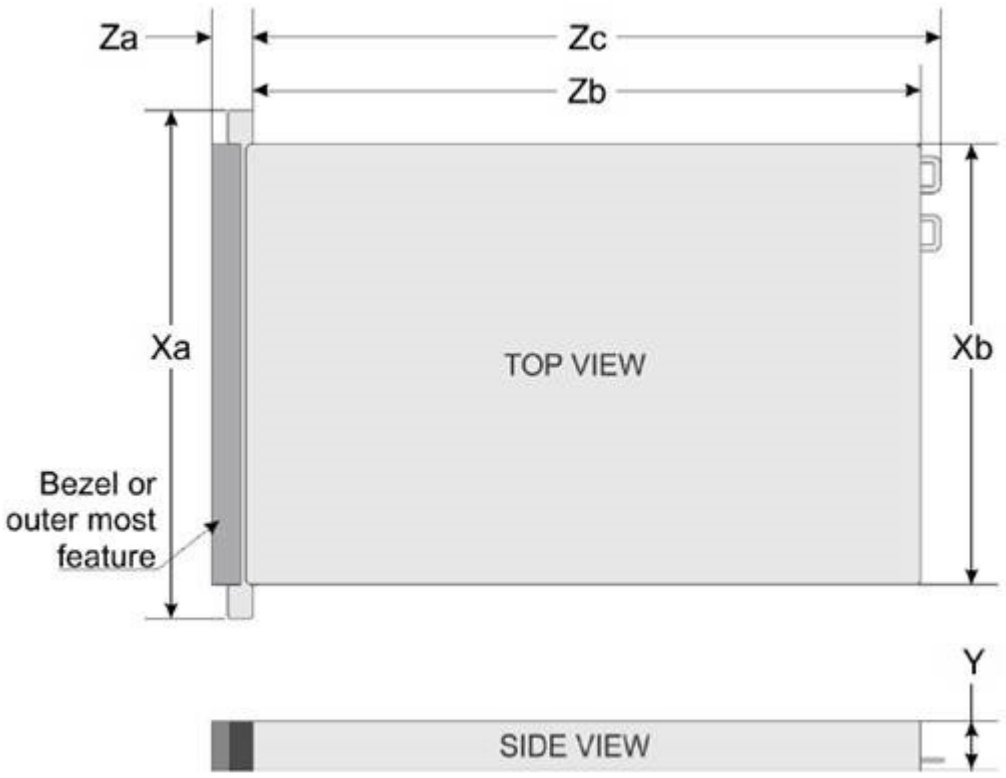
Figure 5: New Configuration of Dual CPU R640 server (H750 and Broadcom 4x1GbE NDC)

Table 13: Back View of Dell PowerEdge R640 Server

No.	Item	Icon	Description
1	PCIe expansion card slot(s)	N/A	Avaya Solutions Platform 1XX systems have a 2x1GbE Broadcom NIC installed in PCIe slot 1 in servers with an H730P Mini RAID controller. The 2x1GbE Broadcom NIC is installed in PCIe slot 2 in servers with an H750 RAID Controller Adapter installed in PCIe Slot 1. This NIC card in **Dual CPU** systems with the H750 RAID Controller has a full-height PCIe faceplate and **ports enslf0 and enslf1 are numbered left-to-right**. In **single CPU** configurations the 2x1GbE NIC, located in PCI slot2 has a half-height PCIe faceplate and **ports enslf0 and enslf1 are numbered right to left**. See figures above.
2	Power supply unit (2)	N/A	Power Supplies can accept voltages from 100-240VAC.
3	NIC port (4)		The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. (**eno1** – **eno4** – left to right viewing from rear of server {**eno1** = Mgmt_VM_Network and **eno2** = Services})
4	USB 3.0 port		The USB ports are of 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
5	VGA port		Enables you to connect a display device to the system.
6	Serial port		Enables you to connect a serial device to the system.
7	iDRAC9 dedicated port		Enables you to remotely access iDRAC.
8	CMA power port	N/A	The Cable Management Arm (CMA) power port enables you to connect to the CMA.
9	System identification button		The System Identification (ID) button is available on the front and back panel of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the Step Through mode.
10	PERC H750 RAID Controller Adapter	N/A	The H750 is a RAID disk array controller made by Dell for its PowerEdge servers. This controller replaces the H730P Mini RAID controller shipped in earlier versions of the ASP 1XX. The H750 installs in PCIe slot 1 whereas the H730P is installed in an embedded PCIe slot on the server motherboard.

Dell PowerEdge R640 server dimensions

R640 Server	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
8x2.5 inch HDDs	482.0 mm (18.97 inches)	434.0 mm (17.08 inches)	42.8 mm (1.68 inches)	35.84 mm (1.41 inches)	22.0 mm (0.87 inches	683.05 mm (26.89 inches)	721.91 (28.42 inches)



Weight

System	Maximum Weight
Avaya Solutions Platform 100 series Dell PowerEdge R640	21.9 kilogram (48.28 lbs)

Dell PowerEdge R640 Environmental requirements

The tables in this section list the environmental requirements for the server.

Table 14: Temperature

Temperature	Specifications
Storage	–40°C to 65°C (–40°F to 149°F)
Continuous operation (for altitude less than 950 m or 3117 ft)	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.
Fresh air	For information about fresh air, see Expanded Operating Temperature at https://www.dell.com.
Maximum temperature gradient (operating and storage)	20°C/h (68°F/h)

Table 15: Relative humidity

Relative humidity	Specifications
Storage	5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times.
Operating	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point.

Table 16: Maximum vibration

Maximum vibration	Specifications
Operating	0.26 G_{rms} at 5 Hz to 350 Hz (all operation orientations).
Storage	1.88 G_{rms} at 10 Hz to 500 Hz for 15 min (all six sides tested).

Table 17: Maximum shock

Maximum shock	Specifications
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 6 G for up to 11 ms.
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms.

Table 18: Maximum altitude

Maximum altitude	Specifications
Operating	3048 m (10,000 ft)
Storage	12,000 m (39,370 ft)

Table 19: Operating temperature de-rating

Operating temperature de-rating	Specifications
Up to 35°C (95°F)	Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 950 m (3,117 ft).
35°C to 40°C (95°F to 104°F)	Maximum temperature is reduced by 1°C/175 m (1°F/319 ft) above 950 m (3,117 ft).
40°C to 45°C (104°F to 113°F)	Maximum temperature is reduced by 1°C/125 m (1°F/228 ft) above 950 m (3,117 ft).

Dell PowerEdge R640 Power requirements

The ASP 100 R640's are provided with two AC power supply units (PSU) and support them. The system supports a maximum of two AC PSU.

Table 20: PSU specifications

PSU	Class	Heat dissipation (maximum)	Frequency	Voltage
750 W AC	Platinum	2891 BTU/hr	50/60 Hz	100–240 V AC, autoranging

Table 21: ASP 100 Series - Dell R640 Power Requirements

ASP 100 Series Dell R640	System VA rating	Heat Output (BTU/hr)	Peak Power Max. (Watts)
Profile 2	200	680	270
Profile 3	340	1161	457
Profile 4	283	1066	365
Profile 5	504	1721	655
Profile 51	528	1802	685

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 = 1024^3 bytes), unless explicitly specified (for example, **`df -H`** for decimal).

Cockpit displays storage in decimal units (for example, GB = 1000^3 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.

Table continues…

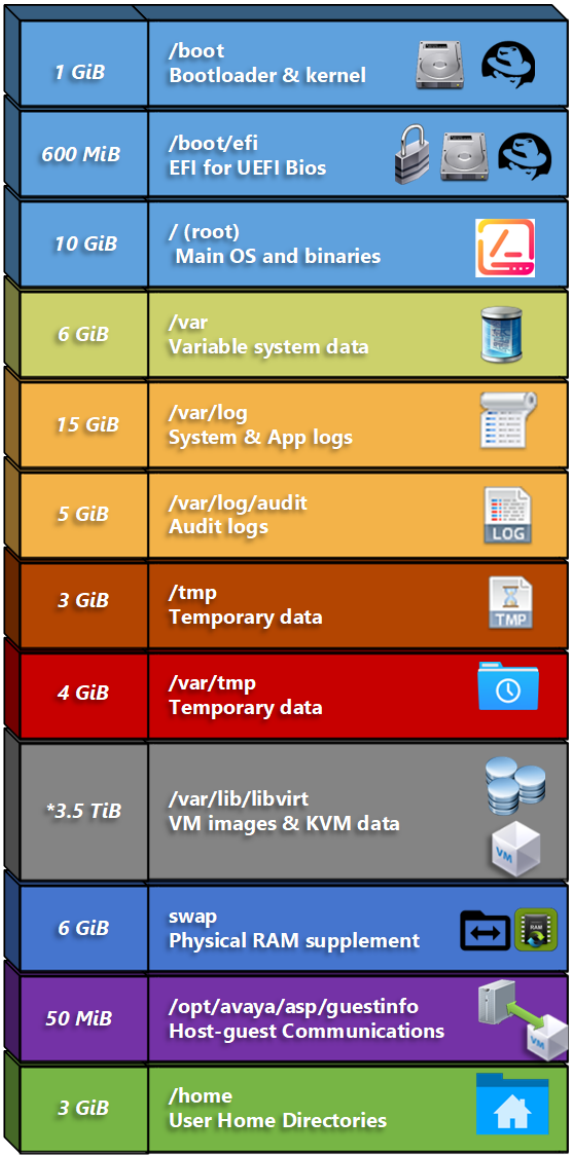
Partition	Size	Notes
`/boot/efi`	600 MiB	This partition uses the EFI System Partition (ESP) filesystem and is required for systems with a UEFI BIOS. For ASP deployments, all server hardware profiles except the S8300E use UEFI BIOS and therefore require this partition.
`/`	10 GiB	This is the root partition, 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`	R660xs/R640: ~1.7 – 3.5 TiB	This partition contains the KVM (Hypervisor) data. In particular, the VM disk files are stored in the directory `/var/lib/libvirt/images`. **Note:** The total available storage size may vary depending on the server hardware profile (for example, S8300E, R640/R660xs). The displayed storage for `/var/lib/libvirt` accounts for a system-reserved allocation of approximately 53.7 GiB, which is used by other system partitions.
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.

Table continues…

Partition	Size	Notes
`/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:



*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

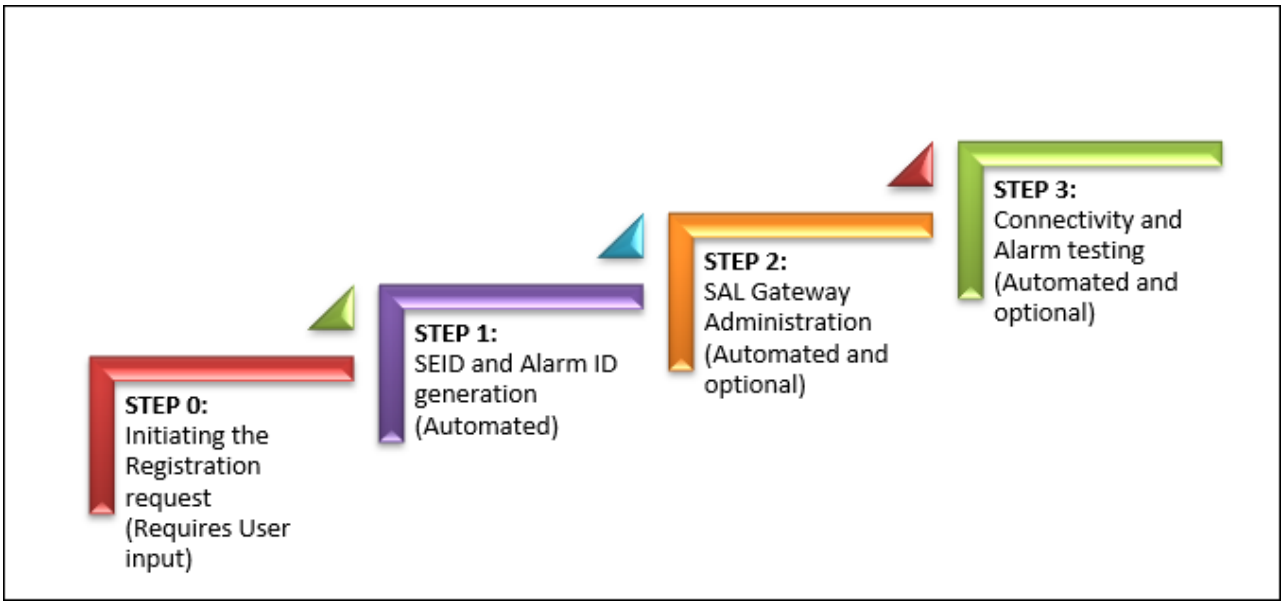
In order to receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in the HealthCheck tool.

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

General information on registration can be found at 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: 00XXXXXXXX (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 names for iDRAC and the KVM on RHEL host.

  The iDRAC IP address is linked with the Avaya Solutions Platform server. The KVM on RHEL Host IP address is linked with the Avaya Solutions Platform KVM on RHEL host.
- Ensure that you have placed a SAP order with the Avaya Solutions Platform 130 material codes.

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

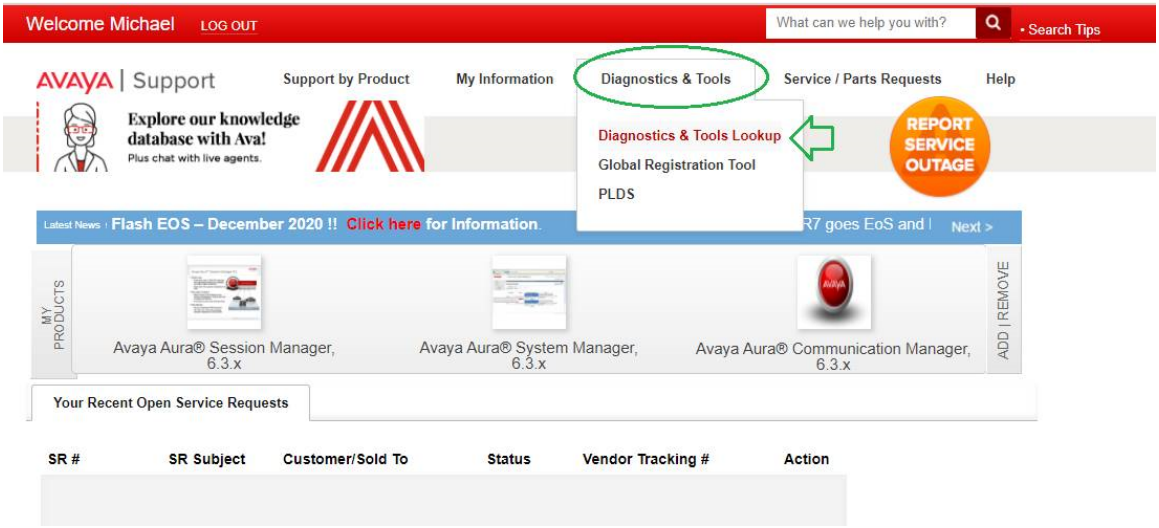
  The ASP 130 R6.0.x new material codes are the following:

  - 700519836 ASP 130 DELL R660 HYPERVISOR A1 SERVER BUNDLE

- 700519837 ASP 130 DELL R660 HYPERVISOR A2 SERVER BUNDLE
- 700519838 ASP 130 DELL R660 HYPERVISOR A3 SERVER BUNDLE
- 700519839 ASP 130 DELL R660 HYPERVISOR A31 SERVER BUNDLE

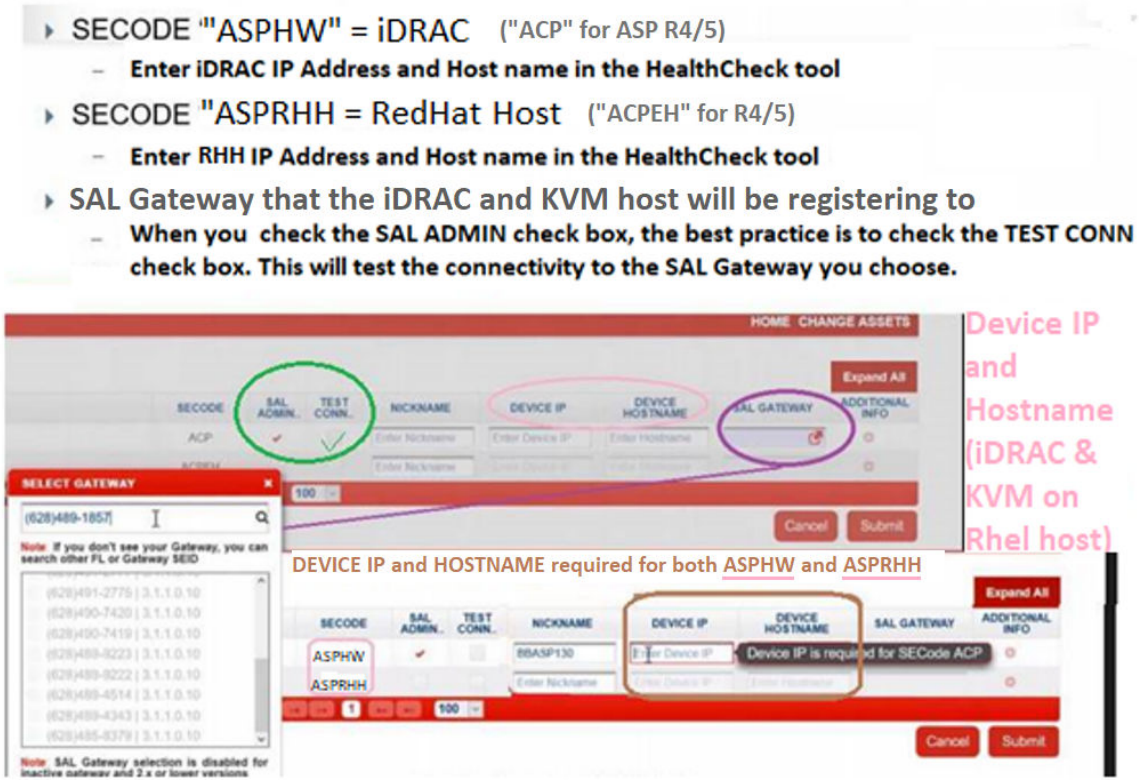
Procedure

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 130 tracking code asset and enter the quantity in the **Location ID** field. Click **Register**.

10. Enter the details in the **ASPHW**, **ASPRHH** (R660xs), and **SAL Gateway** fields for the Avaya Solutions Platform 130.



11. Click **Submit**.
12. 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 ASP 120 migrates from AVP 8.1.x to ASP R6.0.x (KVM on Red Hat Enterprise Linux 8.10)

About this task

The Avaya Solutions Platform 120 material codes are end of sale.

Existing customers migrating from ASP 120 (AVP 8.1.x) to KVM On RHEL 8.10 can keep the existing material codes in their “Install base” record but must use the new tracking code for SAL/ Alarming connectivity. Follow the below steps:

Keep ASP 120 Hardware Material code in install base.

Before you begin

- ASP 120 software migration to ASP 130 R6.0.x (Dell R640) requires ordering appropriate material codes:

  4434562 ASP 120 AVP UPG ASP 130 R6 RHEL LIC
- Ordering the above will trigger the following 4434496 ASP 130 R6 RHEL LIC (not orderable, this is an entitlement) which will be present in the customer record.

Procedure

1. Offboard AVPVM and AVPUTI Solution Element IDs (SEIDs) from ASP 120 from SAL Gateway (SALGW).

2. Technical Onboard ASP 120 in SALGW with new tracking code: 434534 ASP 120 UPG TO RHEL TRK to set ASPHW SE code (for iDRAC) and ASPRHH SE code (for KVM on RHEL Host).

3. Retain ASP 120 Hardware Material codes in Install base. See codes below:

   700514094 ACP 120 DELL R640 SRVR P2 BUNDLE or

   700514095 ACP 120 DELL R640 SRVR P3 BUNDLE or

   700514194 ACP 120 DELL R640 SRVR P4 BUNDLE or

   700514096 ACP 120 DELL R640 SRVR P5 BUNDLE

Registering device after ASP 130 migrates from ASP 130 (ESXi) to ASP 6.0.x (KVM on Red Hat Enterprise Linux 8.10)

About this task

Existing customers migrating from ASP 130 (ESXi) to KVM On RHEL 8.10 can keep the existing material codes in their “Install base” record but must use the new tracking code for SAL/Alarming connectivity. Follow the below steps:

Keep ASP 130 Hardware Material code in install base.

Before you begin

- ASP 130 software migration to ASP 130 R6.0.x (Dell R640 or new Dell R660xs) requires ordering appropriate material codes:

  4434563 ASP 130 R4 UPG ASP 130 R6 RHEL LIC

  4434495 ASP 130 R5 UPG ASP 130 R6 RHEL LIC

- Ordering the above will trigger the following 4434496 ASP 130 R6 RHEL LIC (not orderable, this is an entitlement) which will be present in the customer record.

Procedure

1. Technical Onboard ASP 130 in SALGW with new tracking code: 434532 ASP 130 UPG to RHEL TRK to set ASPHW SE code (for iDRAC) and ASPRHH SE code (for KVM on RHEL Host).
2. Retain ASP 120 Hardware Material codes in Install base.

Chapter 4: Hardware Installation

Installation checklist

Use the following checklist to complete the installation of the server.

No.	Task	Description	Notes	✔
1	Discharge electrostatic energy.	See Electrostatic discharge on page 37.		
2	Inspect package contents.	See Package contents (New ASP 130 R6.0.x Dell R660xs only) on page 38.		
3	Install the server using the rail kit.	See Installing the server (New ASP 130 R6.0.x Dell R660xs only) on page 39.		
4	Attach cables.	See Attaching cables on page 43.		
5	Connect power.	See Connecting power on page 44.		

The following items are application-specific. Refer to the application-specific documentation for additional information on:

- Initial configuration and IP address assignment.
- Ethernet port cabling.
- Application shutdown procedures.

Electrostatic discharge

Electrostatic discharge (ESD) is a discharge of stored static electricity that can damage equipment and impair electrical circuitry. Electrostatic voltages can result from friction including, pulling cabling through conduits, walking across carpeted areas, and building static charge in clothing. When you improperly handle electronic components, ESD damage occurs and can result in complete or intermittent failures. While networking equipment is commonly designed and tested to withstand common mode ESD events, voltage can sometimes discharge to some connector pins, which can potentially damage the networking equipment.

To protect against ESD damage, take the following measures before you connect data cables to the device:

- Always use antistatic wrist straps. Make sure you adjust the strap to provide good skin contact.
- Ensure that you properly ground work surfaces and equipment racks for protection against electrostatic discharge. You must connect the common point to the building ground wire. In a properly wired building, the nearest reliable ground is typically at the electrical outlet.
- Avoid contact between equipment and clothing. The wrist or ankle strap protects only the equipment from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Avoid touching any connector pins.
- Do not remove the wrist or ankle strap until the installation is complete.

Package contents (New ASP 130 R6.0.x Dell R660xs only)

The following items are provided with your server. Contact Avaya Support if any of the following items are not present.

- Dell sliding rail assembly kit
  - Two Dell sliding rail assemblies
  - Two velcro straps
  - Four screws and washers
- Cable management arm kit
  - Cable management arm
  - Static support tray
  - Status indicator cable
  - Cable tie wraps
  - Right attachment bracket
  - Left attachment bracket
- Server faceplate
- Server faceplate key
- Rack Installation Instructions Booklet
- Enterprise Products Safety, Environmental and Regulatory Information Booklet.

Installing the server (New ASP 130 R6.0.x Dell R660xs only)

About this task

Use this procedure to install the server using the provided rail kit. The following procedure is a copy of the Dell rail installation instructions that accompany the Avaya Dell R660xs packaging. This information is intended to instruct the user on how to install the rail kit into a rack and how to connect power and network cables. The server depicted in these drawings is a generic server drawing. For specific ASP 130 port designations, refer to figures 2 and 3 of Rear view of Dell™ PowerEdge™ R660xs Server on page 17 of this document.

Before you begin

Warning:

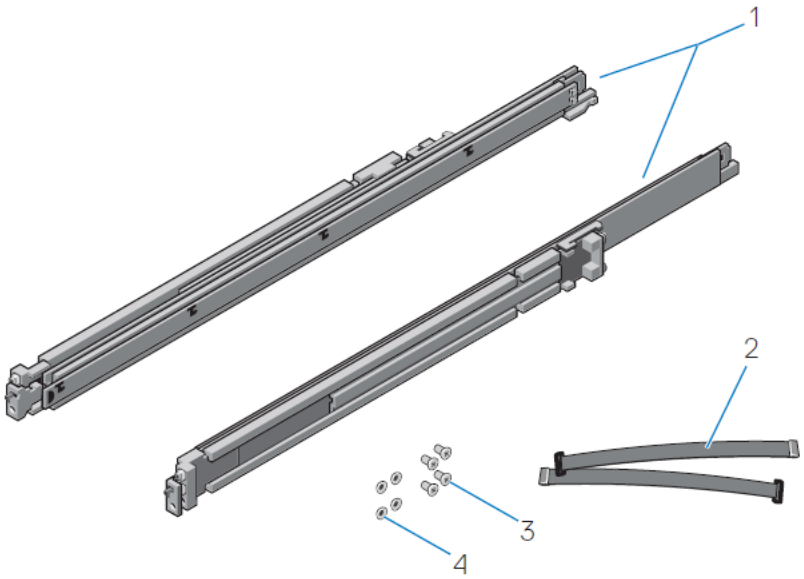
- Before you begin, read and follow the safety instructions in your *Enterprise Products Safety, Environmental and Regulatory Information Booklet* shipped with your system.
- Reference the Rail Installation Guide shipped with the rail kit. This may have updated instructions that supersede this document.
- To avoid injury, do not attempt to lift the system by yourself.
- Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws. Verify that the rack is grounded in accordance with local electrical code.

Note:

- Avaya customers are required to have a VGA monitor, USB keyboard, and USB mouse (optional) available for use by installation and servicing technicians.
- This rail kit is compatible with square, unthreaded round, and threaded round hole racks.

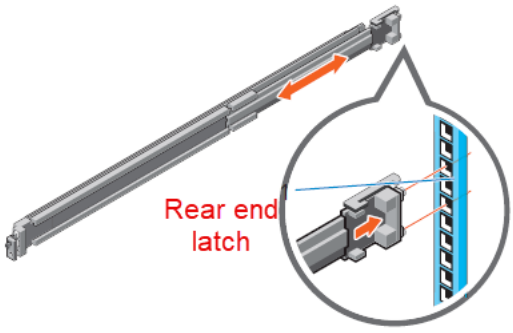
Procedure

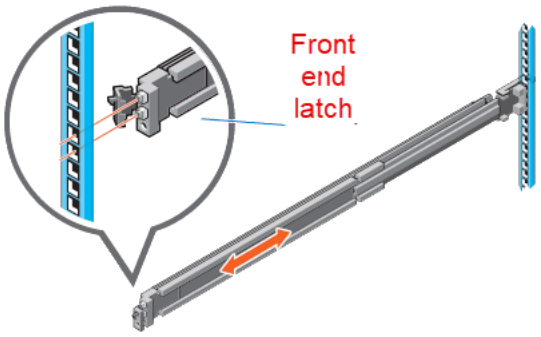
1. Identify and separate the components of the sliding rail assembly kit.



- Two sliding rail assemblies — (1)
- Two velcro straps — (2)
- Four screws — (3)
- Four washers — (4)

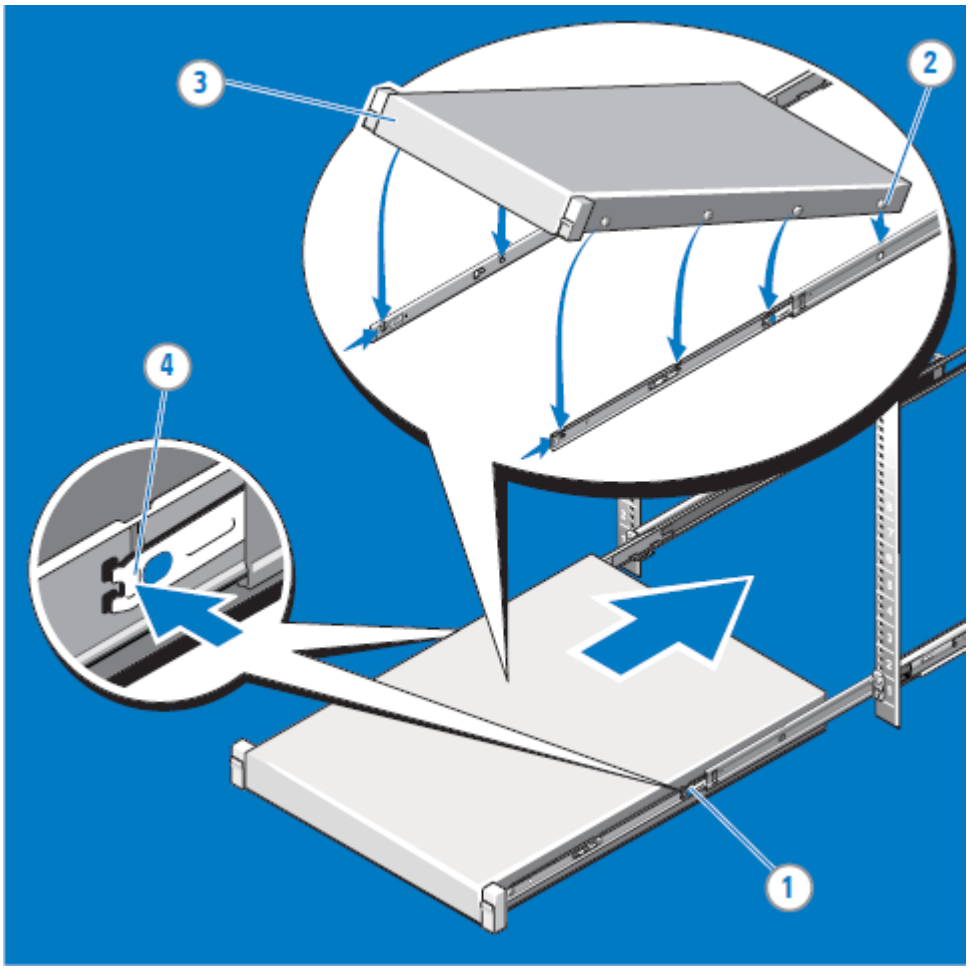
2. Place the kit components within easy reach of your work area.
3. Perform the following actions to install the left and right rails, beginning with the left rail:





Task order	Task
1	Fully extend the rear sliding bracket of the rail so that the rail is as long as possible.
2	Position the rail end piece labeled FRONT facing inward and orient the rear end piece to align with the holes on the rear rack flanges.
3	Push the rail straight toward the rear of the rack until the latch locks into place.
4	For the front end piece, rotate the latch outward and pull the rail forward until the pins slide into the flange, and release the latch to secure the rail in place.
5	Repeat the preceding steps to install the right rail.

4. Perform the following actions to install the system in the rack:



Task order	Task
1	Pull the inner slide rails out of the rack until they lock into place.
2	Locate the rear rail standoff on each side of the system and lower them into the rear J-slots on the slide assemblies.
3	Rotate the system downward until all the rail standoffs are seated in the J-slots.
4	Push the system inward until the lock levers click into place. Press the slide-release lock buttons on both rails and slide the system into the rack

5. To secure the rails to the rack for shipping or in an unstable environment, install the supplied screws to the rails. For square hole racks, install the supplied conical washer to the screw before installing the screw. For unthreaded round hole racks, install only the screw without the conical washer.

Attaching cables

About this task

Use this procedure to attach network and I/O cables to the system.

Note:

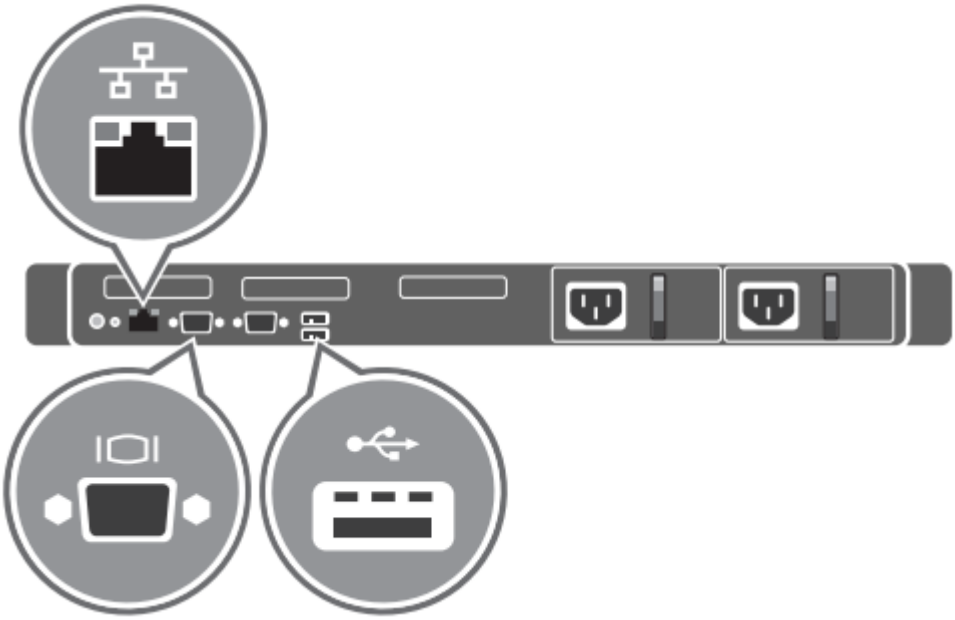
Consult application-specific documentation for information on peripheral and management device connectivity.

Before you begin

- Ensure the system has been installed and secured as outlined in Installing the server (New ASP 130 R6.0.x Dell R660xs only) on page 39 before you attach cables.
- Ensure you have taken precautions against electrostatic discharge as outlined in Electrostatic discharge on page 37 before you begin.
- Customers must supply cables and/or transceivers compatible with their network infrastructure. For 1GbE interface, always use 1000BaseT UTP (CAT5e) cables as a minimum or 1000BaseTX UTP (CAT6) cables. For 10/25GbE interfaces the appropriate transceivers and cables are dependent on the customer network infrastructure. Proper cables (fiber optic or Direct Attach Copper [DAC]) and compatible transceivers are required to operate the 10/25 GbE interfaces. These interfaces use the industry-standard Small Form-Factor Pluggable 28 (SFP28) form factor. Customers must select cables and transceivers that are supported and qualified by their respective network switch vendor. Refer to the switch vendor's documentation for the approved SFP28 cables and transceivers to ensure compatibility and correct operation.

Procedure

1. Connect the network cables to the appropriate RJ45 ports (or SFP28 ports if 10/25GbE NIC is utilized) on the system.
2. Connect optional peripherals using the USB ports on the system. If configuring KVM on RHEL 8.10 for the first time, a USB keyboard will be required.
3. Connect an optional management device using the console port on the system. If configuring KVM on RHEL 8.10 for the first time, a VGA monitor will be required.



The image is a generic illustration. For detailed information on the back view of the server, see Rear view of Dell™ PowerEdge™ R660xs Server on page 17.

Connecting power

About this task

Use this procedure to connect power to the system.

Note:

A region-specific power cable is shipped separately from the server package based on what was entered in the Configurator Tool.

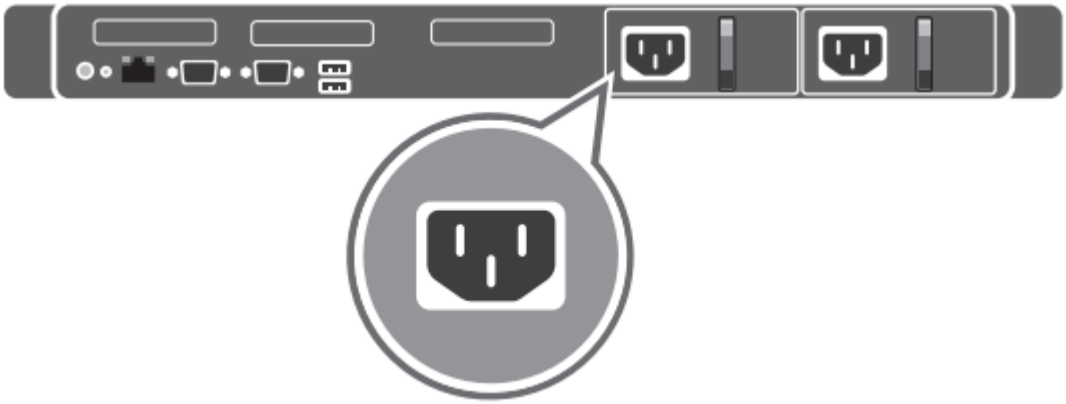
Before you begin

Ensure the system has been installed and secured before you attach power cables. Ensure you have take precautions against electrostatic discharge before you begin. See the following sections for more information:

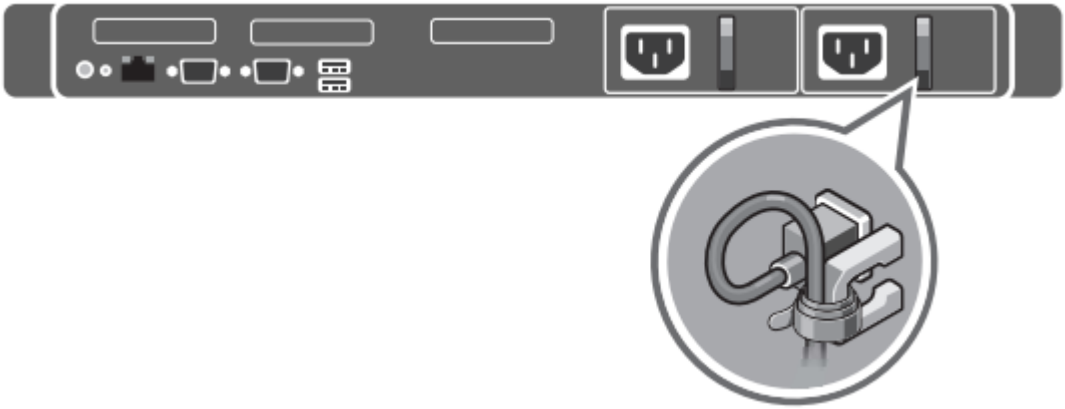
- Installing the server (New ASP 130 R6.0.x Dell R660xs only) on page 39
- Electrostatic discharge on page 37

Procedure

1. Connect the system to the appropriate power source.

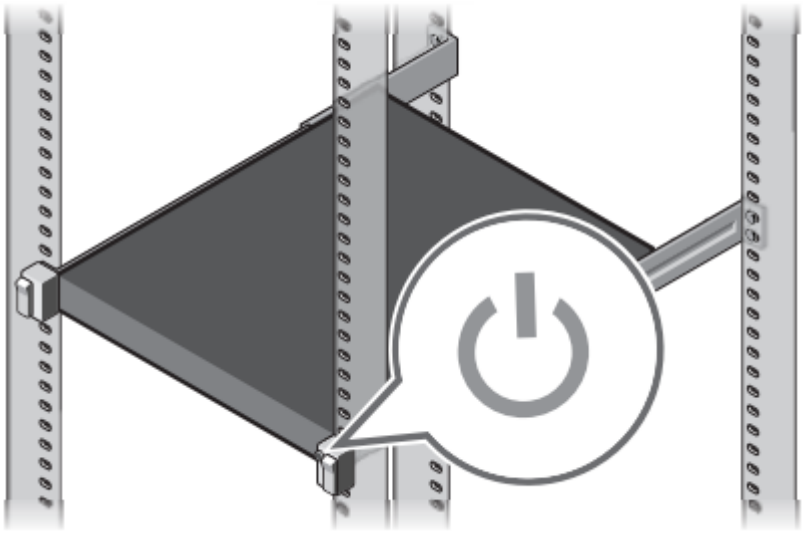


2. Loop and secure the power cable using the retention strap.



3. Attach USB keyboard and VGA monitor to system before powering up.
4. Power on the system.

   The following image shows the location of the power button.



Chapter 5: Summary of Migration from ASP R4.x, R5.x, AVP (ASP 120) to ASP R6.0.x

Purpose

This chapter provides a summary of the steps required to migrate an existing ASP Dell R640 running ASP R4.x, ASP R5.x, AVP (ASP 120) to ASP R6.0.x.

About this task

This process is only applicable for ASP 120/130 Dell R640 servers.

Summary of steps:

- When migrating Avaya R640 profile 2 (P2), profile 3 (P3) or profile 4 (P4) systems, obtain 2 additional Avaya sourced 600GB hard disk drives (HDDs)/server. Contact Avaya Sales for acquiring the additional HDDs (700514178 ACP DELL 600GB 10K SAS 2.5 HDD).
- When migrating an Avaya R640 profile 5 (P5) or profile 51 (P51), no additional HDDs need to be added to the server, but a reconfiguration of the RAID controller must be performed to ensure optimal array performance.
- Perform a backup of the customer's data that will be needed for deployment of the customer's data in Avaya's RHEL 8.10 environment. For ESXi, capture all Host IP and naming information (host name, domain, NTP, DNS, etc.). Reference individual application documentation for details on backup procedures as well as required configuration details that must be captured. Ensure application level backups are stored off of the server as the server's HDDs will be cleared.
- Acquire a monitor and USB keyboard and mouse. Two USB ports are located in the front of the server and two are in the rear. Reserve the rear, bottom USB port for RHEL 8.10 installation media.
- BIOS/FW update of the underlying ASP R640 hardware platform MUST be on Avaya certified v14 (*PSN027109u*) or later.
- Utilize the steps in Chapter 12: RAID configuration to clear the data on the existing HDDs and reconfigure.
- Once RAID configuration has been performed, utilize the steps in Chapter 9: Performing server recovery and/or software remastering.
- Install the appropriate KVM application images, configure applications, restore backups.

Chapter 6: Configuration

Purpose

This chapter provides instructions required after physical installation to complete the system setup of an Avaya integrated staged server, prior to deploying Avaya Application images.

Dell R660xs and Dell R640 Configuration

Overview

The Avaya Solutions Platform 130 (ASP 130) R6.0.x is supported on Dell R640 and Dell R660xs servers. This section provides the instructions required after physical installation to complete the KVM on Red Hat Enterprise Linux 8.10 configuration with the customer's specific environment information before deploying Avaya Applications. New Dell R660xs servers ship with KVM on Red Hat Enterprise Linux 8.10 installed. Existing ASP 130 R4/5.x (Dell R640s) need to follow the migration documentation to migrate to ASP 130 R6.0.x. This section focuses on new Dell R660xs servers shipping from Avaya's integrator.

Configuring KVM on Red Hat Enterprise Linux 8.10 Network Settings

About this task

Use this procedure to configure KVM on Red Hat Enterprise Linux 8.10 Network Settings.

Before you begin

Ensure that you have the following:

- Dell R660xs Server or Dell R640 Server
- Console VGA Monitor
- USB Keyboard
- Laptop with a SSH emulator (for example, putty)

Note:

Ensure the SSH client used is the latest version available to ensure compatibility with ASP R6.0.x cryptographic policy.

- Rufus software (for a reinstall/remaster only)

Note:

A new ASP 130 R6.0.x (Dell R660xs) will ship from the Avaya integrator with KVM on RHEL 8.10 pre-loaded.

Procedure

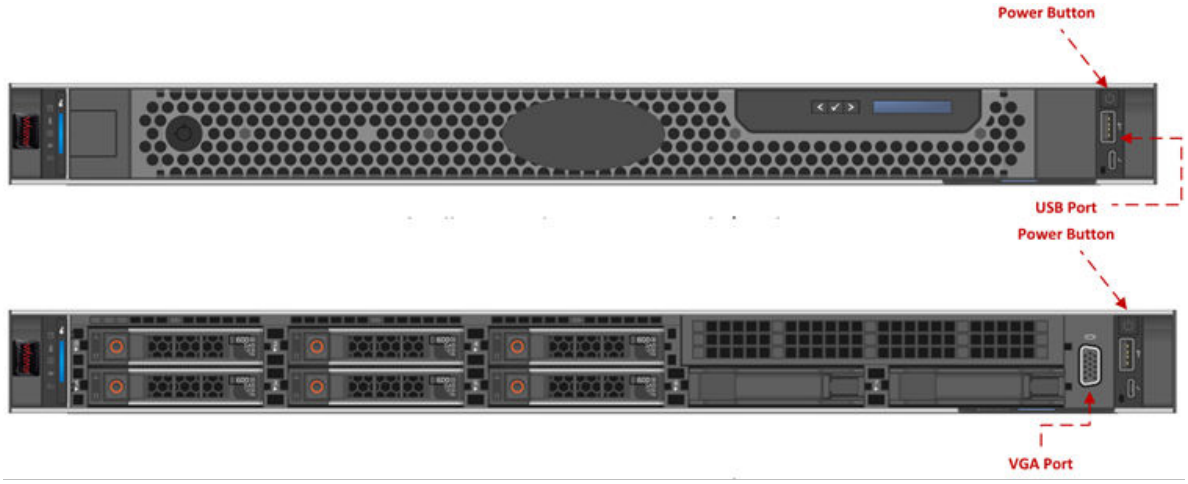
1. Media for new installations and upgrades is required to go into the bottom USB slot on the back of the server since it is the only USB slot that is USB 3.0 compliant.
2. Connect a VGA monitor and USB keyboard to the front ports of the server. Connections for the VGA monitor and USB keyboard are also located on the rear of the server.

   Note:

   If the monitor is connected to the front VGA port, the rear VGA port will not function.

   - The Monitor and Keyboard are required to enable and configure the iDRAC and to update R660xs BIOS/Firmware (if necessary).
   - During bootup of server you press F2 to enable and configure iDRAC. See iDRAC chapter for details.
   - If any BIOS/FW updates are required, they will be posted in a PSN available on support.avaya.com.
3. Remove faceplate to access front VGA and USB ports.

   The following pictures are just a representation and should only be used as an example.



   There are two options when configuring the host:

   a. Monitor and keyboard

   b. Services laptop

      - Change laptop address to 192.11.13.5 with a subnet mask of 255.255.255.252.
      - Connect laptop to services port.

