Installing the Avaya Solutions Platform 130 Series

Release 5.1.x
Issue 11
September 2024

Notice

Documentation disclaimer

Link disclaimer

Warranty

Hosted Service

Licenses

Copyright

Virtualization

Third Party Components

Service Provider

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

Contents

Chapter 1: Introduction

Purpose

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

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

Avaya Solutions Platform 130 Appliance was formerly called Avaya Converged Platform 130 Series (ACP 130). This document might still refer to Avaya Solutions Platform 130 Appliance as Avaya Converged Platform 130 Series or ACP 130 in some places.

Change history

Issue	Date	Summary of changes
11	September 2024	• Updated the document list in Avaya Solutions Platform 130/S8300 documentation on page 189. • Cosmetic updates, including image resizing and formatting adjustments throughout the guide.
10	August 2024	Updated Chapter 8 to reflect the following licensing changes in ASP R5.1.0.5: • All NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. • A unique standard license key will be provided on a label on the ASP 130 server lid.
9	April 2024	Updated Resources section to reflect ASP 5.1.0.4 and Avaya Certified BIOS/Firmware Update, v13.
8	January 2024	• Updated a bullet point about the Host Management Network Port Group in OOBM mode configuration in ASP 130 on page 68. • Added a note in Configuring OOBM on ASP 130 before deploying VMs on page 70 and Configuring OOBM on ASP 130 after deploying VMs on page 73.

Table continues…

Issue	Date	Summary of changes
		• Modified procedural steps and replaced a few screenshots in Reconfiguring vmk0 IP Address after enabling OOBM in ASP 130 on page 77. • Added a note in Disabling OOBM on Avaya Solutions Platform 130 on page 81. • Modified procedural steps in Reconfiguring vmk0 IP Address after disabling OOBM in ASP 130 on page 84.
7	December 2023	Updated the following sections: • Avaya Solutions Platform 100 series overview • Supported software • What's New in Avaya Solutions Platform Release 5.1.x. • Avaya Solutions Platform Appliance profiles. • Registering a new device. • Viewing the status of your registration request. • Registering device after ASP 120 migrates from AVP 8.1.x to ESXi 7.0. • Installing the server. • Configuring ESXi Network Settings. • Chapter 6: Services Port Verification • Configuring OOBM on ASP 130 before deploying VMs. • Configuring OOBM on ASP 130 after deploying VMs. • Disabling OOBM on Avaya Solutions Platform 130. • Reconfiguring vmk0 IP Address after disabling OOBM in ASP 130. • Performing server recovery and/or software remastering. • Software remastering. • Installing the Avaya Enhanced Access Secure Gateway. • Signing the Certificate Signing Request (CSR) by an Organizational CA. • Configuring SNMP v2c using iDRAC9. • Configuring SNMP v3 using iDRAC9. • How to Query for SNMP EngineID. • Chapter 12: Additional Configuration Guidelines • Updating the NIC Teaming configuration on a standard vSwitch. • ASP 130 TLS protocol configuration for vSphere 7.0 Environment. • Application Deployment on the ASP 130.

Table continues…

Issue	Date	Summary of changes
		• Deploying an OVA using the ESXi VMware Host Client. • Setting Autostart values on VMware Host Client deployed VMs. • Avaya Solutions Platform 130 documentation. • Viewing Avaya Mentor videos
6	August 2023	Updated the shell script name from `asp_oobm_v1.sh` to `asp_oobm_v2.sh` throughout the document.
5	June 2023	Updated the shell script name from `asp_oobm_v1.sh` to `asp_oobm_v2.sh`.
4	January 2023	Updated the document to include Release 5.1.x changes.
3	November 2022	Updated sections to depict R640 hardware changes of H730P Mini to H750 Adapter and Intel 4x1GbE NDC to Broadcom 4x1GbE NDC. Tentatively targeted for 4QCY2022.
2	July 2022	Updated the “Registering device after ASP 120 migrates from AVP to ESXi” section. Added “Chapter 7: Securing Network Configuration on Avaya Solutions Platform 130”.
1	April 2022	Release 5.1 document.