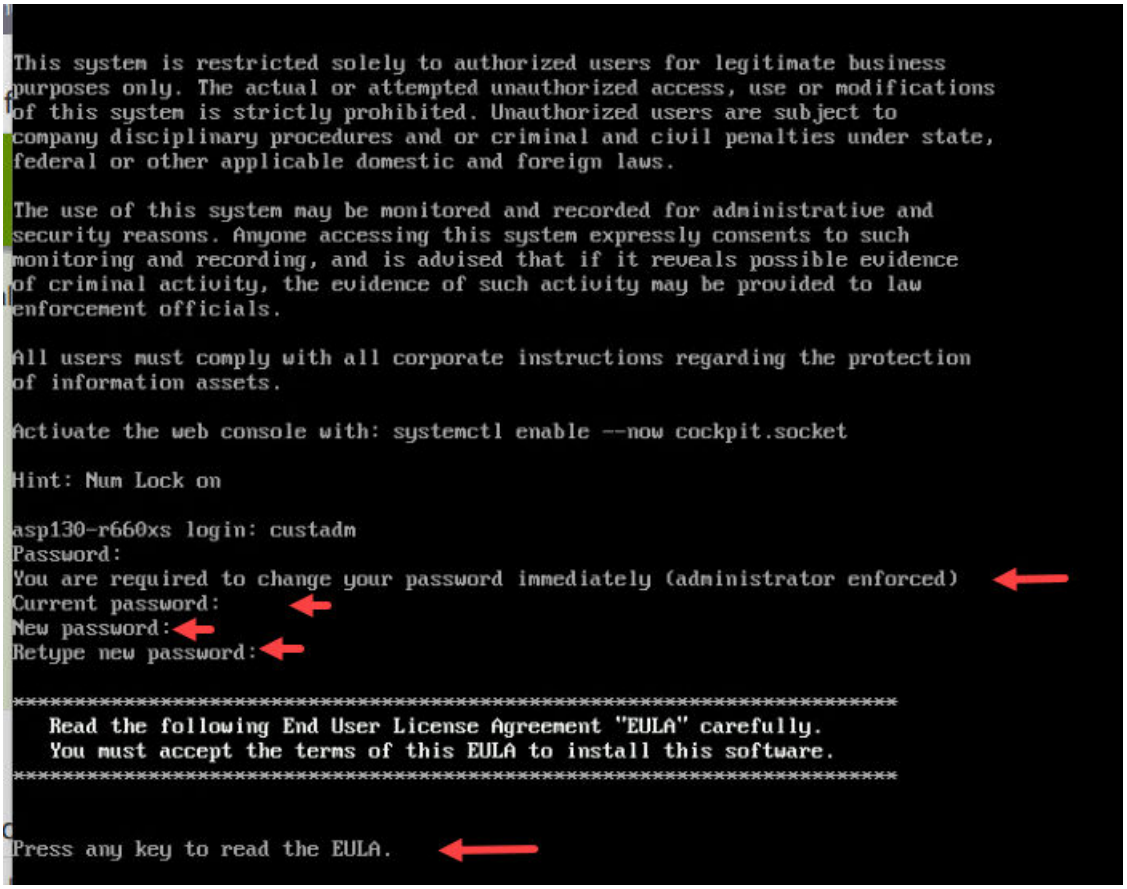
- If using the services laptop, once server is powered up, launch a SSH session to the KVM on RHEL host. (192.11.13.6).

4. Power on the server.

   The initialization process will take a few minutes. Do not press any additional keys until prompted to do so.

5. Login using credentials: `custadm/ACP130_pw`. The configuration script will ask to change the custadm credentials immediately. Minimum password requirements include 8 characters and 1 number, 1 capital letter and 1 lower case letter. Passwords cannot be a common dictionary word or contain the username and must be different from the last 10 passwords (when changed in the future).

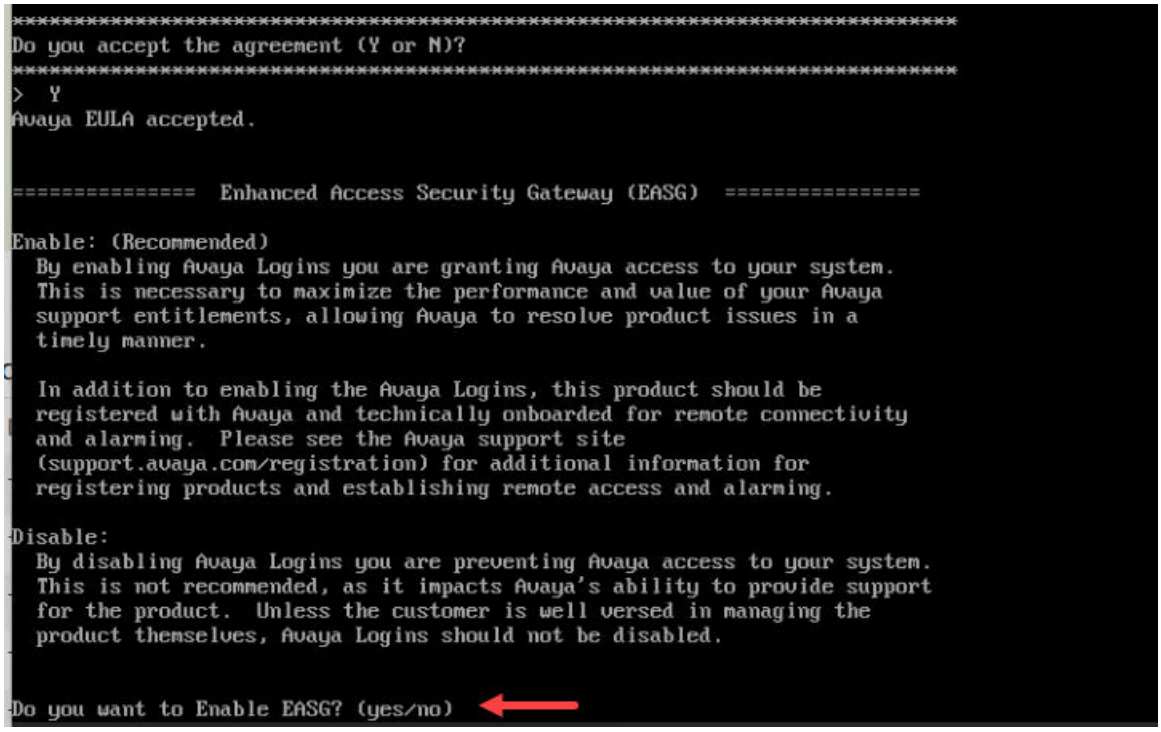
   The example below is using the console for access. If connected via the services port, after retyping the new password, the SSH session will terminate. Re-establish the SSH session and login with the new **`custadm`** credentials.



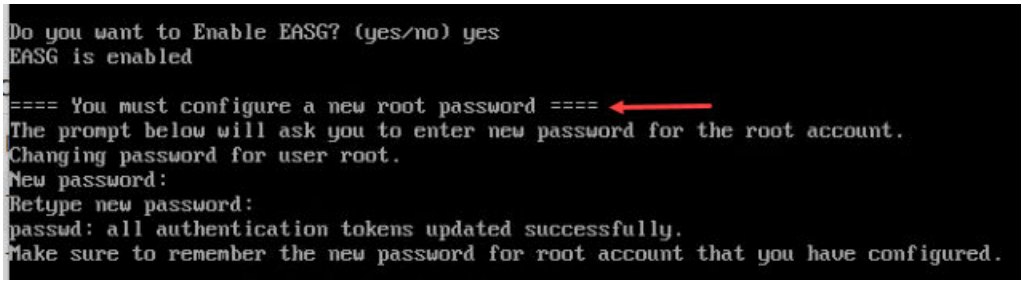
6. Read and accept the EULA.

   After the EULA is accepted, the Red Hat cockpit will be accessible from a PC connected to the services port using the URL `https://192.11.13.6:9090`. The SSH access will also be available from a PC connected to the services port (at `192.11.13.6`). This can be used in case you do not have a keyboard and monitor connected.

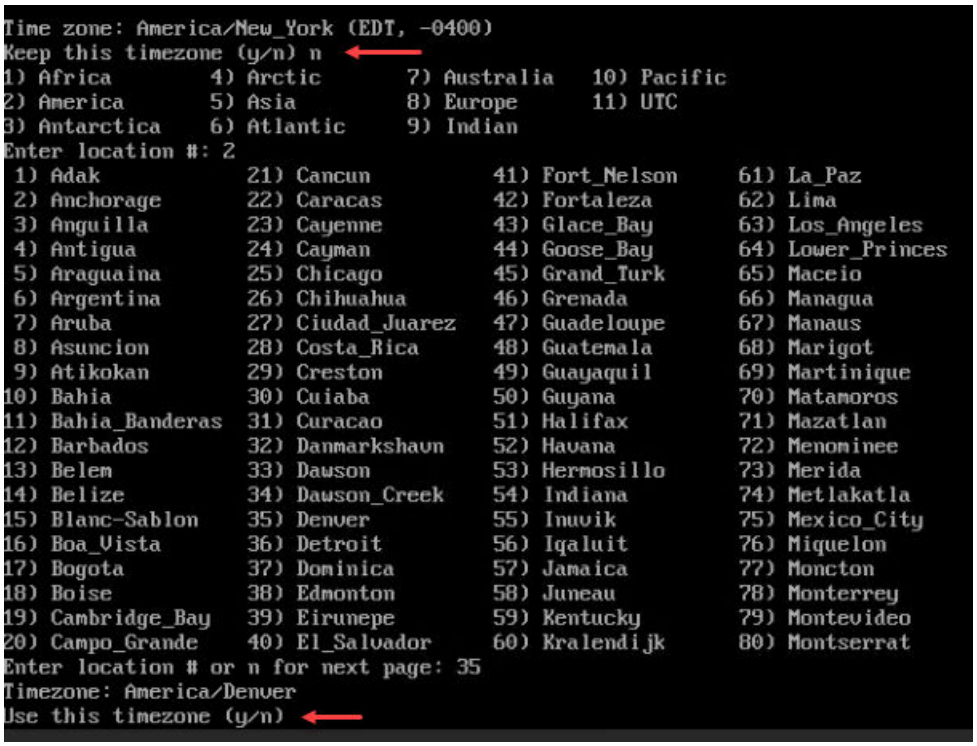
7. The configuration script will ask if EASG needs to be Enable or Not. Answer as required. Avaya highly recommends EASG be enabled to facilitate troubleshooting.



8. The Configuration script will ask to change the root account password.



9. Follow the prompts to configure the timezone.



10. Follow the prompt to configure the following parameters:
    a. Enable/Disable OOBM

       Reference Securing Network Configuration (OoBM) on page 90 prior to making desired selections.

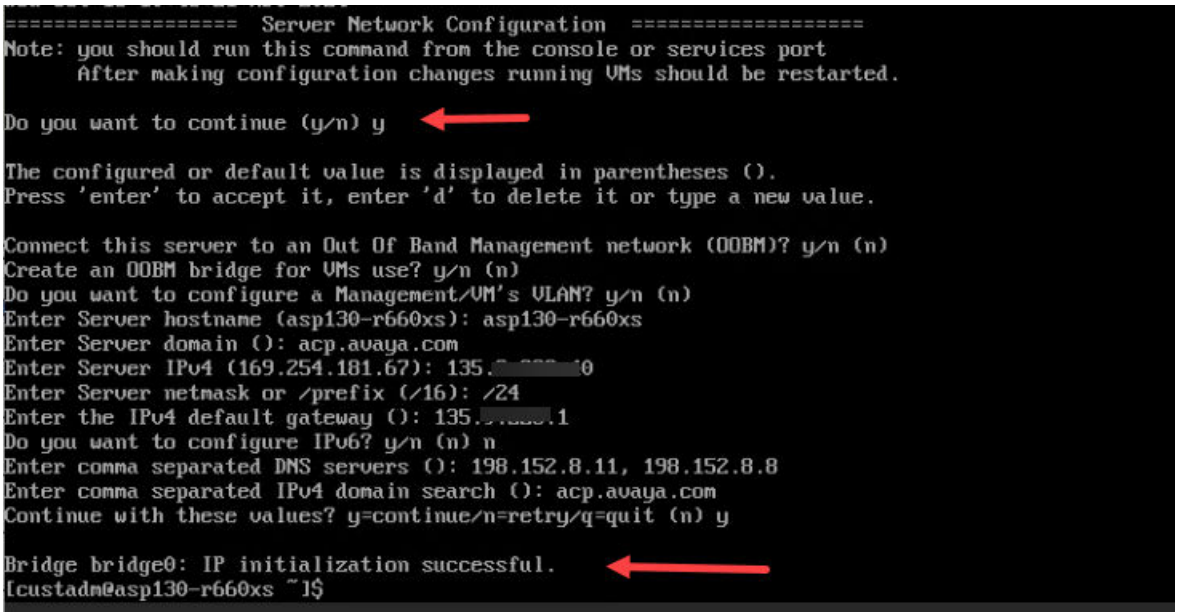
    b. **(Optional)** Assign a VLAN ID
    c. Server hostname
    d. Server domain
    e. Server IPv4 address
    f. Server netmask
    g. IPv4 default gateway
    h. IPv6 (optional)
    i. DNS server(s) comma separated
    j. IPv4 Domain search
    k. Continue with these values (y = continue, n = retry, q = quit)

Note:

'Enter Server domain' option will only be displayed if user enters a 'shortname' in the 'Enter Server hostname' field. If an FQDN is entered, prompt will skip to 'Enter Server IPv4' field.

Pressing `d` will delete the existing value for those fields where the user is required to enter a value.

Ensure that `Bridge bridge0: IP initialization successful` is displayed after continuing with the above values.



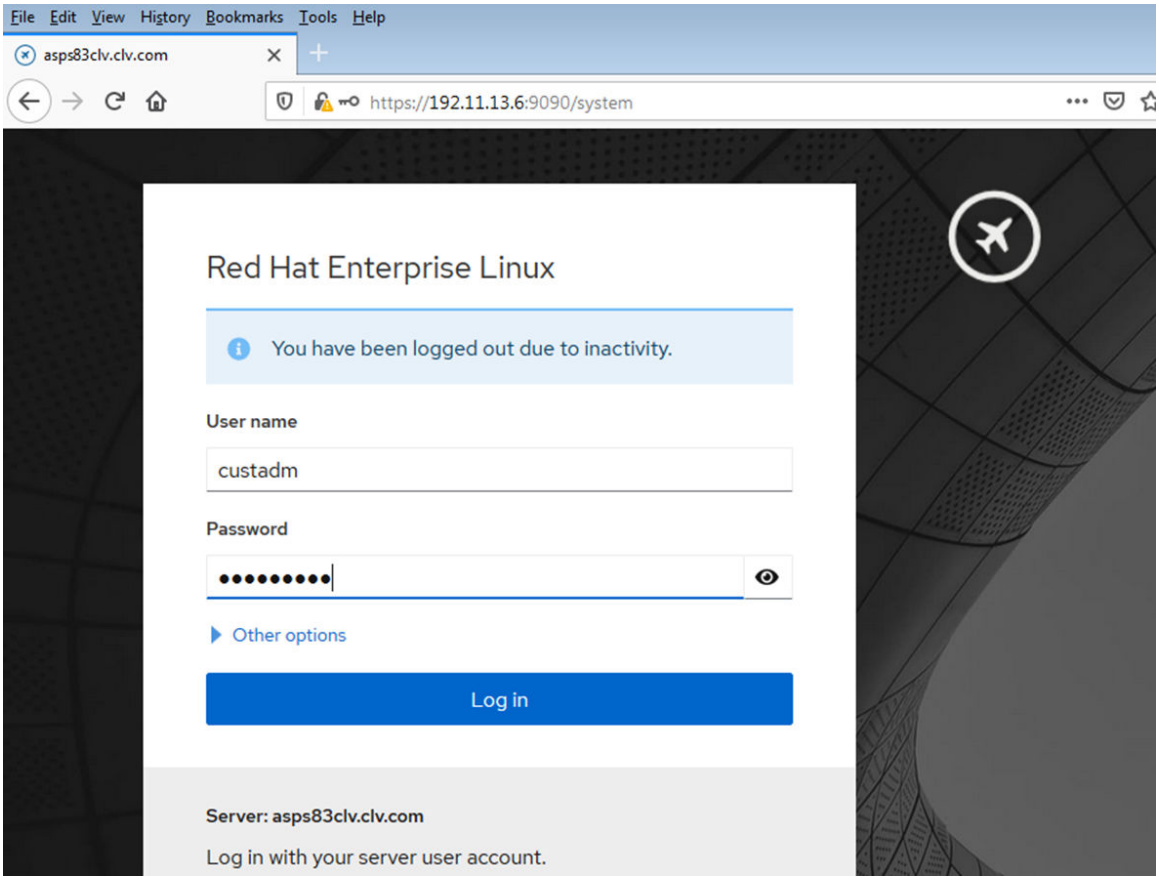
11. Run the command **`ip addr`** and verify your network information is correct. An active network link needs to be connected for IP information to display.

Note:

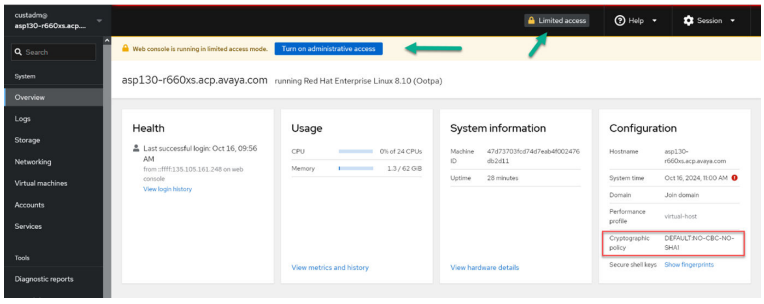
- Services port IP address will only be displayed if an active link is connected to eno8403 (NIC 2).
- Look for bridge0 and ensure IP address and mask assigned above is present.
- Search for bridge0. RHEL dynamically assigns numbers that will identify the interface (example 1 first time loaded KVM on RHEL assigned ID 9 to bridge0, 2nd time loaded assigned ID 182 to bridge0).
- The **`configNetwork`** command can be used later to change values.

```
[custadm@asp130-r660xs ~]$ 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: eno8303: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master bridge0 state UP group default qlen 100
0
    link/ether d0:46:0c:6f:9e:5e brd ff:ff:ff:ff:ff:ff
    altname enp1s0f0
3: eno8403: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether d0:46:0c:6f:9e:5f brd ff:ff:ff:ff:ff:ff
    altname enp1s0f1
    inet 192.11.13.6/30 brd 192.11.13.7 scope global noprefixroute eno8403
       valid_lft forever preferred_lft forever
    inet6 2a07:2a41:ad07:10c:a8d9:9fb3:9404:da65/64 scope global dynamic noprefixroute
       valid_lft 2591893sec preferred_lft 604693sec
    inet6 fe80::6187:9963:7618:616b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: enol2419: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:04:e6:82:9a:b4 brd ff:ff:ff:ff:ff:ff
    altname enp63s0f0
5: enol2429: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:04:e6:82:9a:b5 brd ff:ff:ff:ff:ff:ff
    altname enp63s0f1
6: enol2399: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:04:e6:82:9a:b2 brd ff:ff:ff:ff:ff:ff
    altname enp62s0f0
7: enol2409: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether d4:04:e6:82:9a:b3 brd ff:ff:ff:ff:ff:ff
    altname enp62s0f1
10: bridge0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether d0:46:0c:6f:9e:5e brd ff:ff:ff:ff:ff:ff
    inet 10.[redacted]/24 brd 10.129.152.255 scope global noprefixroute bridge0
       valid_lft forever preferred_lft forever
```

12. Login to the cockpit by opening a browser and enter the IP address you assigned to as Server IPv4 and append port 9090 to it. Login and verify system parameters. Login using the **custadm** credentials.



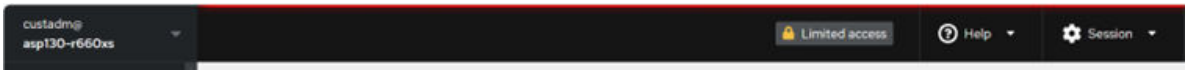
13. Once logged in, view the Overview page and additional tabs for configuration verification. Additional configuration can be performed from this interface. Verify that the Performance profile and the Cryptographic policy matches the image below. This indicates that the installation completed successfully. Cockpit is now available for additional configuration and deployment of VMs.



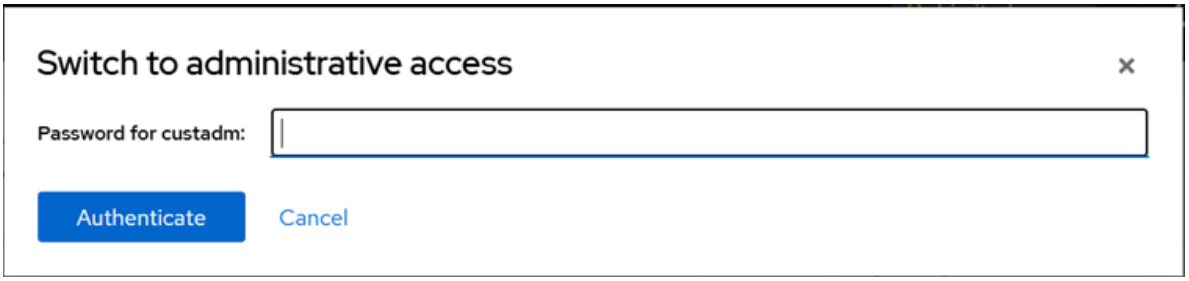
Note:

If this is a remaster or new install, REMOVE the jump drive from the system.

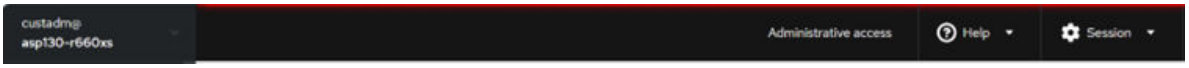
14. For administration actions you will need to click on the button labelled **Limited access**.



15. Enter the password for custadm at the message box below.



The button at the top will change to show **Administrative access**.



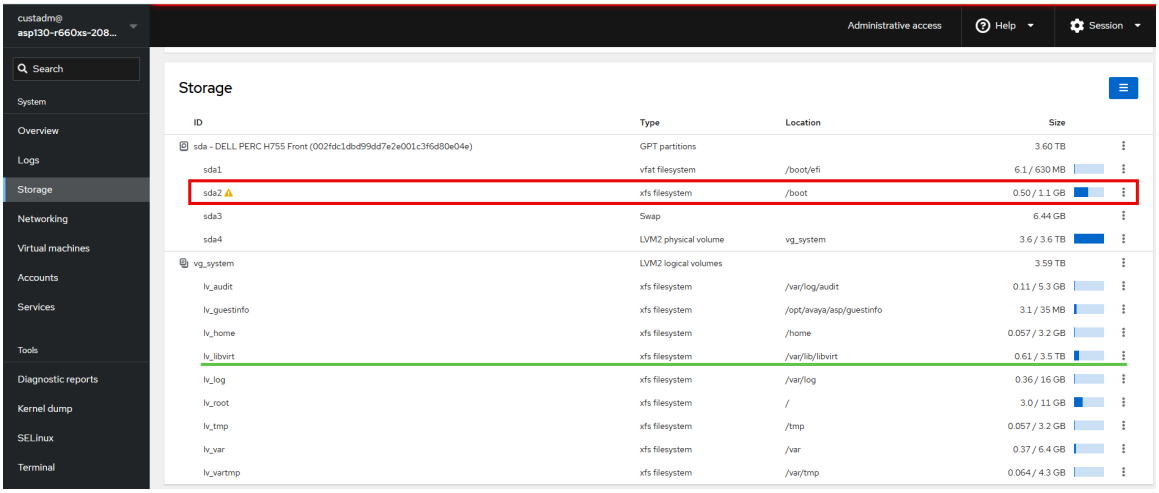
Note:

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

16. The screen shot below shows the `/var/lib/libvirt` partition. 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.

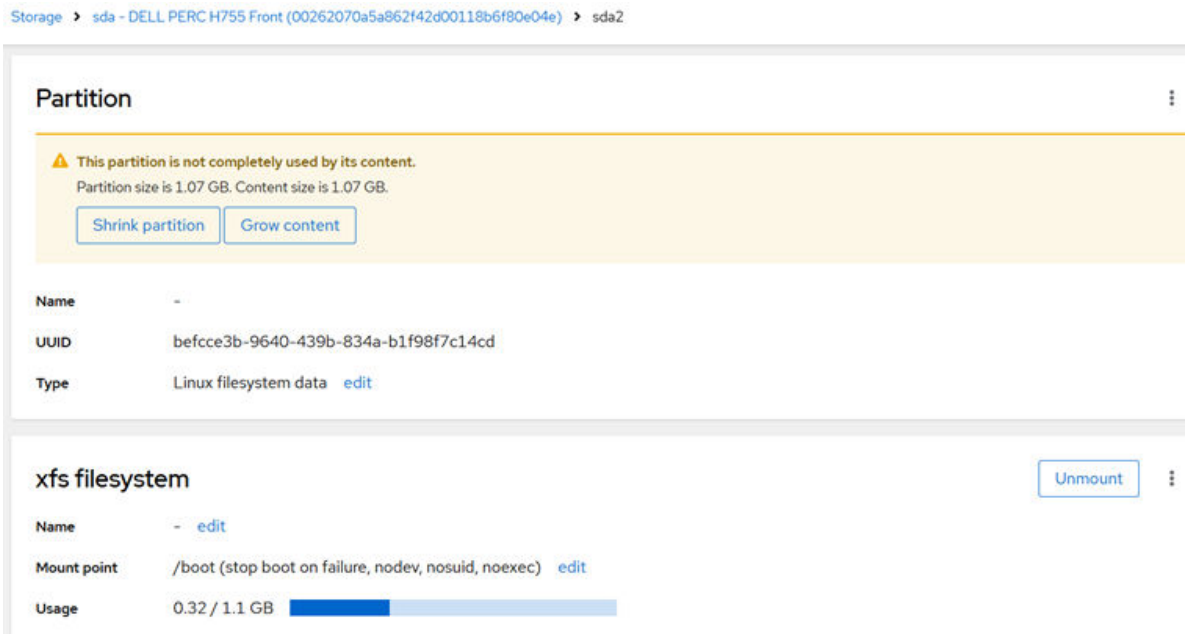
Note:

The sda4 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.



17. 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.

The sda2 LVM2 physical volume shows a yellow (triangle!) warning icon. Clicking on it will show following kind of message:



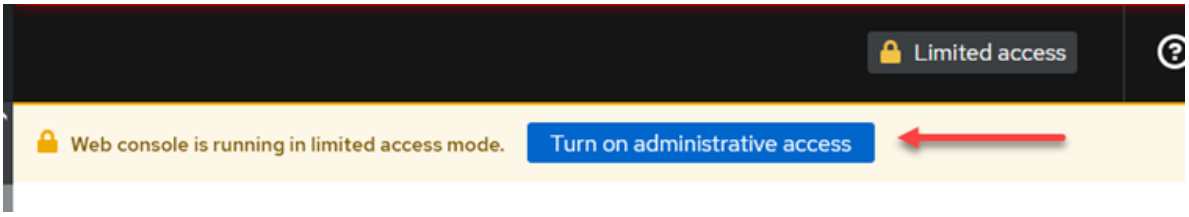
Note:

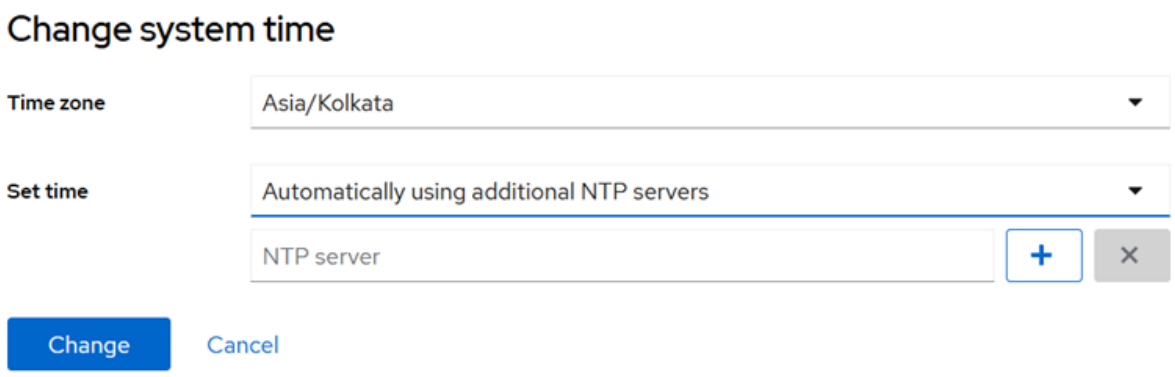
Do NOT attempt to either grow or shrink partition.

18. 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 will be shown.

    The system defaults to the RHEL 8 default NTP pool configuration. But those often will 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.

    Note that there are three options available in the **Set time** field: Manually (set date/ time explicitly), Automatically using NTP (RHEL 8 default NTP pool configuration), and Automatically using additional NTP Servers (enter customer specific NTP servers).





19. 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.
20. The hostname (along with domain) can be changed by clicking on **Edit** beside the Hostname field.
    a. Under **Real host name** enter FQDN of server (ex. `abc1.avaya.com`).
    b. Do not enter short name (enter FQDN).
    c. Ignore **Pretty host name** entry (leave blank).

21. Enter the hostname (along with domain) in the field **Real host name** and click **Change**.

Note:

If a remaster/new install, don't forget to remove jump drive from the system. It is not mounted and can be removed.

Important:

Do not make any changes/edits beyond what is documented in this manual as it will result in an unsupported configuration. This includes attempting to grow or shrink partitions.

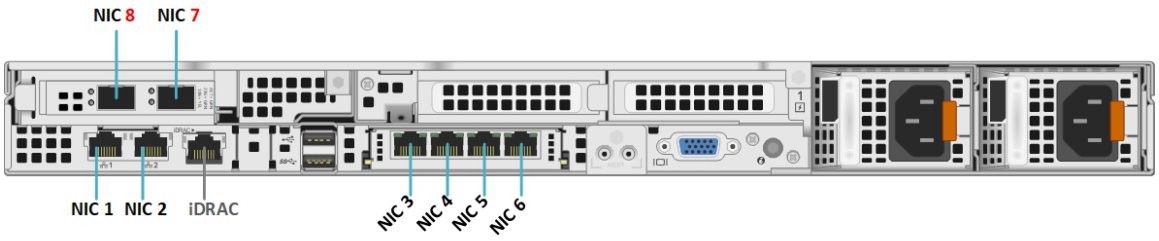
NIC assignment mapping

Following the migration of an ASP Dell R640 running on ESXi to ASP 130 R6.0.x, there is a change in the NIC port naming convention. The ports previously labeled as vmnic0-3 on the

4-port motherboard NIC and vmnic4-5 on the 2-port PCIe NIC are renamed to eno1-4 on the motherboard. The port names for ports 5 and 6 vary depending on the specific configuration within the ASP R6.0.x hypervisor environment.

This section outlines the NIC assignment configuration for the supported Dell servers in the Avaya Solutions Platform (ASP) Release R6.x, operating with KVM on RHEL 8.10, along with its various profile configurations.

R660xs A3-A31Current Configuration (H755)



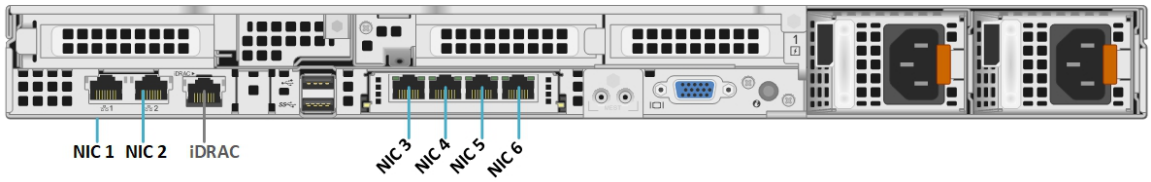
Profiles A3-A31: Rear View of Dell PowerEdge R660xs – Dual CPU Server

Avaya KVM on RHEL 8.10 to R660xs NIC mapping for A3 and A31

R660xs NIC assignment	RHEL eth name	Comments
NIC 1	eno8303	LOM – NIC order left to right
NIC 2	eno8403	LOM – Services – NIC order left to right
NIC 3	eno12399	1st OCP port – NIC order left to right
NIC 4	eno12409	2nd OCP port – NIC order left to right
NIC 5	eno12419	3rd OCP port – NIC order left to right
NIC 6	eno12429	4th OCP port – NIC order left to right
*NIC 7	ens1f0np0	10/25GbE in A3 and A31 systems NIC order is *right to left*
*NIC 8	ens1f1np1	10/25GbE in A3 and A31 systems. NIC order is *right to left*

*Available for use beginning with ASP R6.0.0.4.0 and with BIOS/FW v2 or later.

R660xs A1-A2 current configuration (H755)

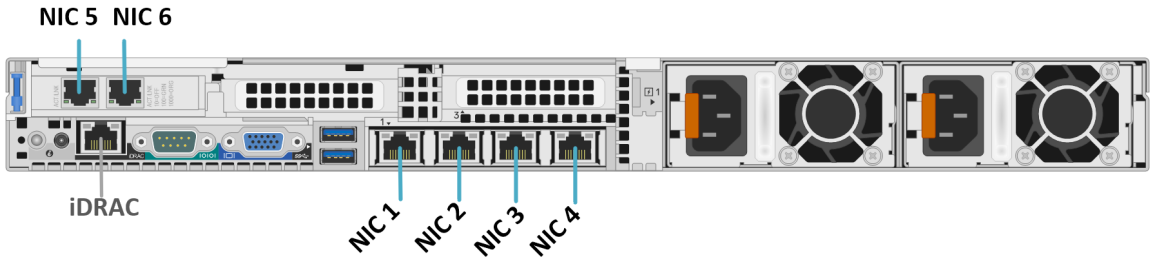


Profiles A1-A2: Rear View of Dell PowerEdge R660xs – Single/Dual CPU Server

Avaya KVM on RHEL 8.10 to R660xs NIC mapping for A1 and A2

R660xs NIC assignment	RHEL eth name	Comments
NIC 1	eno8303	LOM – NIC order left to right
NIC 2	eno8403	LOM – Services NIC order left to right
NIC 3	eno12399	1st OCP port – NIC order left to right
NIC 4	eno12409	2nd OCP port – NIC order left to right
NIC 5	eno12419	3rd OCP port – NIC order left to right
NIC 6	eno12429	4th OCP port – NIC order left to right

R640 P2/P4 Single CPU Configuration (H730P)

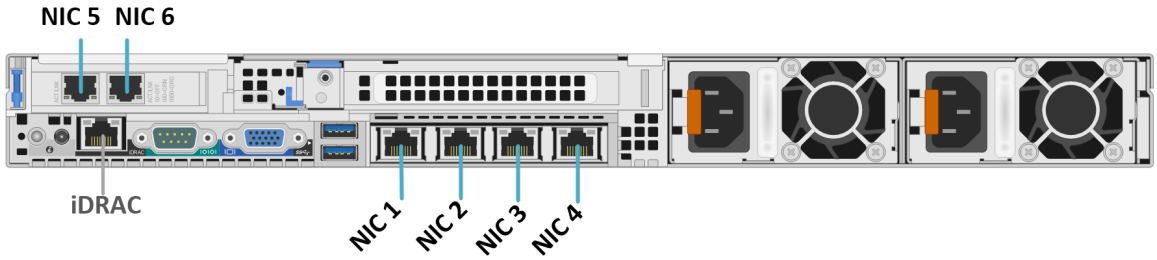


Back view of Dell PowerEdge R640 Single CPU server with H730P Mini Raid Controller & Intel 4x1 GbE NDC

Avaya KVM on RHEL 8.10 to R640 NIC mapping for P2, P4 - H730P - Intel NDC/Broadcom NIC

R640 NIC assignment	RHEL eth name	Comments
NIC 1	eno1	NDC order left to right
NIC 2	eno2	NDC – Services NIC order left to right
NIC 3	eno3	NDC – order left to right
NIC 4	eno4	NDC – order left to right
NIC 5	ens1f0	Broadcom NIC order left to right
NIC 6	ens1f1	Broadcom NIC order left to right

R640 P3/P5/P51 Dual CPU Configuration (H730P)

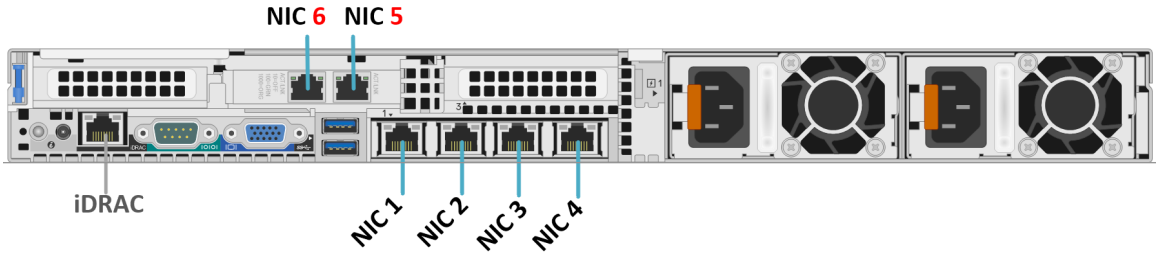


Back view of Dell PowerEdge R640 dual CPU server with H730P Mini Raid Controller & Intel 4x1 GbE NDC

Avaya KVM on RHEL 8.10 to R640 NIC mapping for P3, P5, 51 - H730 - Intel NDC/Broadcom NIC

R640 NIC assignment	RHEL eth name	Comments
NIC 1	eno1	NDC order left to right
NIC 2	eno2	NDC – Services NIC order left to right
NIC 3	eno3	NDC – order left to right
NIC 4	eno4	NCD – order left to right
NIC 5	ens1f0	Broadcom NIC order left to right
NIC 6	ens1f1	Broadcom NIC order left to right

R640 P2/P4 single CPU Configuration (H750)

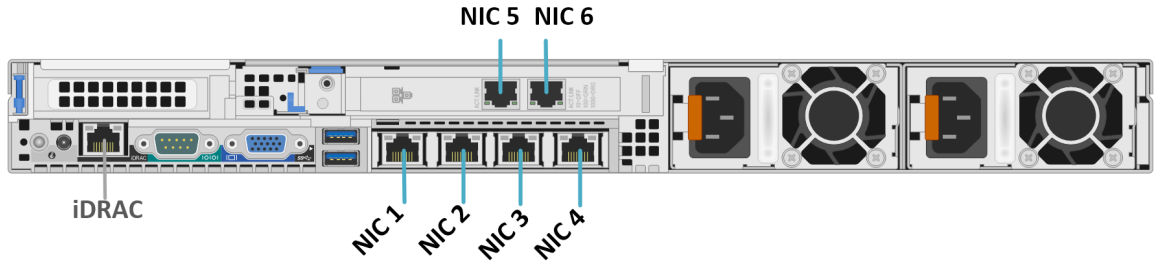


Back view of Dell PowerEdge R640 Single CPU server with H750 Raid Controller & Broadcom 4x1 GbE NDC

Avaya KVM on RHEL 8.10 to R640 NIC mapping for P2, P4 - H750 – Broadcom NDC/Broadcom NIC

R640 NIC assignment	RHEL eth Name	Comments
NIC 1	eno1	NDC order left to right
NIC 2	eno2	NDC – Services NIC order left to right
NIC 3	eno3	NDC – order left to right
NIC 4	eno4	NCD – order left to right
NIC 5	ens2f0	Broadcom NIC order *right to left*
NIC 6	ens2f1	Broadcom NIC order *right to left*

R640 P3/P5/P51 Dual CPU Configuration (H750)



Back view of Dell PowerEdge R640 Dual CPU server with H750 Raid Controller & Broadcom 4x1 GbE NDC

Avaya KVM on RHEL 8.10 to R640 NIC mapping for P3, P5, 51 – H750 – Broadcom NDC/ Broadcom NIC

R660xs NIC assignment	RHEL eth name	Comments
NIC 1	eno1	NDC order left to right
NIC 2	eno2	NDC – Services NIC order left to right
NIC 3	eno3	NDC – order left to right
NIC 4	eno4	NCD – order left to right
NIC 5	enp216s0f0	Broadcom NIC order left to right
NIC 6	enp216s0f1	Broadcom NIC order left to right

Configuring NIC bonding (only available in ASP R6.0.0.1 and later)

Note:

Avaya always recommends software currency (latest release). For detailed instructions on NIC bonding and VLAN configuration, see the following:

- ASP 130 R6.0.0.3 and earlier – VLAN & VLAN TRUNKING CONFIGURATION GUIDE-Rev2
- ASP 130 R6.0.0.4 and later – VLAN & VLAN TRUNKING CONFIGURATION GUIDE-Rev1

NIC bonding overview

NIC bonding provides a redundant path for the management and application traffic by combining two or more network interfaces into a single logical interface. NIC bonding is a Red Hat feature, not an Avaya feature. Customers wishing to configure NIC bonding on the ASP 130 are required to use Avaya's instructions.

Note:

The only supported bond configuration mode within the ASP 130 solution is Active/Backup.

Note:

Support for configuring NIC Bonding was introduced in ASP R6.0.0.1 with enhancements to the **`configNetwork`** script.

Note:

This guide uses P[n] and NIC[n] to refer to the same network interface. For example, P1 is the same as NIC 1.

Administering NIC Bonding in KVM on RHEL 8.10

Red Hat Enterprise Linux (RHEL) offers a variety of options and configurations for setting up network bonding. While the Red Hat vendor does not provide a single "best" recommended configuration, it is important to note that for Avaya ASP 130 R6.0, the only tested and supported configuration method is adding a bond with physical interfaces. Be aware that combining bridges, bridges with VLAN tags, or virtual machine interfaces when adding a bond is not supported by

Avaya. When applicable to keep a streamlined and consistent behavior the default bridge0 will be the primary reference point for NIC bonding behaviors and expectations.

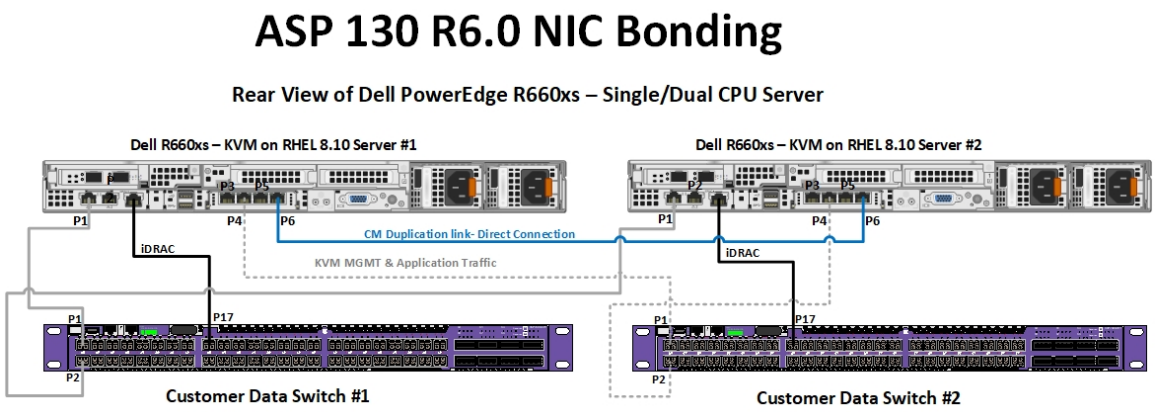


Figure 2: Example diagram of single NIC bond configuration in an ASP 130 R6.0.x – Infrastructure Layer

Note:

The data switch ports listed in the following table are for demonstration purposes and are intended to serve as a reference only.

	Server NIC	R660xs Hypervisor	R640 Hypervisor	Data Switch 1	Data Switch2	Usage	Native VLAN
Server #1	P1	eno8303	eno1	P1	-	KVM MGMT & Application Traffic	MGMT & VoIP VLAN
Server #1	P4	eno12409	eno4	-	P1	KVM MGMT & Application Traffic	MGMT & VoIP VLAN
Server #1	iDRAC	N/A	N/A	P17	-	Dell iDRAC Interface	MGMT VLAN
Server #2	P1	eno8303	eno1	P2	-	KVM MGMT & Application Traffic	MGMT & VoIP VLAN
Server #2	P4	eno12409	eno4	-	P2	KVM MGMT & Application Traffic	MGMT & VoIP VLAN
Server #2	iDRAC	N/A	N/A	---	P17	Dell iDRAC Interface	MGMT VLAN

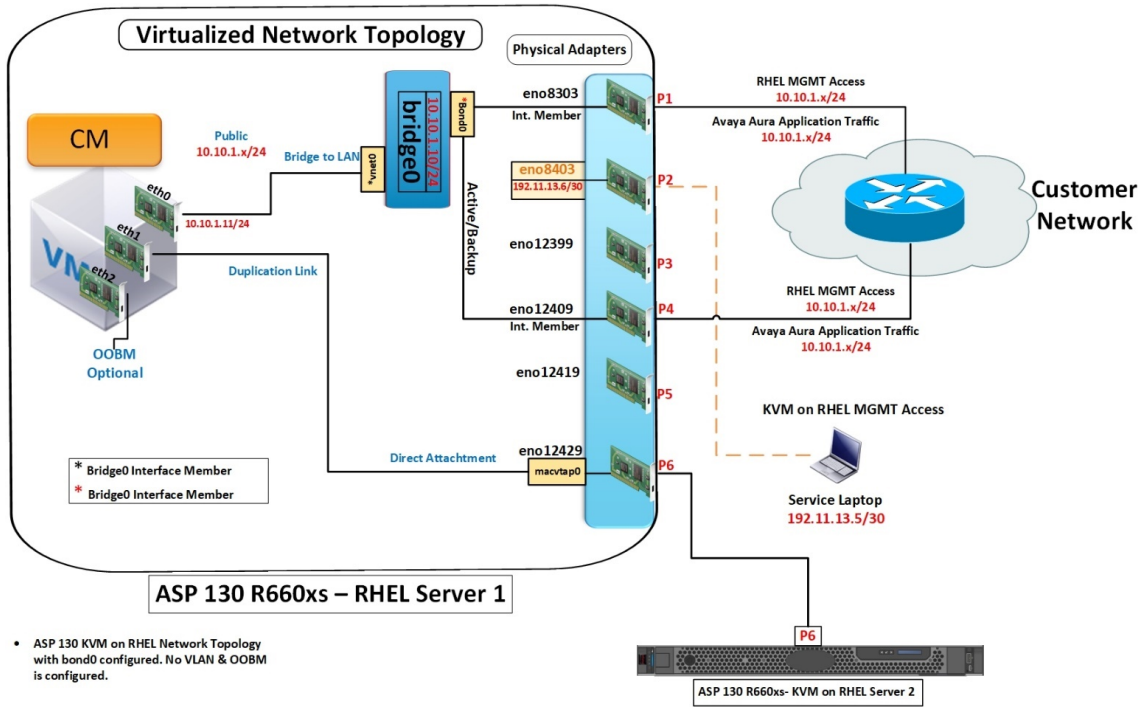


Figure 3: Example diagram of single NIC bond configuration in an ASP 130 R6.0.x – Hypervisor Layer

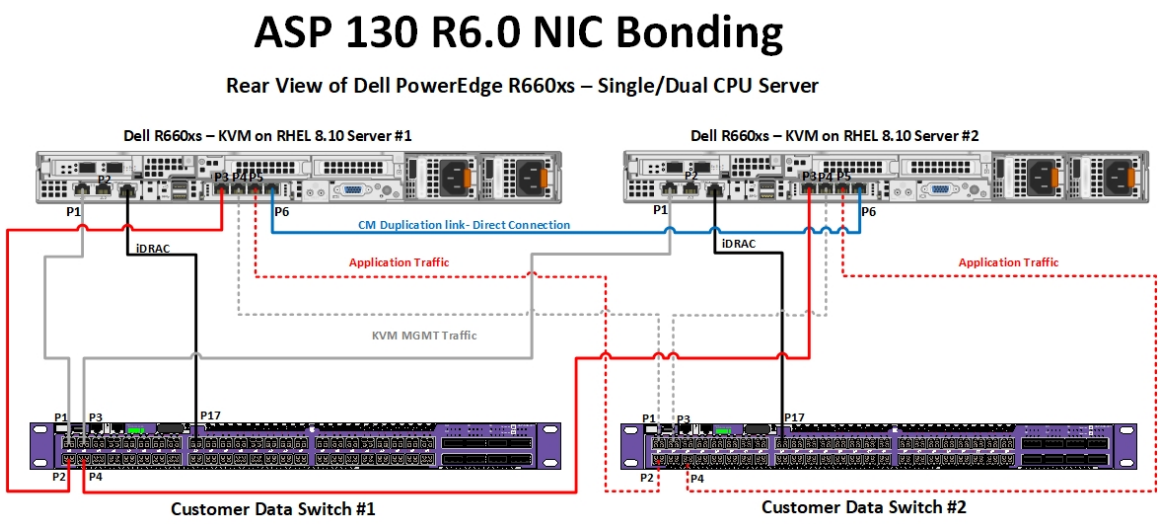


Figure 4: Example diagram of dual NIC bond configuration in an ASP 130 R6.0.x – Infrastructure Layer

Note:

The data switch ports listed in the following table are for demonstration purposes and are intended to serve as a reference only.

	Server NIC	R660xs Hypervisor	R640 Hypervisor	Data Switch 1	Data Switch2	Usage	Native VLAN
Server #1	P1	eno8303	eno1	P1	-	KVM MGMT Traffic	MGMT VLAN
Server #1	P4	eno12409	eno4	-	P1	KVM MGMT Traffic	MGMT VLAN
Server #1	P3	eno12399	eno3	P2	-	Application Traffic	VoIP VLAN
Server #1	P5	eno12419	ens1f0	-	P2	Application Traffic	VoIP VLAN
Server #1	iDRAC	N/A	N/A	P17	-	Dell iDRAC Interface	MGMT VLAN
Server #2	P1	eno8303	eno1	P3	-	KVM MGMT Traffic	MGMT VLAN
Server #2	P4	eno12409	eno4	-	P3	KVM MGMT Traffic	MGMT VLAN
Server #2	P3	eno12399	eno3	P4	-	Application Traffic	VoIP VLAN
Server #2	P5	eno12419	ens1f0	-	P4	Application Traffic	VoIP VLAN
Server #2	iDRAC	N/A	N/A	-	P17	Dell iDRAC Interface	MGMT VLAN

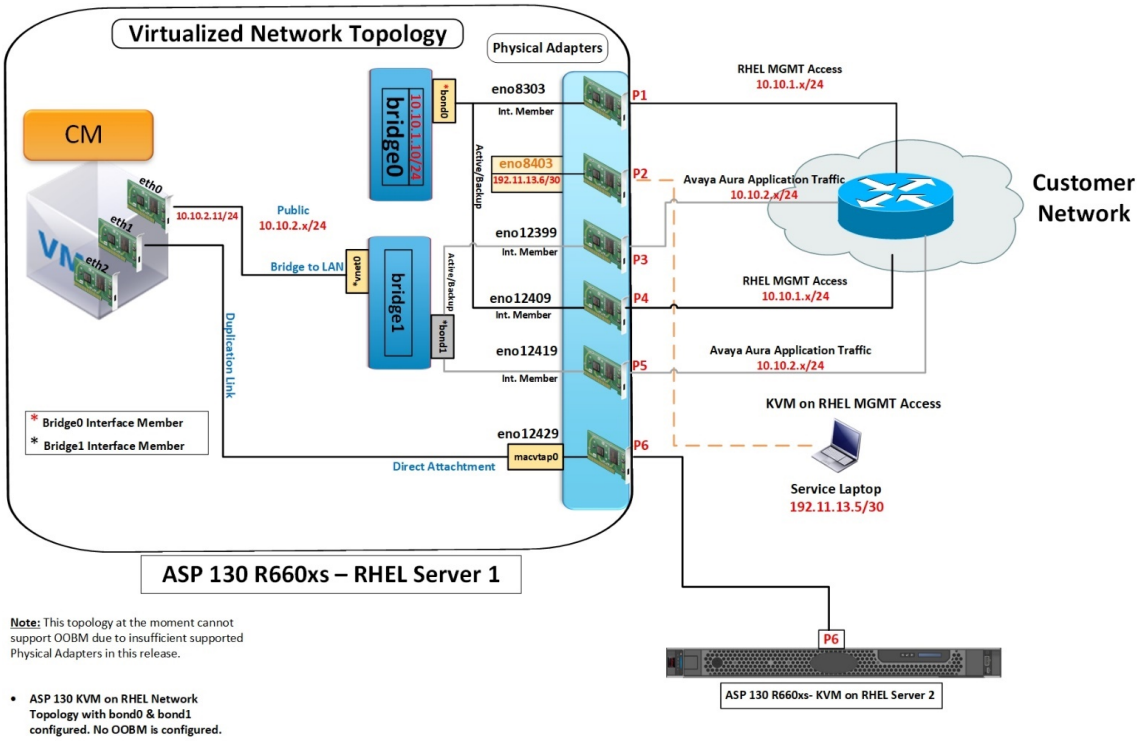


Figure 5: Example diagram of Dual NIC bond configuration in an ASP 130 R6.0.x – Hypervisor Layer

Management Interface configuration in the host for network bonds

The KVM on RHEL 8.10 management interface can be configured to support NIC Teaming to provide network redundancy. The following guidelines will help to configure the proper NICs on the server for that functionality. The network configuration script **`configNetwork`** available with the ASP 130 R6.0 software image allows the configuration of network bonding (single bond), however, for more complex network configurations Cockpit (user web interface for Red Hat Enterprise Linux) can be used. In this configuration example, a single bond0 will be created and assigned to bridge0.

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

Verifying the ASP software version

Execute the **swversion** command to obtain the current ASP software version information. Example below is from ASP R6.0.0.0. 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.

```
[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
```

Adding a bond using the network configuration script

About this task

Note:

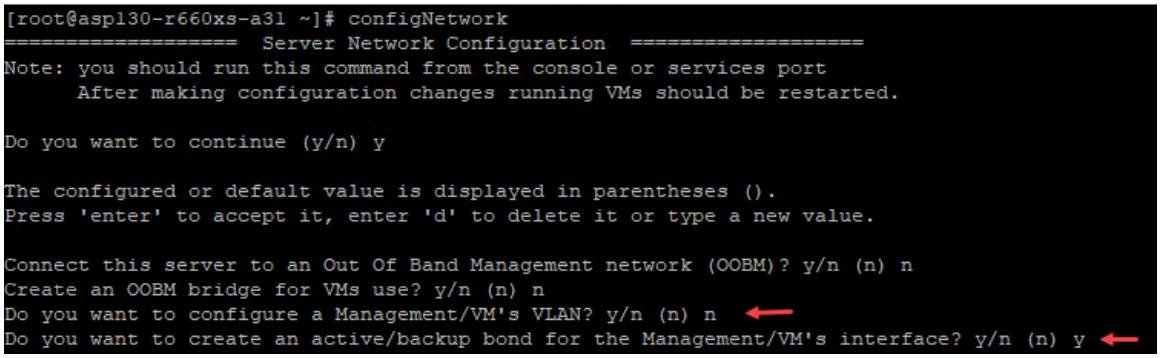
When making network configuration changes to the primary interface connecting to the server via the console or services port is required. Network services get restarted as the script makes changes terminating any existing connections over the network to the primary interface.

Before you begin

- One available network interface in the host.
- Connect the designated server port to the customer data switch, referencing the provided cable diagram to ensure proper wiring configuration.

Procedure

1. Connect to the KVM on RHEL server using the services port connection.
2. Log in to the KVM on RHEL host by using a Secure Shell (SSH) client e.g., PuTTY.
3. Authenticate using the existing custadm credentials or sroot EASG if enabled.
4. Execute the following CLI command: **`configNetwork`**.
5. Follow the script prompts:
   a. Type `y` to continue if the connection is via services port.
   b. Type `n` to continue (OOBM configuration is not part of this procedure).
   c. Type `n` to continue.
   d. Option A: Type `n` (VLAN configuration is not part of this procedure).



   e. Option B: The network script automatically detects if a VLAN has been previously configured on the management interface. If a VLAN is found, the script will display a `Y` by default. To retain the current VLAN configuration, simply press **Enter** without making any changes to keep the existing VLAN configuration intact.

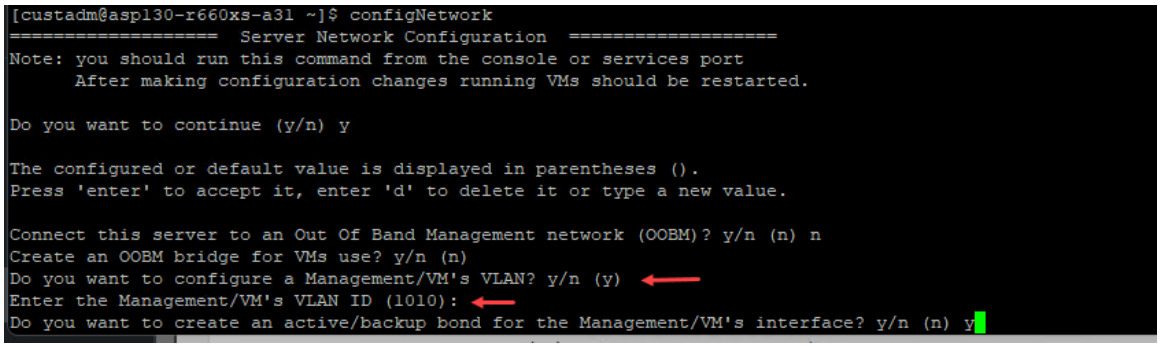


Figure 6: Output Example displays a VLAN 1010 present in the system

   f. Type `y` to configure an active/backup bond for management/VM interface.
   g. Enter a number that corresponds to the desired network interface.

      For this example, option `0` server P4 / hypervisor eno12409 interface will be selected.

h. Type `y` to create an active/backup bond with eno8303 and eno12409.

i. Press **Enter** key (7 times) until prompt displays `Continue with these values? y=continue/n=retry/q=quit (n)`. If satisfy with current selections type **y**.

Note:

Although multiple changes at the same time are supported by the network script, IP address changes are not part of this procedure.

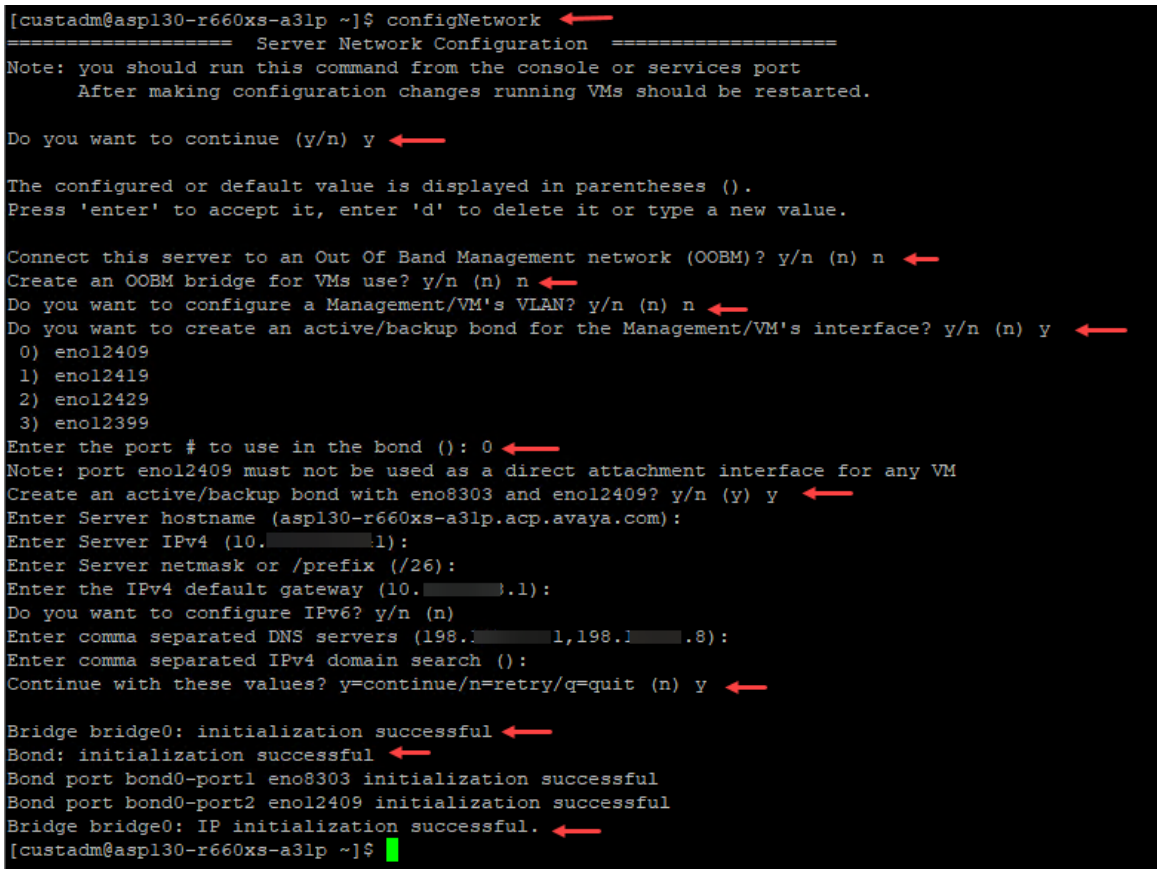


Figure 7: Example Output When a VLAN Has Not Been Configured Previously (Option A)

```
[root@aspl30-r660xs-a31 ~]# configNetwork
==================  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) n
Create an OOBM bridge for VMs use? y/n (n) n
Do you want to configure a Management/VM's VLAN? y/n (n) y
Enter the Management/VM's VLAN ID (): 1010
Do you want to create an active/backup bond for the Management/VM's interface? y/n (y)
 0) eno12409
 1) eno12419
 2) eno12429
 3) eno12399
Enter the port # to use in the bond (eno12409):
Note: port eno12409 must not be used as a direct attachment interface for any VM
Create an active/backup bond with eno8303 and eno12409? y/n (y)
Enter Server hostname (aspl30-r660xs-a31.acp.avaya.com):
Enter Server IPv4 (10.      1):
Enter Server netmask or /prefix (/26):
Enter the IPv4 default gateway (10.1      .1):
Do you want to configure IPv6? y/n (n)
Enter comma separated DNS servers (198.      11,198.      8):
Enter comma separated IPv4 domain search (acp.avaya.com):
Continue with these values? y=continue/n=retry/q=quit (n) y

Bridge bridge0: initialization successful
Bond: initialization successful
Bond port bond0-port1 eno8303.1010 initialization successful
Bond port bond0-port2 eno12409.1010 initialization successful
Bridge bridge0: IP initialization successful.
[root@aspl30-r660xs-a31 ~]#
```

Figure 8: Example Output When a VLAN Has Been Configured Previously (Option B)

6. Execute the following CLI command for bond configuration validation: **`nmcli con`**

```
[custadm@aspl30-r660xs-a31 ~]$ nmcli con
NAME              UUID                                  TYPE      DEVICE
Mgmt_VM_Network   d0395275-ba6b-4ae3-ad33-16b679bec9ac  bridge    bridge0
Services          f21f3299-a47f-414c-a8a1-b3324701b681  ethernet  eno8403
vnet0             077e3e2f-8f3d-4962-bd20-2b422c9e2706  tun       vnet0
vnet1             16b28e57-ba2c-4c3e-b4e6-a4d0ebf8fab6  tun       vnet1
vnet3             42468248-17d8-426d-8b44-fd4f717a8153  tun       vnet3
bond0-port1       bf8c2904-70b8-4290-99df-21407061146b  ethernet  eno8303
bond0-port2       e88152e6-bf10-4c5e-a214-4ced2febe5db  ethernet  eno12409
bridge0-port      228ad7d8-45ca-4451-8b5b-46ffc53fcb0c  bond      bond0
```

Figure 9: Example Output: Bond configuration without VLAN

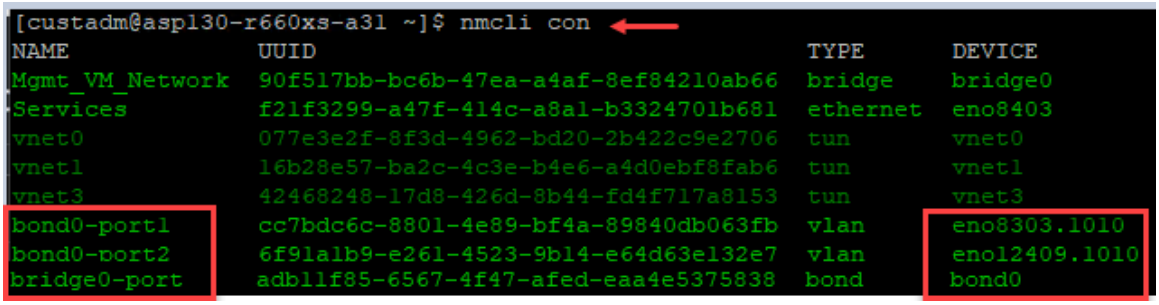


Figure 10: Output example: Bond configuration with VLAN

Configuring a second network bond using Cockpit

About this task

The updated network script **`configNetwork`** available with ASP R6.0.0.4.0 and later can now configure a second bond (bond1) on a second bridge (bridge1). For more information, see ASP 130 R6.0.0.4 and Later- VLAN & VLAN TRUNKING CONFIGURATION GUIDE-Rev1.

Putting VoIP and Data on separate networks is a best recommended, industry standard. Isolating VoIP traffic from Data/Management traffic helps to enhance network security and enables customers to implement QoS adequately. It also helps by simplifying network traffic management and troubleshooting as each network can be monitored independently. By independently monitoring each network, a network administrator can quickly identify and address issues specific to either VoIP or data/management services, improving response times and minimizing downtime.

Note:

Call signaling in VoIP communications, whether directed to Communication Manager (CM), Session Manager (SM), or media servers, is still classified as VoIP traffic, even if media (RTP packets) is not transmitted as part of the call signaling process.

Before you begin

- An existing bond for the management and application traffic is expected to be already configured. Reference to Adding a bond using the network configuration script on page 67 if required prior to proceeding.
- Two available network interfaces in the host.
- Connect the designated server ports to the customer data switch, referencing the provided cable diagram to ensure proper wiring configuration.

Procedure

1. Using a Web browser tab, navigate to the KVM on RHEL server IP Address e.g.: `https://192.11.13.6:9090`
2. Authenticate using the existing custadm credentials.
3. If not already in “Administrative access”, click on the upper-right corner “Limited access” and enter the password for the custadm account.
4. From the left pane menu, select **Networking** > **Add Bond**.

5. Select the following:
   - Name: **bond1**.
   - Interfaces: check boxes for **eno12399** & **eno12419**.

     Note:

     This configuration does not support Out-of-Band Management (OOBM) and Communication Manager (CM) Duplex mode simultaneously, due to the lack of sufficient, supported network interface cards (NICs) in this release.

     Note:

     If OOBM is already configured DO NOT use **eno12399**. If this KVM host is not part of a CM Duplex solution as an alternative **eno12429** can be used.
   - Mode (leave default selection): **Active backup**.
   - MAC, Primary, Link monitoring, Monitoring interval, link up delay, link down delay: Leave default values.
6. Click **Add** button to create bond.
7. From the left pane menu, click on **Networking** > **Add bridge**.
8. Select the following:
   - **Name**: bridge1
   - **Ports**: previously created **bond1**.
9. Click **Add** button to create bridge.
10. Under Interfaces, select the newly created **bridge1**.
11. Click edit for IPv4 and validate the following:
    - **Address** is set to disabled.
    - There are no entries grayed out for DNS, DNS search domains and routes.
12. Click **Save**.
13. Repeat steps for IPv6.
14. Migrate Avaya Aura® applications virtual network interfaces to the newly created bridge accordingly.

    Note:

    To make network changes to virtual machines, these must be in a power off state.

    Note:

    When segregating networks a new network segment for VoIP will be provisioned. Work with the customer network administrators to ensure Avaya Aura® applications are re-IP accordingly.

Configuring VLAN

VLAN configuration overview

The content in previous releases of this document is now covered in detailed application notes referenced below.

VLAN configuration in ASP R6.0.0.4.0 and later

Starting with ASP R6.0.0.4.0 and later releases, the **`configNetwork`** script has been significantly improved to support the following configuration scenarios:

- Dual bridge configuration (bridge0 & bridge1) is now supported.
- Dual bond configuration is now supported when configuring 2 bridges:
  - bond0 → bridge0
  - bond1 → bridge1
- VLAN Trunking support – when configuring VLAN trunking:
  - Script can now configure 1-5 VLANs
  - Script can configure a dedicated bridge for every required VLAN.
  - VLAN trunking can be configured on either bridge0 or bridge1.
  - Introduce support of the Dell BCM57414 2x10/25GbE Network Interface Card exclusively on the Dell R660xs profiles A3 and A31 with BIOS/FW v2 or later.
  - Support VLAN trunking on the higher density ports 10/25 GbE.
- Link Aggregation Control Protocol(LACP) support is also introduced providing full active/active link redundancy and traffic load balance.

  For a complete step-by-step guide and configuration examples, refer to the new *VLAN & VLAN Trunking configuration guide* for ASP 6.0.0.4.0 and later:

  https://support.avaya.com/css/public/documents/101095129.

VLAN configuration in ASP R6.0.0.3 and earlier

For customers with a host running ASP 6.0.0.3.0 and earlier releases, refer to the *VLAN & VLAN Trunking configuration guide* for ASP 6.0.0.3.0 and earlier releases:

https://support.avaya.com/css/public/documents/101093465

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

Verifying the ASP software version

Execute the **swversion** command to obtain the current ASP software version information. Example below is from ASP R6.0.0.0. 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.

```
[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
```

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:

- **`setBootPassword`** – set a boot password so someone at the console cannot change the kernel boot options or boot single user (default disabled).
- **`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 (only available in ASP R6.0.0.1.1 and later)

SNMP overview

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

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.

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.

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: () Test1v3
 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: Test1v3
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 test1v3 -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"
```

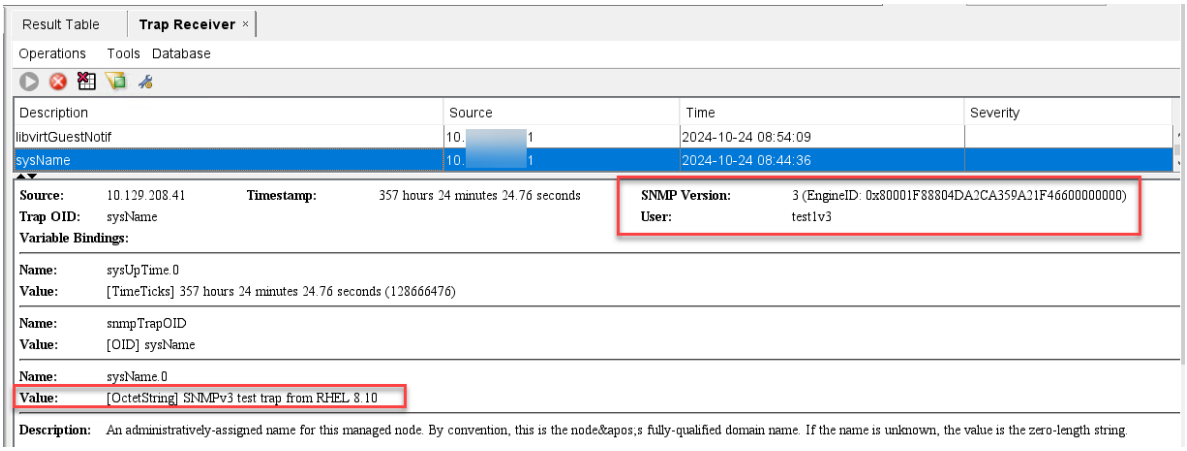


Figure 11: Trap View from NMS Tool – Use for Example Only

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.

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.

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"
```

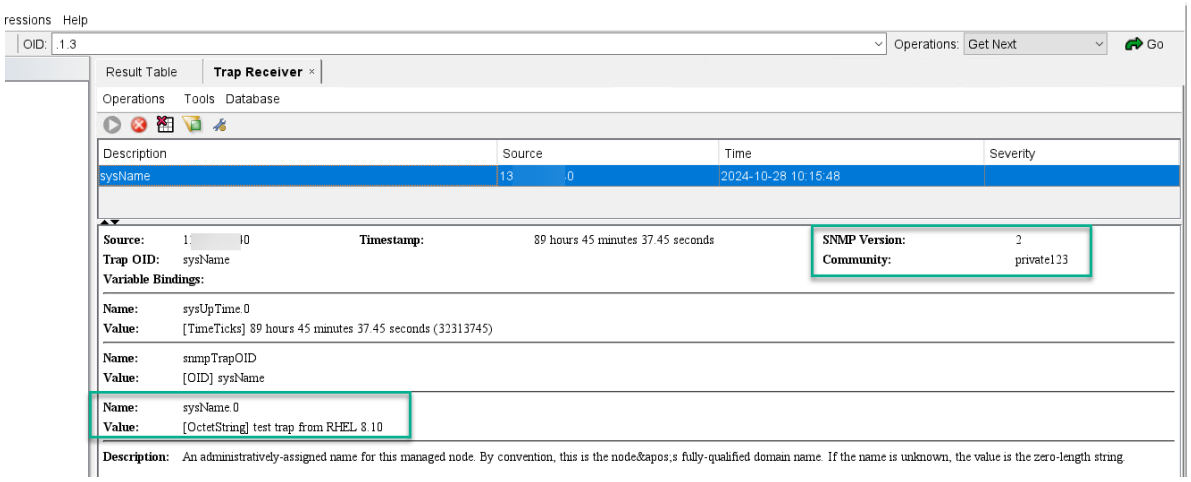


Figure 12: Trap View from NMS Tool – Use for Example Only

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]	laErrMessage.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]	laErrMessage.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]	laErrMessage.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]	laErrMessage.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]	laErrMessage.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]	laErrMessage.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 130 snmpd.conf file has been set to: memSysAvail <=4000000 (4GB)	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

Chapter 7: 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.

Procedure

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

   For example:

```
[custadm@asp130-r660xs ~]$ nmcli connection
NAME             UUID                                  TYPE      DEVICE
Mgmt_VM_Network  752f89b7-b88a-4d19-9e80-22780767cb9a  bridge    bridge0
bridge0-port     39d39997-a927-409a-8ea9-3e52511bf793  ethernet  eno8303
eno12399         0511544c-3643-4c19-ae35-edf837ad51ce  ethernet  --
eno12409         2a5d44f5-ee72-40e2-9ffb-4ad1a0170722  ethernet  --
eno12419         ed57f1cf-e0ed-463b-887c-4fe52b69bfb7  ethernet  --
eno12429         3f7276a8-b7ce-4997-bd09-837dc78dc51c  ethernet  --
eno8303          e3111d99-7aa6-467c-b15e-29b3e671bfe7  ethernet  --
Services         6e6abe63-0b19-4841-b994-62873d86080a  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.

   ASP R6.0.x R660xs

Connection Profile Name	R660xs Device Name	Notes
Mgt_VM_Network	bridge0 (eno8303)	Default w/out OOBM enabled
VM_Network		With OOBM enabled
Services	eno8403	`192.11.13.6` services port
OOBM_Network	bridgeOOB (eno12399)	Optional: Must be enabled during configuration

ASP R6.0.x R640

Connection Profile Name	R640 Device Name	Notes
Mgt_VM_Network	bridge0 (eno1)	Default w/out OOBM enabled
VM_Network		With OOBM enabled
Services	eno2	192.11.13.6 services port
OOBM_Network	bridgeOOB (eno3)	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.

Additional ports are available on the server, the ones listed above are most relevant for installation.

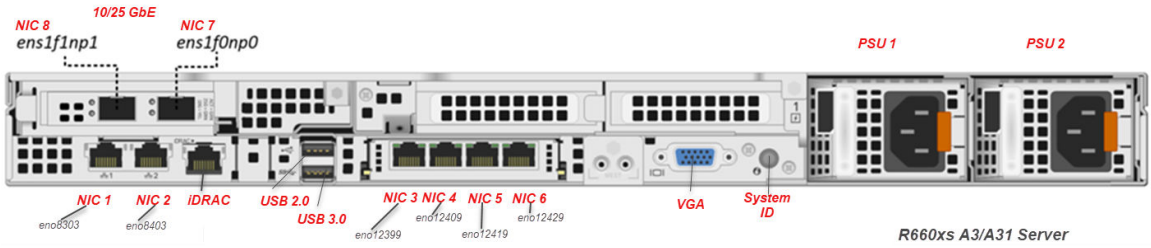
Example of a typical configuration

This drawing is for example purposes only. Before deploying and distributing virtual machines across the ASP 130 servers, verify the solution using the Avaya One Source Configurator (A1SC).

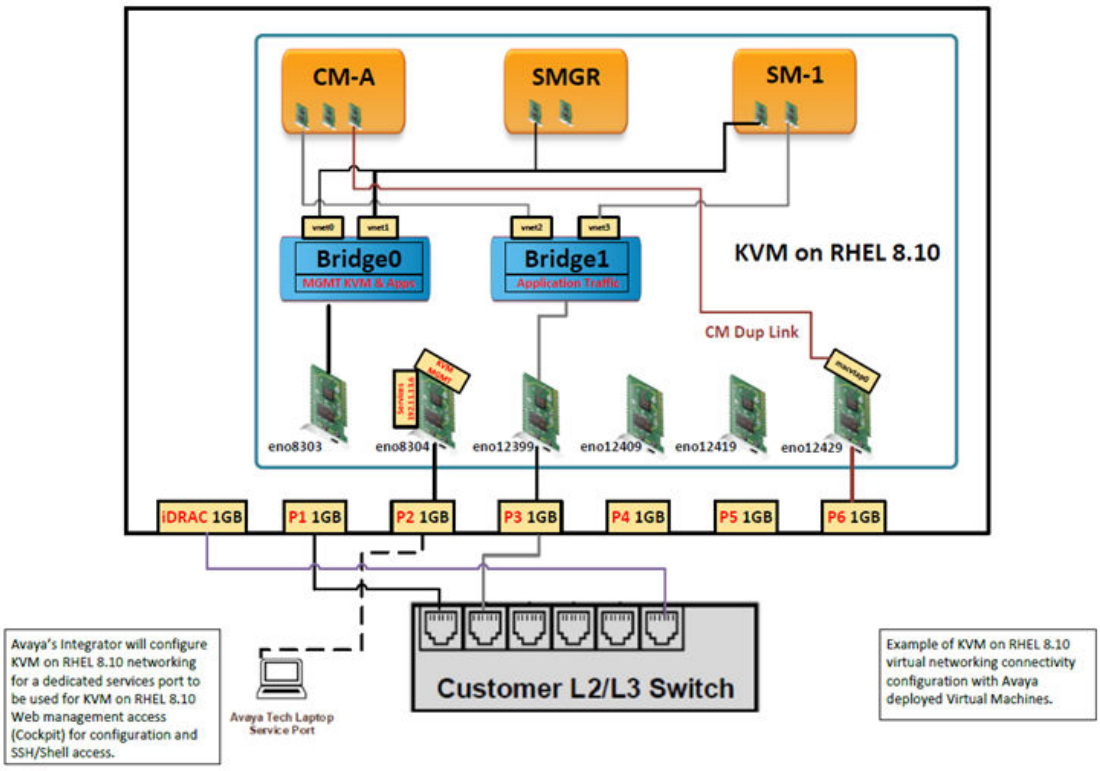
The following illustration represents a sample Application deployment with a configured Services port:

Note:

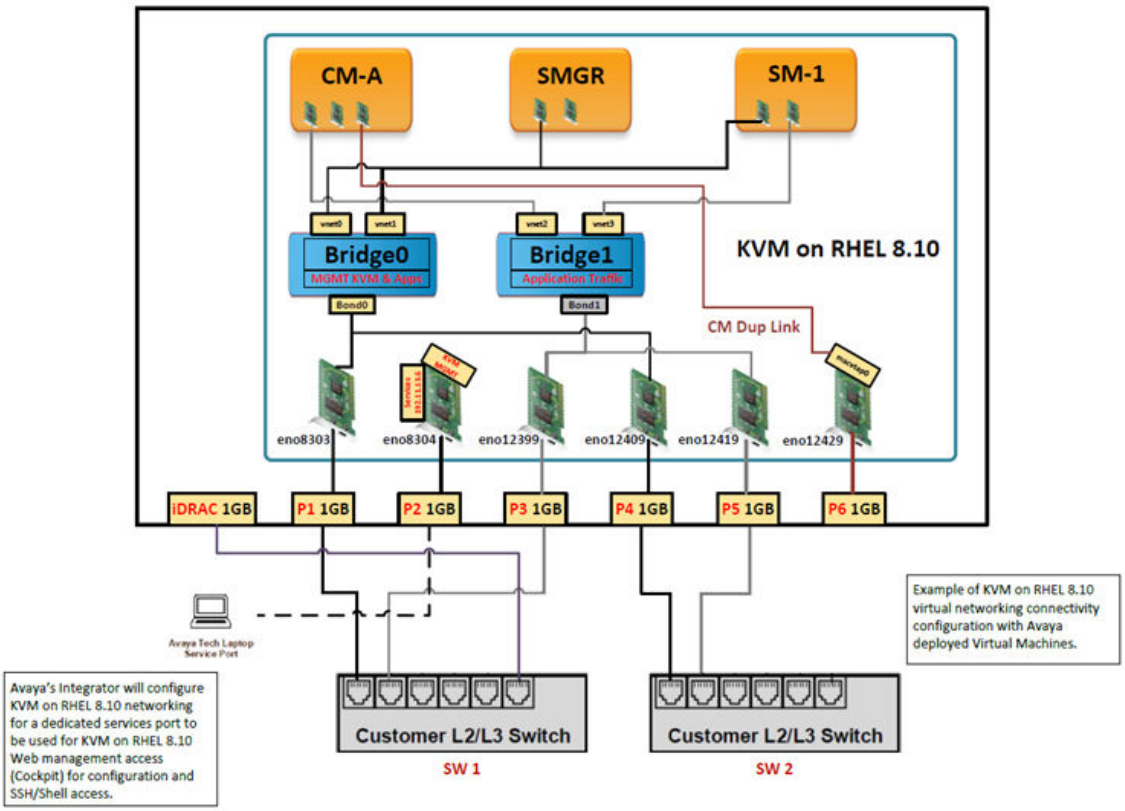
In ASP R6.0.x KVM on RHEL 8.10, the bridge “replaces” the ESXi vSwitch and Virtual Machine port group.



This diagram is for the default configuration without bonding (single wires).



This diagram is for the configuration with bonding (2 wires per bridge) which supports redundancy.


CM-A
SMGR
SM-1
Bridge0
MGMT KVM & Apps
Bridge1
Application Traffic
KVM on RHEL 8.10
Bond0
Bond1
CM Dup Link
eno8303
eno8304
eno12399
eno12409
eno12419
eno12429
iDRAC 1GB
P1 1GB
P2 1GB
P3 1GB
P4 1GB
P5 1GB
P6 1GB
Avaya Tech Laptop Service Port
Customer L2/L3 Switch
SW 1
Customer L2/L3 Switch
SW 2
Example of KVM on RHEL 8.10 virtual networking connectivity configuration with Avaya deployed Virtual Machines.
Avaya's Integrator will configure KVM on RHEL 8.10 networking for a dedicated services port to be used for KVM on RHEL 8.10 Web management access (Cockpit) for configuration and SSH/Shell access.

Chapter 8: Securing Network Configuration (OoBM)

This chapter describes secure network configuration details on Avaya Solutions Platform 130 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.

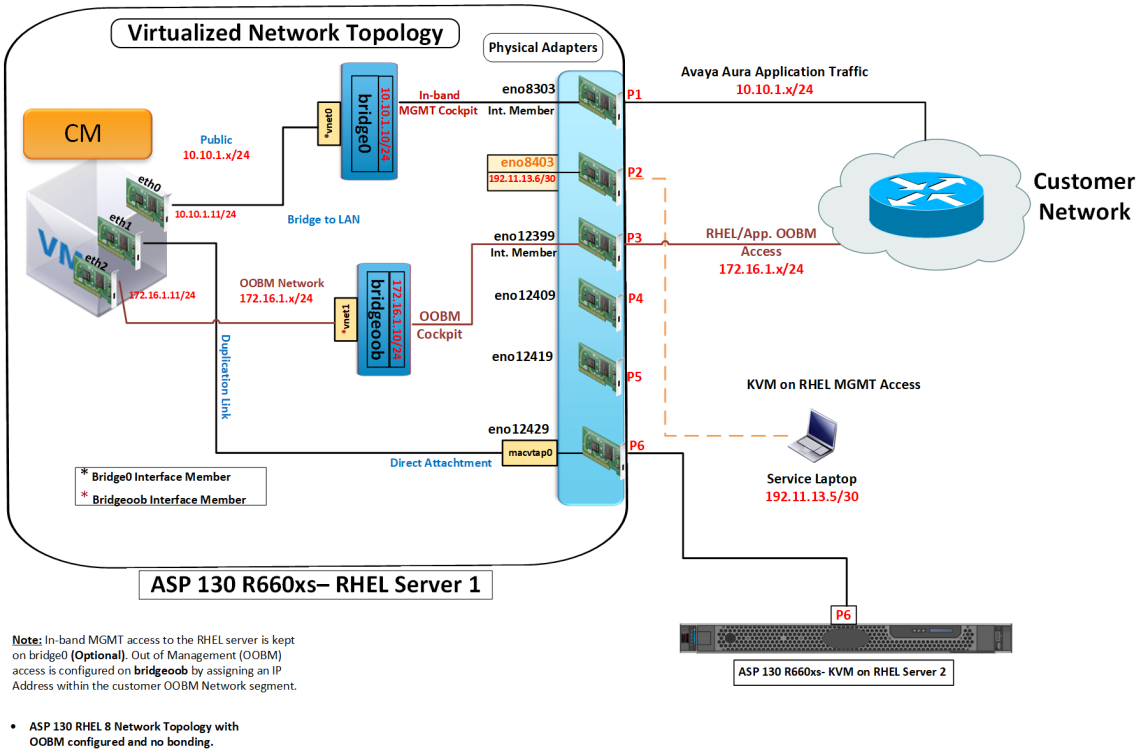
```
Connect this server to an Out of Band Management network (OOBM)? y/n
(n)n
```

```
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
```

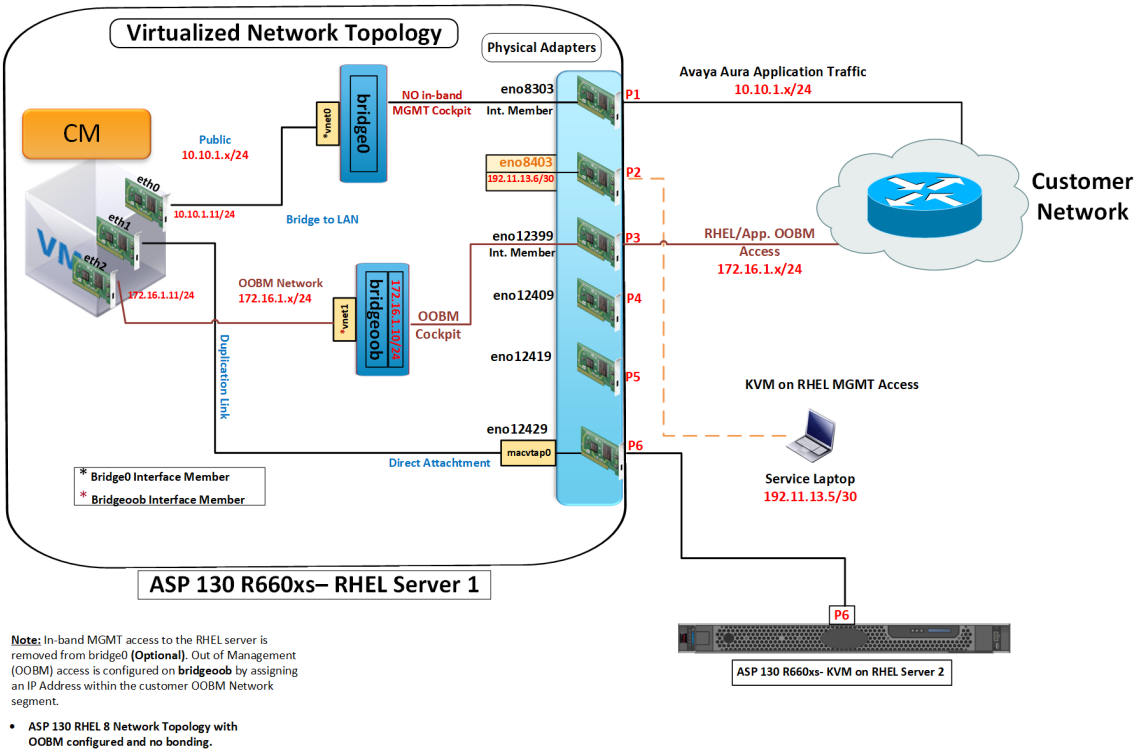


Note: In-band MGMT access to the RHEL server is kept on bridge0 **(Optional)**. Out of Management (OOBM) access is configured on **bridgeoob** by assigning an IP Address within the customer OOBM Network segment.

- **ASP 130 RHEL 8 Network Topology with OOBM configured and no bonding.**

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).



Note: In-band MGMT access to the RHEL server is removed from bridge0 **(Optional)**. Out of Management (OOBM) access is configured on **bridgeoob** by assigning an IP Address within the customer OOBM Network segment.

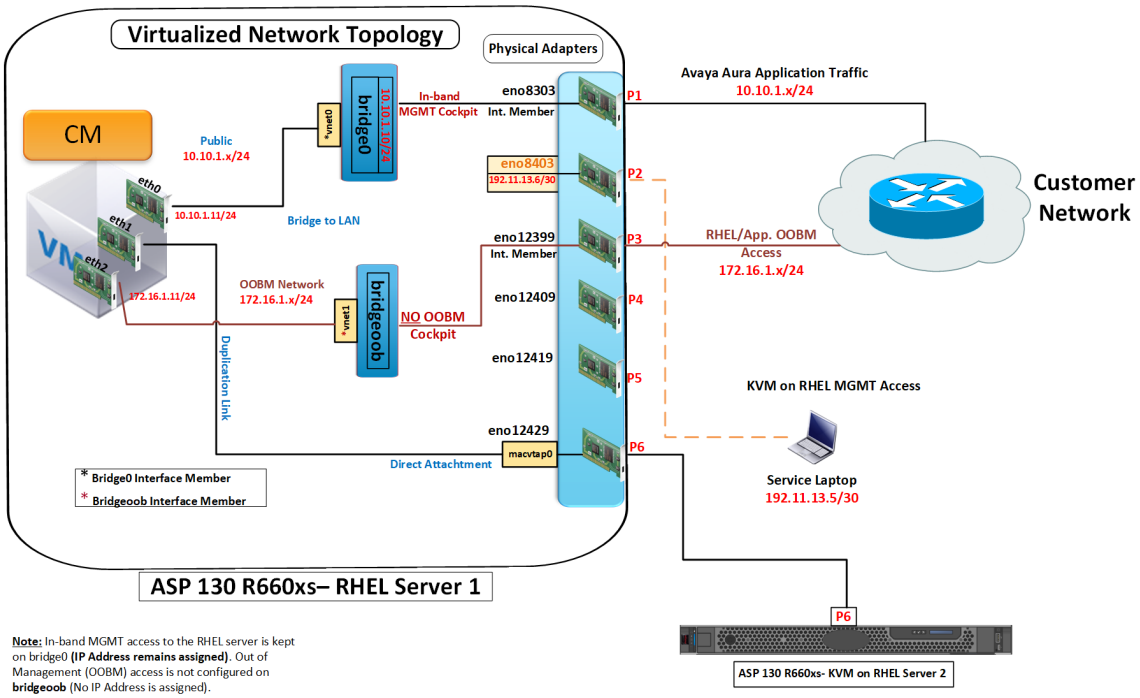
- **ASP 130 RHEL 8 Network Topology with OOBM configured and no bonding.**

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
```



Note: In-band MGMT access to the RHEL server is kept on bridge0 **(IP Address remains assigned)**. Out of Management (OOBM) access is not configured on **bridgeoob** (No IP Address is assigned).

- **ASP 130 RHEL 8 Network Topology with OOBM configured and no bonding.**

Chapter 9: Performing server recovery and/or software remastering

About this task

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.

Before you begin

Ensure that you have the following:

- Console VGA monitor.
- USB Keyboard.
- Appropriate ASP 6.0.x software downloaded from PLDS.
- Latest Avaya certified BIOS/FW update for ASP 130. For reference, search the Avaya support web site for: *Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update* or *Avaya Solutions Platform 100 Series Dell® R660xs Avaya Certified BIOS/Firmware Update* (future) and select the latest version of the PSN.

  If server is not on the latest BIOS/FW, update it before or after server recovery/software remastering.
- Obtain and review *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series*.
- Have a copy of the customer's IP and naming information for each application and the host server.
- Obtain latest application backups and application software.

Replacing the host server

About this task

In the event of a hardware failure, you will need to replace the host server on Avaya Solutions Platform 130 Appliance. Avaya is assessing the feasibility of importing Hard Disk Drives (HDDs) for a future release. Currently, importing HDDs from a failed server is not supported.

For the Dell R640: Reference *Dell R640 FRU replacement* and *RAID Configuration* chapters of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series R6.0.x* for detailed steps.

For the Dell R660xs: Reference *Dell R640 FRU replacement* and *RAID Configuration* chapters of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series R6.0.x* for detailed steps (to be provided in a future release of the document).

A high level summary of steps is provided below.

Procedure

1. For both Dell R640 and R660xs, reuse the HDDs from the failed server if feasible. These HDDs will be cleared and reused in the replacement server.
2. Follow the detailed steps for RAID configuration in *RAID Configuration* chapter of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series* R6.0.x document. Once the RAID configuration is complete, follow the steps in the *Software remastering* section below.
3. Update the BIOS/Firmware of the platform. For reference, search the Avaya Support web site for: *Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/ Firmware Update or Avaya Solutions Platform 100 Series Dell® R660xs Avaya Certified BIOS/Firmware Update* (future) and select the latest version of the PSN.
4. Enable and configure iDRAC on the replacement server. For more information, see *Avaya Converged Platform 130 Series iDRAC9 Best Practices*.