Prerequisites

Before installing or migrating Avaya Solutions Platform 130, ensure that you have the following knowledge, skills, and tools.

Knowledge

- VMware ESXi installation and configuration.
- Avaya Virtualization Platform (AVP) administration (not required but helpful).

Skills

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

Tools

- Monitor, keyboard, mouse, and DVD burner for ESXi installation.
- Laptop for services port access.

Chapter 2: Overview

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 at Avaya's Integrator. ASP 110 base servers may consist of a Dell R240, R340, or R640 depending upon the configuration. (There is no ASP 110 Release 5.x. See ASP Release 4.0 documentation.)
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). AVP 7.1.3.3 or AVP 8.0.1 or greater is required. ASP 120 shipped with AVP 8.1 preloaded. AVP 8.1 is the final release and no longer supported with Avaya Aura® 10.x or ASP Release 5.x. ASP 120 can migrate to ASP 130. See ASP Release 4.0 and 5.x documentation.
3. ASP 130: This is the Dell R640 currently shipped from Avaya's Integrator with a VMware Standard ESXi 7.0 license preloaded.

Note:

This document focuses on Avaya Solutions Platform 130 Appliance (ASP 130) only. Avaya Solutions Platform 130 Appliance utilizes VMware vSphere ESXi 7.0 with a Standard License. Avaya does not permit or support the repurposing of Servers that deviate from their original integrated configuration.

Note:

The ASP S8300 solution was introduced with ASP **R5.1**. This is the S8300E that ships from Avaya's integrator with ESXi 7.0 already installed and the VMware Foundation Licensed preloaded.

Key features

The Dell PowerEdge R640 is the underlying 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.

Supported software

The Avaya Solutions Platform 130 Appliance supports virtualization. The Avaya Solutions Platform 130 Appliance uses an Avaya customized image of VMware vSphere ESXi 7.0 as the hypervisor.

Avaya Solutions Platform 130 Dell® R640 servers are supplied under 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 Avaya provided updates can be used. Updating BIOS, FW, or ESXi directly from the Dell or VMware's web sites will result 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 (https://support.avaya.com/css/P8/documents/101062774).

What's New in Avaya Solutions Platform Release 5.1.x

- EASG is supported starting with Avaya Solutions Platform Release 5.1
- A new directory (`/opt/avaya/etc/`) is created with both the Avaya Solutions Platform 130 zip upgrade file and the Avaya Solutions Platform 130 ISO install file. The Avaya Tools VIB will create this directory.
- The Avaya Solutions Platform 130 Release 5.1.x has the Avaya Tools VIB, which replaces the functionality of `Avaya-Config-v1` script file in the Avaya Solutions Platform 130 Release 4.0 and Release 5.0
  - In Avaya Solutions Platform 130 Release 4.0 and Release 5.0, the `Avaya-Config-v1` script file configured the services port and had to be copied to the shell and manually applied.
  - In Avaya Solutions Platform Release 5.1.x, this is no longer necessary. The Avaya Tools VIB is a part of the Avaya Solutions Platform 130 Release 5.1.x ISO and zip files.

- The Avaya Solutions Platform 130 Release 5.1.x ISO for fresh install, recovery or catastrophic/forklift migrations includes the Avaya Tools VIB.
    - The Avaya EASG VIB must be downloaded separately from PLDS and copied to the shell, and manually applied after the ISO is installed.
- The Avaya Solutions Platform 130 Release 5.1.x upgrade zip file contains the Avaya Tools VIB and the Avaya EASG VIB, thus no need to download the Avaya EASG VIB from PLDS.
    - The Avaya Solutions Platform 130 Release 5.1.x zip file is used for upgrades only.
- From Avaya Solutions Platform Release 5.1 onwards, **Autostart** is enabled and the **Autostart start delay** and **stop delay** fields are set to **0**.
- Reference to the latest Avaya Solutions Platform 130 Release Notes available on https://support.avaya.com for detailed information about each specific release.