Software remastering

If it is determined that the server hardware is healthy and software needs to be reinstalled, a remaster of the server software is required. Screen shots and file names used in the following procedures are just a representation and should only be used as an example. This procedure is necessary to support migration of ASP R4.x, R5.x, AVP (ASP 120) Dell R640 servers to ASP R6.0.x after RAID has been reconfigured on the Dell R640.

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.

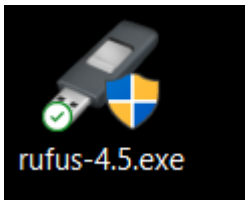
Latest releases:

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

- Download the ASP R6.0.x R640/R660xs ISO installer file (reference *PCN2173* and *ASP 6.0.x Release Notes* for the latest available downloads) from PLDS to the local Windows PC to be used for creating USB installation media.

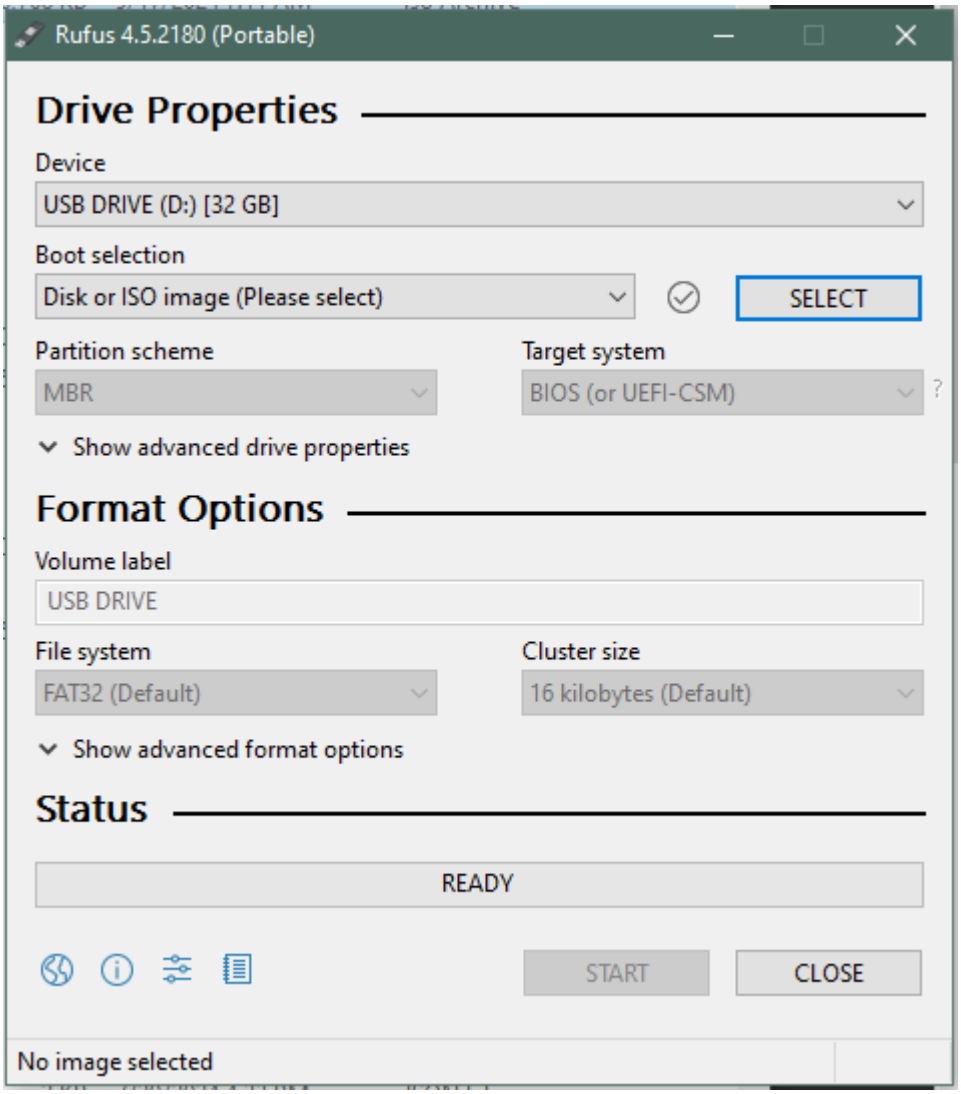
Procedure

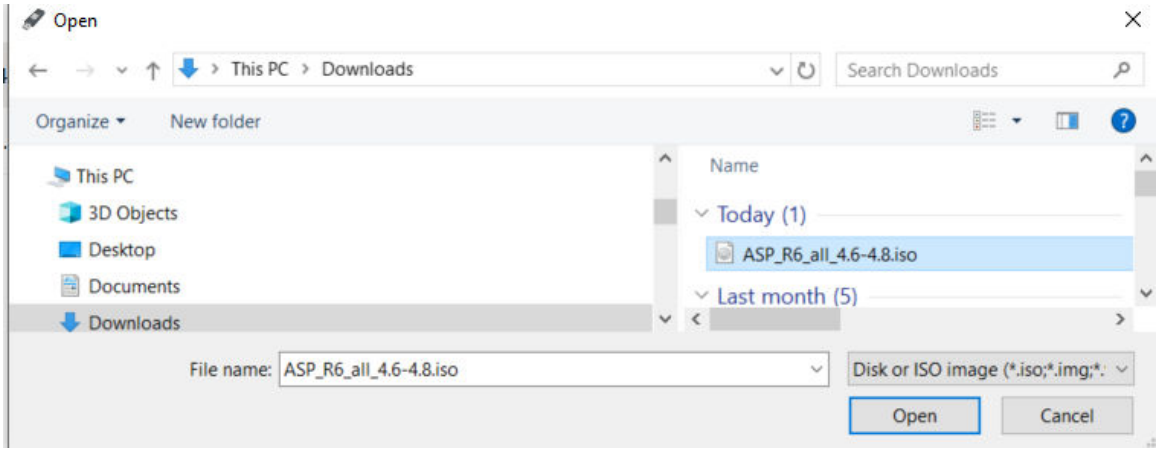
1. Insert the 4GB or larger USB flash drive into your Windows PC where the ISO installer file was downloaded.
2. Open Rufus.



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 R640/R660xs ISO installer file (reference file previously downloaded (see prerequisites above)).

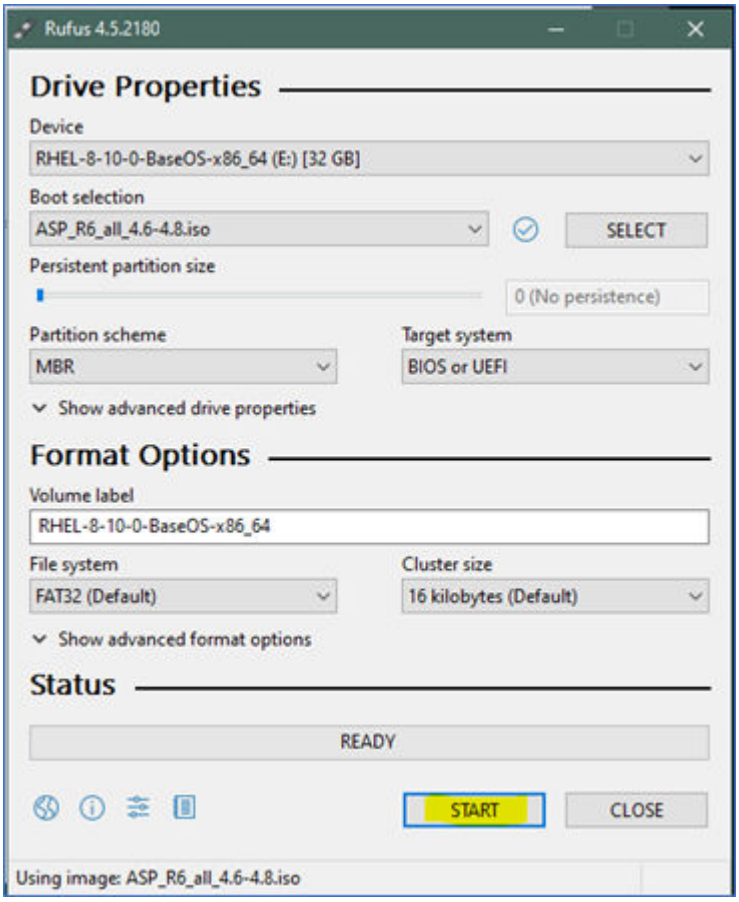
5. Select that ISO file and select **Open**.

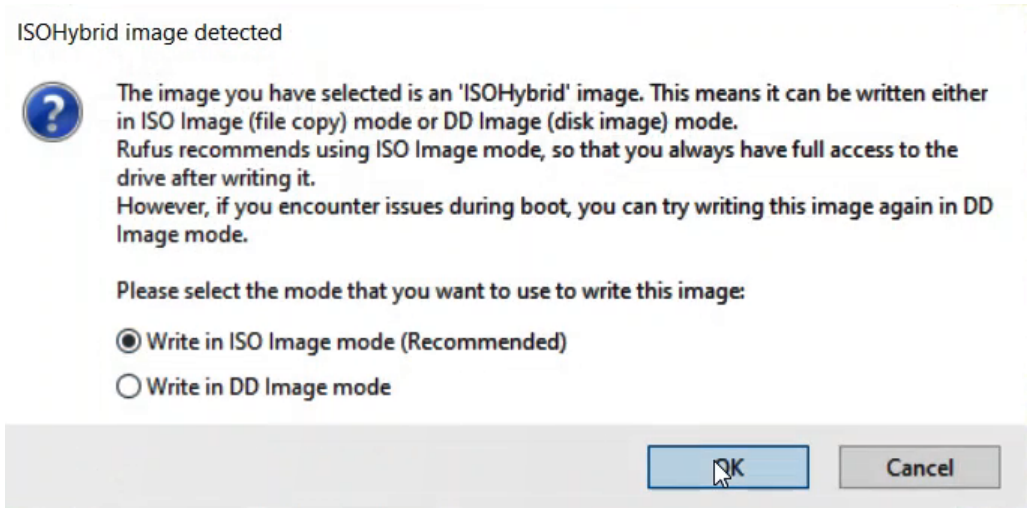


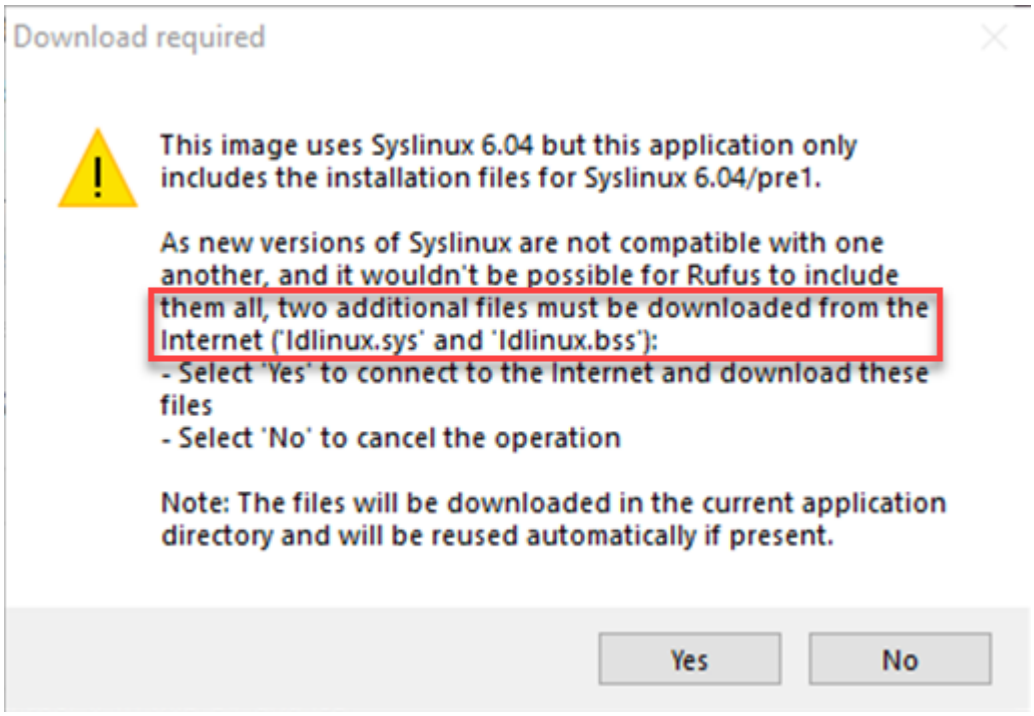


6. Rufus screen should look similar to screen shot below dependent on USB drive size. Press **START** to initiate the process. If the message box below appears after **START** selection, keep the default (Write in ISO Image mode) and press **OK**. Allow to overwrite USB jump drive if prompted.

   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.

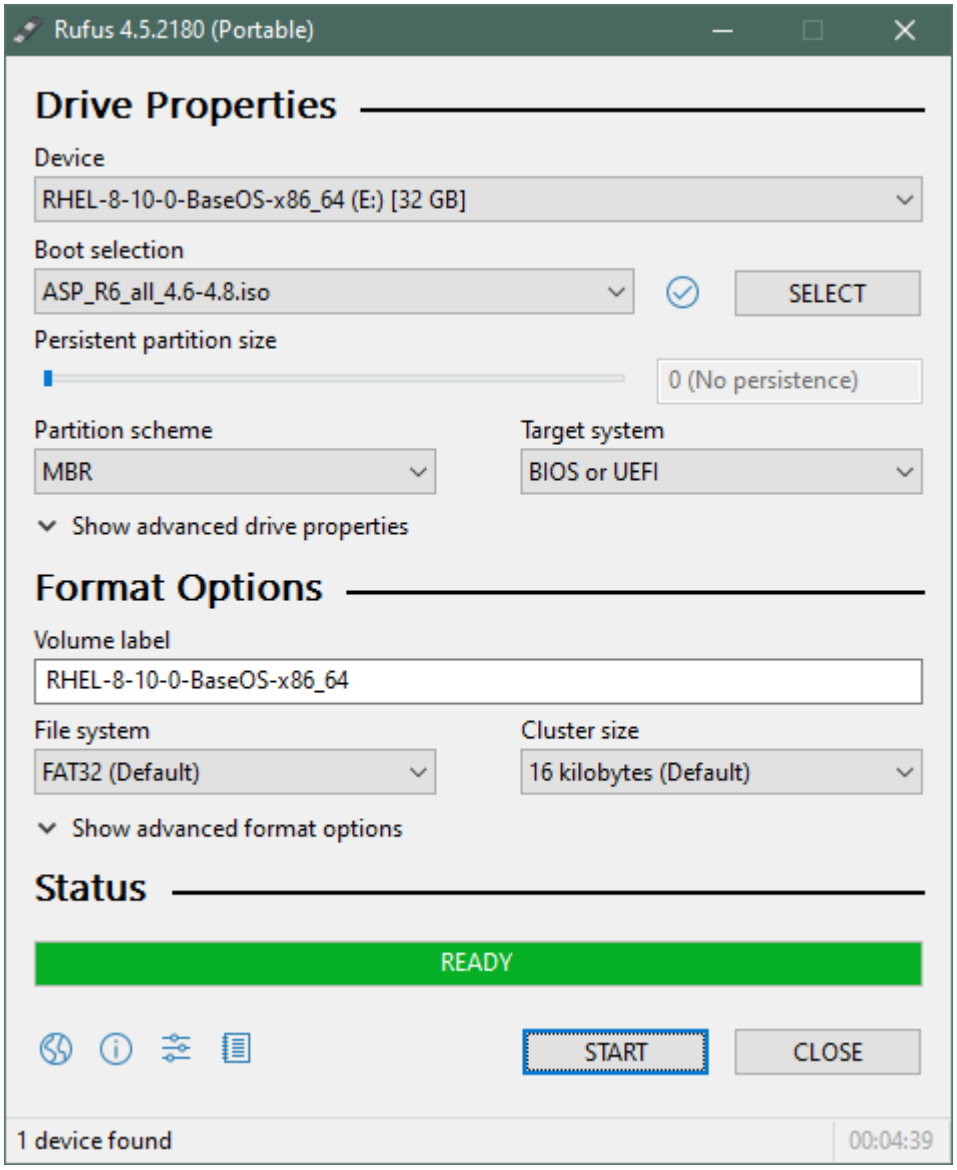






7. When the process has completed and Status shows READY, Rufus should be closed, and the Flash drive ejected from the computer. This jump drive now has the ASP R6

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



Installing the ASP R6.0.x KVM on the Dell R660xs and Dell R640

About this task

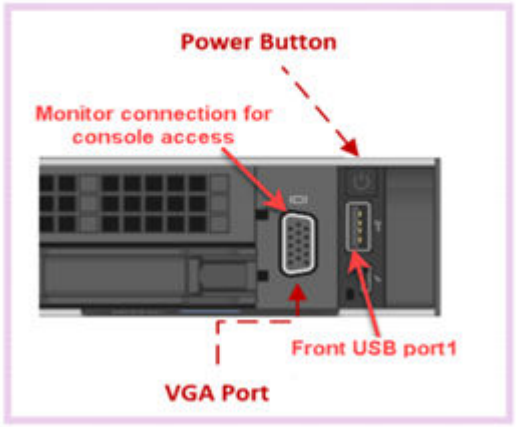
The procedure is similar for the Dell R660xs and Dell R640. The following pictures are just a representation and should only be used as an example.

Before you begin

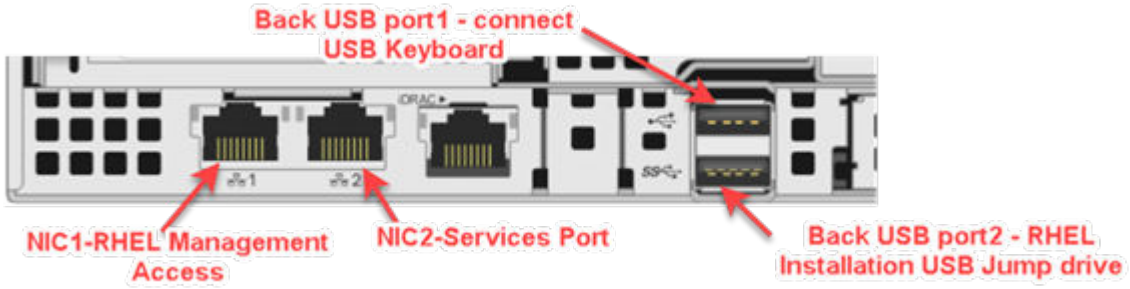
- Ensure the R660xs or R640 server's NIC 1 port is properly connected to a data switch port which provides network connectivity to Avaya's network. This access is not required during installation. It is required after the installation.
- One available routable IP address. This is the same IP address that will used later in the installation.

Procedure

1. Connect a monitor to the front VGA port of the R660xs/R640.
2. Connect a keyboard to the front USB port of the R660xs/R640.

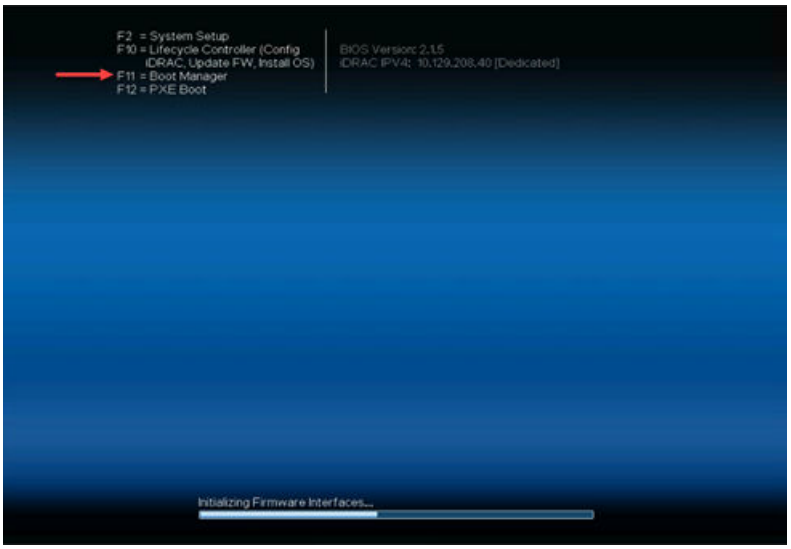


3. Insert the USB ASP R6 Software Installation Media in the back, bottom USB Port2 of the server.

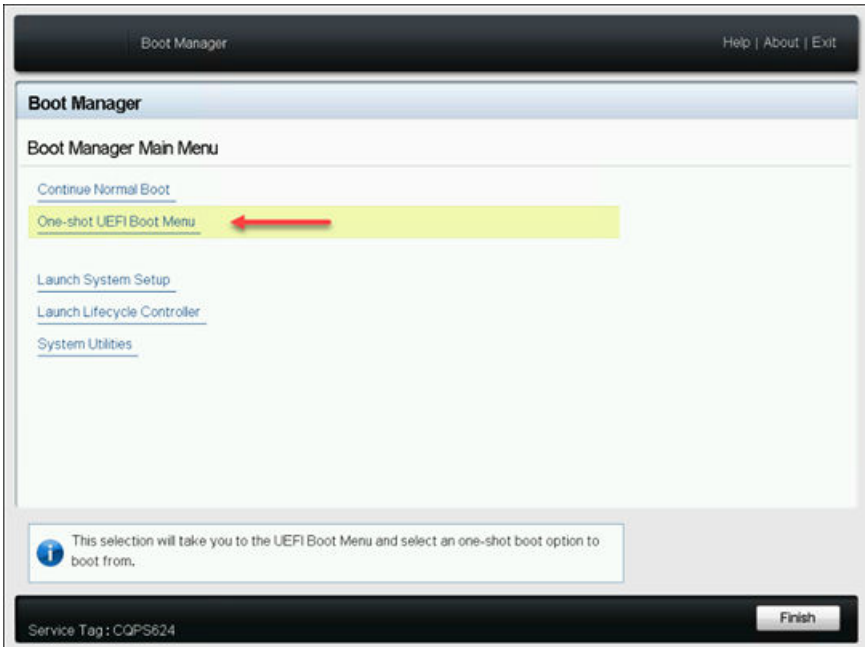


4. Power on or reboot the server.

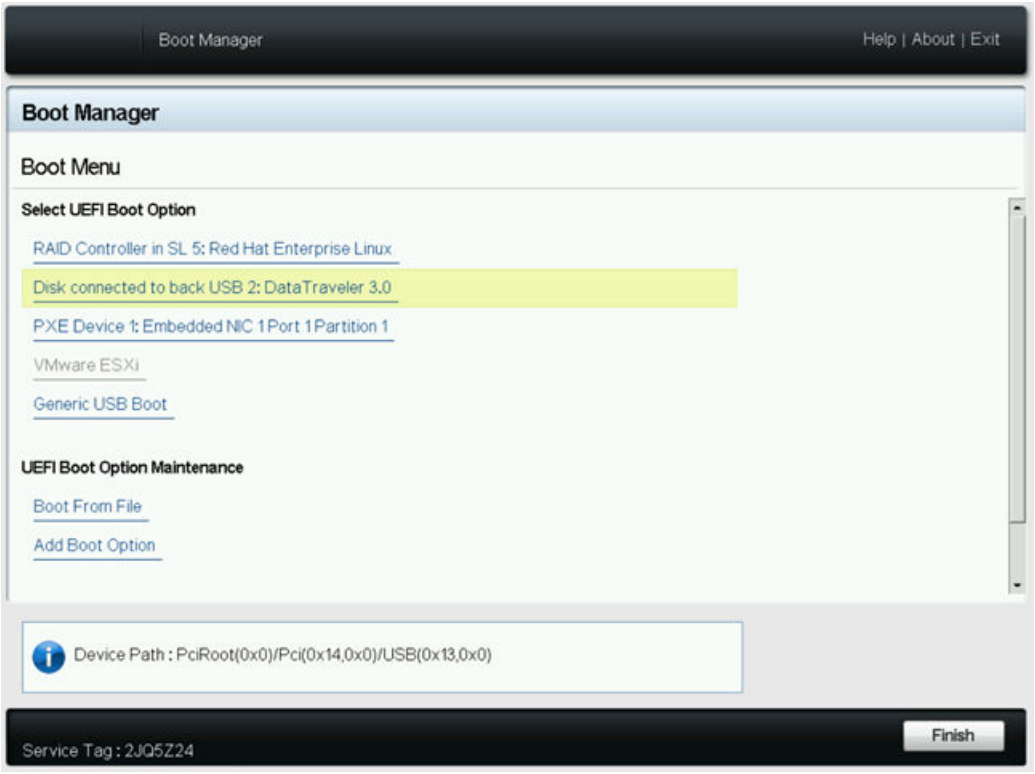
5. During server POST, press **F11** when prompted to enter the Boot Manager.



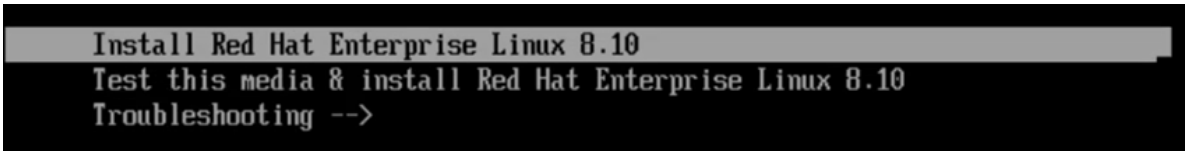
6. From keyboard, arrow down to highlight **One-shot UEFI Boot Menu** and press **Enter**.



7. From the keyboard, arrow down and highlight **Disk connected to back USB 2**: and press **Enter**. The server will now boot from the ASP R6 Dell R640 R660xs Install USB Media installed in the back USB port2 after POST completion.

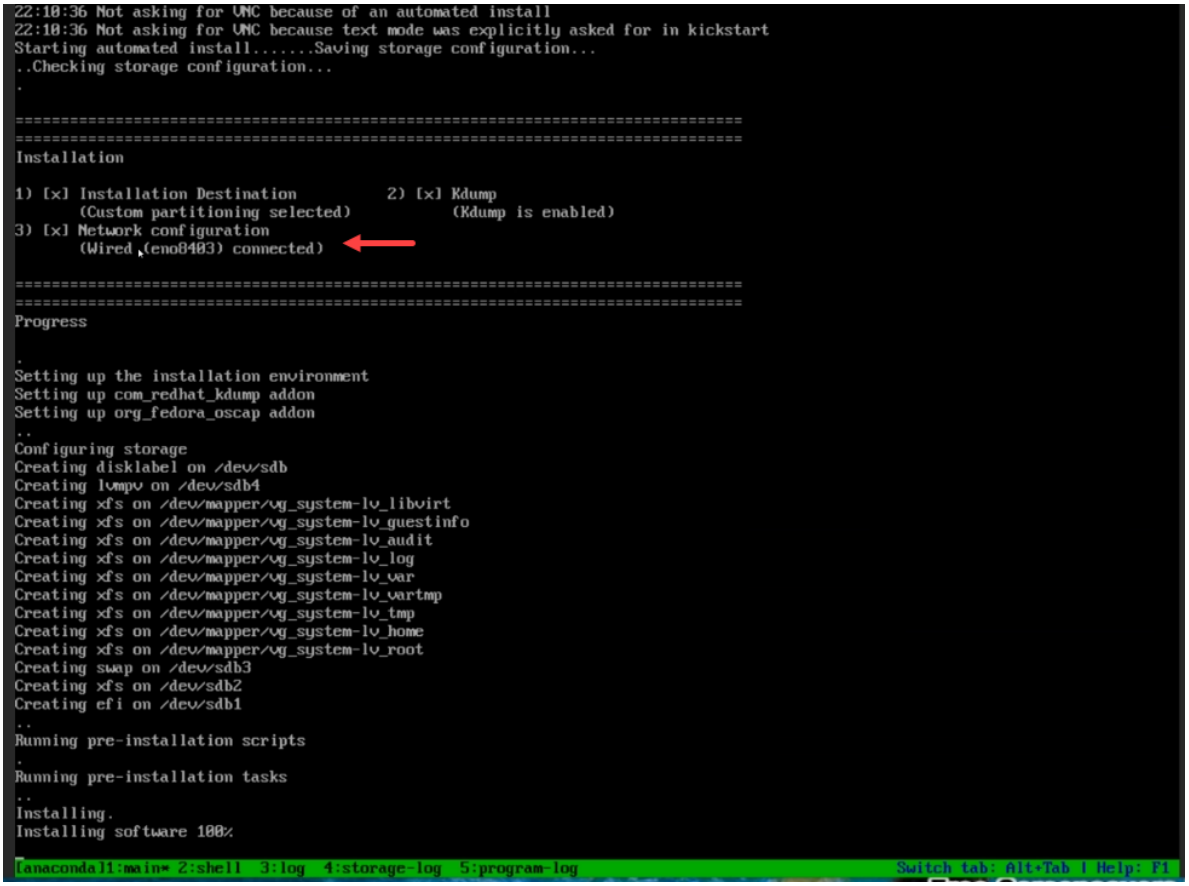


8. Server should start booting from the back USB ASP R6 Software Installation Media. When the screen below appears, you will find the entry **Install Red Hat Enterprise Linux 8.10** already highlighted. After 7 seconds, selected entry will be started automatically or you can press **Enter**. No more user interaction is required until software is installed and server reboots. Monitoring of installation progress is advised.



9. When the screen below appears, the boxes shown below (1-2) should be automatically selected with an X. **Box 3 is ALWAYS checked as part of the services port**

configuration. If the boxes (1-2) were automatically selected with an X, the system will continue to install.



10. Once software is installed, the system will reboot. When the system has first time booted, a login prompt should be displayed at the console. Do not login immediately; within a minute the server will reboot a second time for additional background configuration of the system. When the system has 2nd time booted a login prompt will be displayed at the console. Login using credentials: `custadm/ACP130_pw`.

    Caution:

    Do not attempt to login with the root account at this time.

11. Follow the steps at Configuring KVM on Red Hat Enterprise Linux 8.10 Network Settings on page 48.

Next steps

After the software is loaded on the server, do the following:

- If required, configure iDRAC.

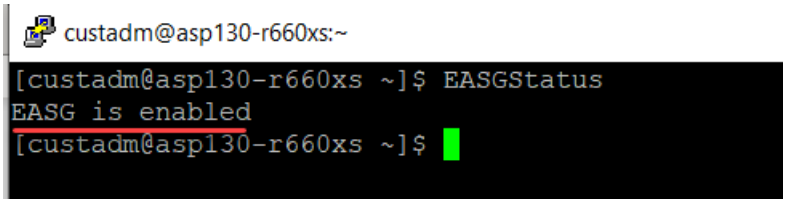
Verifying Avaya Enhanced Access Secure Gateway

About this task

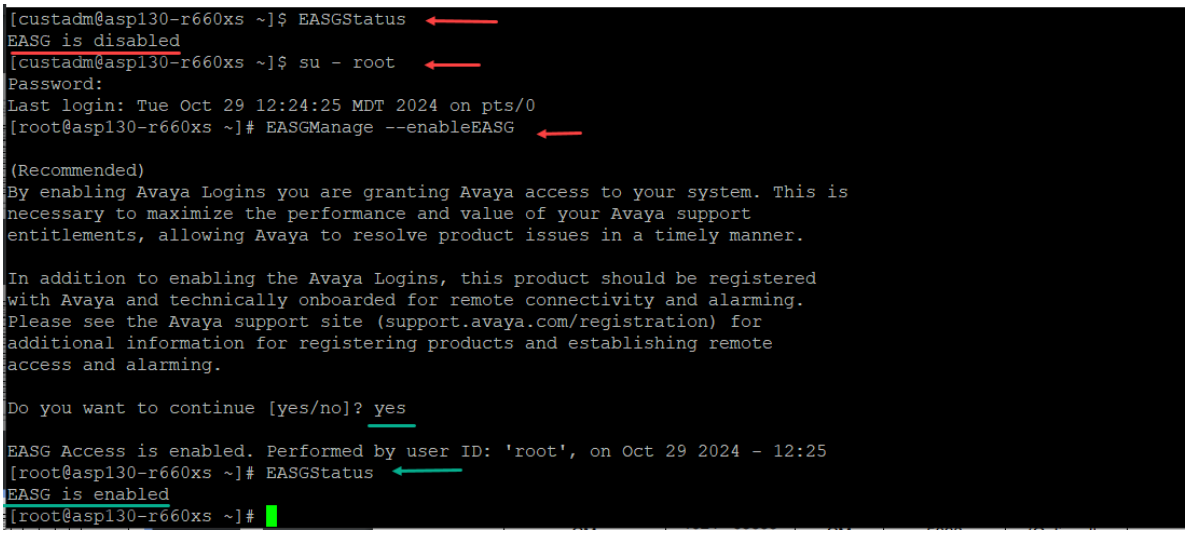
Verify Avaya Enhanced Access Secure Gateway status and enable/disable as necessary.

Procedure

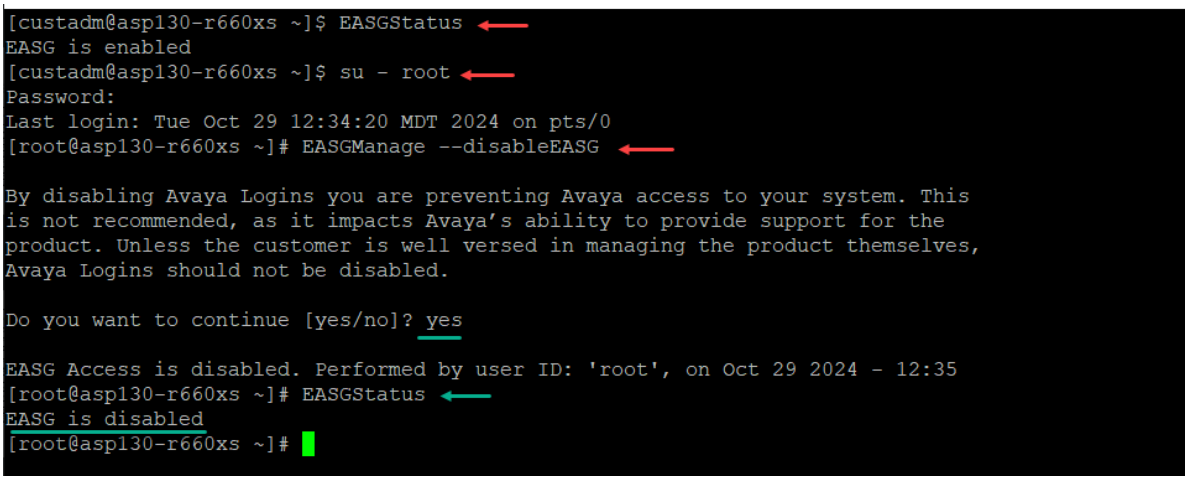
1. SSH to the desired KVM on RHEL 8.10 host with **custadm** credentials.
2. To verify current EASG status, execute: **EASGStatus**.



3. To enable EASG, su to root and execute **EASGManage --enableEASG**.



4. To disable EASG, su to root and execute **`EASGManage --disableEASG`**.



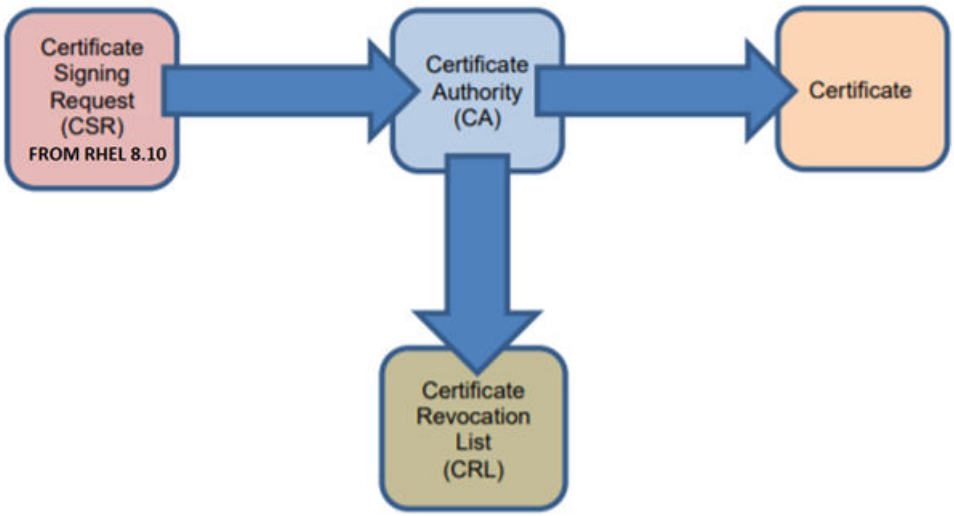
Chapter 10: Certificate Administration

Overview

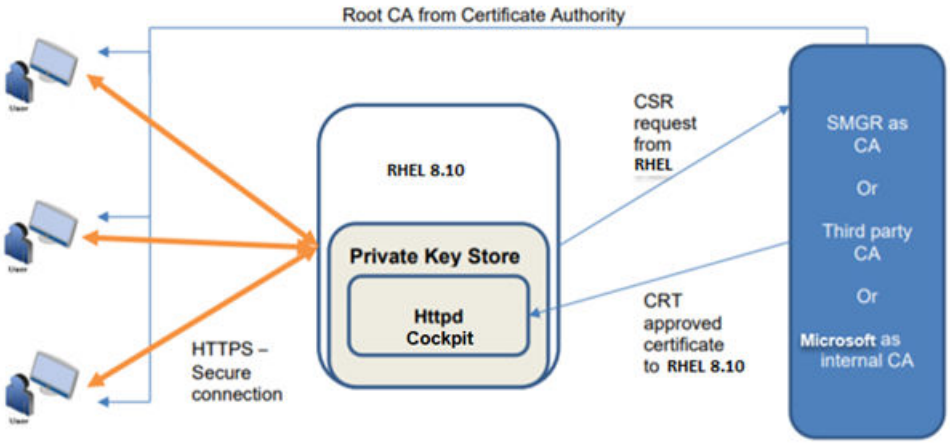
Secure Sockets Layer (SSL) with CA Signed Certificates

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:



Self-Signed Certificates: Definition and role in Transport Layer Security (TLS)

A self-signed certificate is a digital certificate that is signed by the same entity that created it, rather than by a trusted Certificate Authority (CA). In the context of TLS, this certificate is used to establish an encrypted connection between a client and a server, but it lacks validation from a trusted third-party CA.

While a self-signed certificate can encrypt traffic and ensure that the communication remains private, it does not provide any guarantee that the server is who it claims to be. Without a CA's endorsement, a self-signed certificate is not inherently trusted by clients (such as web browsers). This means that the client cannot automatically verify the identity of the server, and the client will often display warnings when encountering a self-signed certificate. Therefore, industry standards always recommend, when possible, to replace self-signed certificates with CA signed certificates.

Types of SSL certificates in KVM on RHEL 8.10

Note:

Cockpit certificates are stored under `/etc/cockpit/ws-certs.d/`

Default System Generated Self-Signed Certificates

When KVM on RHEL 8.10 gets deployed a system generated self-signed certificate for Cockpit (RHEL Web UI) gets created. Certificate information has a fixed system default configuration: `asp130-r660xs`, `localhost`, `127.0.0.1`.

System generated self-signed certificates auto-renew and have a default (configurable) expiry of 395 days. These also auto-regenerate by the system if removed by the user.

Example:

```
[custadm@asp130-r660xs ws-certs.d]$ sudo ls -lrt /etc/cockpit/ws-certs.d/
[sudo] password for custadm:
total 12
-rw-------. 1 root root 1704 Dec 18 07:09 0-self-signed.key
-rw-r--r--. 1 root root 1769 Dec 18 07:09 0-self-signed.cert
-rw-r--r--. 1 root root 2204 Dec 18 07:09 0-self-signed-ca.pem
[custadm@asp130-r660xs ws-certs.d]$
```

User Generated Self-Signed Certificates

A new, user generated self-signed certificate can be generated on demand to replace the default Cockpit SSL certificate with the proper server information during or after server implementation.

User generated SSL certificates can be created with a much longer expiry of a year e.g. 10 years, however best security practices recommend a 1-year expiry. User must renew and keep up with "user generated SSL certificates".

Custom CA signed Certificates

Secure, strongly recommended. Aligns with industry security best practices. Can be created on demand by user.

SSL Certificates can be created with a much longer expiry than a year e.g., 10 years, however, best security practices recommend a 1-year expiry. Users must renew and keep up with custom certificates. Including certificate revocation.

Organizational CA can be used such us Microsoft Windows Server or Avaya Aura® System Manager to sign and generate certificates.

Creating SSL self-signed certificates in KVM on RHEL 8.10

Validating SSL certificate expiry

About this task

During the installation of KVM on RHEL 8.10, the system generates a self-signed certificate that contains `localhost|asp130-r660xs` as the common name. After you configure the hostname in the system, a mismatch between the hostname and the common name in the certificate occurs.

Subject Alt Names

DNS Name	asp130-r660xs
DNS Name	localhost
IP Address	127.0.0.1

This procedure can also be used when a user generated self-signed SSL certificate installed in Cockpit is about to or has already expired.

Note:

This activity can be conducted 100% remotely and it is a NOT 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 windows during off business hours when possible or low traffic hours.

Caution:

Avoid making configuration changes to the host when conducting this procedure.

Before you begin

- Access to the ASP 130 R640/R660xs server management network either thru a SAL Gateway connection (remotely) or direct service port connection (onsite).
- SSH tool i.e. Putty (not provided by Avaya).
- custadm password.

Procedure

1. Log in to the first KVM on RHEL 8.10 host by using a Secure Shell (SSH) client i.e. Putty (not provided by Avaya).
2. Authenticate using the existing custadm credentials.
3. Run the following commands to validate current SSL certificate expiry:

```
cd /etc/cockpit/ws-certs.d/
ls -lrt
openssl x509 -in <*selfsigned.cert*> -noout -text | grep "Not After"
```

Note:

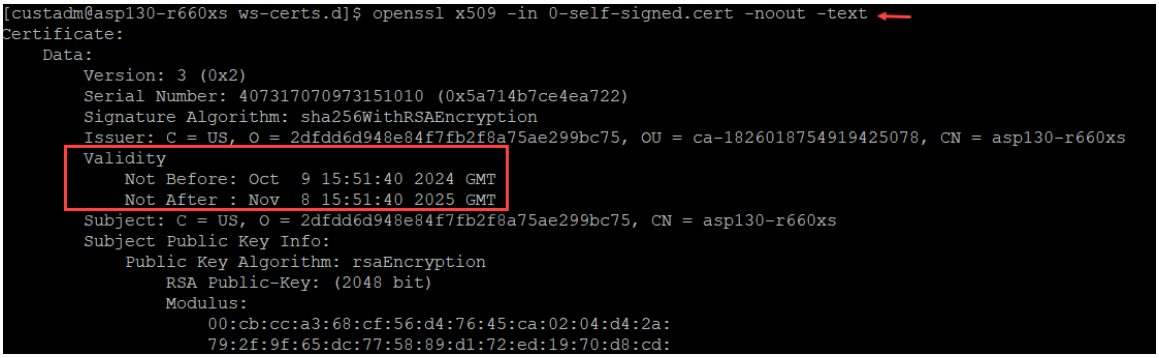
The `0-self-signed.cert` certificate, is the default, system auto-generated certificate that gets installed during the KVM on RHEL installation. The same command can be executed for other certificates (if present) if the default one has been re-generated.

Example:

```
openssl x509 -in 0-self-signed.cert -noout -text | grep "Not After"
```

Or to see full certificate chain:

```
openssl x509 -in 0-self-signed.cert -noout -text
```



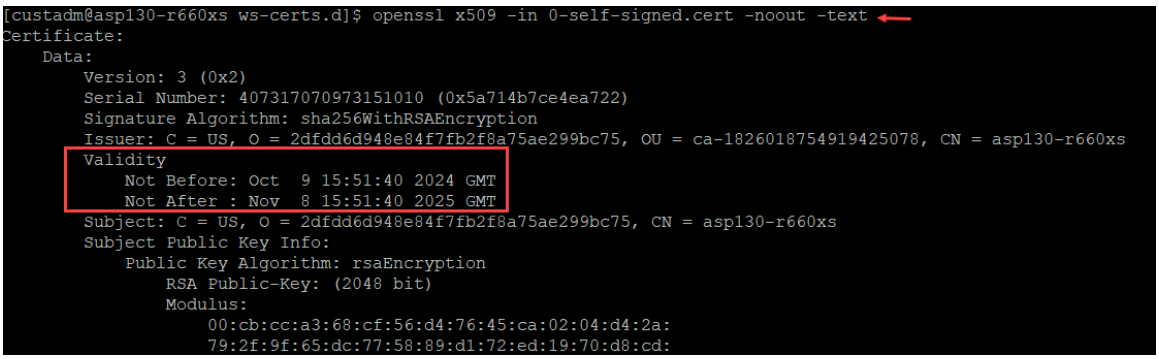
4. If the “Not After” date displayed is older than the current KVM on RHEL 8.10 host date, proceed with re-generating the SSL Self-signed Certificate.

   Output example:

```
Machine Date:
Thu Jul 22 13:07:12 UTC 2024
Validity
            Not Before: Jul 19 13:40:14 2023 GMT
            Not After : Jul 19 13:40:14 2024 GMT
```

   Or to see full certificate chain:

```
openssl x509 -in 0-self-signed.cert -noout -text
```



5. If the “Not After” date displayed is older than the current KVM on RHEL 8.10 host date, proceed with re-generating the SSL Self-signed Certificate.

   Output example:

```
Machine Date:
Thu Jul 22 13:07:12 UTC 2024
Validity
            Not Before: Jul 19 13:40:14 2023 GMT
            Not After : Jul 19 13:40:14 2024 GMT
```

Regenerating system SSL self-signed certificates

About this task

This procedure is only required if the IP address or FQDN/Hostname in KVM on RHEL 8.10 has been changed or modified. System SSL self-signed certificates auto-renew and have a default expiry of 390 days.

Note:

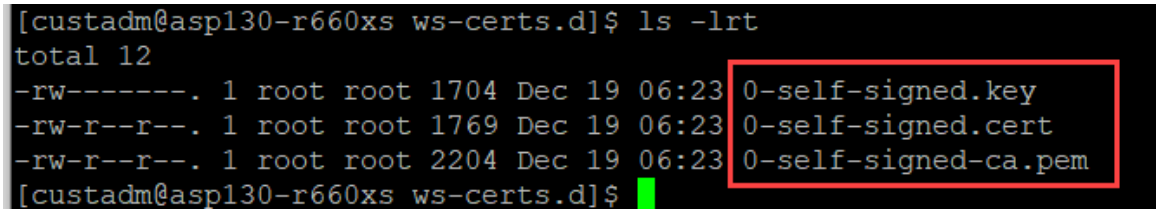
Custom CA signed SSL certificates or user generated SSL certificates take precedence over system generated SSL certificates. If either of these certificates have been previously implemented on the system, regenerating system default certificates is not required. Instead proceed to the User generated or Custom CA certificates section.

Procedure

1. Log in to the first KVM on RHEL 8.10 host by using a Secure Shell (SSH) client i.e. Putty (not provided by Avaya).
2. Authenticate using the existing custadm credentials.
3. Execute the following commands:

```
cd /etc/cockpit/ws-certs.d/
ls -lrt
####Ensure there are only system generated certificates otherwise STOP####
```

Example:

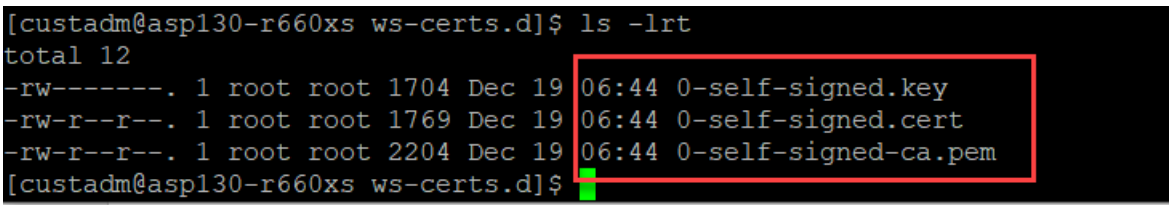



```
sudo rm 0-* -f
######[Enter password for custadm] #####
sudo systemctl daemon-reload
sudo systemctl restart cockpit
ls -lrt
```

Example:

Note:

3 new files starting with ‘0-self-signed’ will get auto-generated. Files should have current system date.



Creating a user generated SSL Self-signed Certificate

Procedure

1. Log in to the first KVM on RHEL 8.10 host by using a Secure Shell (SSH) client i.e. Putty (not provided by Avaya).
2. Authenticate using the existing custadm credentials.

3. Run the following command to re-generate the self-signed certificate on the connected host:

```
cd /etc/cockpit/ws-certs.d/
sudo openssl req -x509 -nodes -days <#days> -newkey rsa:2048 -keyout
/etc/cockpit/ws-certs.d/<cockpit-file>.key -out /etc/cockpit/ws-certs.d/<cockpit-
file>.cert
```

Note:

In the following example the value associated with days is set to 730 days (2 years), default certificate has a validity of 365 days (1 year). Update value accordingly to align with customer company security policies and best practices.

Note:

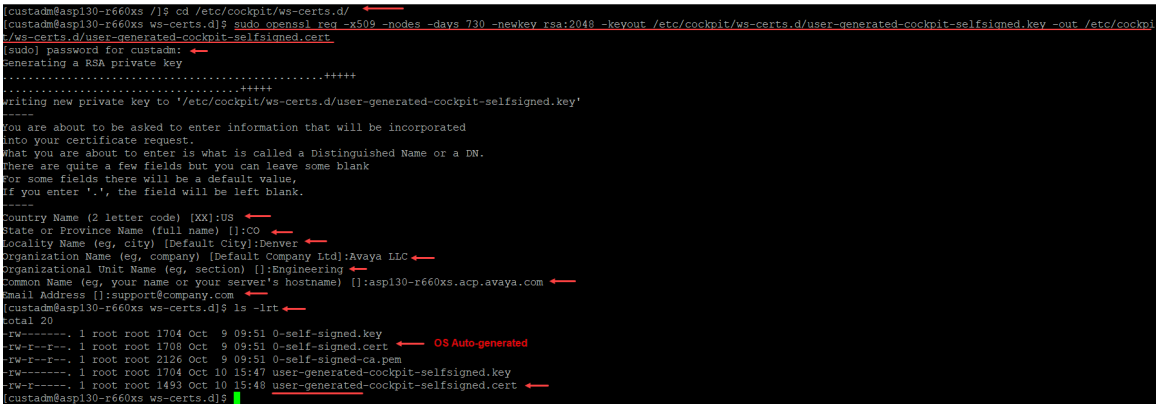
The encryption Key file and Certificate file name must be the same. Labels used in this example are just for representation purposes only. Change as needed to align with customer requirements.

Example:

```
sudo openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout
/etc/cockpit/ws-certs.d/user-generated-cockpit-selfsigned.key -out
/etc/cockpit/ws-certs.d/user-generated-cockpit-selfsigned.cert
Enter custadm password
```

System will ask to the end user to enter information that will be incorporated into the certificate request, use below information as an example, update values accordingly to match customer site information:

```
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CO
Locality Name (eg, city) [Default City]:Denver
Organization Name (eg, company) [Default Company Ltd]:Avaya LLC
Organizational Unit Name (eg, section) []:Engineering
Common Name (your server's FQDN) []:asp130-r660xs.acp.avaya.com
Email Address []:support@company.com #### Press Enter###
ls -lrt
```



4. Run the following command to restart the Cockpit Service in the KVM on RHEL 8.10 host:

```
sudo systemctl daemon-reload
Enter custadm password
sudo systemctl restart cockpit
```

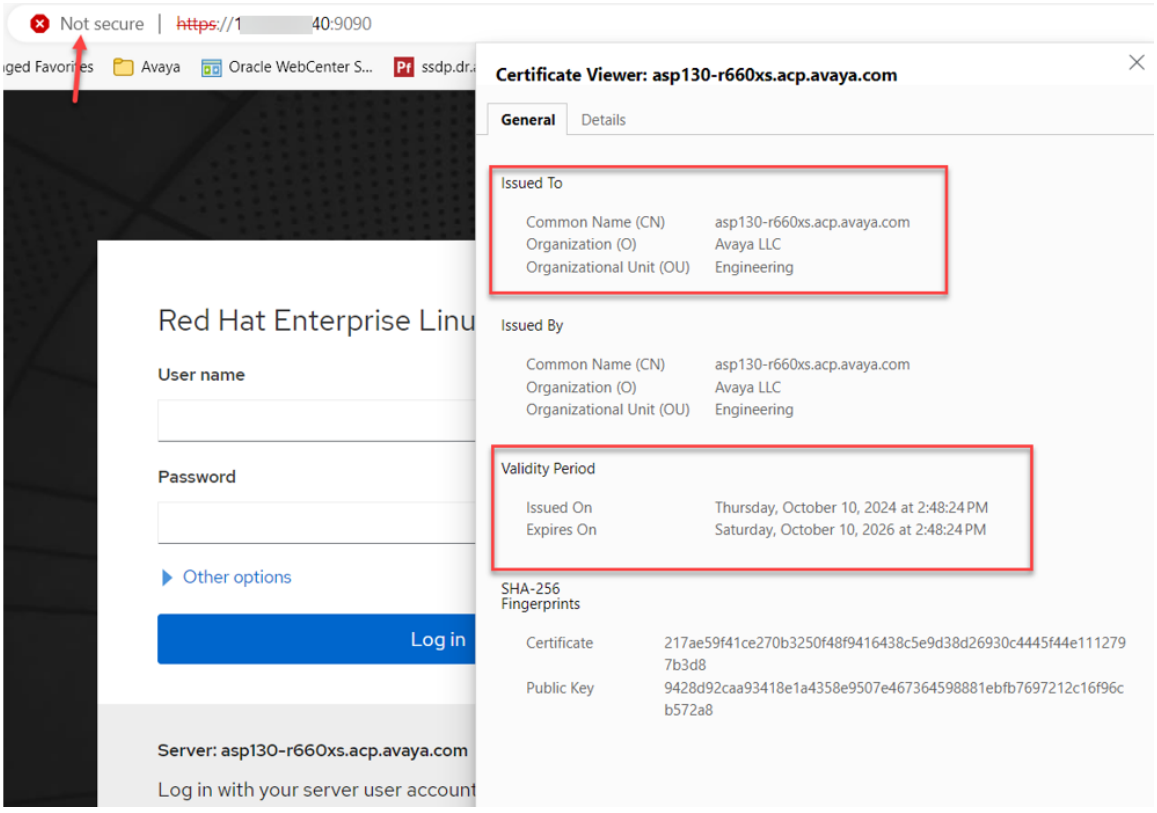
5. Before attempting to re-login to the KVM on RHEL 8.10 web user interface (Cockpit) to validate the new SSL certificate installed, clear browser history, cache, and cookies from all previously used browsers.

Note:

Reference to each browser documentation if needed when doing so.

Note:

Browsers will continue to report the connection to cockpit as not secure, even if the regenerated self-sign certificate gets installed on the client PC. This is because nowadays browsers consider self-signed certificates as insecure, same as with industry standard security scans. Avaya strongly recommends customers to replace SSL self-signed certificates with CA signed certificates.



Next steps

Repeat the entire process in all remaining ASP 130 R640/R660xs servers.

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:

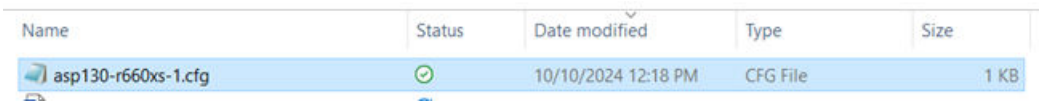
```
[ req ]

days = 365

default_md = sha512

default_bits = 2048

default_keyfile = asp130-r660xs.acp.avaya.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:asp130-r660xs.acp.avaya.com, DNS:asp130-r660xs, IP:192.168.200.57

[ req_distinguished_name ]

countryName = US

stateOrProvinceName = CO

localityName = Denver
```

```

0.organizationName = Avaya LLC

organizationalUnitName = ASP-Engineering

commonName = asp130-r660xs.acp.avaya.com

emailAddress = support@company.com

[ alt_names ]

DNS.1 = asp130-r660xs.acp.avaya.com

DNS.2 = asp130-r660xs

IP.1 = 192.168.200.57

```

3. Save the configuration file with a file extension of `cfg`. For example: `asp130-R660xs-1.cfg`.

Note:

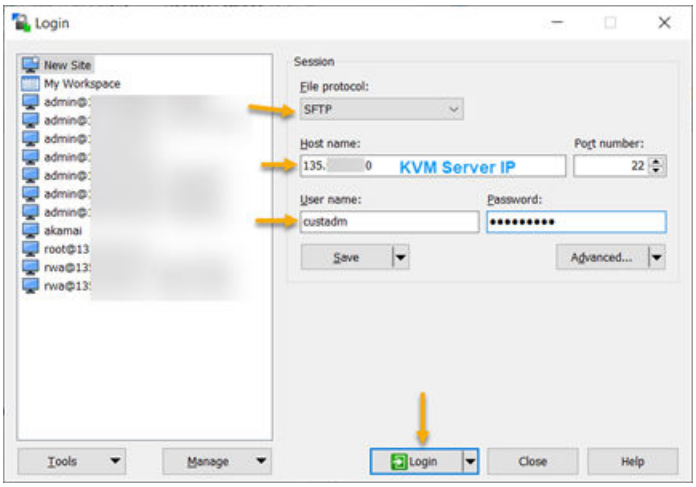
Depending on the used text editor, the configuration file may have to be saved as a text file first, therefore this will be saved with a `.txt` extension. The newly saved configuration file can then be “renamed” along with changing the extension from `.txt` to `.cfg`



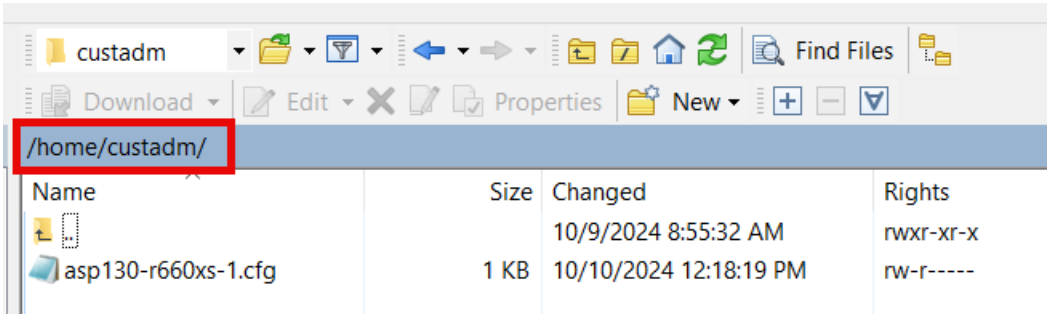
Note:

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.

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



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



6. 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 116 must be completed before continuing with the following procedure.

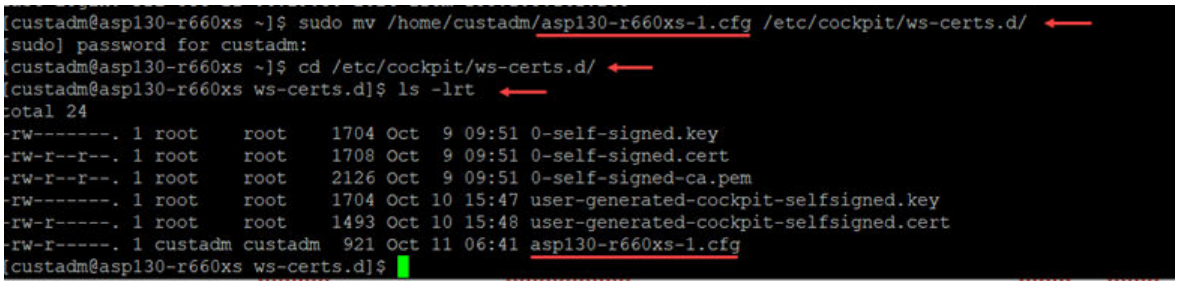
Procedure

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)



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.

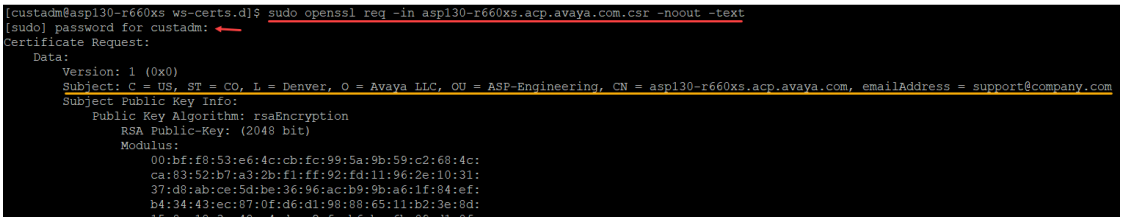
Note:

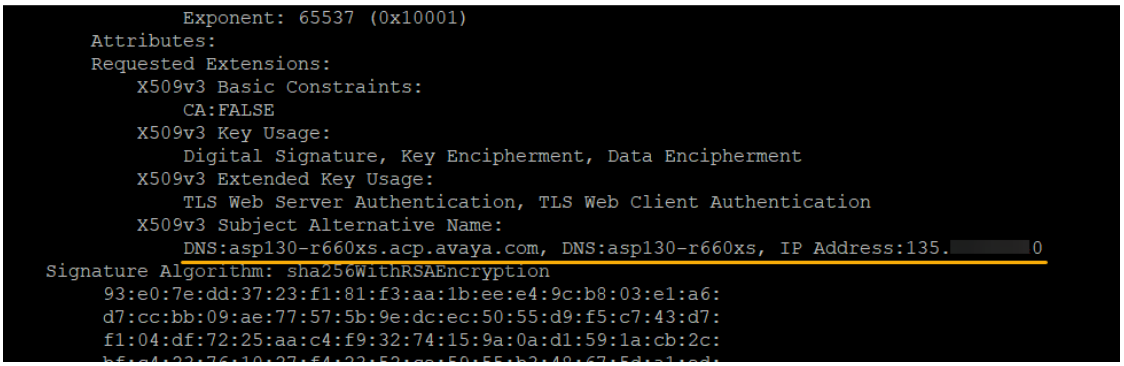
The following figure shows an out example using the configuration file previously created and transferred during Creating the Certificate configuration file for KVM on RHEL 8.10 host on page 116 `asp130-r660xs-1.cfg`. Contemplate that configuration files will change per each KVM on RHEL 8.10 host when generating the certificate signing request (CSR).

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).





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`

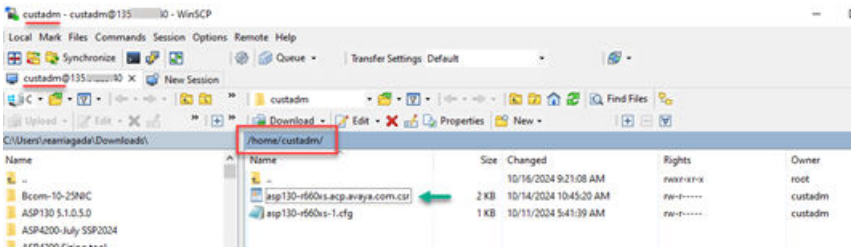
Example:

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

3. 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 120.

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 127.

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 116 and Generating the Certificate signing Request in KVM on RHEL 8.10 on page 120 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 116.

   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 116.

   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 116.

   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 116.

   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 116.

   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 116.

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 116.

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 116.

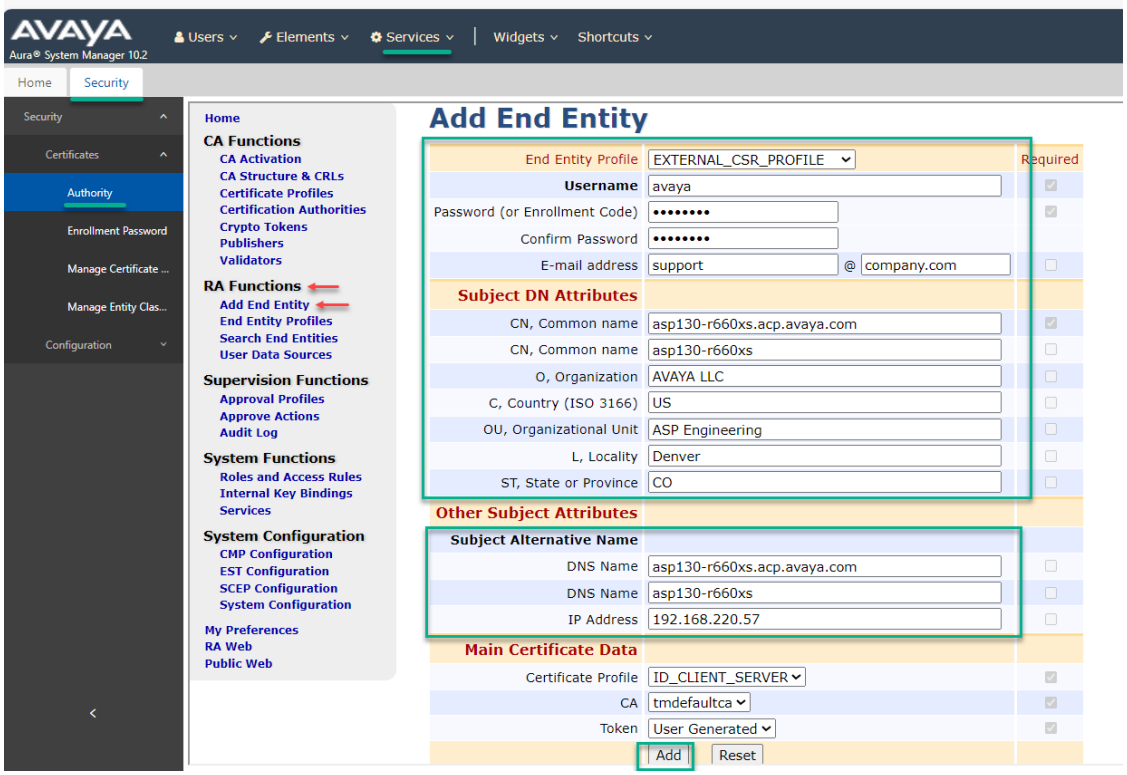
b. **DNS Name:** Enter the DNS.2 value set in the `asp130-r660xs-1.cfg` (for example) configuration file during Creating the Certificate configuration file for KVM on RHEL 8.10 host on page 116.

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 116.

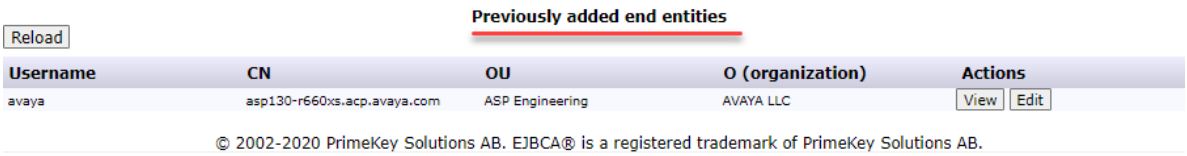
6. Review and save:

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 116 `asp130-r660xs-1.cfg`.

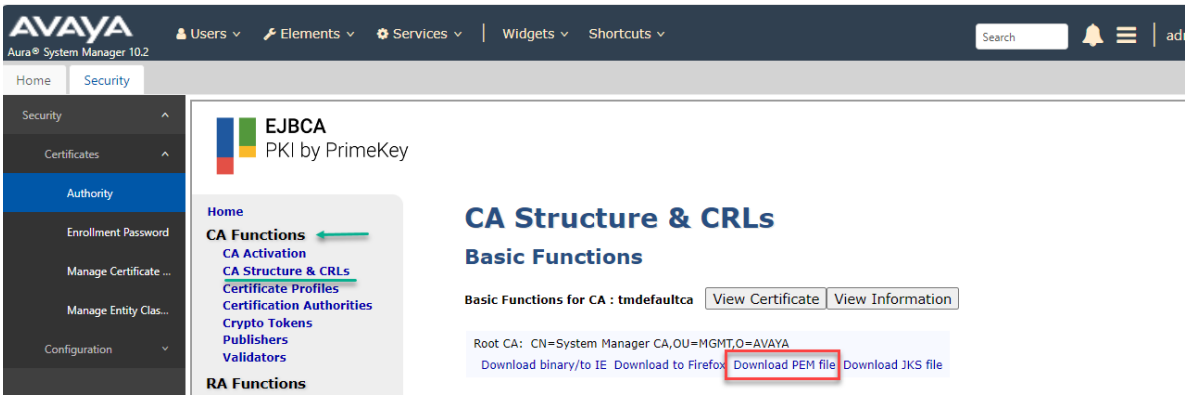
b. When ready, click the **Add** button to save the changes and create the new Entity.



New entity will be displayed.

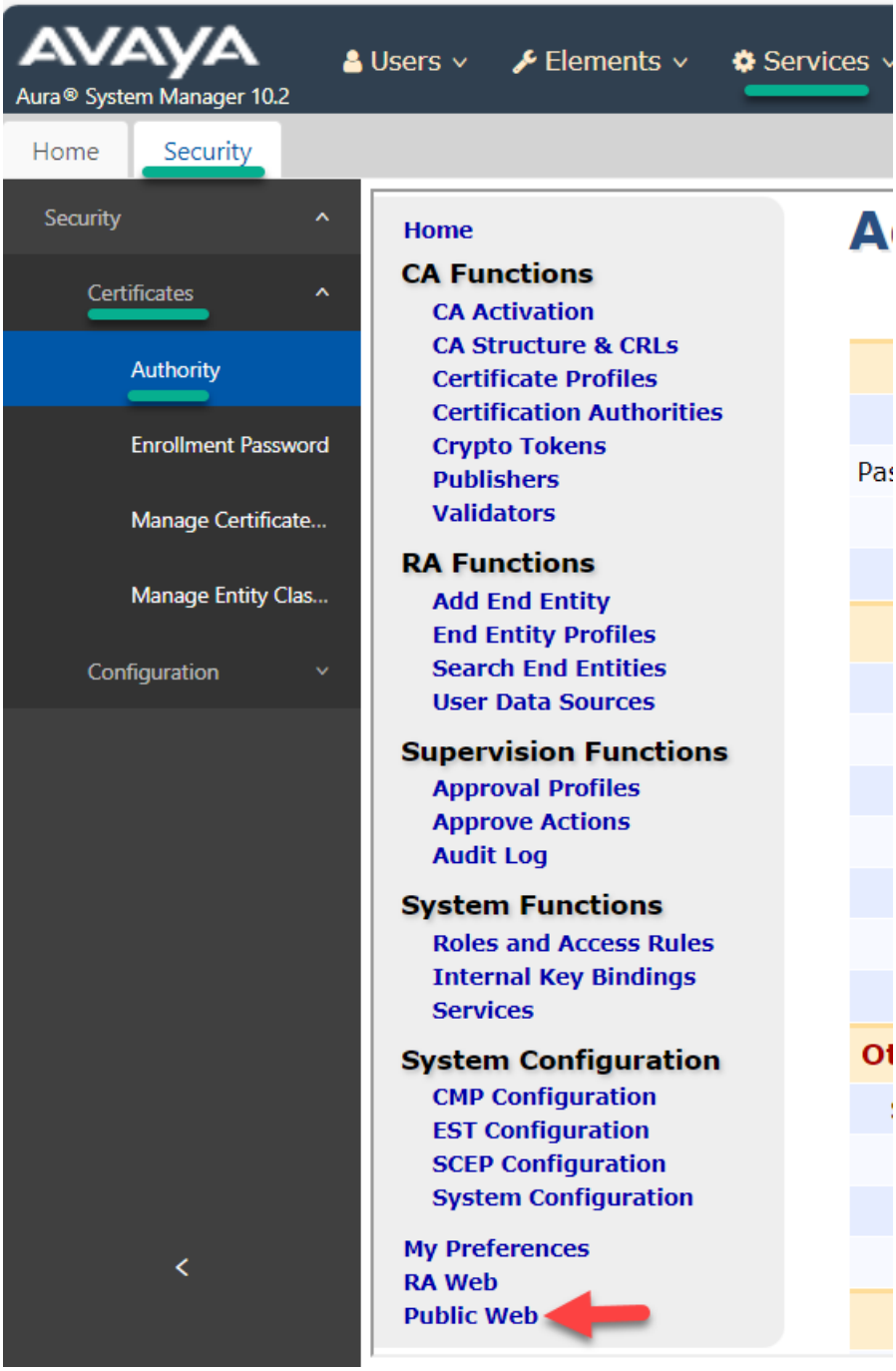


7. From the middle column menu, under **CA Functions**, select **CA Structure & CRLs**.
8. Click on **Download PEM file**.



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`

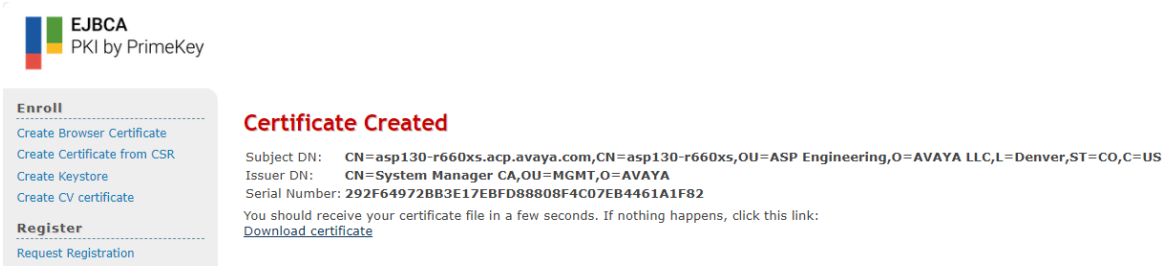
c. **Request file:** Select **Choose File** to import the CSR file created during Generating the Certificate signing Request in KVM on RHEL 8.10 on page 120 e.g. `asp130-r660xs.acp.avaya.com.csr`

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.

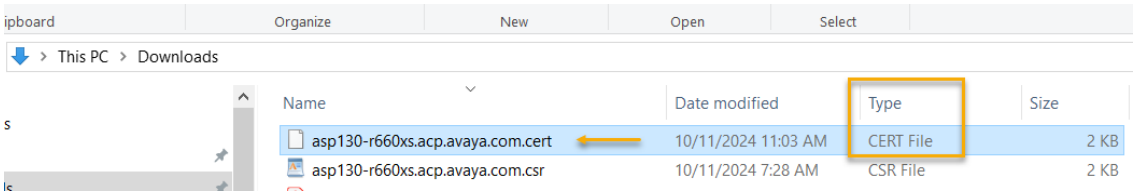


13. Navigate to the location where the certificate is downloaded.

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 116, Generating the Certificate signing Request in KVM on RHEL 8.10 on page 120, and Signing the Certificate Signing Request (CSR) by an Organizational CA on page 122 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:

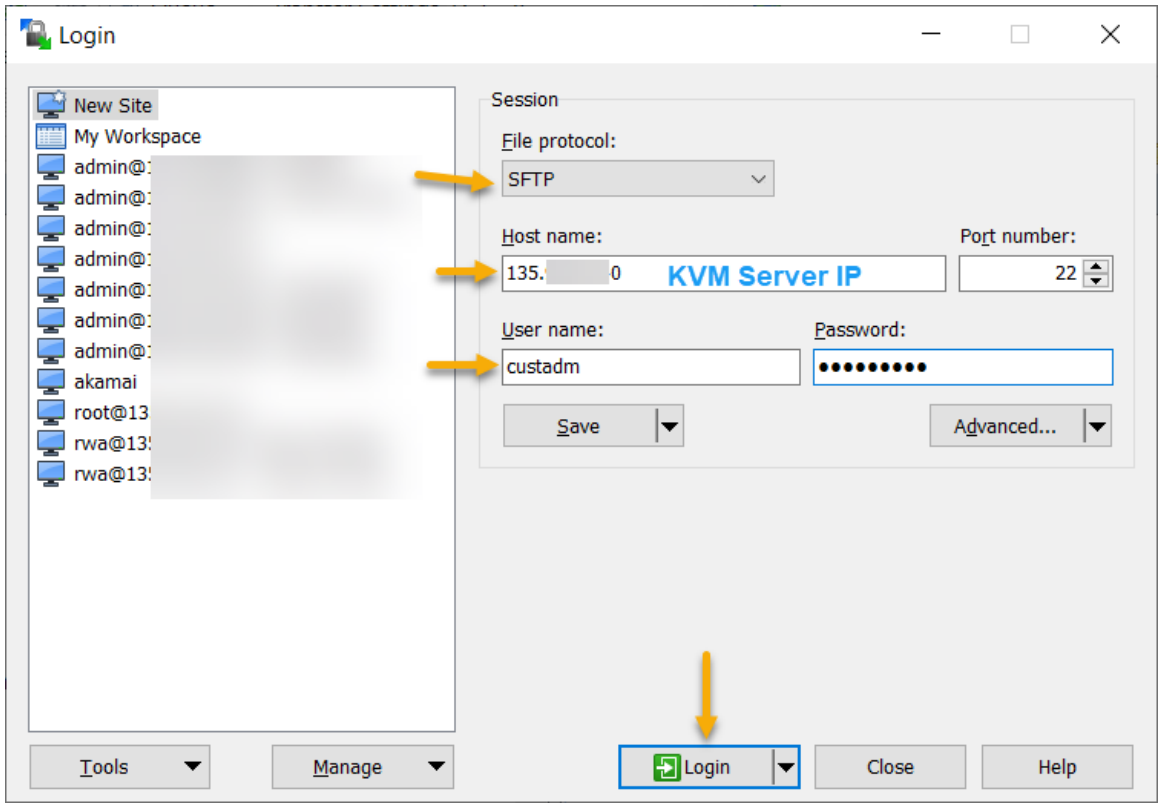
```
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIJAPXW+CuNYS6QMA0GCSqGSIb3DQEBCwUAMD8xKTAnBgNV
BAoMIGI0OGE2NGNkNmMwNTQ1YThhZTgxOTEzZDE5YmJjMmRjMRIwEAYDVQQDDAls
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIJAPXW+CuNYS6QMA0GCSqGSIb3DQEBCwUAMD8xKTAnBgNV
BAoMIGI0OGE2NGNkNmMwNTQ1YThhZTgxOTEzZDE5YmJjMmRjMRIwEAYDVQQDDAls
...
-----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 116 procedure.



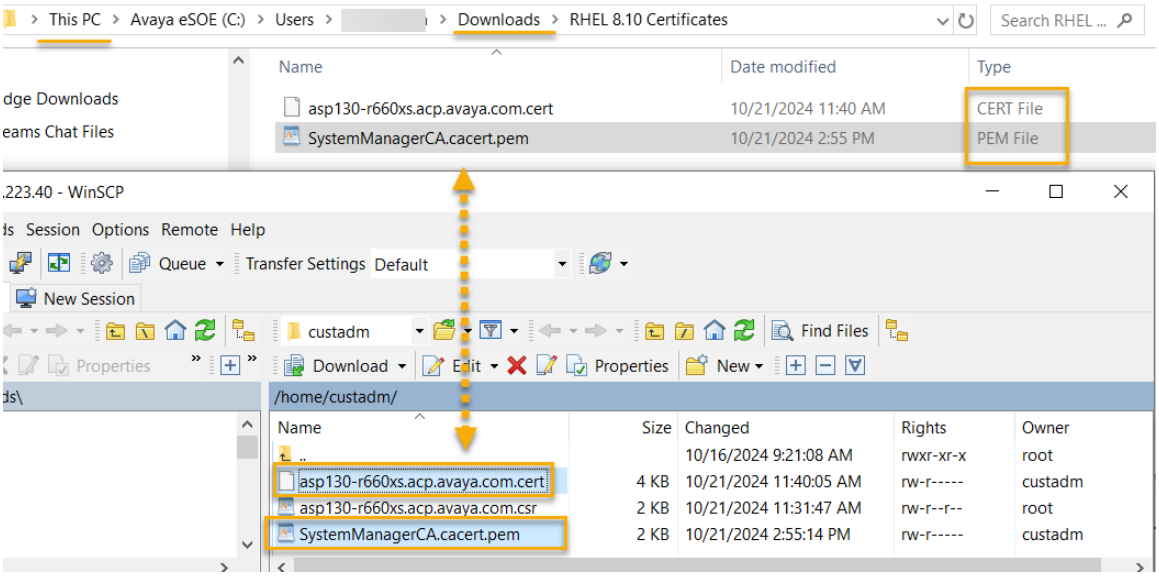
2. Transfer the returned signed certificate by the Certificate Authority (CA) with `cert` extension to the `custadm` home directory.

   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-----. 1 root    root    1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert
-rw-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-----. 1 root    root    1269 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.csr
-rw-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-----. 1 root    root    1493 Oct 10 15:48 user-generated-cockpit-selfsigned.cert.bak
-rw-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-----. 1 root    root    1269 Oct 11 07:36 aspl30-r660xs.acp.avaya.com.csr
-rw-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@asp130-r660xs ws-certs.d]$ sudo systemctl daemon-reload
[sudo] password for custadm:
[custadm@asp130-r660xs ws-certs.d]$
[custadm@asp130-r660xs ws-certs.d]$
[custadm@asp130-r660xs ws-certs.d]$ sudo systemctl restart cockpit
[custadm@asp130-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 asp130-r660xs.acp.avaya.com systemd[1]: Starting Cockpit Web Service...
Oct 11 13:05:48 asp130-r660xs.acp.avaya.com systemd[1]: Started Cockpit Web Service.
[custadm@asp130-r660xs ws-certs.d]$
```