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. Only Avaya provided updates can be used. Updating directly from the vendor’s web site will result 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 ESXi updates should only be obtained from Avaya. Updating directly from the hardware vendor or VMware’s websites will result in an unsupported configuration. Avaya creates a customized ESXi image based on VMware and Dell software packages. This ensures 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 VMware 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 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.
- 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.

Front view of Dell™ PowerEdge™ R640 Server

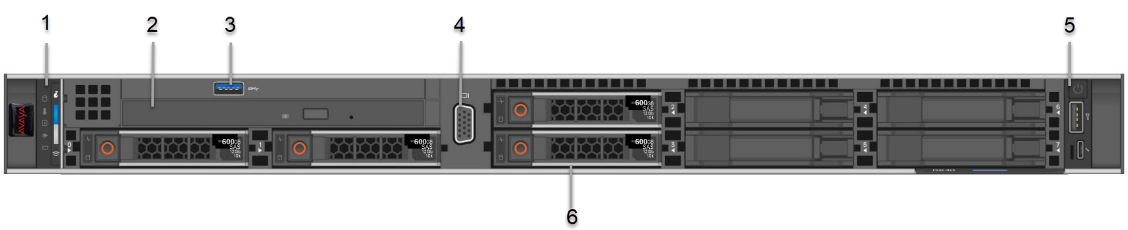


Figure 1: Front view of Dell PowerEdge R640 server

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.

Table continues…

No.	Item	Icon	Description
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.

Back 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 occur 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)

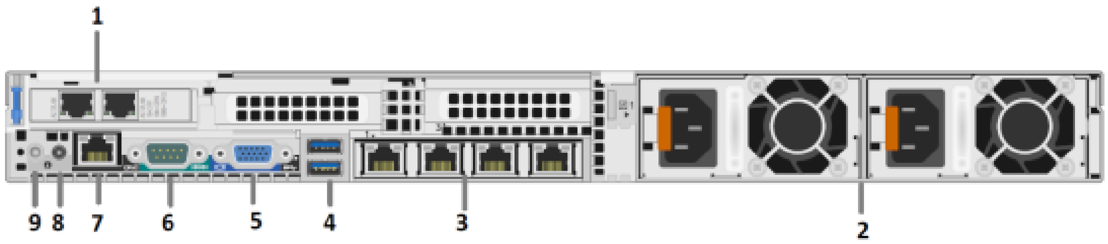


Figure 2: Back View of Dell PowerEdge R640 Single CPU Server with H730P Mini RAID Controller

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

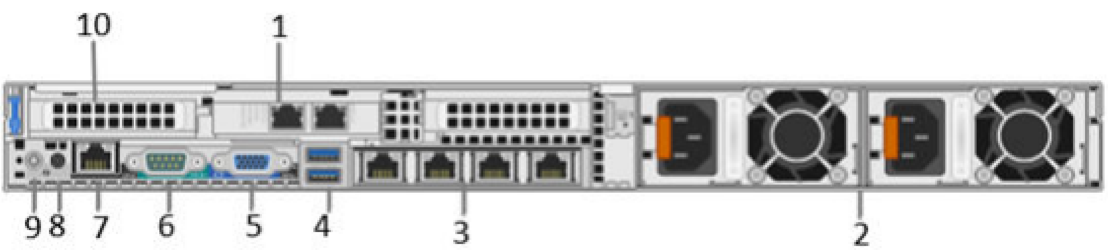


Figure 3: Back View of Dell PowerEdge R640 Single CPU Server with H750 RAID Controller Adapter

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

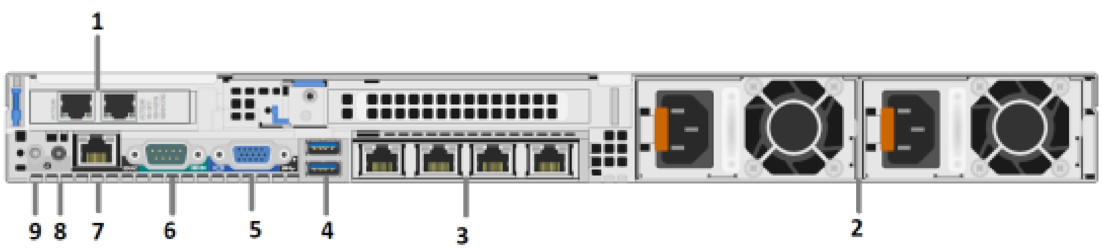


Figure 4: Back View of Dell PowerEdge R640 dual CPU Server with H730P Mini RAID Controller