Following example displays a discrepancy between the key file name and current system short hostname `asp130r660xs` vs `asp130-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 ExecStart=/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 asp130-r660xs.acp.avaya.com systemd[1]: Starting Cockpit Web Service...
Oct 11 13:52:03 asp130-r660xs.acp.avaya.com cockpit-certificate-ensure[7237]: cockpit-certificate-ensure: open: /etc/cockpit/ws-certs.d/asp130r660xs.acp.avaya.com.key: No such file or dire>
Oct 11 13:52:03 asp130-r660xs.acp.avaya.com systemd[1]: cockpit.service: Control process exited, code=exited status=1
Oct 11 13:52:03 asp130-r660xs.acp.avaya.com systemd[1]: cockpit.service: Failed with result 'exit-code'.
Oct 11 13:52:03 asp130-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@asp130-r660xs ~]$ ls -lrt
total 12
-rw-r--r--. 1 root    root    1269 Oct 21 12:31 asp130-r660xs.acp.avaya.com.csr
-rw-r-----. 1 custadm custadm 3335 Oct 21 12:40 asp130-r660xs.acp.avaya.com.cert
-rw-r-----. 1 custadm custadm 1241 Oct 21 15:55 SystemManagerCA.cacert.pem
[custadm@asp130-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>.crt
  -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:

```
TVQsTzlBVkFZQTAdBgNVHQ4EFgQUHUIIpVLFJxARtr6OlqkpEo7WNLgwDQYJKoZI
hvcNAQELBQADggEBAGek0PDYNjsT/DXNeWMWg+J7W3CtTOkhRDeAFDRRMj8nDfIS
ceZ/ii2jsoZ/AgnJJ1DHbNWf0atz/SUVsUDhkz48XbF10vH4kQAhiKg4Ml5ZyLrc
FfsFGfdOptaSk83HOjg/e+uJTbcHf9E6qhu0IFzmjovRteYiyidqrO60FUcU4Sky
CNuDLJusa/8IP5YoDIGhCH1M06ILbwqaWobu7nsxuLYICRXU0YfUAi81710XRPbY
6QBWvbtyrffulld18Bwyu//cBPJe7ymqjFhFlA7OMQIBmA4U9d9GeBuotExuR9DC
bnSL4RsVq/ArJ/lz9zVLMffsYhPIGVwljF9EwXY=
-----END CERTIFICATE-----
subject=CN = asp130-r660xs.acp.avaya.com, CN = asp130-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

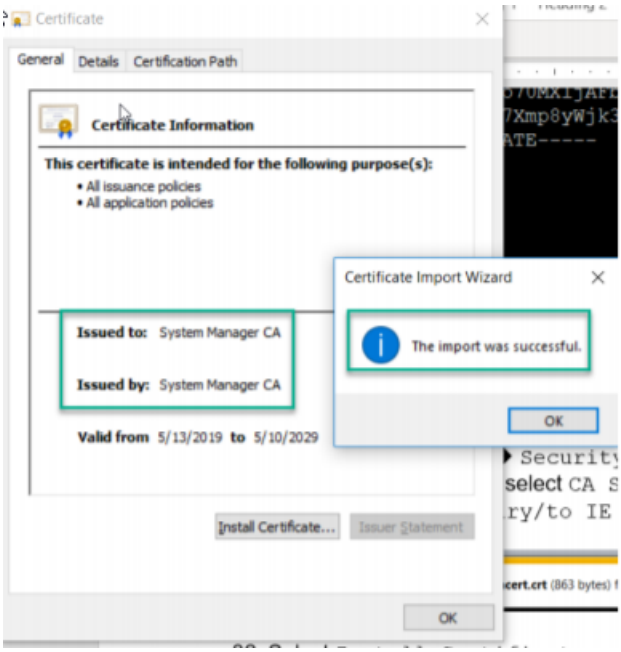
Customers using an External CA or Microsoft CA, should have by now the root certificate provided by the CA in CRT format.

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.

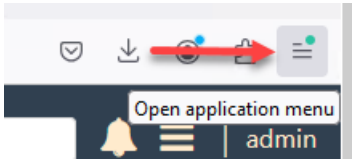
Before you begin

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

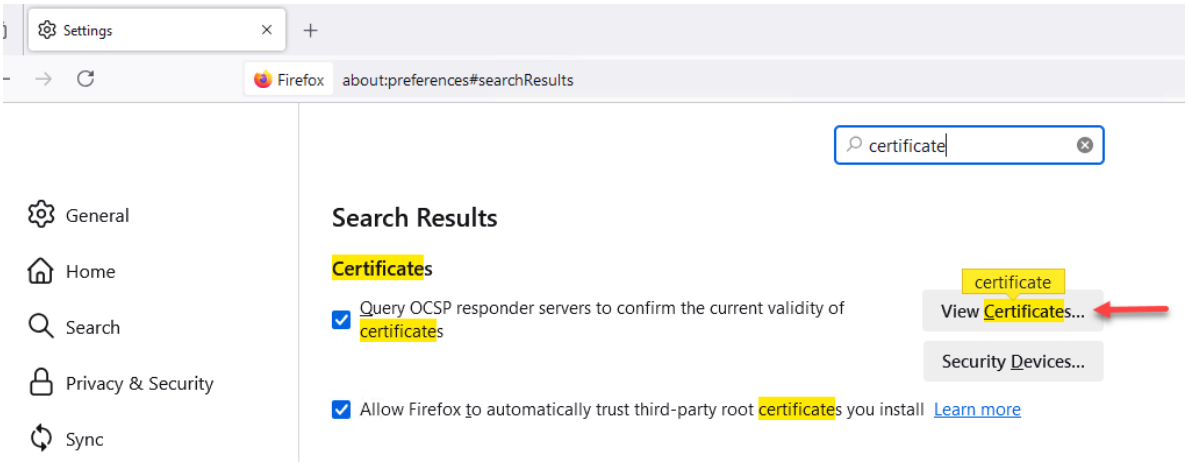
Procedure

1. Open a web browser using Firefox and access Avaya Aura® System Manager.
2. 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**.

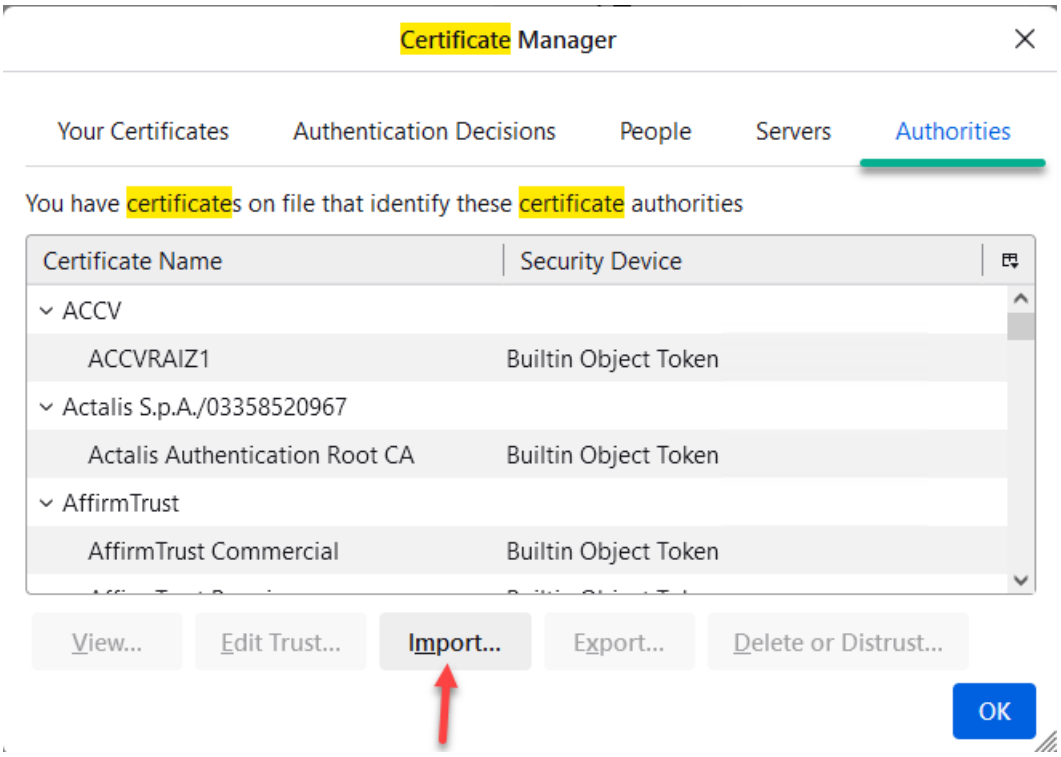
   A file with a name `cacert` downloads automatically.
6. Click on the 3 lines icon in the browser upper-right corner and select **Settings**.



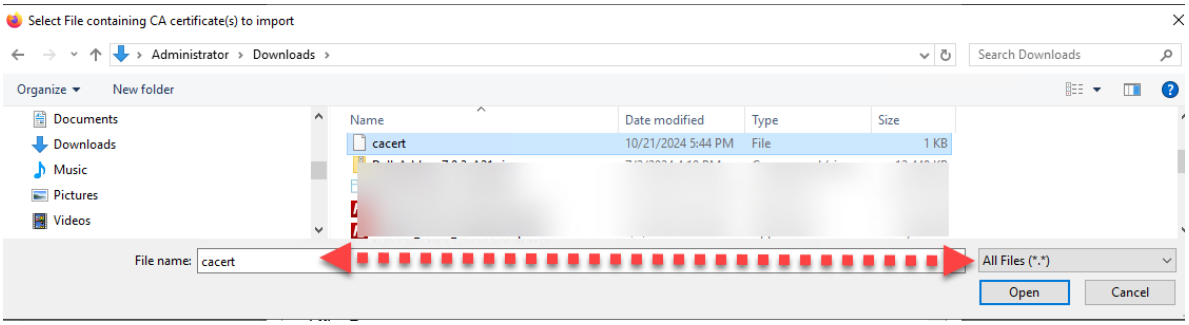
7. In the **Find in Settings** field type in `Certificate` and click on **View Certificates...**.



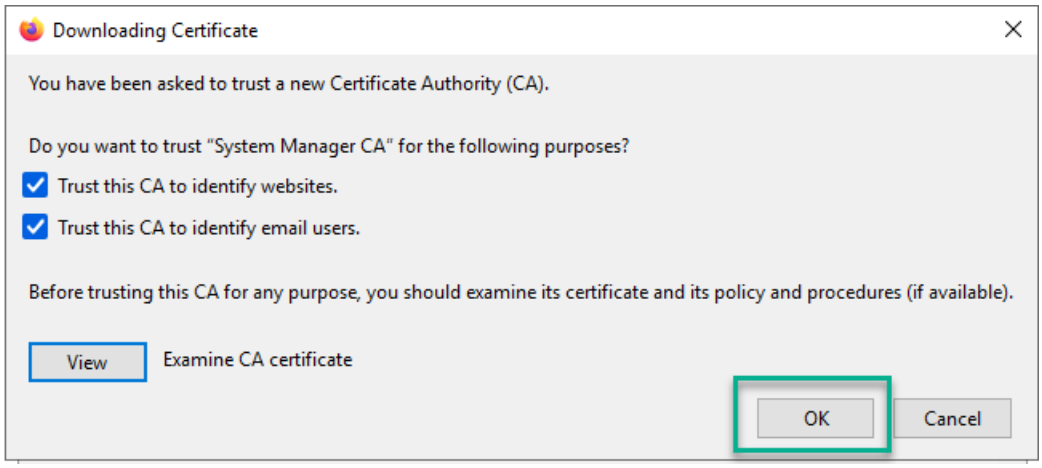
8. Under the Authorities tab, click on **Import...**.



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**.

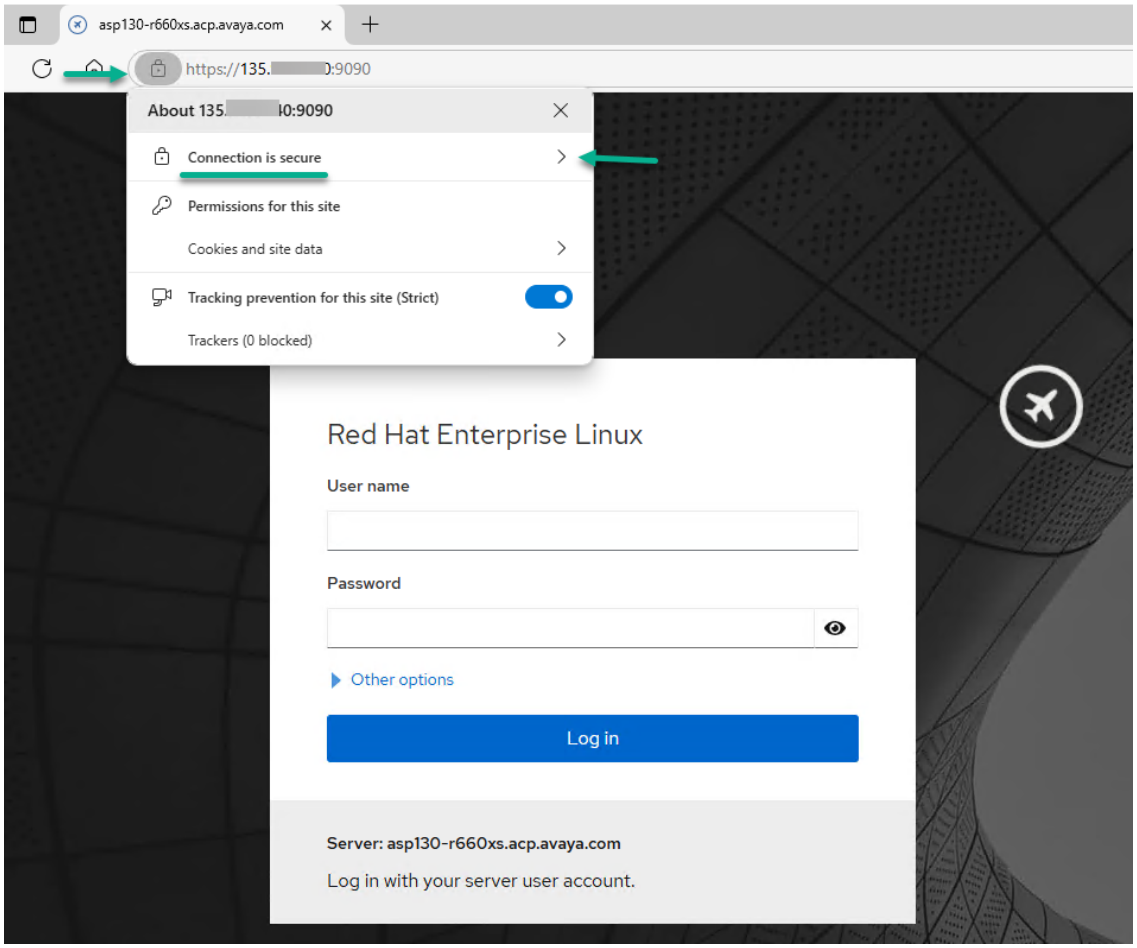


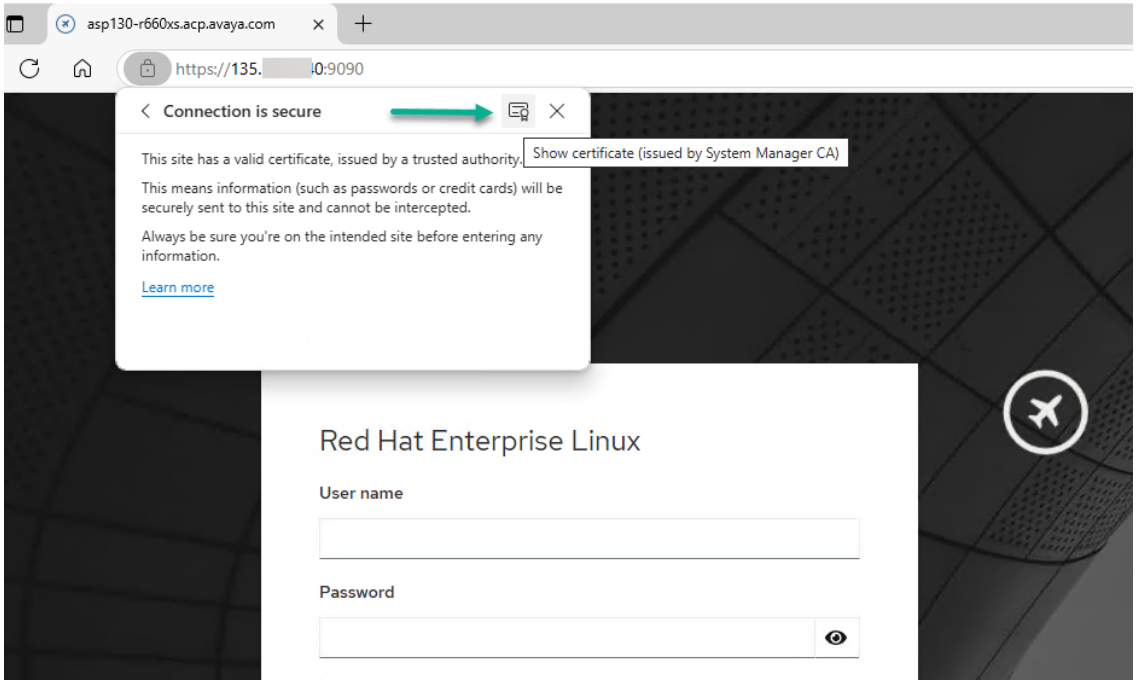
11. Clear the history, cache, and cookies from all previously used browsers. Reference to each browser documentation if needed when doing so.
12. Open a new Web browser to the corresponding KVM on RHEL 8.10 cockpit by either using the FQDN or IP Address, for example`https://<cockpit-ip>:9090`.

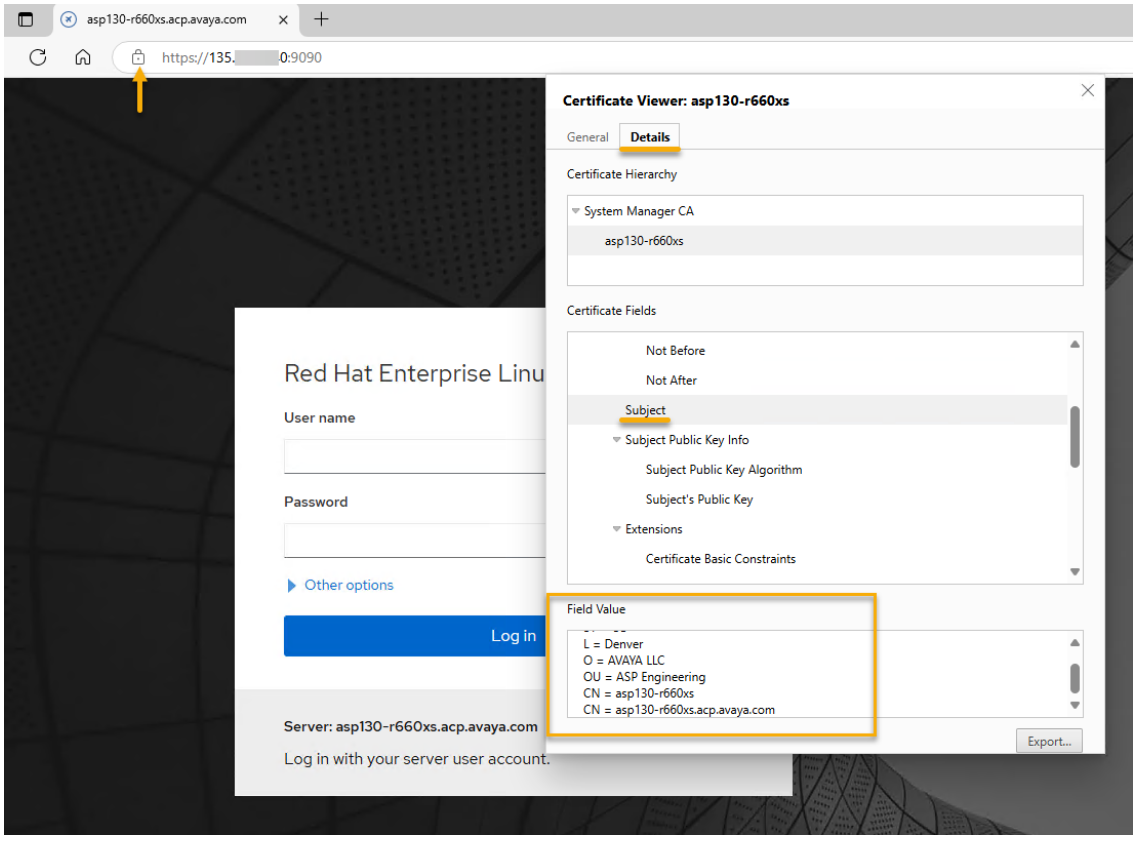
Note:

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.


asp130-r660xs.acp.avaya.com
https://135.[redacted]0:9090
About 135.[redacted]0:9090
Connection is secure
Permissions for this site
Cookies and site data
Tracking prevention for this site (Strict)
Trackers (0 blocked)
Red Hat Enterprise Linux
User name
Password
Other options
Log in
Server: asp130-r660xs.acp.avaya.com
Log in with your server user account.


asp130-r660xs.acp.avaya.com
https://135. 0:9090
Connection is secure
This site has a valid certificate, issued by a trusted authority.
Show certificate (issued by System Manager CA)
This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.
Always be sure you're on the intended site before entering any information.
Learn more
Red Hat Enterprise Linux
User name
Password


asp130-r660xs.acp.avaya.com
https://135. 0:9090
Certificate Viewer: asp130-r660xs
General
Details
Certificate Hierarchy
System Manager CA
asp130-r660xs
Certificate Fields
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Basic Constraints
Field Value
L = Denver
O = AVAYA LLC
OU = ASP Engineering
CN = asp130-r660xs
CN = asp130-r660xs.acp.avaya.com
Export...
Red Hat Enterprise Linu
User name
Password
Other options
Log in
Server: asp130-r660xs.acp.avaya.com
Log in with your server user account.

Chapter 11: 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 12: Dell R660xs and R640 RAID Configuration

Introduction

The Dell R640 RAID controller (H730P Mini or H750) and the Dell R660xs RAID Controller (H755) are enterprise-class controllers providing a robust infrastructure to maximize server uptime.

The instructions below are similar for both the Dell R660xs and the Dell R640. Screen shots are for a Dell R640 but are applicable to the Dell R660xs. The Controller name will be different for the R660xs (H755) and some wording of the navigation menus may differ slightly.

Note:

The user needs a VGA monitor, a USB keyboard, and a USB mouse to configure the RAID Controller.

Preparing to configure the RAID controller

About this task

Use this procedure to configure the Dell R660xs RAID controller (H755) or the Dell R640 RAID controller (H730P Mini or H750). To do that the user must first delete all the existing configurations from the controller. The controller configuration process for creating ASP 130 R640 RAID configurations for profiles 2, 3, 4, 5 and 51 is the same whether the server has an H730P or H750 controller. There are minor differences between the H730P and H750 in the wording and display of the level selections.

These steps are required for migration of ASP R4.x, R5.x, AVP (ASP 120) on a Dell R640 to ASP R6.0.x.

The steps for the ASP 130 R660xs (H755) are similar to the steps below, again with minor differences in the level selections. The screen shots below are from a Dell R640 H730P.

Important:

This procedure will delete all previously written data on the HDDs. Use this procedure only if the previously configured RAID array/virtual drive needs to be deleted and re-created.

Before you begin

- Ensure the server has the correct number of HDDs installed for the server profile.

Caution:

When performing this procedure all data on the HDDs will be destroyed. Reference the R640 server figure below.

Procedure

1. When all necessary data has been copied and backed up from the customer's R640 server, power off the server. The R640 power button (5) can be pushed and held until the server powers off.
2. When migrating an R640 P5 or P51 server, the user can move to step 3 below. When migrating an R640 P2, P3 or P4 server insert the additional two 600GB HDDs into the next 2 available HDD slots. Slots are numbered 0-7. Slot designations are shown on the front of the server. See server figure below.
   - R640 P2 – Insert additional HDDs into slots 3 and 4 (slots 0-2 should already be populated with HDDs).
   - R640 P3 or R640 P4 – Insert additional HDDs into slots 4 and 5 (slots 0-3 should already be populated with HDDs).

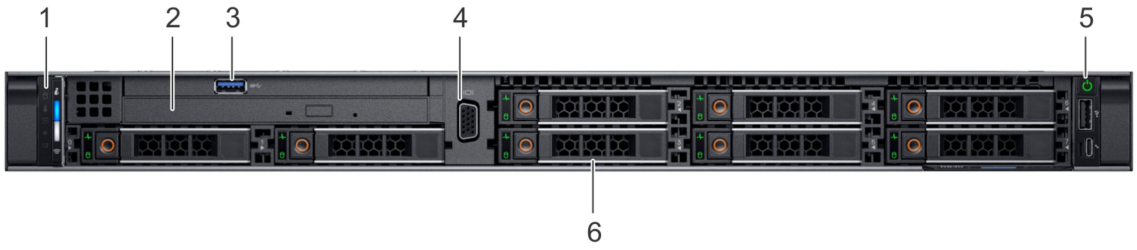


Figure 13: Avaya Dell R640 P51 Server

Item	Function	Description
1	Left control panel	Contains system health and status
2	Optical drive	Slim SATA DVD-ROM drive
3	USB Port	2 USB ports on front and 2 on rear of R640 server
4	VGA Port	One port on front and one on rear. If front port is connected, rear port will disable.
5	Power button	Controls power to the system
6	Drive Slots	8 - 2.5 inch slots available for Hard Disk Drives(HDD) S

3. Once the HDDs have been inserted in their correct slots, power up the server by pressing the power button. Server will begin hardware boot.
4. Select **<F2> System Setup** when hardware boot screen appears. Blue highlight indicates **System Setup Menu** selected.

5. Select **Device Settings**.

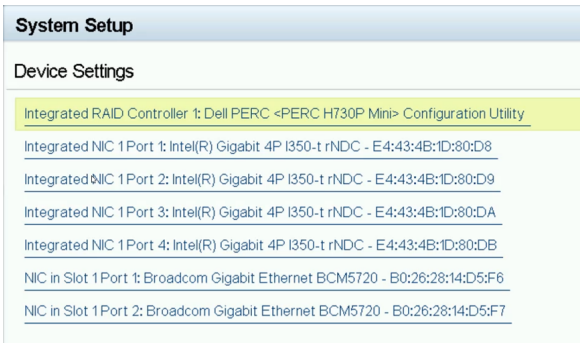


Figure 14: R640 with H730P RAID controller

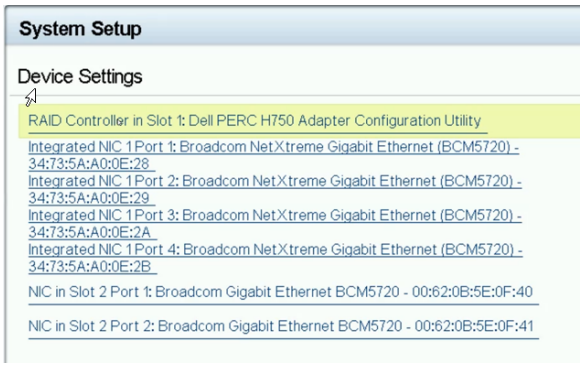
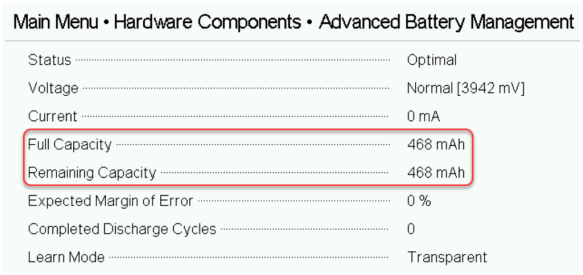


Figure 15: R640 with H750 RAID controller

6. Select the top option, which is the RAID Controller in your system. Earlier versions of the R640 had a PERC H730P, later versions had the PERC H750. Their configuration interface is very similar.
7. If your system has the H750 RAID controller select **Main Menu**.
8. Both controllers use the same interface and commands at this point. The H750 menus will display an additional **Dashboard View** in the menu header. Select **Hardware Components** to view the RAID battery quality of your system's RAID controller.



9. Select **Battery Management** and then select **Advanced** to view the capacity details of the RAID battery. Ensure that the Full Capacity of the Battery is above 250mAh and the Remaining Capacity is equal to or within 30mAh of the Full Capacity value. If the Full Capacity value is below 250mAh then it is recommended that a new RAID battery or RAID

controller with battery be ordered and installed ASAP. The user may continue this process, but the RAID battery may need to be replaced within a year. A RAID battery is considered failed (RAID cache set to Write-Through mode) when its Full Capacity value is 135mAh or less. If your battery is failed do not proceed until a new battery is installed. Select **Back** twice to return to the RAID Controller Main Menu.

10. Both controllers use the same interface and commands from this point on to create the RAID array so steps will be identical for both controllers. The H750 menus will display an additional Dashboard View in the menu header. When on this page select **Configuration Management**.
11. Select **Clear Configuration**.

    Caution:

    Ensure all required customer data was backed up before proceeding with this next step! If data still requires backup, then select **No** and select **Back/Exit** to get out of these menus to perform appropriate backup of data.

12. Check **Confirm**, select **Yes** and then **OK** to clear the current RAID array.

    By pressing **OK** all data on the HDDs will be cleared/destroyed.

13. If after clearing the RAID controller configuration a **Manage Foreign Configuration** option is shown, then one or more of the HDDs inserted was from another RAID array and was not a new HDD. Select **Manage Foreign Configuration**. If there is no **Manage Foreign Configuration** option, then the user can move onto step 16 below.
14. Select **Clear Foreign Configuration**.
15. Check **Confirm**, select **Yes** and then **OK** to clear the current RAID array.
16. Select **Back** to move to the higher-level RAID Controller menu.
17. Select **Physical Disk Management**.

Figure 16: 5 HDDs required for R640 Profile 2

Figure 17: 6 HDDs required for R640 Profile 3, 4, and 5

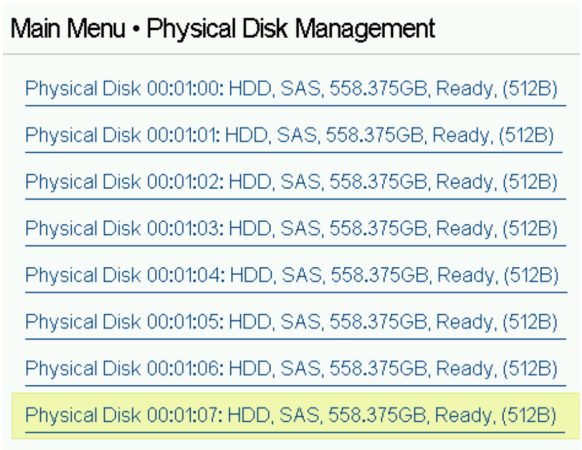


Figure 18: 8 HDDs required for R640 Profile 51

18. The user should see the expected number of HDDs (Physical Disks) Ready for creating the appropriate RAID array for the R640 Profile # they are attempting to create. If all Disks are not in a Ready state move back to step 10 and perform a Clear on the Select Back to move to Main Menu.

Creating a virtual disk

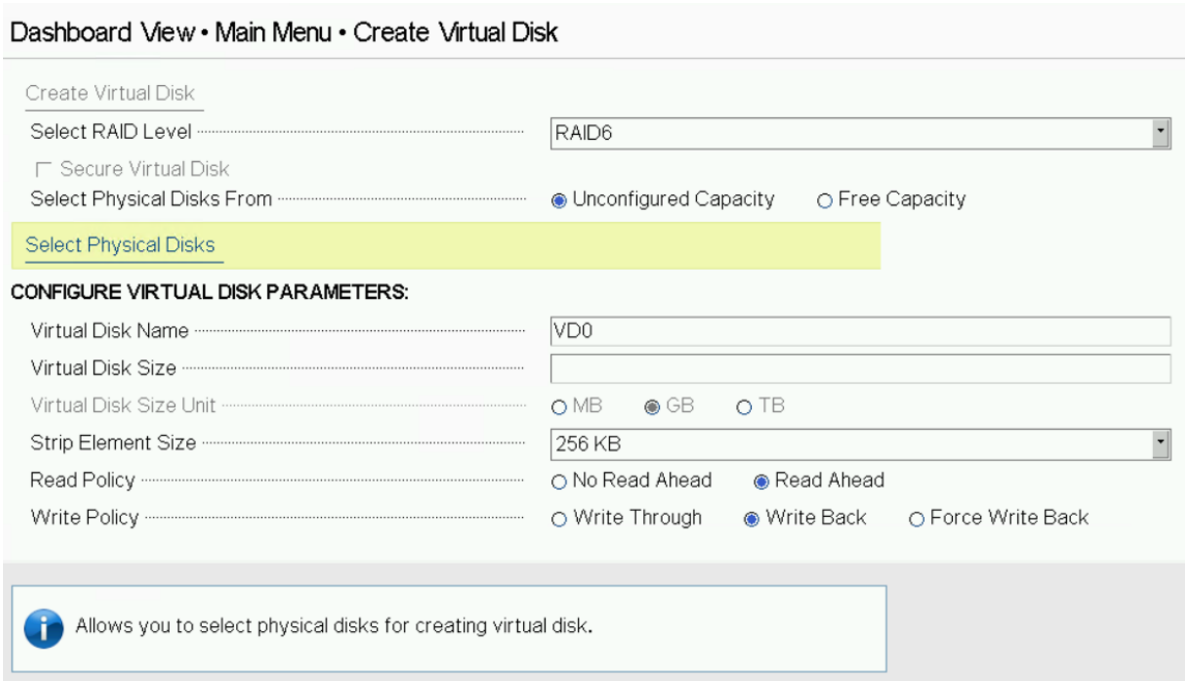
About this task

Use this procedure to create a virtual disk by selecting the RAID level, physical disks, and virtual disk parameters.

Procedure

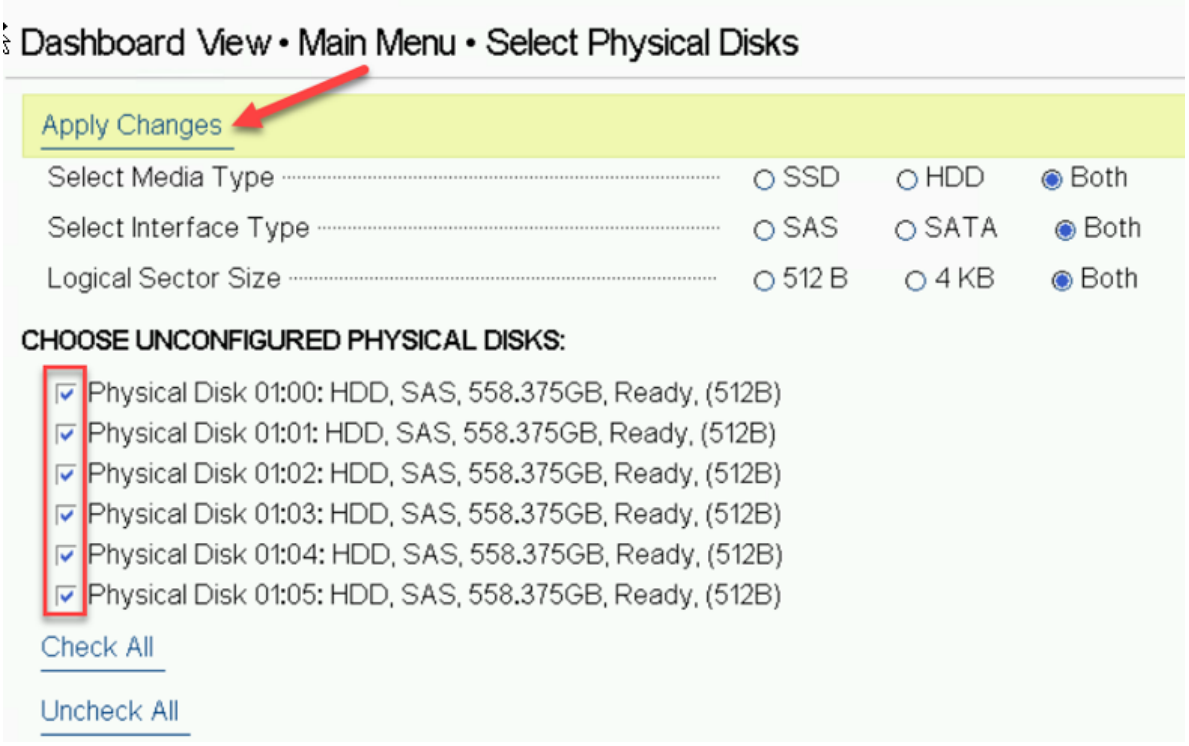
1. Select **Configuration Management**.

2. Select **Create Virtual Disk**.

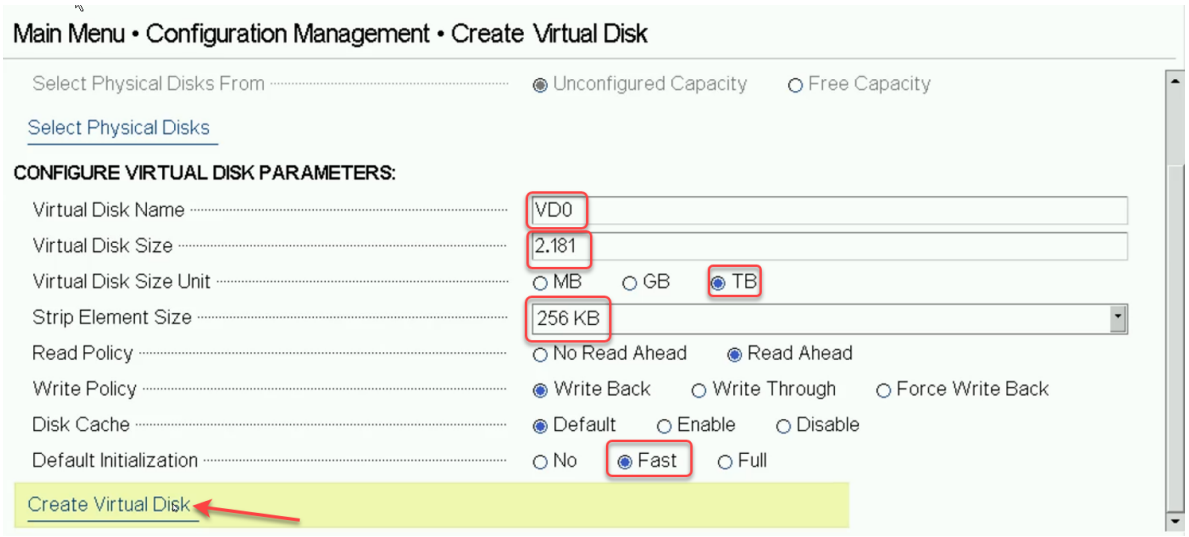


3. Select the RAID level specified by the Avaya ASP 130 Profile configuration. ASP 130 P2 must be set for RAID 5. All other ASP 130 profiles must be set for RAID 6. Enter the

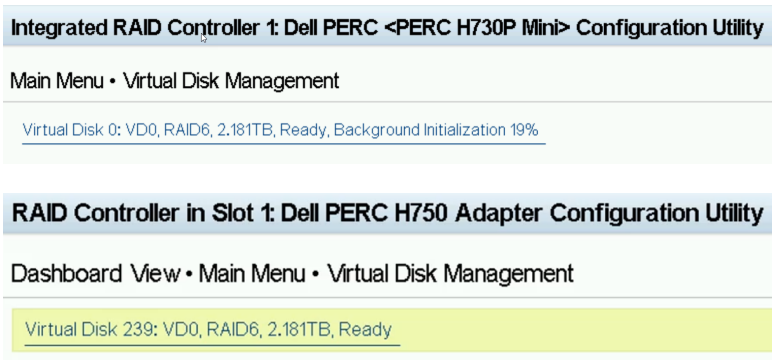
Virtual Disk Name as `VD0` and set the **Strip Element Size** to `256KB`. Now scroll down and select **Fast Default Initialization**. Next press **Select Physical Disks**.



4. The number of disks displayed should match the number of disks needed to build the ASP profile the user is creating. In the example above 6 HDDs are shown and must be selected to create an ASP 130 Profile 3, 4 or 5. Once the correct number of disks are verified and selected, click **Apply Changes** and then **OK**. Leave **Media Types** at their default settings. User will be moved back to the Create Virtual Disk Menu page.



5. Notice that the Virtual Disk Size is now populated to reflect its number and size of HDDs and RAID array type. ASP 130 P2, P3 and P4 should show a size of 2.181TB. ASP 130 P51 should show a size of 3.271TB. Ensure the **Virtual Disk Name** is set to `VD0`, the **Strip Element** size is `256KB` and **Default initialization** is set to `Fast`. When values are confirmed select **Create Virtual Disk**.
6. Check **Confirm**, select **Yes** and then **OK** to create the RAID array. RAID array is now created. To view, select **Back** twice to get to top level Main menu.
7. Select **Virtual Disk Management**.



8. The Virtual Disk is now displayed. Ready status will turn to Ready, Background Initialization xx% within 10 minutes of creation. Software installation can be performed during background initialization. Notice that the H730P Controller designates its first created disk as Virtual Disk 0; Whereas the H750 Controller designates its first created disk as Virtual Disk 239. This is expected behavior. The user defined Virtual Disk Name is still set to VD0 on both Controllers. Select **BACK** and then **Finish/Finish** to move back to the System Setup Main Menu.

   Examples of the different ASP 130 Virtual Drives:

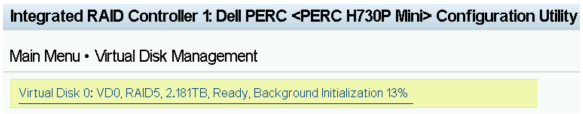


Figure 19: ASP130 P2 with H730P RAID Controller

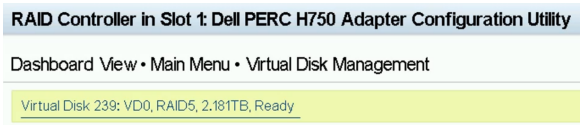