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

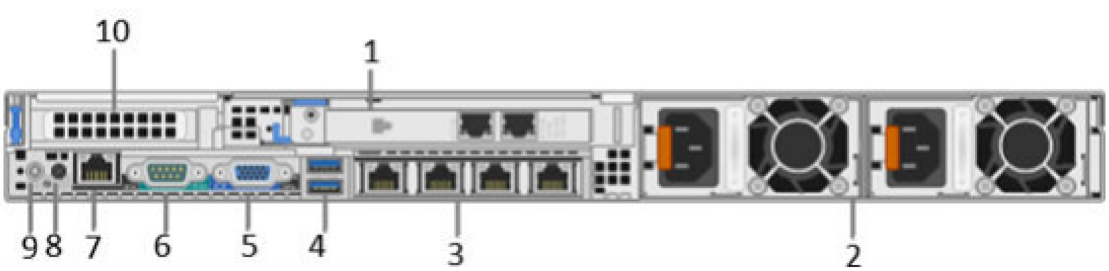


Figure 5: New Configuration of Dual CPU R640 server (H750 and Broadcom 4x1GbE NDC)

Table 1: 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 **vmnic 4&5 are numbered left-to-right.** In **single CPU** configurations the 2x1GbE NIC, located in PCI slot2 has a half-height PCIe faceplate and **vmnic 4&5 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. (vmnic0 – vmnic3 – Left to right viewing from rear of server)
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.

Avaya Solutions Platform Appliance profiles

In the Avaya Solutions Platform 100 Series, server constructs are shared among Avaya Solutions Platform 110 Appliance, Avaya Solutions Platform 120 Appliance, and Avaya Solutions Platform 130 Appliance. The first table below designates ASP 100 Series servers with Intel Skylake CPUs. Those CPUs are no longer shipping in ASP 100 Series servers and have been upgraded to Intel Cascade Lake CPUs as designated in the second table below. Both CPU types will support ASP

130 4.0, 5.0, and 5.1.x Releases. Base Server type (CPU Type) must be known when using the Avaya One Source (A1S) Configurator tool prior to any application upgrade.

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:

In the October 2020 time frame the ASP 130 Server CPU transitioned from a Skylake to the Cascade Lake CPU. The SAP order codes did not change. Refer to PSN020500u – *Avaya Solutions Platform ASP 1XX server platform*, it will have new base and FRU servers introduced but finished good / order codes remain the same for reference.

Table 2: 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	4	4	6	8
RAID Options	5	6	6	6	6
Usable Virtual Disk Capacity	1.2 TB	1.2 TB	1.2 TB	2.4 TB	3.6 TB
Network 1 Gb ports	6	6	6	6	6
Power Supplies (750W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