Figure 20: ASP130 P2 with H750 RAID Controller

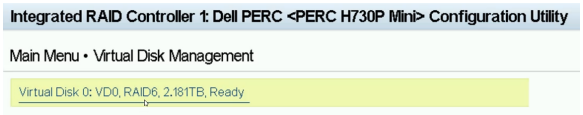


Figure 21: ASP130 P3, P4 and P5 with H730P RAID Controller

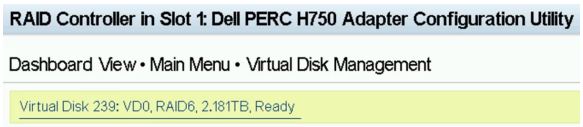


Figure 22: ASP130 P3, P4 and P5 with H750 RAID Controller

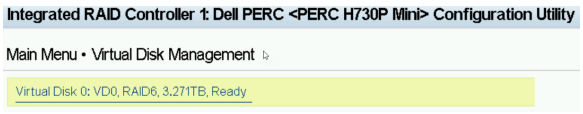


Figure 23: ASP 130 P51 with H730P RAID Controller

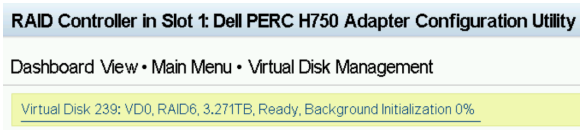


Figure 24: ASP130 P51 with H750 RAID Controller

9. Select **Back** and then **Finish/Finish** (H730P) or **Back/Back** and then **Finish/Finish** (H750) to get to the System Setup Main Menu.
10. Select **System BIOS**.
11. Select **Boot Settings**.
12. Set **Generic USB Boot** and **Hard-disk Drive Placeholder** to **Enabled** and then select **Back**.
13. Select **Finish** and then **Yes** to save the settings changes just made. Server must reboot to rescan boot setting changes. Click **OK**, **Finish** and **Yes** to reboot the server. Server will now reboot.
14. Select **<F2> System Setup** when hardware boot screen appears.
15. Select **System BIOS**.
16. Select **Boot Settings**.
17. Verify that **Generic USB Boot** and **Hard-disk Drive Placeholder** are set to **Enabled** and then select **UEFI Boot Settings**.

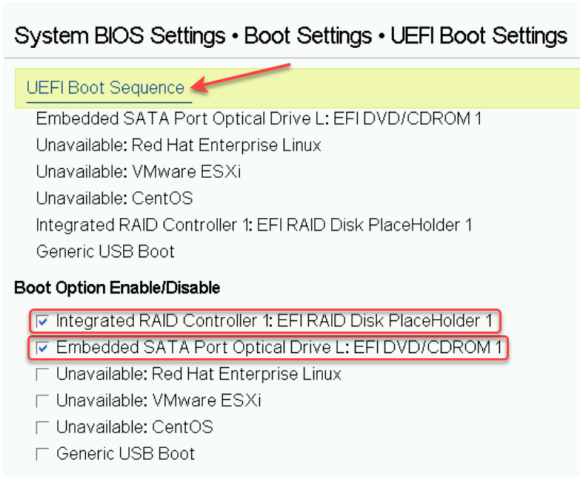


Figure 25: R640 ASP130 with H730P RAID Controller

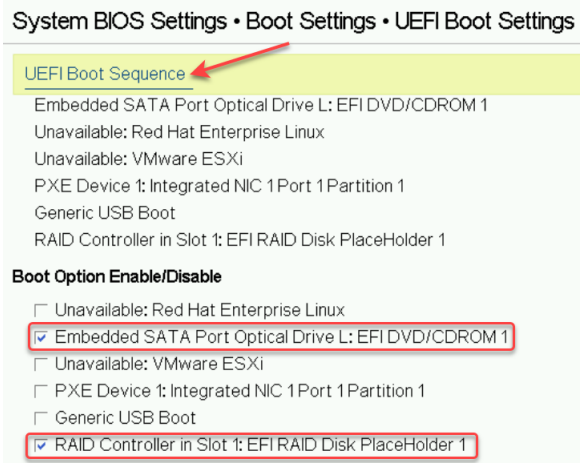


Figure 26: R640 ASP130 with H750 RAID Controller

18. When on this page confirm or change the **Boot Option Enable/Disable** so that only the **Embedded SATA Port Optical L: EFI DVD/CDROM 1** and the **RAID Controller (1) or (in Slot 1): EFI RAID Disk PlaceHolder 1** are set to **Enabled** (checked). All other options can be ignored. Now click the **UEFI Boot Sequence** link. A Change Order pop-up window will display.

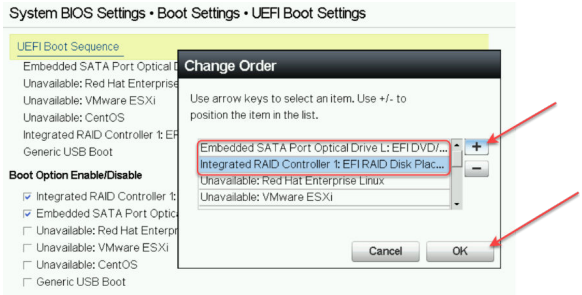


Figure 27: R640 ASP130 with H730P RAID Controller

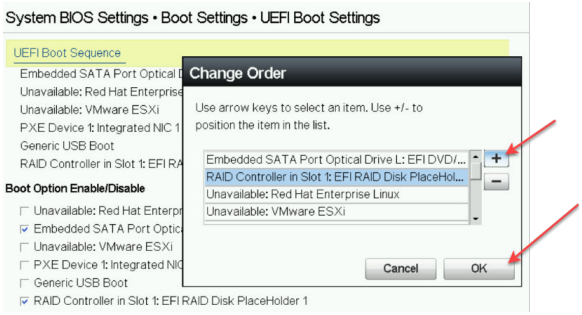


Figure 28: R640 ASP130 with H750 RAID Controller

19. In the pop-up window select the enabled Boot Option devices and move them to the top of the UEFI Boot Sequence as shown. Select the Boot device to be moved and then click the "**+**" to move the device up in the boot sequence. Place the **Embedded SATA Port Optical L: EFI DVD/CDROM 1** first in the boot sequence followed by the **RAID Controller (1) or (in Slot 1): EFI RAID Disk PlaceHolder 1** as shown above. All other boot place holders can be ignored. When the two aforementioned devices have been placed in the proper boot sequence click **OK**.

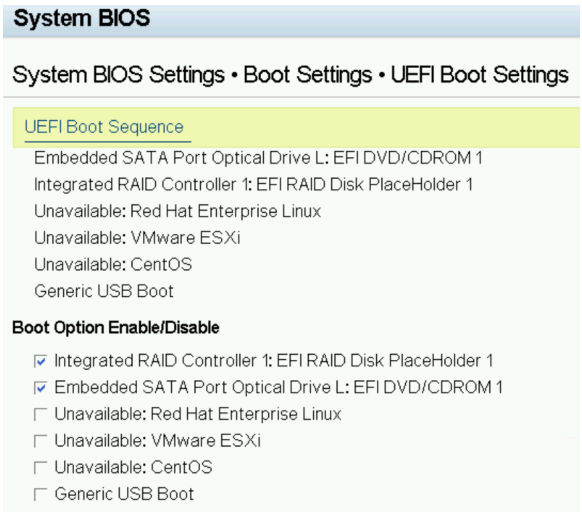


Figure 29: R640 ASP130 with H730P RAID Controller

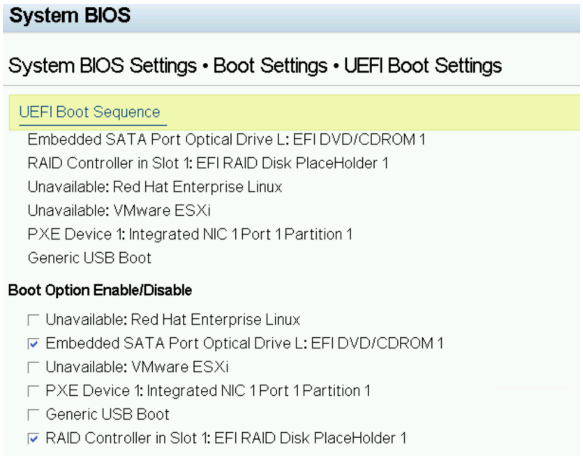


Figure 30: R640 ASP130 with H750 RAID Controller

20. Confirm that the UEFI Boot Sequence has the **Embedded SATA Port Optical L: EFI DVD/CDROM 1** first in the boot sequence followed by the **RAID Controller (1) or (in Slot 1): EFI RAID Disk PlaceHolder 1** as shown above. Also confirm that the only devices that are enabled under the Boot Option Enable/Disable heading are the **Embedded SATA Port Optical L: EFI DVD/CDROM 1** and the **RAID Controller (1) or (in Slot 1): EFI RAID Disk PlaceHolder**. When confirmed select **Back** twice to move to the System BIOS Settings screen.
21. Click **Finish**, then click **Yes** and then click **OK** to save System BIOS Settings changes.
22. Click **Finish**, then click **Yes** to exit and reboot the server.

Next steps

ASP 130 R6.0.x (KVM on RHEL 8.10) software installation can now proceed.

Virtual disk size

The following tables provide the expected virtual disk sizes for the RAID configuration.

Dell R640 with additional HDDs added

RAID configuration	Raw Storage	Usable Capacity in Terabytes (TB)	Usable Capacity in Tebibytes (TiB)	Usable Capacity in Gigabytes (GB)	Usable Capacity in Gibibytes (GiB)	ASP Base Profile
5	5x600 GB = 3.0 TB	2.4	2.181	2398	2233	2
6	6x600 GB = 3.6 TB	2.4	2.181	2398	2233	3, 4, 5
6	8x600 GB = 4.8 TB	3.6	3.271	3597	3350	51

Dell R660xs

RAID configuration	Raw Storage	Usable Capacity in Terabytes (TB)	Usable Capacity in Tebibytes (TiB)	Usable Capacity in Gigabytes (GB)	Usable Capacity in Gibibytes (GiB)	ASP Base Profile
5	5x600 GB = 3.0 TB	2.4	2.181	2398	2233	1
6	6x600 GB = 3.6 TB	2.4	2.181	2398	2233	2, 3
6	8x600 GB = 4.8 TB	3.6	3.271	3597	3350	31

Note:

The table provides the usable capacity in Gibibytes and Tebibytes in addition to Gigabytes and Terabytes, as operating systems may calculate data storage space in this way.

Checking information about the virtual disk

About this task

Use this procedure to check the basic properties of a specific virtual disk. This procedure is similar for both the Dell R660xs (H755) and Dell R640 (H730P and H750). Screenshots of H750 will be similar to H755.

Procedure

1. In the **Main Menu** of **Integrated RAID Controller 1: Dell <PERC H730P Mini> Configuration Utility** or on the **Main Menu of the RAID Controller in Slot 1: Dell PERC H750 Adapter Configuration Utility**, click **Virtual Disk Management**.

   The system shows the virtual disks available for software installation.

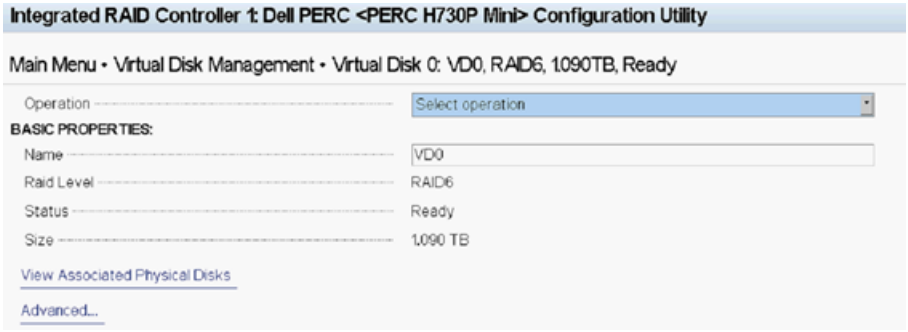
   

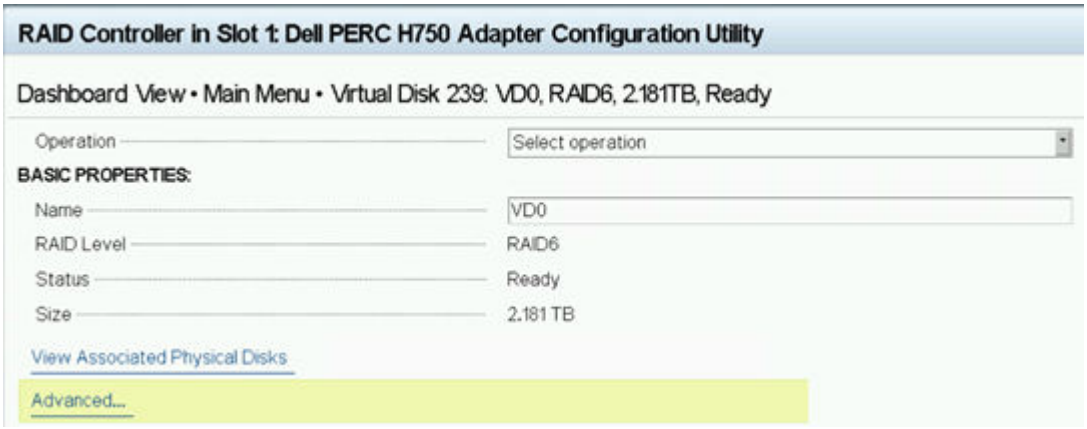
2. Click the virtual disk name.
3. Under Basic Properties, check the information about the virtual disk. You can see the following parameters of the virtual disk:
   - Name

- RAID Level
- Status
- Size

Note:

Notice that the H730 RAID Controller creates its first Virtual Disk starting as number 0 and increments up. Whereas the H750 and H755 Controller creates its first Virtual Disk as number 239 and decrements down in value. This is expected.





4. Click **Back** > **Back** > **Finish** > **Finish** > **Finish** to escape configuration menus.

Result

Server RAID configuration is now complete. The created Virtual Drive is now available for software installation.

Go to Performing server recovery and/or software remastering on page 94 for information on installation of KVM on Red Hat Enterprise Linux Software.

Chapter 13: Dell R660xs and R640 SNMP trap configuration using iDRAC9

SNMP alerts

SNMP is frequently used to monitor systems for fault conditions such as temperature violations, hard drive and fan failures, and voltage fault conditions. The iDRAC generates events that result in Simple Network Management Protocol (SNMP) traps and entries in the iDRAC Lifecycle Log.

The iDRAC generates events in response to changes in the status of sensors and other monitored parameters. When an event with predefined characteristics occurs on your system, the SNMP subagent sends information about the event, along with trap variables, to the management console.

Each event generates an identifier called the trap ID and a list of trap variables that provide additional details about the event. The traps of the iDRAC MIB are organized into five subgroups of traps. Each subgroup corresponds to one of the following five categories of events that iDRAC supports:

- System Trap Group
- Storage Trap Group
- Updates Trap Group
- Audit Trap Group
- Configuration Trap Group

Note:

Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Configuring SNMP v2c using iDRAC9

About this task

You can configure SNMP v2c traps for Dell R640 Avaya Solutions Platform 130 Appliance servers using the iDRAC9 interface.

Note:

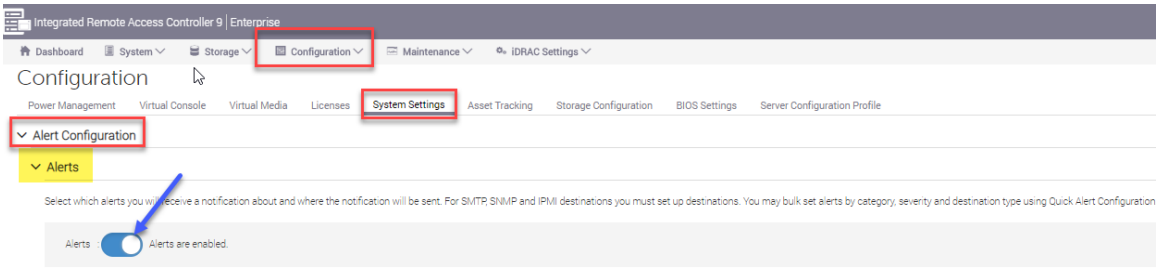
Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Before you begin

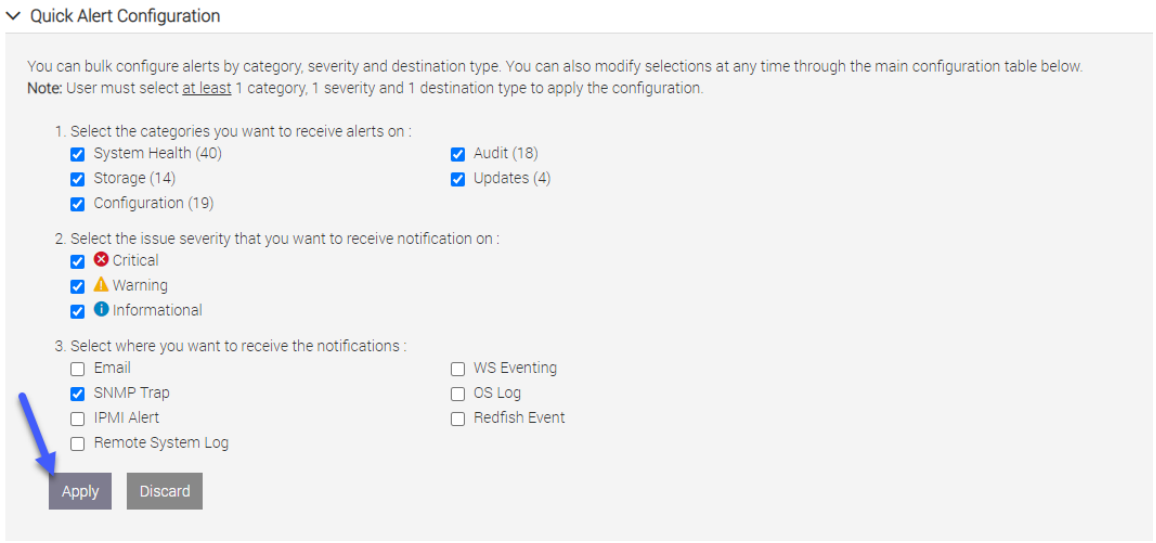
Log into the iDRAC9 web interface using the IP address and login details that were specified while configuring the iDRAC. See the Avaya Solutions Platform 130 Series iDRAC9 Best Practices document for configuring the iDRAC.

Procedure

1. Navigate to **Configuration** > **System Settings** > **Alert Configuration**.
   - Under the **Alerts** options, enable Alerts by clicking on the round icon switch. It will move to the right, turning the area blue.
   - A Success message will display. Click **OK**.



2. Under **Quick Alert Configuration**, select the notification options shown below. Add in other options where customers require additional SNMP output or access to/from other monitoring devices. Click **Apply** to save changes.



3. Redirect to **iDRAC Settings** > **Services** > **SNMP Agent**.
   - From the **Enabled** drop-down menu, select **Enabled**.
   - Enter the **SNMP Community Name**. The name *Public* is an indication of *read-only* access permitted by SNMP agents. Beginning with the release of ASP 130 5.0 Avaya's integrator changes the Community Name to Avaya123.

   Note:

   Avaya strongly recommends changing the SNMP community name to a non-standand name for security purposes.

   - From the **SNMP Protocol** drop-down menu, select **All** to enable SNMP v2C.
   - Click **Apply** to submit changes.

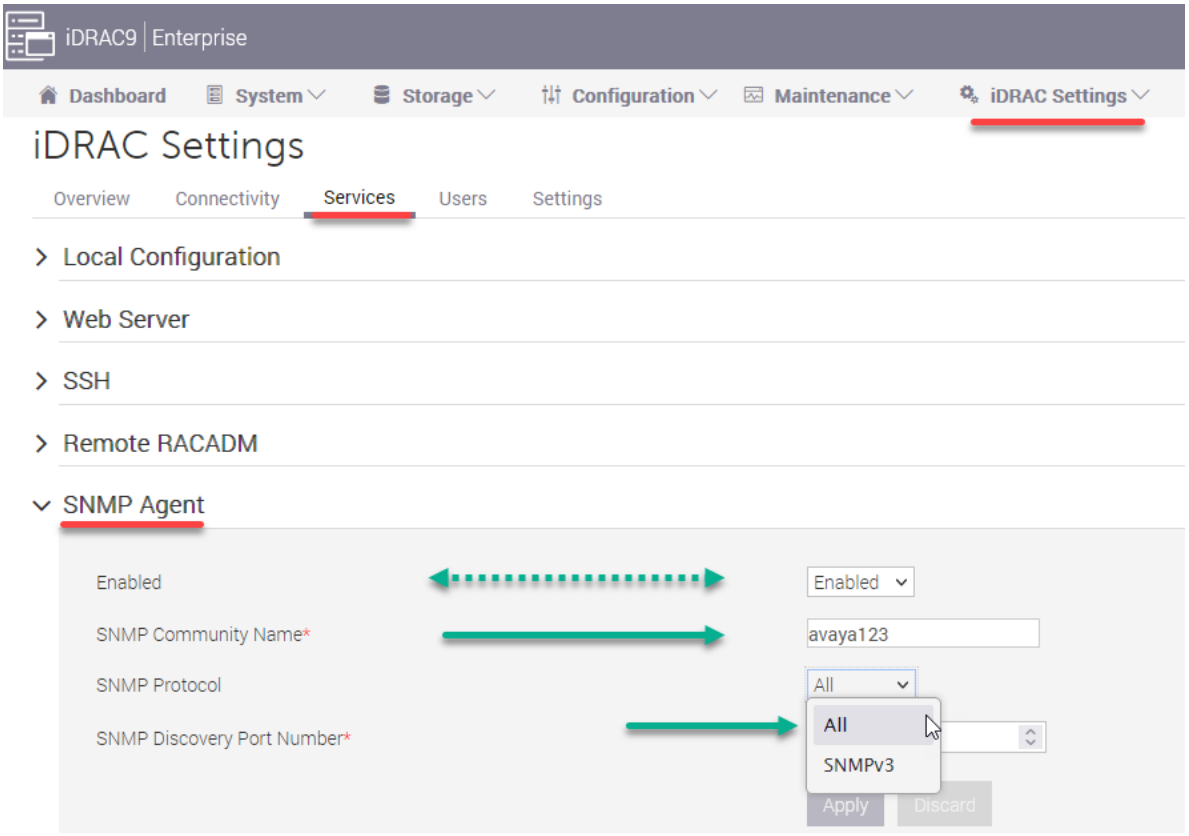


Figure 31: Configuring SNMP v2c using iDRAC9

4. Return to **Configuration** > **System Settings** > **SNMP Traps Configuration**.
   - Enter the IP address of the trap receiver in the **Destination Address** field. If there is more than 1 trap receiver destination, enter those addresses too.
   - Click the **State** box to enable SNMP traps to be sent to the administered location.
   - Click **Apply** to submit the new administration.

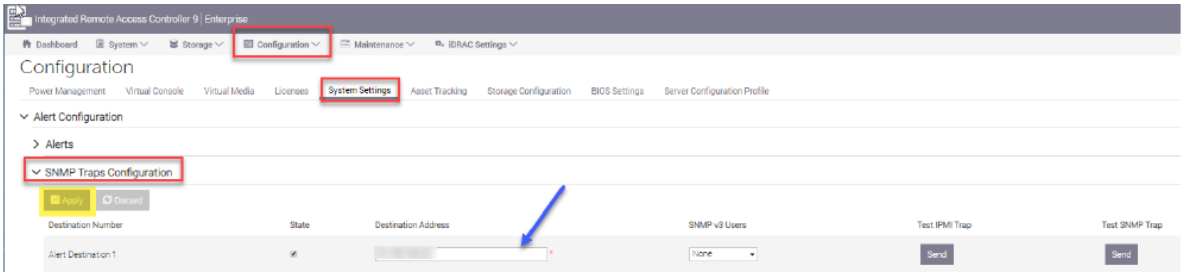
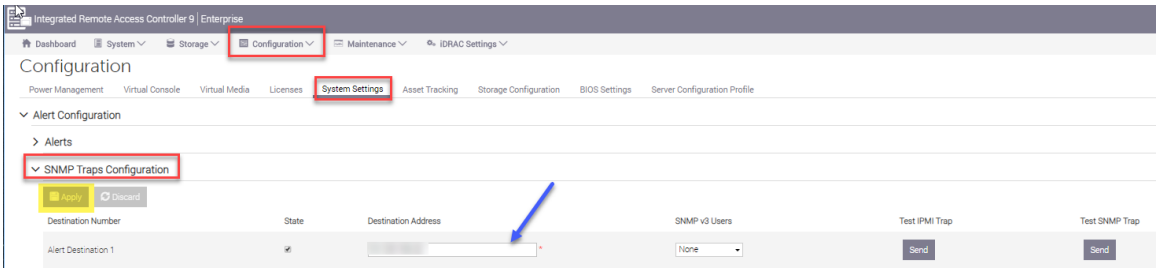


Figure 32: Configuring SNMP Traps

- Enter the IP address of the trap receiver in the **Destination Address** field. If there is more than 1 trap receiver destination, enter those addresses, too.
- Click the **State** box to enable SNMP traps to be sent to the administered location.

- Click **Apply** to submit the new administration.



5. Under the **SNMP Settings** area:

Note:

Avaya strongly recommends changing the SNMP community name to a non-standard name for security purposes.

- You may leave the default of alert port 162; this is the standard SNMP receiving port. You may also enter a different port number, but remember to match this port in both the sending and receiving devices.
- From the drop-down menu for **SNMP Trap Format**, select **SNMPv2**.
- Select **Apply** when settings are complete.

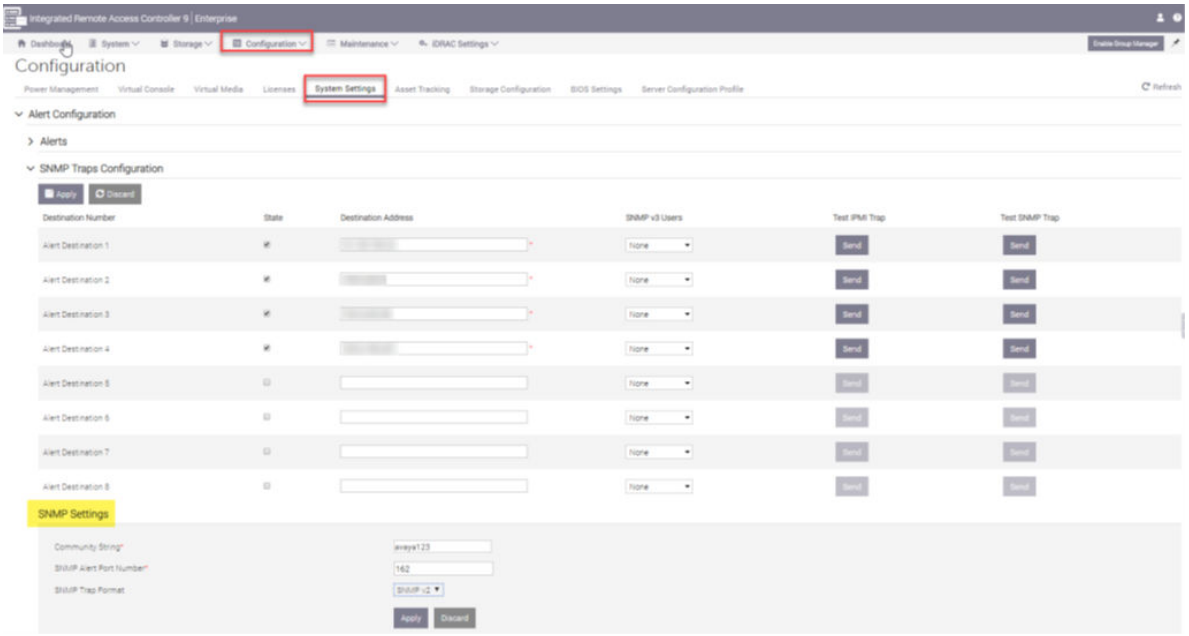


Figure 33: Configuration

6. Once the trap receiver device has also been administered, click the **Send** button under the **Test SNMP Trap** column (related to the specific device), to confirm the receipt of SNMP traps from the iDRAC.

Configuring SNMP v3 using iDRAC9

About this task

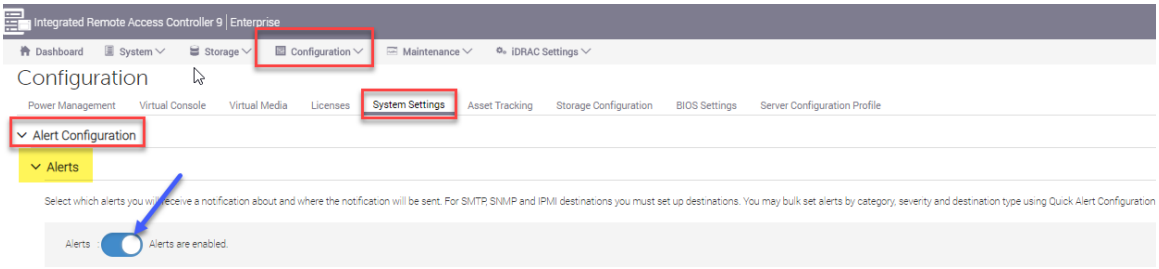
You can configure SNMP v3 traps for Dell R640 Avaya Solutions Platform 130 Appliance servers using the iDRAC9 interface.

Before you begin

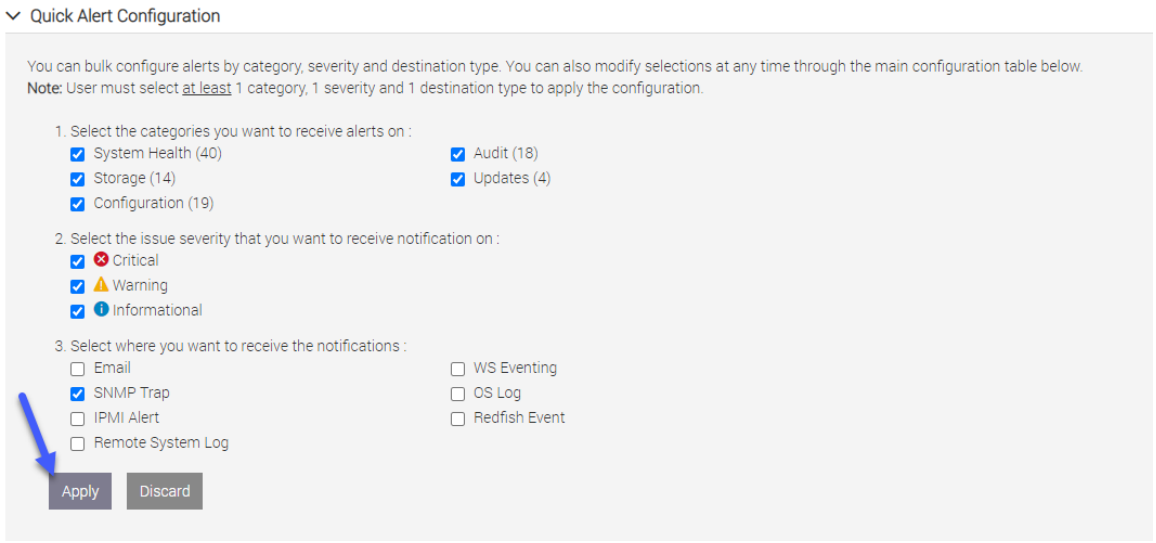
Log into the iDRAC9 web interface using the IP address and login details that were specified while configuring iDRAC. See the Avaya Solutions Platform 130 Series iDRAC9 Best Practices document for configuring the iDRAC.

Procedure

1. Navigate to **Configuration** > **System Settings** > **Alert Configuration**.
   - Under the **Alerts** options, enable Alerts by clicking on the round icon switch. It will move to the right, turning the area blue.
   - A Success message is displayed. Click **OK**.



2. Under **Quick Alert Configuration**, select the notification options shown below. Add in other options where customers require additional SNMP output or access to/from other monitoring devices. Click **Apply** to save changes.



3. Redirect to **iDRAC Settings** > **Services** > **SNMP Agent**.
   - From the **Enabled** drop-down menu, select **Enabled**.
   - Enter the **SNMP Community Name**. The name *Public* is an indication of *read-only* access permitted by SNMP agents. Beginning with the release of ASP 130 5.0, Avaya's integrator changes the Community Name to Avaya123.

Note:

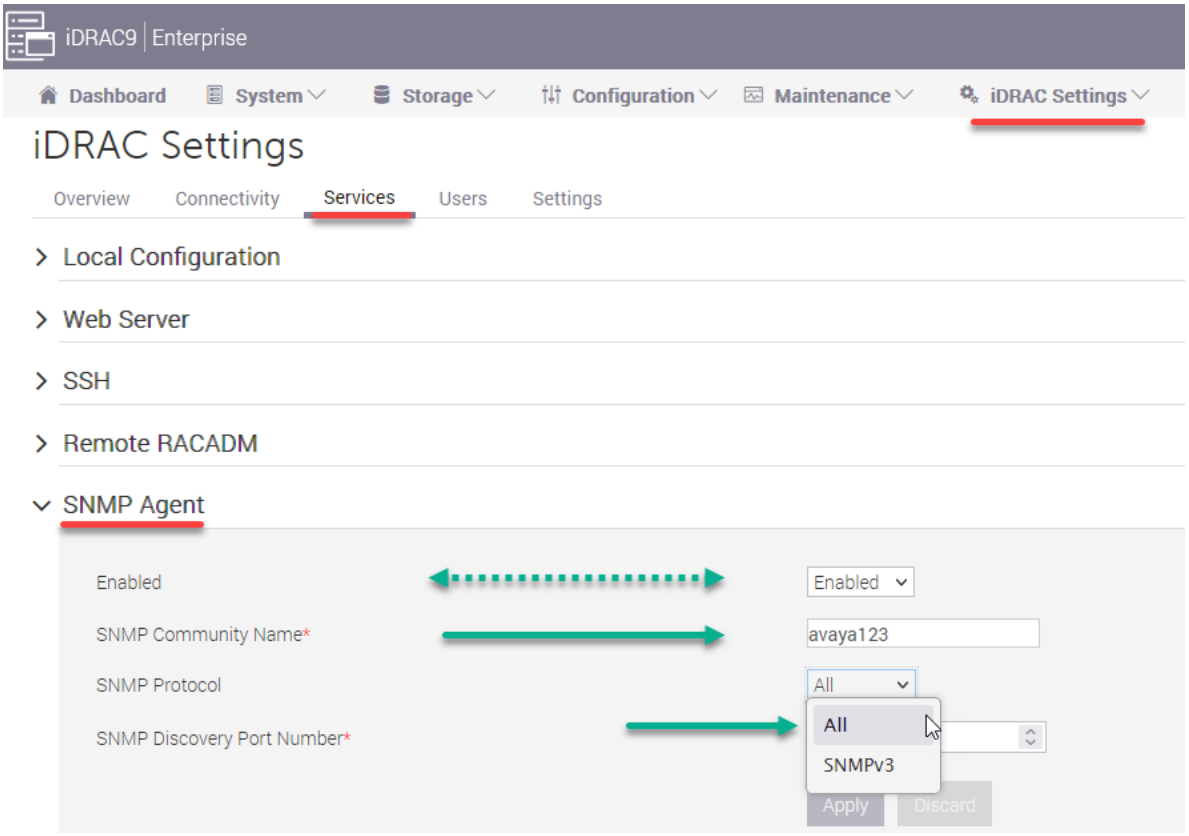
Avaya strongly recommends changing the SNMP community name to a non-standard name for security purposes.

   - From the **SNMP Protocol** drop-down menu, select **SNMP v3**.

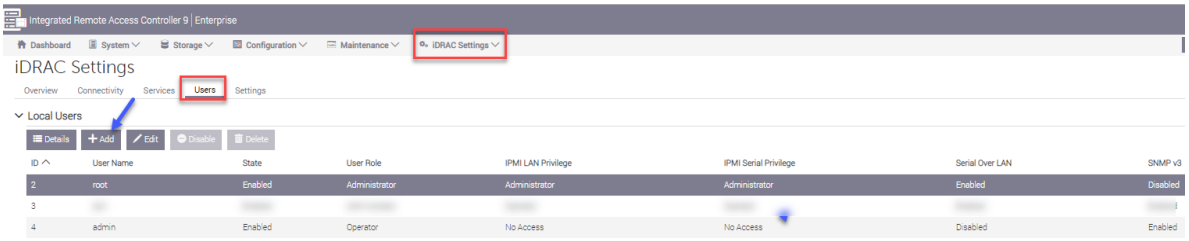
Note:

When setting the SNMP Protocol to SNMP v3 it will disable SNMP v1/v2c on the system.

   - Click **Apply** to submit changes.



4. Now configure the users to validate for secure SNMPv3 exchanges. Go to **iDRAC Settings** > **Users** > **Local Users** and click **+Add** to administer new user information.

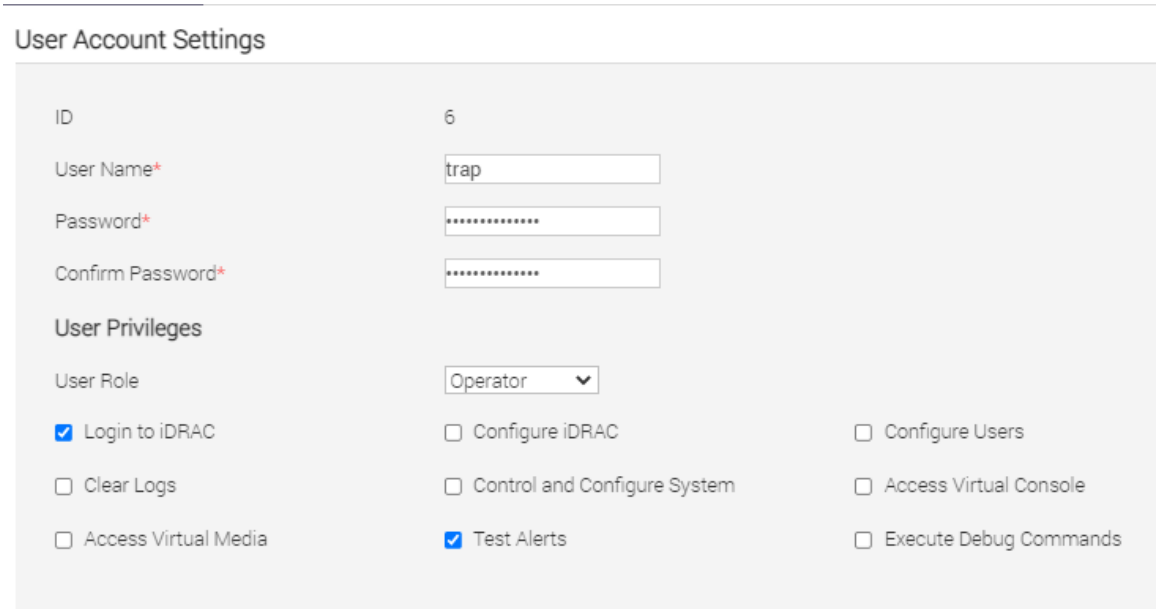


Note:

You may use this form to enter a unique **User Name** and **password** for the Privacy and the Authentication protocols. You may also use the same **User Name** and **password** and assign them to both protocols. Determine which administrative method is preferred before proceeding.

5. Start by filling out the top part of the form: **User Account Settings**.
   - Leave the default **ID** number.
   - Enter a **User Name**.
   - Create a **Password** for the protocol(s) being administered.

- Under **User Privileges**, there is no need to select anything if the trap receiver will never be accessing (logging into) the iDRAC for proactive state-of-health inquiries. If, however, the customer has a device that will be proactively accessing the iDRAC for SNMP status data and has requested the **User** be administered for such access, select **Read Only** from the **User Role** drop-down menu, and the **Login to iDRAC** box will be automatically selected. If Test Alerts are desired select that option and the **User Role** will change to **Operator**.



6. Administer the bottom half of the form: **Advanced Settings** > **SNMP v3 Settings** by scrolling down.
   - From the **SNMP v3** drop-down menu, select **Enabled**.
   - The next 2 boxes represent the protocols that are associated with the previously administered User information.