Table 3: Cascade Lake CPUs

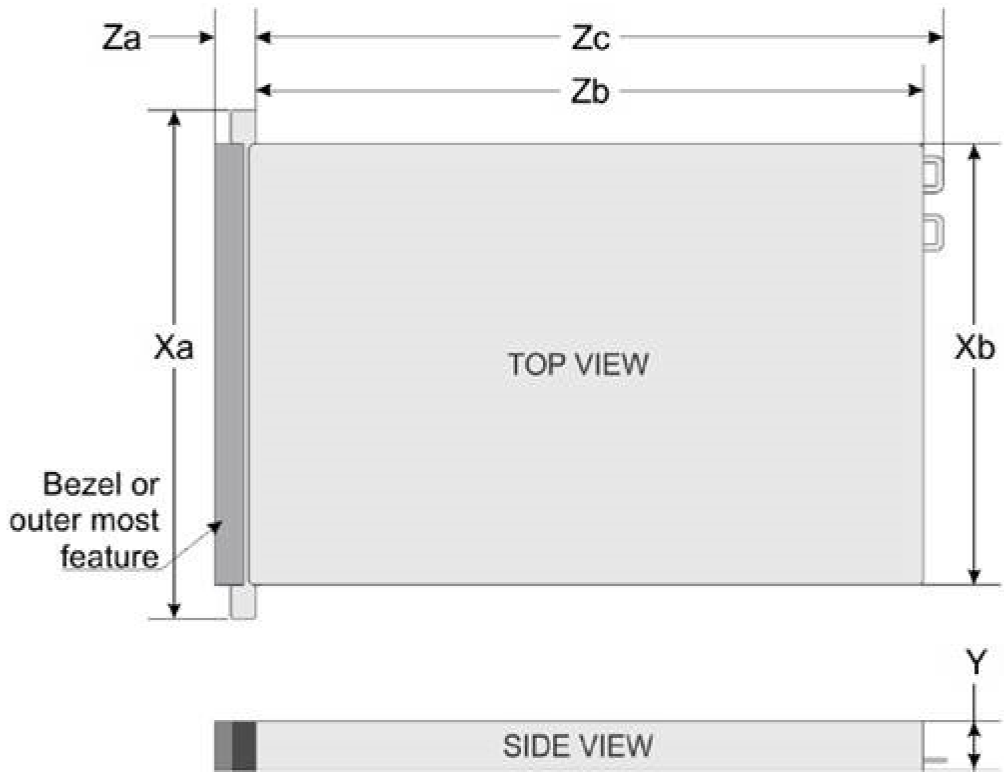
Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
Rack Mount Unit (RMU)	1U	1U	1U	1U	1U

Table continues…

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
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	4	4	6	8
RAID Options	5	6	6	6	6
Usable Virtual Disk Capacity	1.2 TB	1.2 TB	1.2 TB	2.4 TB	3.6 TB
Network 1 Gb ports	6	6	6	6	6
Power Supplies (750W)	2	2	2	2	2
Rail Kit	Y	Y	Y	Y	Y
DVD-ROM Drive	Y	Y	Y	Y	Y

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)

Environmental requirements

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

Table 4: 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 5: 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 6: 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 7: 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 8: Maximum altitude

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

Table 9: 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).

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 10: 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 11: 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

Chapter 3: Registration

Overview

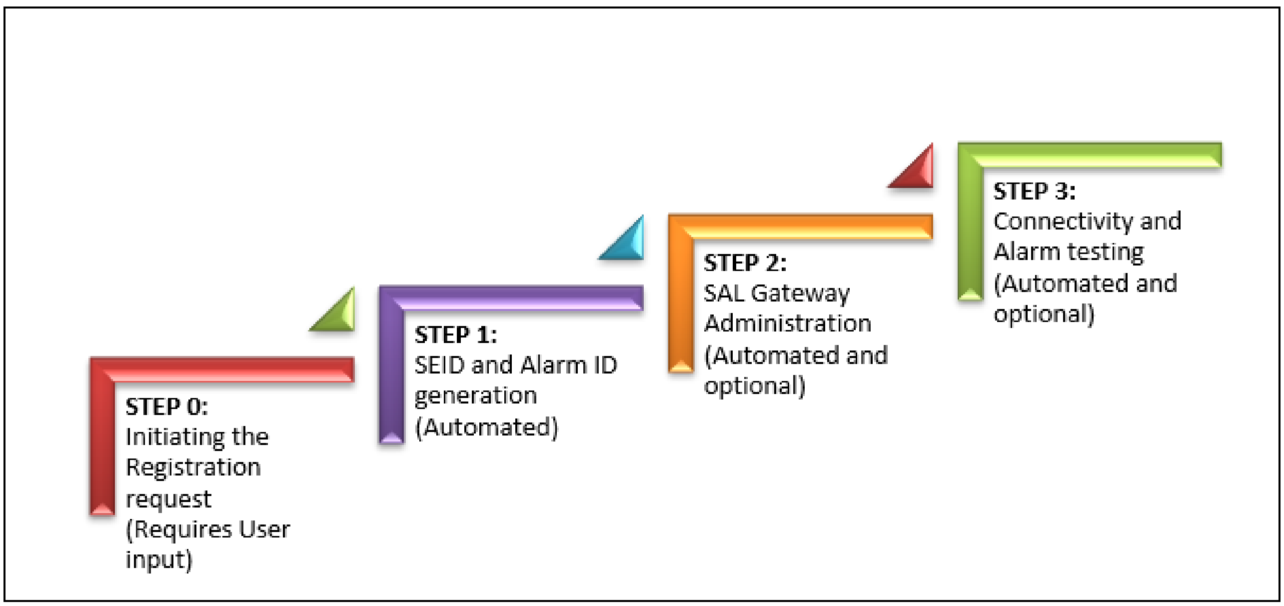
In order to receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in the HealthCheck tool.

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 forward 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.

Important:

Avaya does not support re-purposing CSR3 servers (Dell R630 and HPE Proliant DL360G9) with ESXi. Servers that are re-used by customers must be removed from GRT as they are no longer supported.

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:

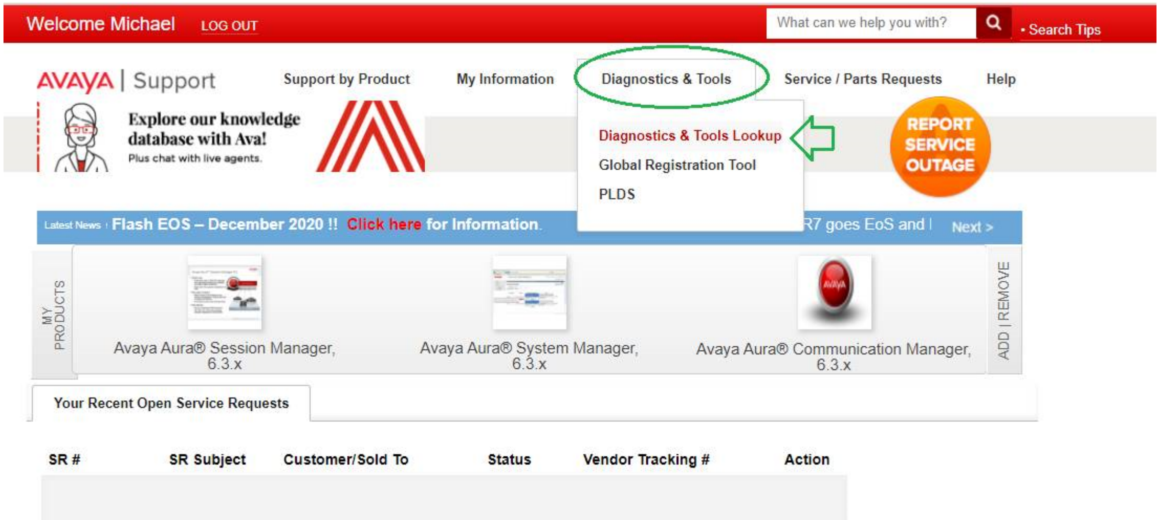
  Secure Access Link Registration (also called technical onboarding) requires a verified customer install base and FL or Sold to.
- Ensure you have your IP address and host names for iDRAC and the ESXi host.

  The iDRAC IP address is linked with the Avaya Solutions Platform server. The ESXi Host IP address is linked with the Avaya Solutions Platform ESXi 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 5.1 Material codes are 700515842 (Profile 2), 700515843 (Profile 3), 700515844 (Profile 4), 700515845 (Profile 5), and 700515846 (Profile 51).