   - Select the appropriate authentication and privacy type required for this SNMP v3 User account.
   - If only 1 of the Authentication or Privacy types will be used with the SNMP v3 User, select the one required by specifying its encryption or hash type from the appropriate drop-down menu and select **None** for the other.
   - From the **Enable Passphrase** drop-down menu, select **Enabled**.

     Note:

     Enable Passphrase only if Authentication and or Privacy type have been configured.
   - Enter the **Authentication** and **Privacy** Passphrase respectively for the previously selected hashes.
   - Click **Save** to apply the administration and then click **Close**.

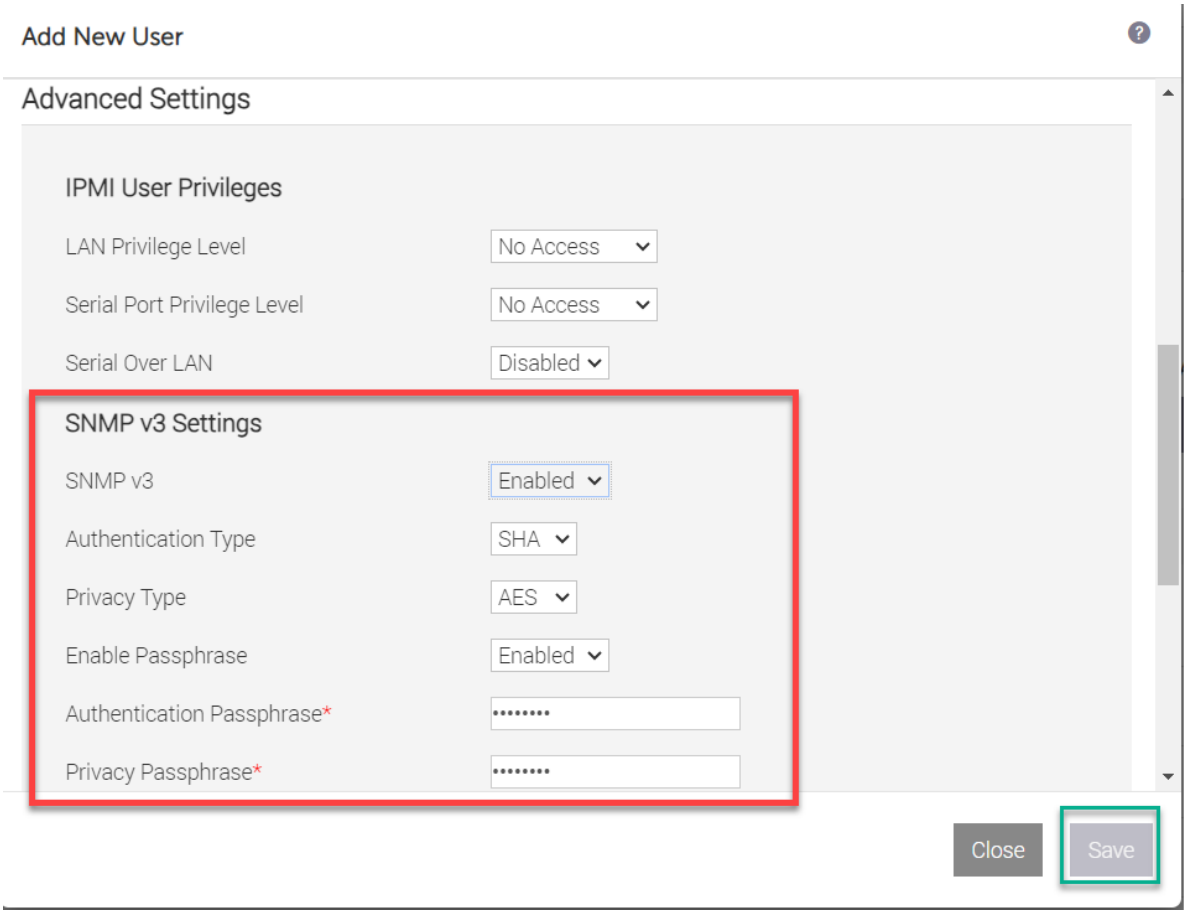
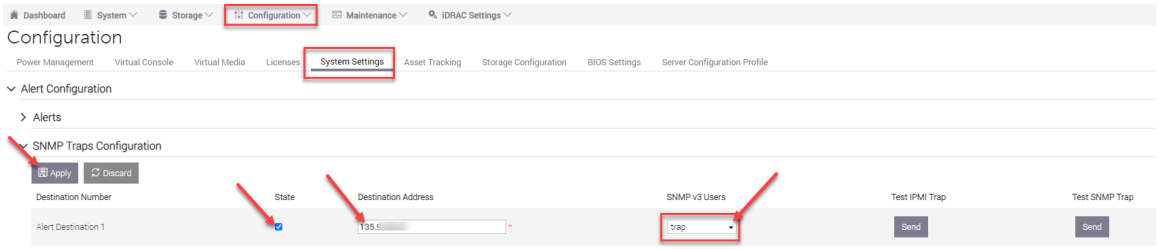


Figure 34: Adding a New User

7. Return to **Configuration** > **System Settings** > **Alert Configuration** > **SNMP Traps Configuration**.
   - Enter the IP address of the SAL GW in the **Destination Address** field. If there is more than 1 destination address, enter those addresses in the next Destination Address field below.
   - Click the **State** box to enable SNMP traps to be sent to the administered location.
   - Click the **SNMP v3 User account** to be used for this destination address. This should populate with the user enabled for snmp v3 configured in the previous steps 4-6.
   - Click **Apply** to submit the new administration.



8. Under the **SNMP Settings** area:
   - Enter the desired community string.
   - You may leave the default of alert port 162; this is the standard SNMP receiving port. You may also enter a different port number, but remember to match this port in both the sending and receiving devices.
   - From the drop-down menu for **SNMP Trap Format**, select **SNMPv3**.
   - Select **Apply** when settings are complete.

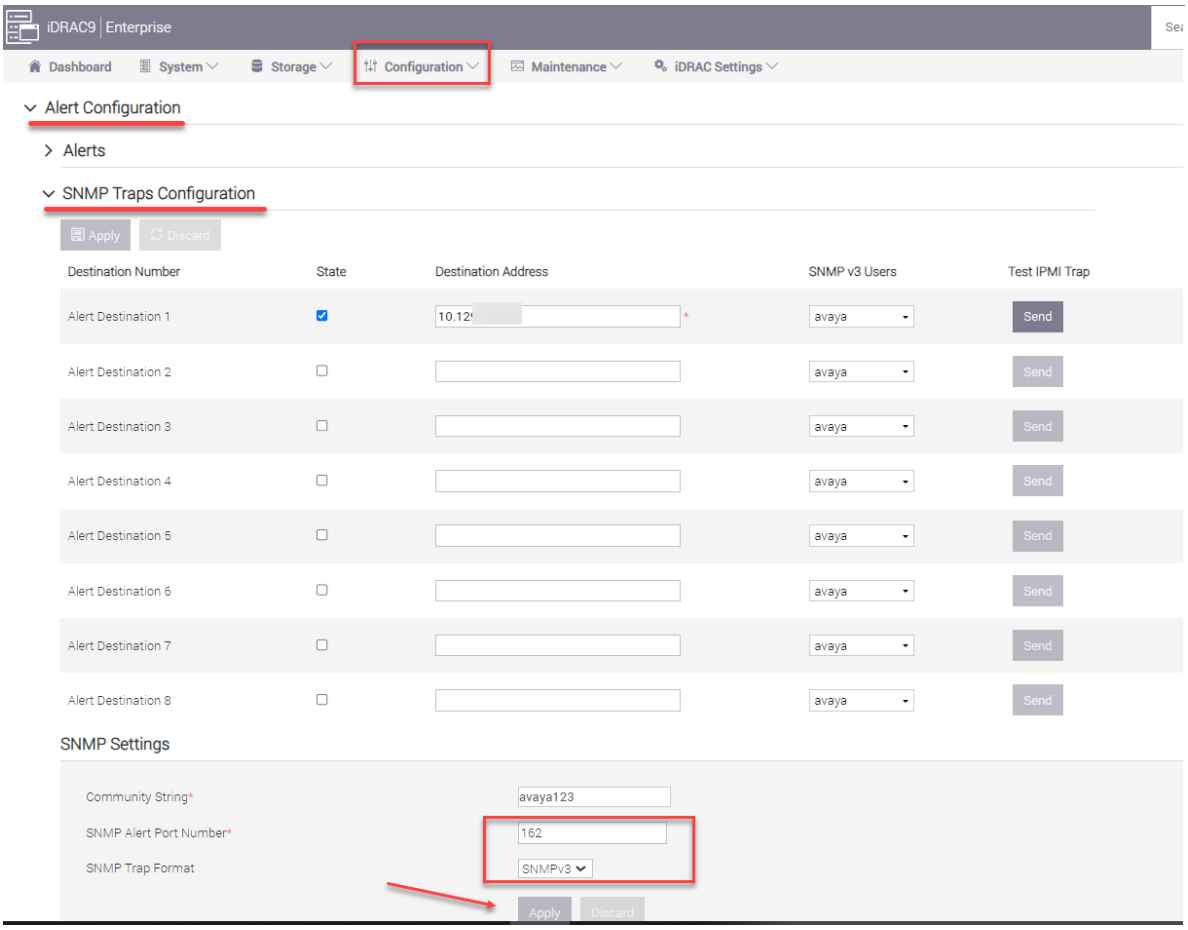


Figure 35: Configuring SNMP Traps

9. After the trap receiver device has also been administered, click the **Send** button under the **Test SNMP Trap** column (related to the specific device), to confirm the receipt of SNMP traps from the iDRAC.

Chapter 14: Additional Configuration Guidelines

This section describes additional configuration guidelines while performing installation for Avaya Solutions Platform 130 and provides topology examples.

Preface

Intended Audience

This chapter is intended for Avaya professional services, partners, and customers that have been tasked to install and configure an ASP 130 Release 6.0.x.

Purpose

The purpose of this chapter is to guide the ASP 130 certified technical professional in understanding the ASP 130 best practices and instructing how to implement these best practices in a customer's environment.

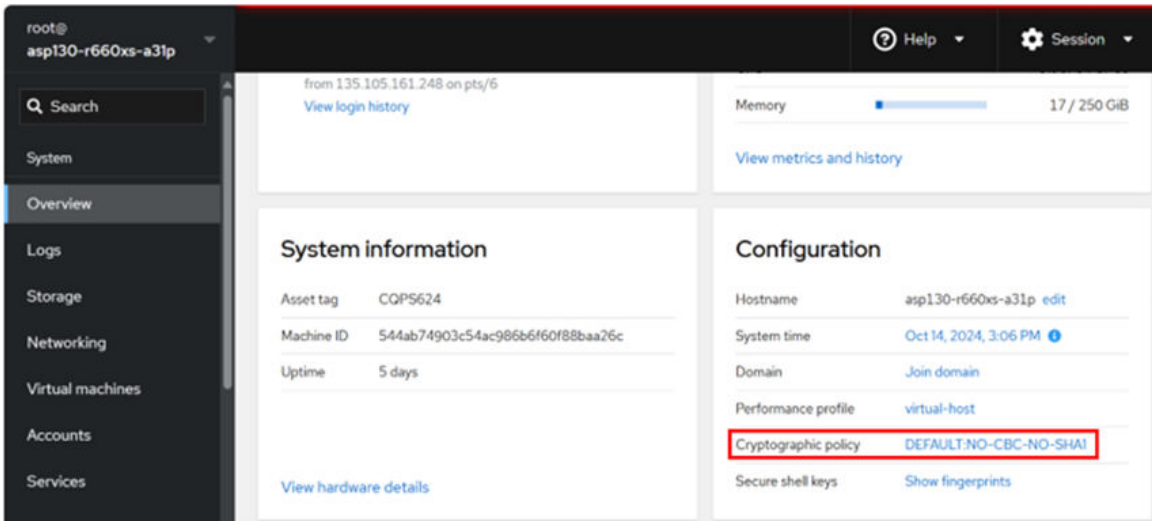
Scope

This chapter only includes the procedures and steps to implement suggested ASP 130 best practices that may improve usability, manageability, security, or performance.

TLS protocol configuration for KVM on RHEL 8.10 Environment

ASP 130 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)

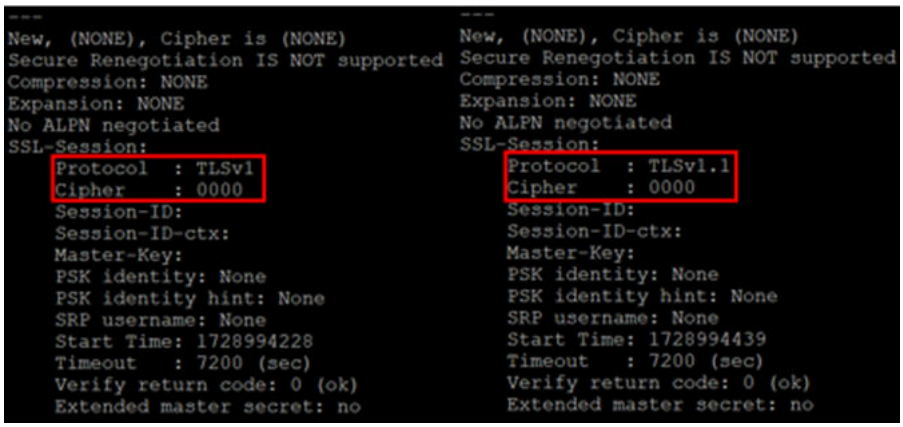
About this task

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:



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

Note:

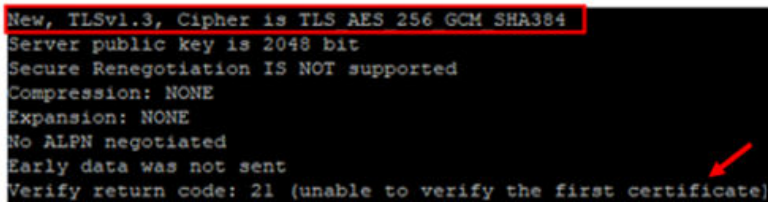
The system will not be able to verify server's identity and certificate unless the installed SSL certificate has been signed by a trusted Certificate Authority. Verify return code: 21 (unable to verify the first certificate) will be displayed. With an SSL certificate Verify return code: 18 (self signed 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 115 for more details.

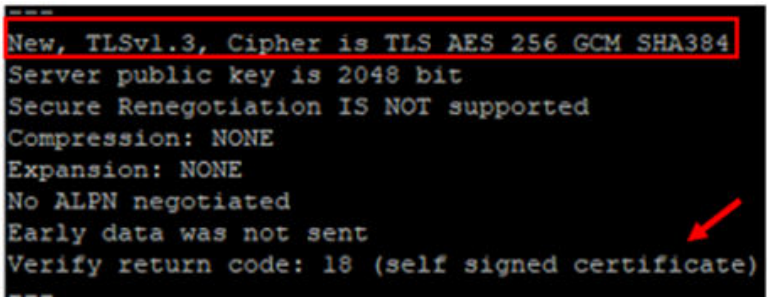
TLS v1.2:

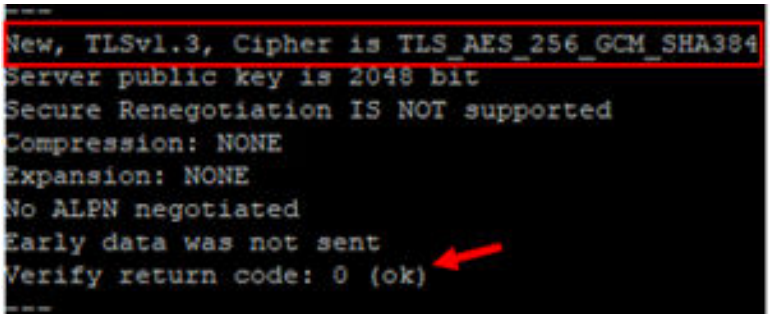

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-RSA-AES256-GCM-SHA384
Session-ID: D3326E0EA86133CCE38E22C2C62C19FA9BBAA435E155BC061EF797B43EAFF8A1
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: 396175A39788BD7D487672FE82D9090A7840D7376FB01C83F55BC7233DD5A196
Session-ID-ctx:
Master-Key: 7FC423BD35FD43816368367D2DEA568BE42BC231E9D3E47DAAF1247A5F8AEF1E6D410F69BAD7F0C4B90D69F57FABAEAE
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 15: Application Deployment on the ASP 130

Application Deployment on the ASP 130

Refer to the application specific deployment guides for the procedure to install the application software on a stand-alone ASP 130 server.

ASP 130 R6.0.x Release Notes maintains a list of applications that are currently supported on ASP R6.0.x. Until an Avaya application is listed as compatible with ASP R6.0.x in the Product Compatibility Matrix on support.avaya.com, and the application has published detailed instructions for deployment on ASP R6.0.x, the application is not considered certified and therefore is not supported.

Before deploying any virtual machines, refer to the *Policies for technical support of the Avaya Solutions Platform (ASP) 130* R6.0.x.

Note:

- Avaya Aura® 10.2 KVM specific images are currently only supported on ASP 130 R6.0.x and ASP S8300 6.0.x. Deployment in a customer-provided KVM on RHEL environment is not allowed.
- SMGR/SDM and SDM Client are not supported at this time for deployment of applications on ASP R6.0.x.
- When available, Avaya Aura® 8.1.x applications cannot be installed using Cockpit. Installation is done using the CLI. Reference individual application deployment guides for details.
- Deployment of application images must follow the A1S configurator host assignment and application footprint.

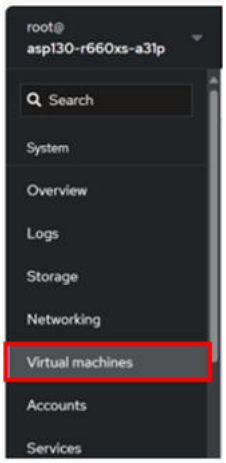
Enabling Autostart on Virtual Machines using the Cockpit UI

About this task

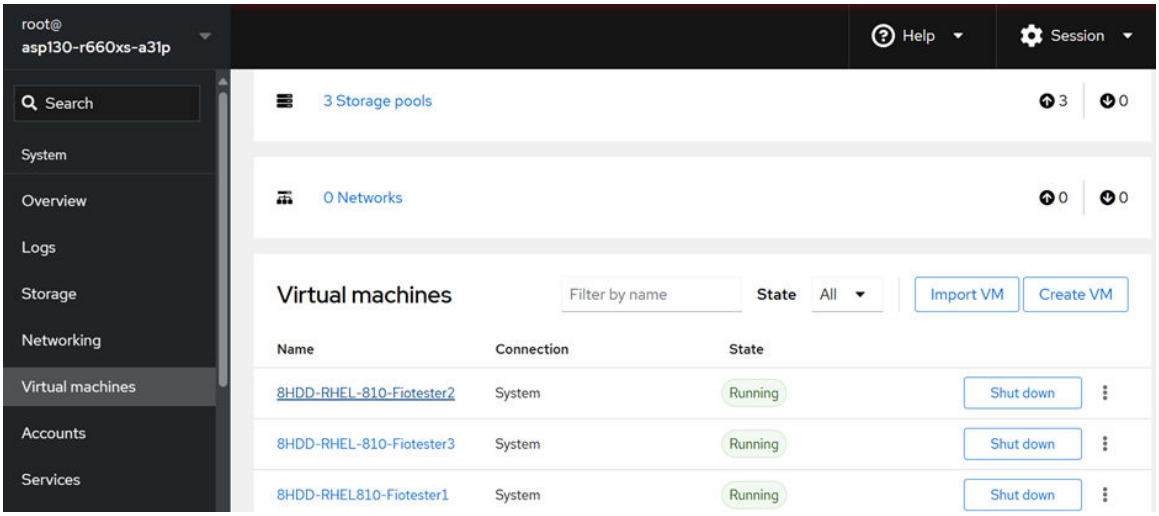
Autostart is disabled on the VMs by default and must be enabled manually for the VMs to start automatically after a reboot of the ASP 130 KVM on RHEL host. Conduct the following steps to enable Autostart on a VM:

Procedure

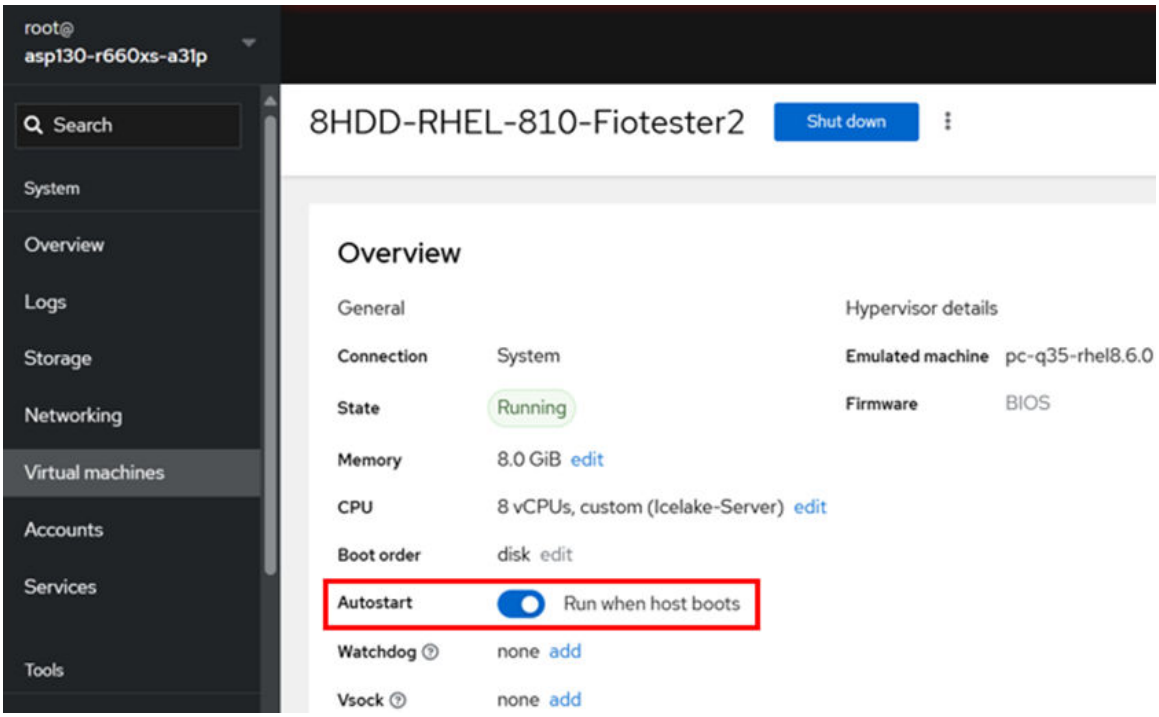
1. Open a web browser to the Cockpit UI `https://server_ip_fqdn:9090/` and log in with the `custadm` or root credentials.
2. From the left pane, go to **Virtual Machines**.



3. Click a VM from the list.



4. Under the Overview section, locate **Autostart** and toggle it on to enable it.



5. Rerun this procedure for all VMs.

Chapter 16: Virtual Machine Backup (clone) – alternative to snapshot

Virtual Machine Backup overview

Many Avaya products that are certified to deploy on Avaya Solutions Platform (for example, Avaya Aura® documentation) refer to snapshots at the application level for various procedures. Snapshots apply to a VMware environment.

With the introduction of the alternative hypervisor in Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), Red Hat does not support VM snapshots on RHEL 8.10. While the command may be present in the OS, use of the command is not allowed as the resulting snapshot will be corrupt.

Virtual Machine Backup (clone) is a feature similar to snapshots. Virtual Machine Backup uses the cloning feature. Use virtual machine backups in place of snapshots for KVM on RHEL 8.10.

Reference application specific documentation for detailed instructions on how to utilize the Virtual Machine Backup (clone).

Note:

Use of the Virtual Machine Backup (clone) requires that the virtual machine be powered off. The space needed for a Virtual Machine Backup is equivalent to the size of the Virtual Machine that is being backed up. It is critical to remove Virtual Machine Backups as soon as possible, no later than 48 hours after they are created, and to always assess available disk space prior to performing a Virtual Machine Backup.

Chapter 17: 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
- iDRAC Support Assist file
- 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.

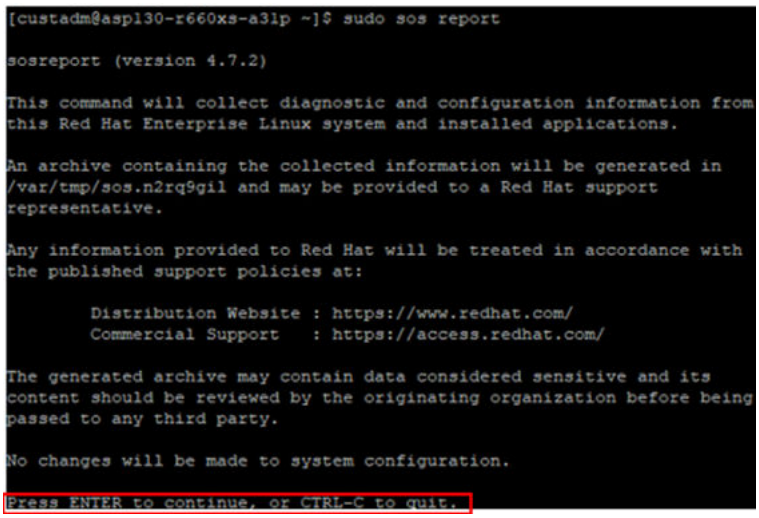
Procedure

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

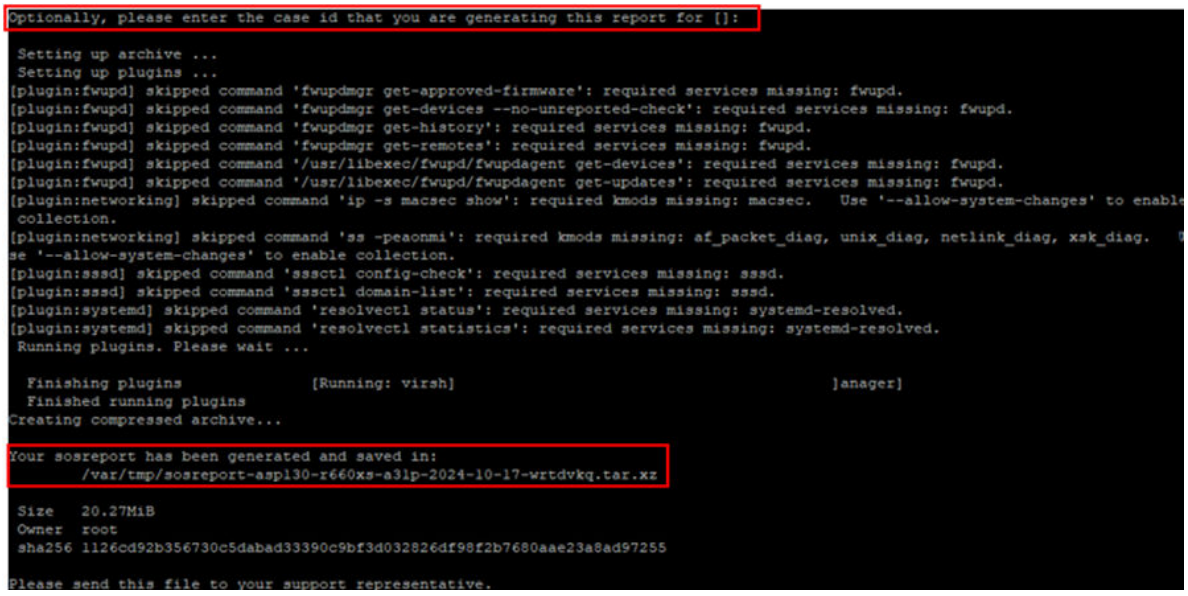
   Note:

   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.



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.



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.

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.

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

About this task

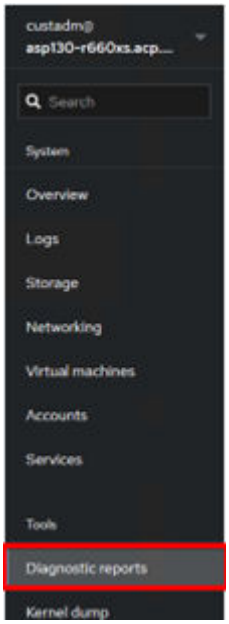
Examples below may reference ASP 130 but will be similar output for ASP S8300.

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.

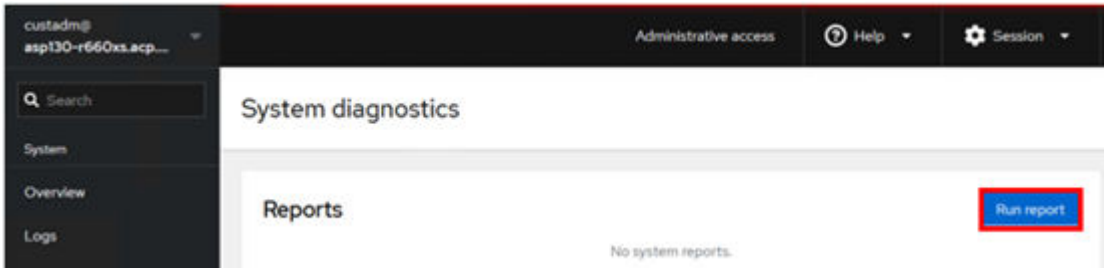
Procedure

1. Open a web browser to the Cockpit UI `https://server_ip_fqdn:9090/` and log in with the `custadm` or root credentials.

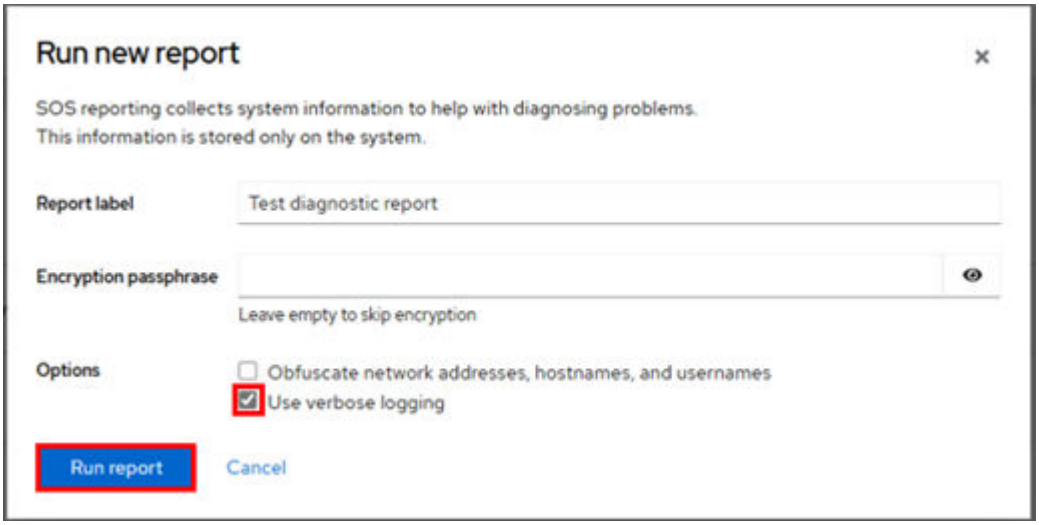
2. From the left pane, go to **Diagnostic reports**.



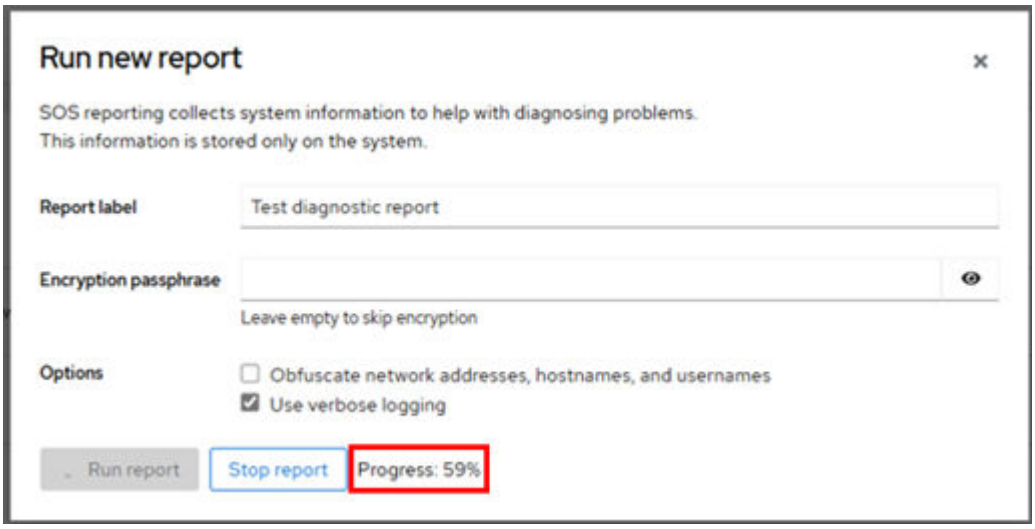
3. Click **Run report**.



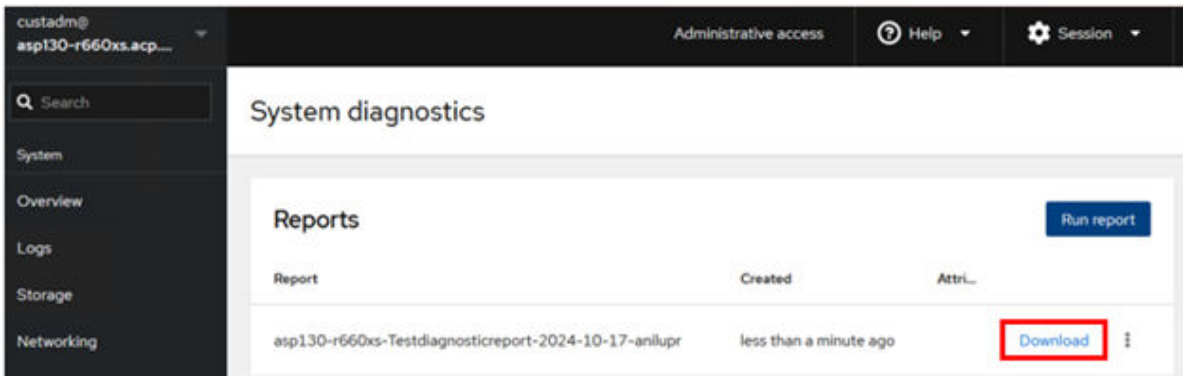
4. Enter the report label and in Options, check **Use verbose logging**. Click **Run report**.



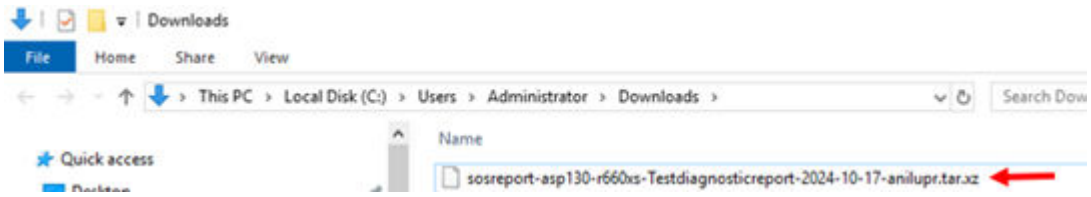
Progress is displayed at the bottom.



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



A `tar.xz` file is downloaded.



Collecting an iDRAC Support Assist file

About this task

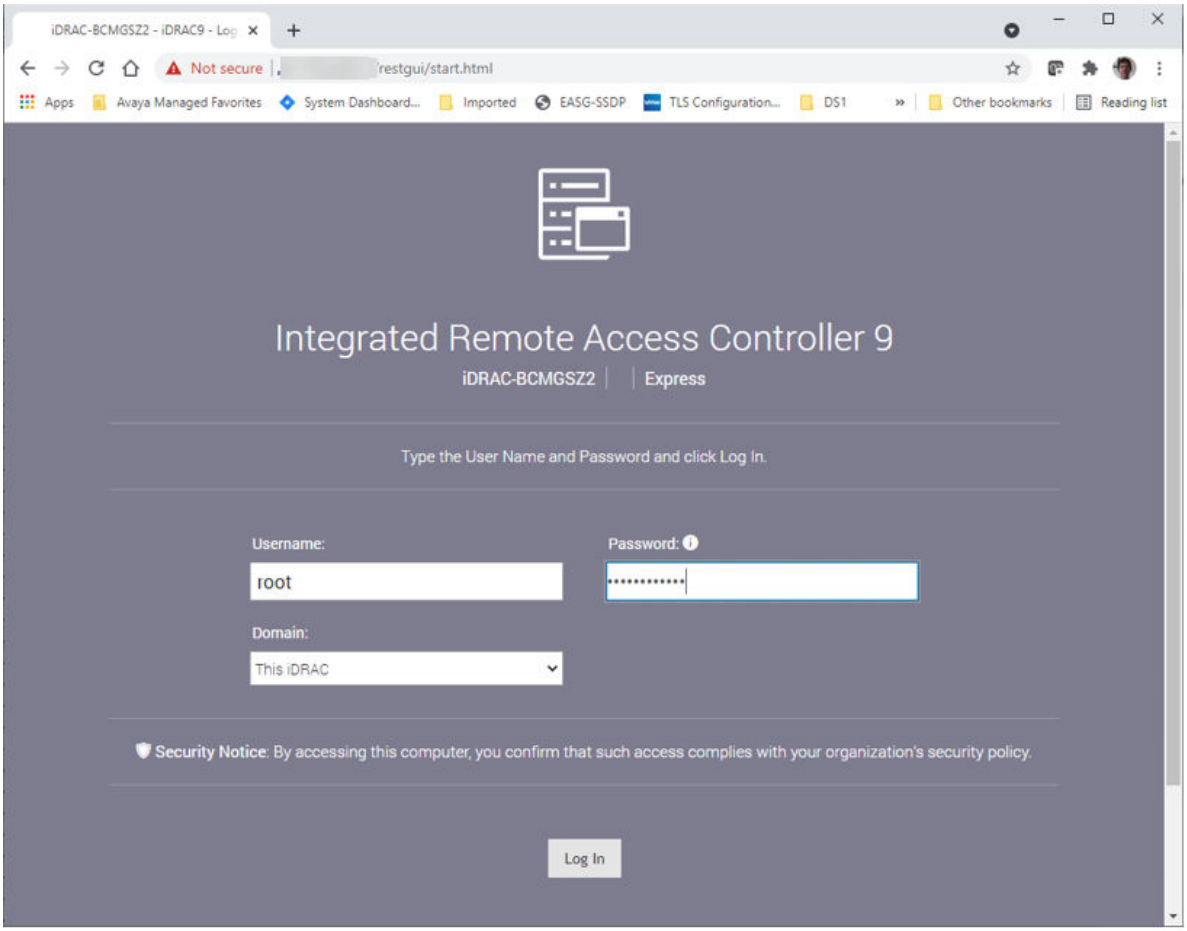
When there is an issue with the ASP 130 server a Support Assist file may need to be generated for debugging purposes. When opening a service request with Avaya this file may be required.

Before you begin

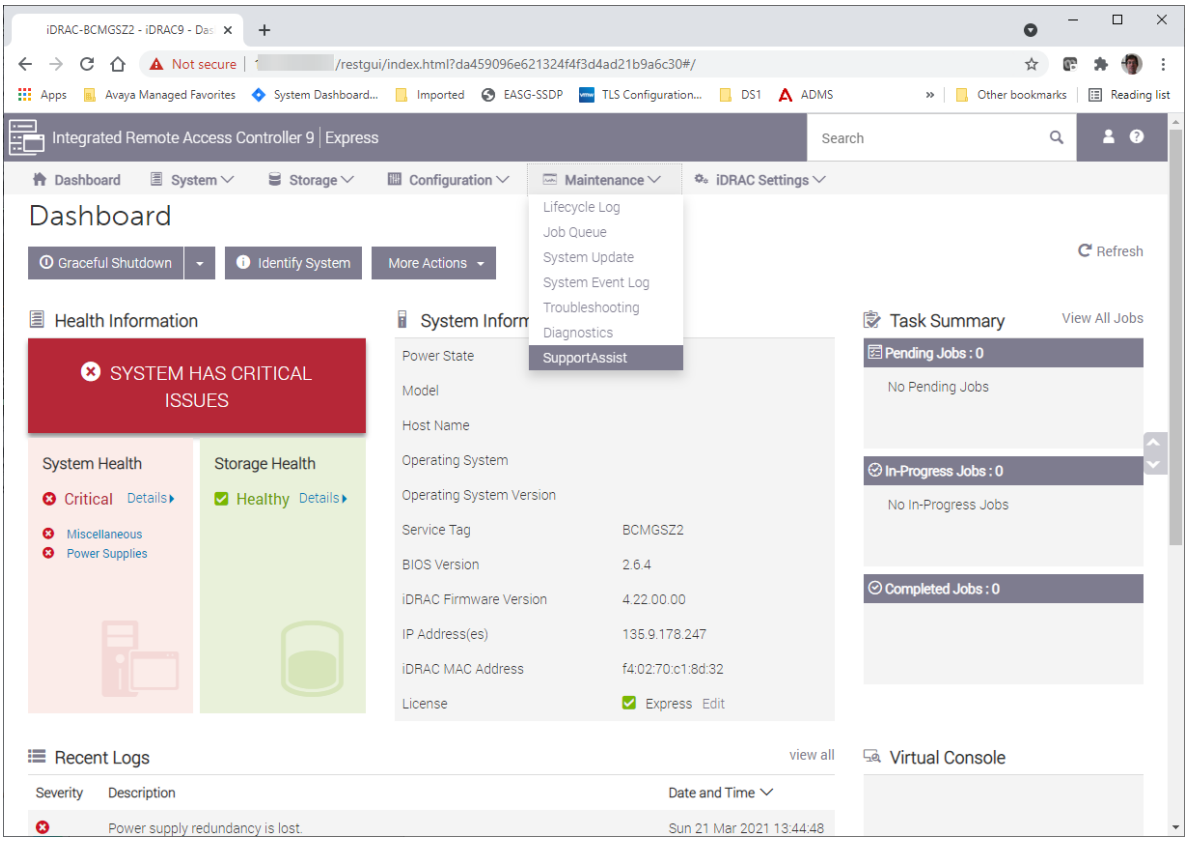
- iDRAC should be enabled and network settings configured accordingly.
- iDRAC should be reachable over the customer's network or an on-site resource available for direct connect to the iDRAC.

Procedure

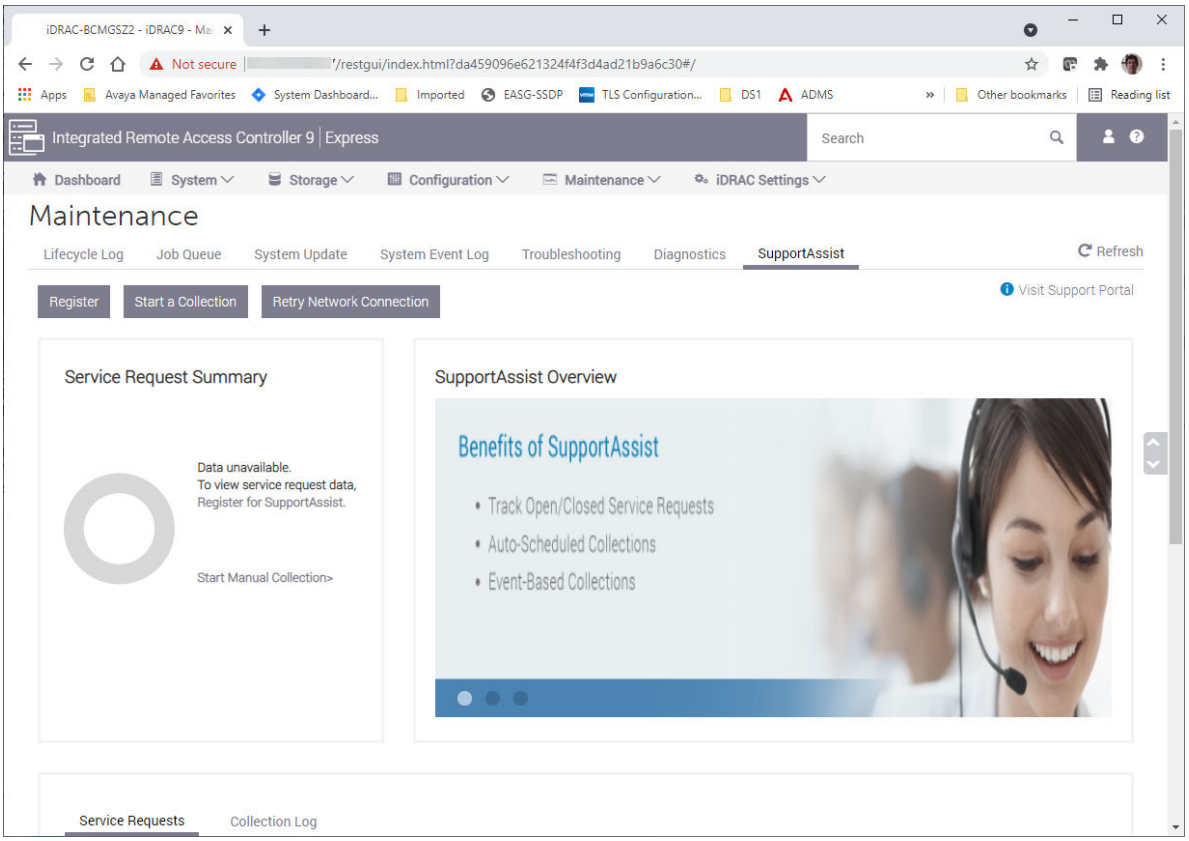
1. Open a browser and login to the iDRAC web interface using the `root` or equivalent account:



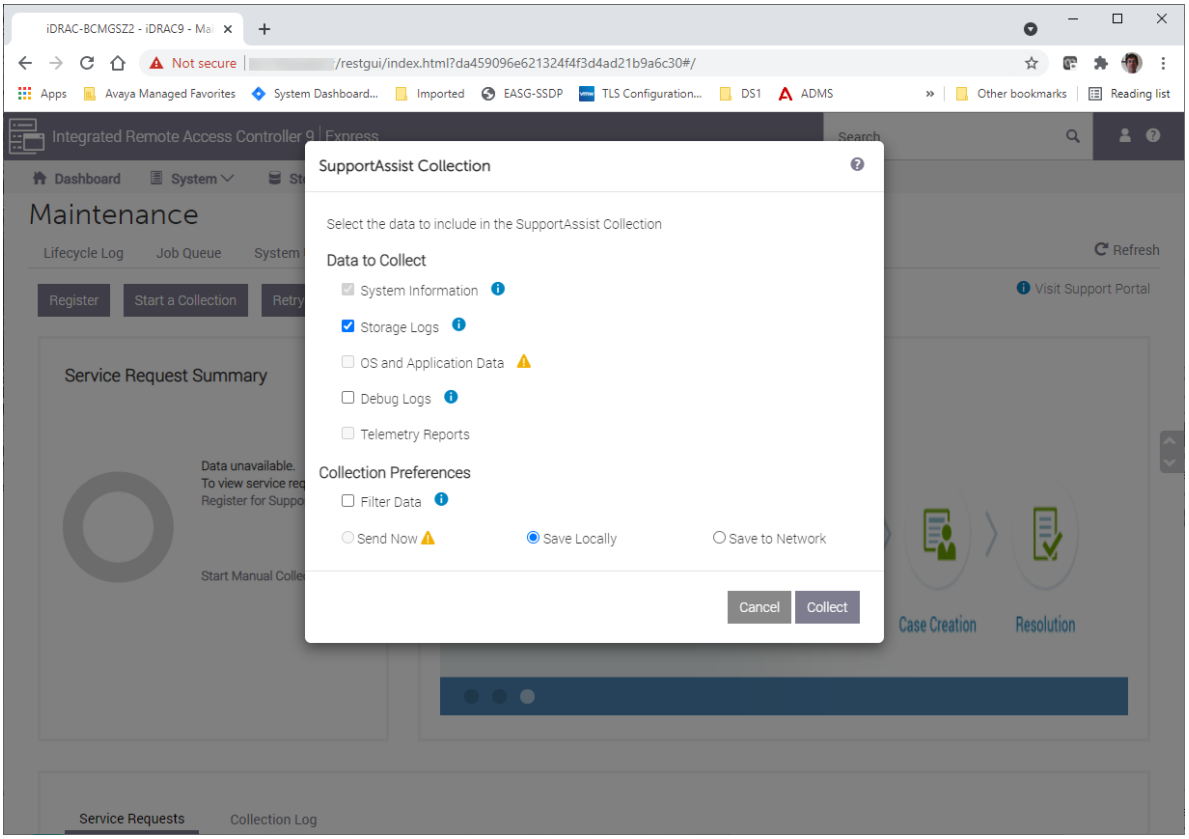
2. Select **Maintenance** > **SupportAssist** from the main screen:



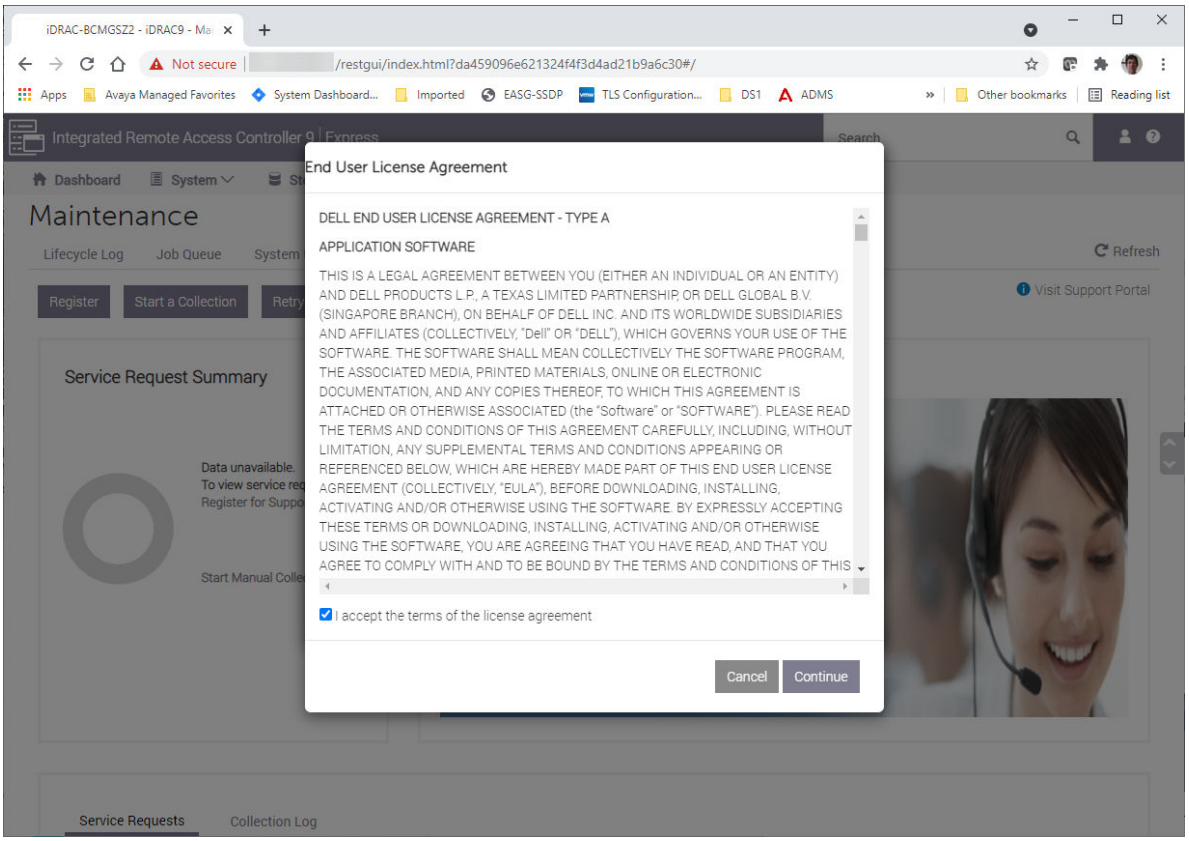
3. In the **SupportAssist** screen, select **Start a Collection**:



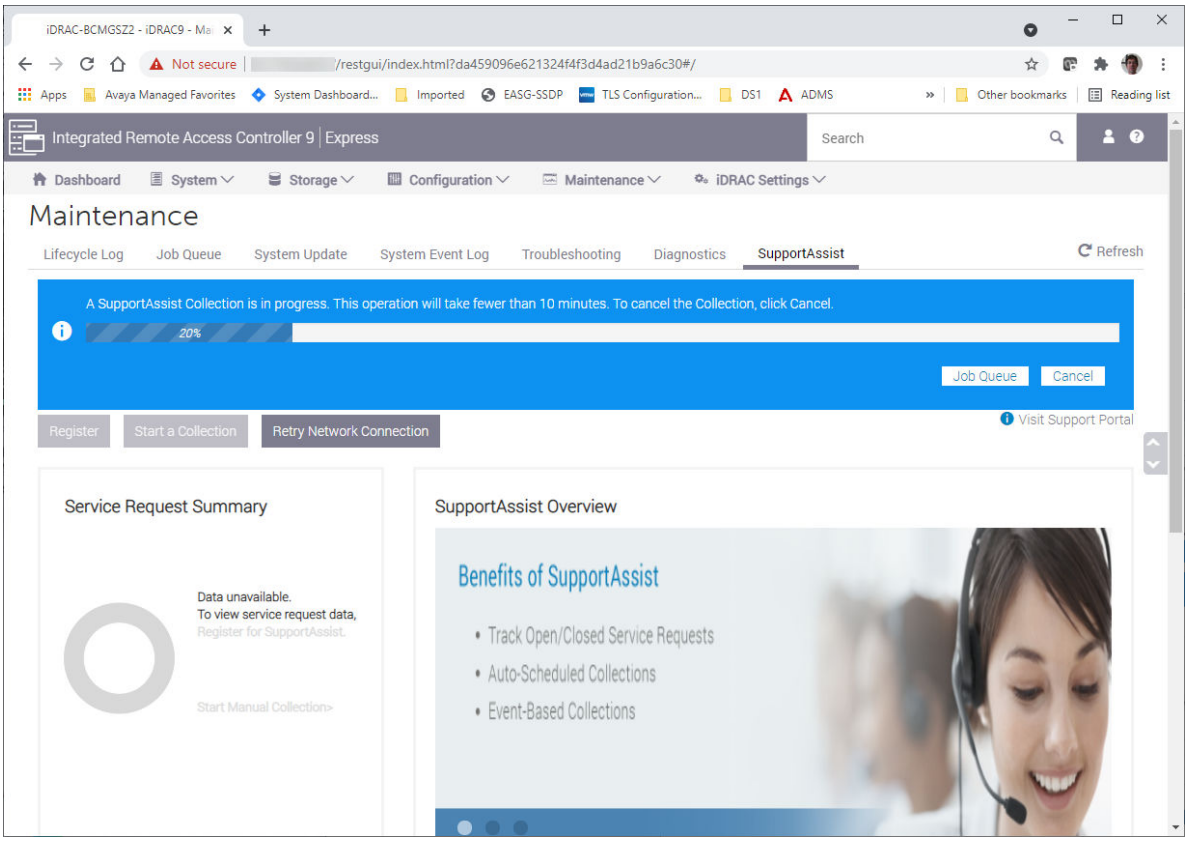
4. In the Collection pop-up, keep the defaults of **System Information** and **Storage Logs** and save locally unless instructed otherwise by Avaya support. Then click on the **Collect** button.



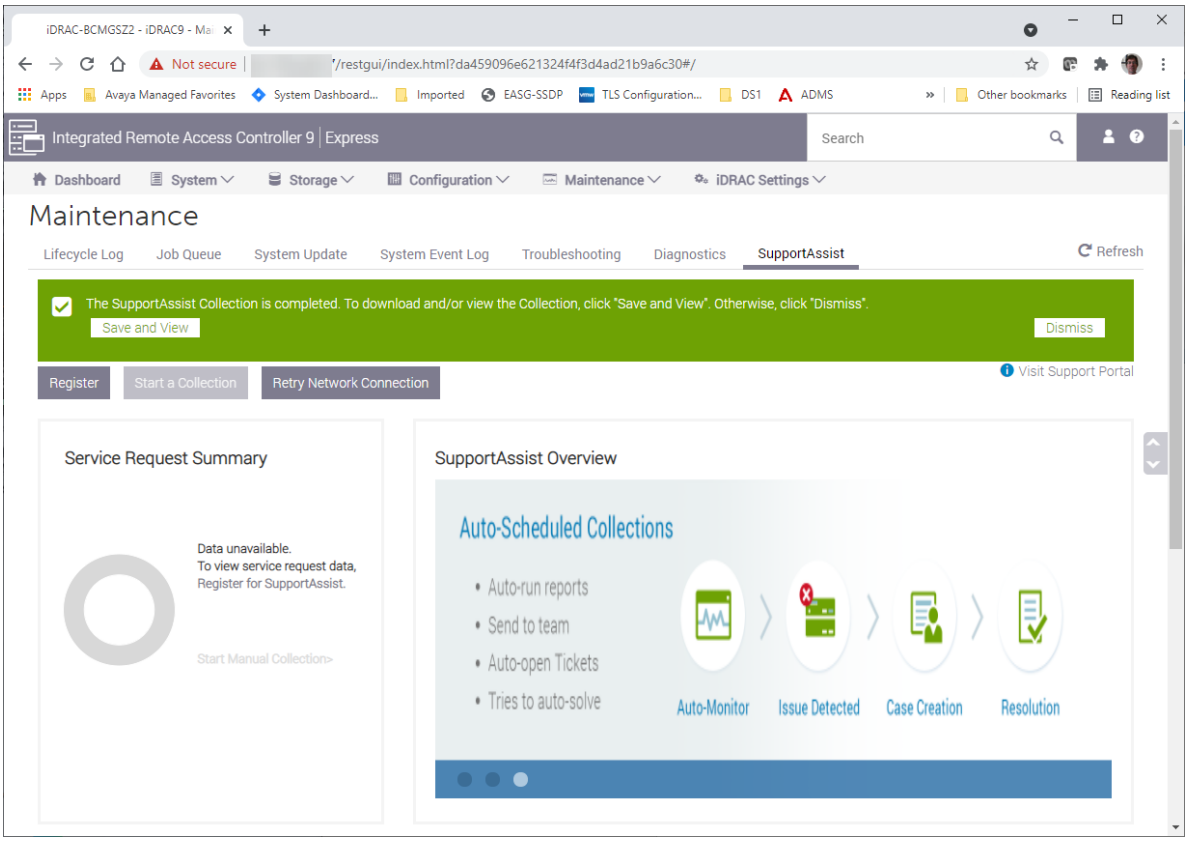
5. Accept the terms of the License Agreement and click **Continue**:



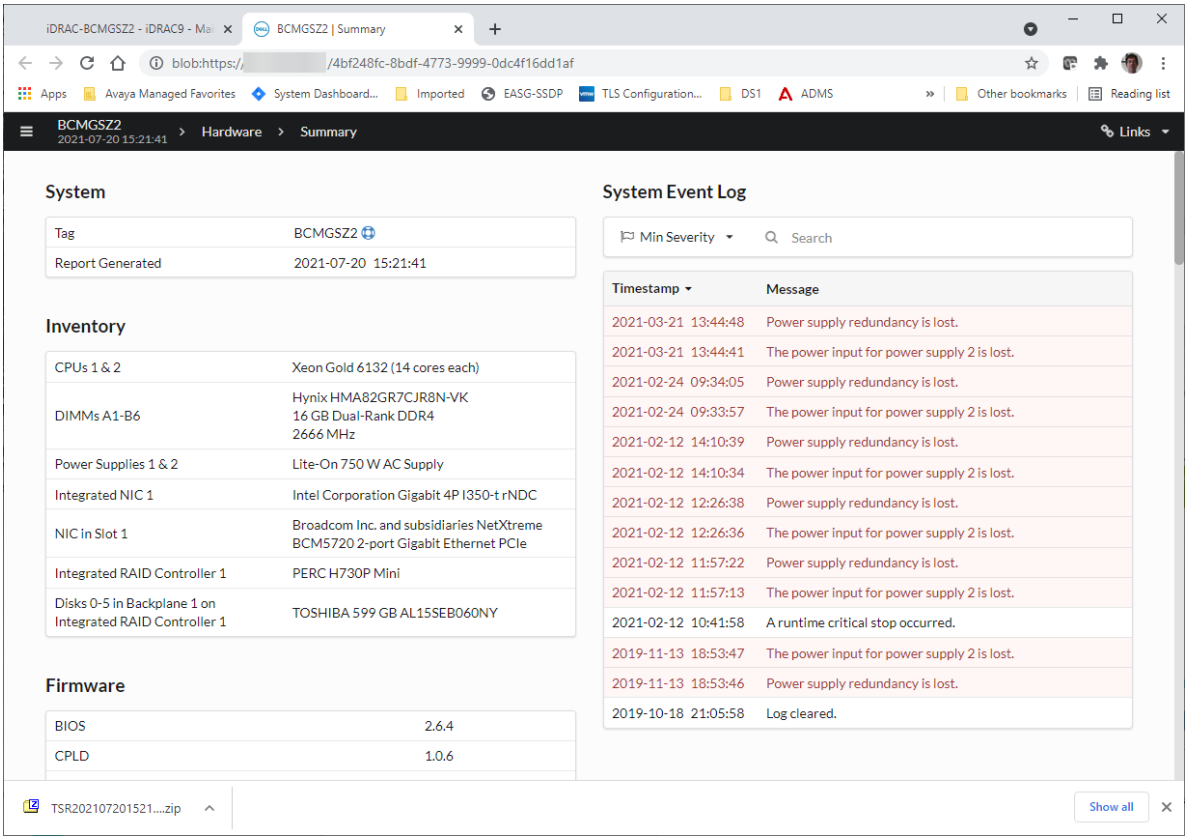
6. This will start the collection and show the progress of the data collection:



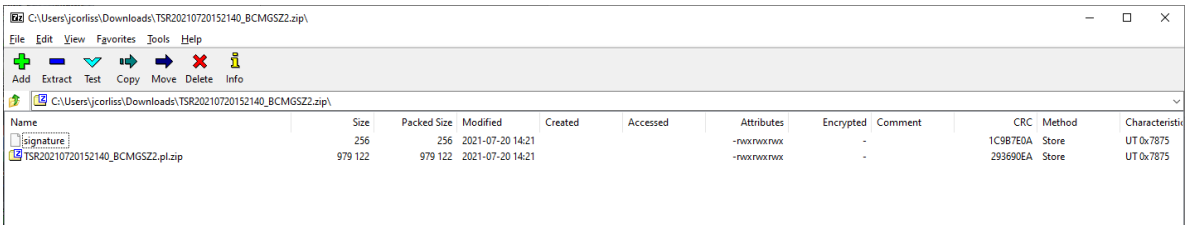
7. When completed you can save the file to your PC – select **Save and View**:



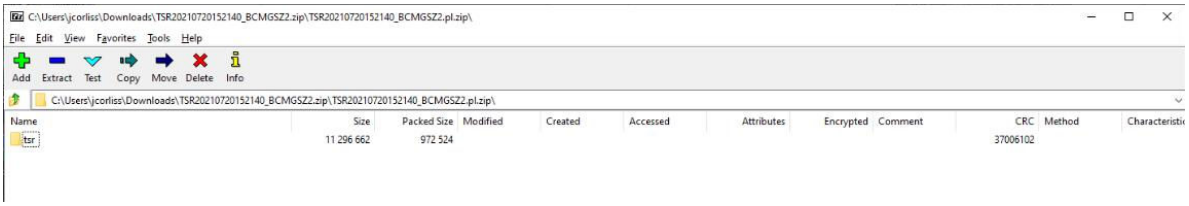
8. This will open a new tab and allow you view the data in a GUI format. It will also download a .zip file of the same information for later viewing:



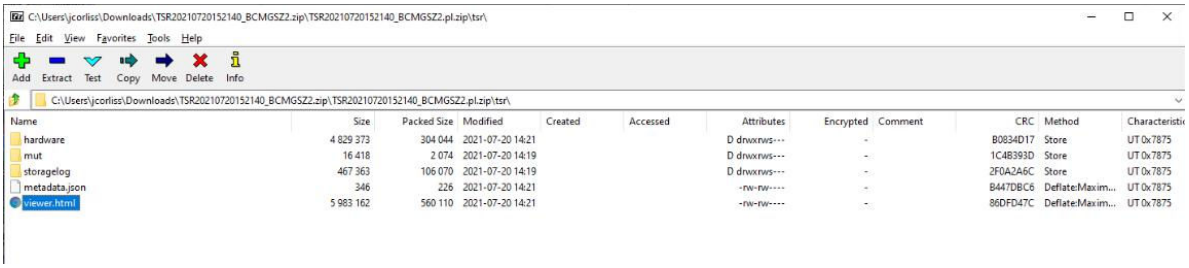
9. To view the same data at a later time from the zip file open the zip file in an archive manager such as 7z:



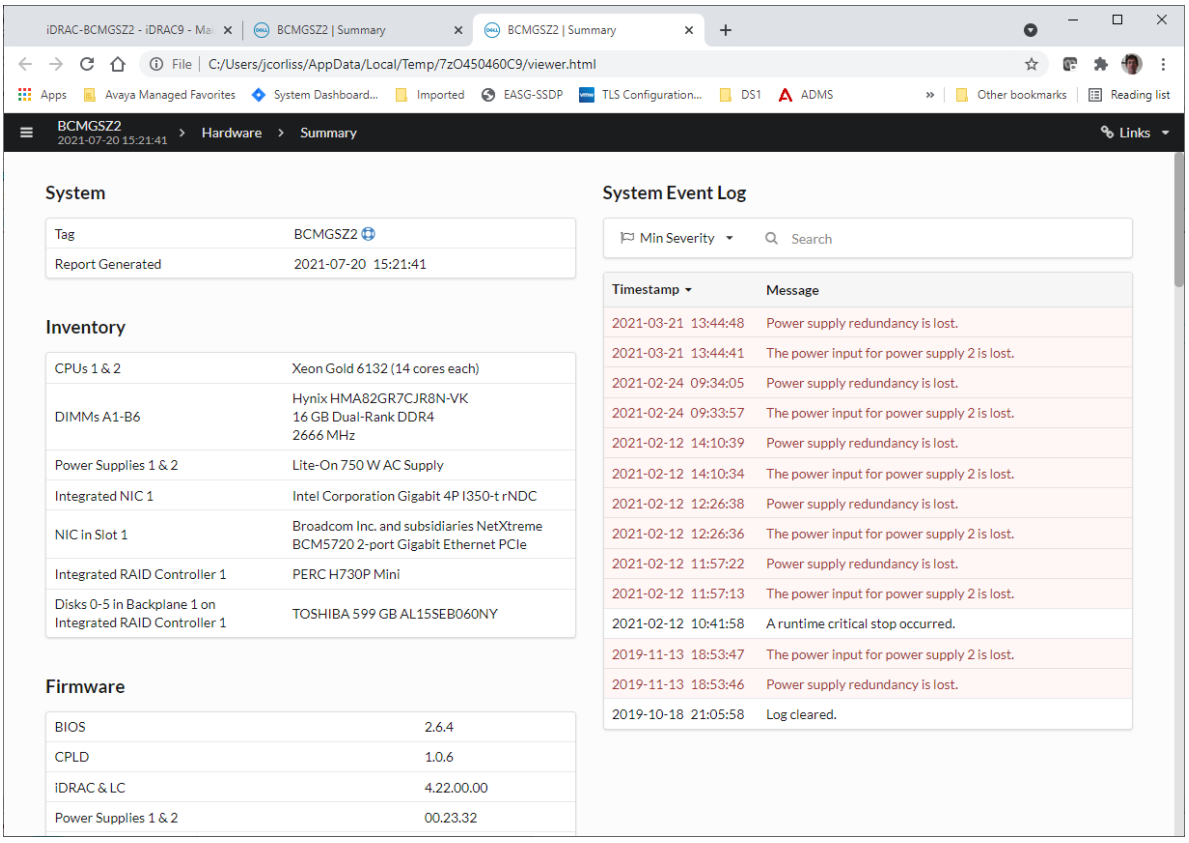
10. In the archive manager, click on the embedded zip file to extract that data. This will present a folder named **tsr**:



11. Open the **tsr** folder. In 7z there is no need to do any further extraction of file to disk. Now select the file named **viewer.html**:



12. Opening the **viewer.html** file will open a tab in your default browser and allow you to browse the **SupportAssist** data:



13. The zip file originally collected may be requested by Avaya support personnel to assist in troubleshooting. Do not contact Dell for assistance or send this output bundle to anyone but your Avaya support team.

Chapter 18: Regulatory Information

Regulatory Information

For a complete listing of the DELL PowerEdge R640 and R660xs regulatory information, navigate to the following:

PowerEdge R660xs - https://www.dell.com/support/home/en-us/product-support/product/poweredge-r660xs/docs and select **Regulatory Information** from the left pane.

PowerEdge R640 https://www.dell.com/support/home/en-us/product-support/product/poweredge-r640/docs and select **Regulatory Information** from the left pane.

Chapter 19: Resources

Avaya Solutions Platform 130/S8300 documentation

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

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

Table continues…

Title	Description
ASP 130 R6.0.0.4.0 and Later VLAN & VLAN TRUNKING CONFIGURATION GUIDE	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.
ASP 130 R6.0.0.3.0 and Earlier VLAN & VLAN TRUNKING CONFIGURATION GUIDE	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.
Port Matrix for ASP S8300	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.
Port Matrix for ASP 130	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.
Policies for technical support of the Avaya Solutions Platform (ASP) 130 and S8300E R6.0.x	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.
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes the best practices of using the Integrated Dell Remote Access Controller (iDRAC).
PSN027113u - Avaya Solutions Platform 100 Series Dell® R660xs Avaya Certified BIOS/Firmware Update, Version 2	Always check for a newer version of Avaya certified BIOS/Firmware. New PSNs are published for each new release.

Table continues…

Title	Description
PSN027112u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 16	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.
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)	**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.
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.3.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.2.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)	

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 http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index

K

L

N

O

P

R

S

T

V

W