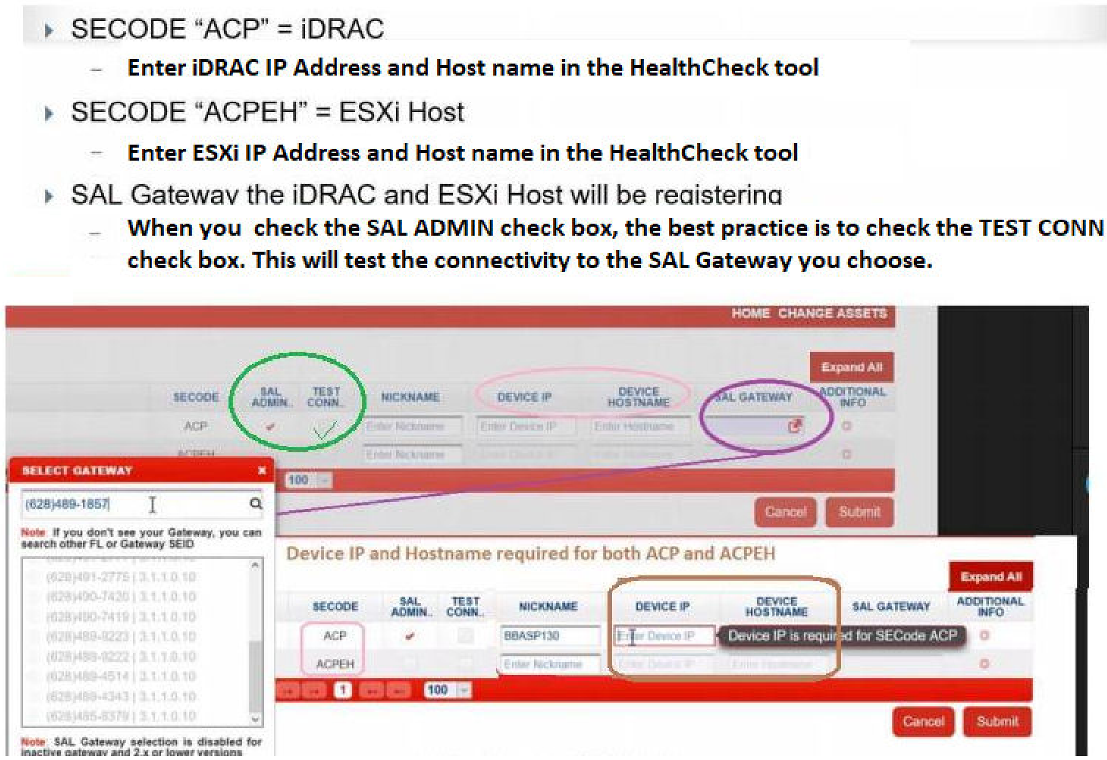
Procedure

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 **ACP**, **ACPEH**, 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 an email notification to the user once 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 a new device is registered with valid SEID and Alarm ID, it must be added to a SAL Gateway as a Managed element. This is required in case of errors or issues so that Avaya Service engineers receive the alarm and request remote access to your device to troubleshoot them.
- Connectivity and Alarm Testing: In case of failure or issues 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 to complete these steps at the earliest.

If you fail to 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 ESXi 7.0

About this task

The Avaya Solutions Platform 120 material codes are end of sale. Existing customers migrating from AVP 8.1.x to ASP 130 R5.1.x (ESXi 7.0) must retain existing material codes in their Install base record (see step 3). Use the new tracking code for SAL/Alarming connectivity by following the steps below:

Before you begin

- After ESXi software migrates to ASP 130 5.1.x (Dell R640), order material code 413030 ASP 120 UPG TO ASP130 ESXI R7 and Avaya PLDS generates 413031 ASP 130 R5 ESXI R7.X as entitlement in customer record into install base.

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 (415781 ASP 120 UPG TO ESXI TRK) to set ACP SE code (for iDRAC) and ACPEH SE code (for ESXi Host).

   Note:

   Use specific material codes for onboard application and deployment respectively.

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

Chapter 4: 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 28.		
2	Inspect package contents.	See Package contents on page 29.		
3	Install the server using the rail kit.	See Installing the server on page 30.		
4	Attach cables.	See Attaching cables on page 34.		
5	Connect power.	See Connecting power on page 35.		

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

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

- Dell A7 ReadyRails II sliding rail assembly kit
    - Two Dell A7 ReadyRails II sliding rail assemblies
    - Two hook and loop straps
- 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

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 R640 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 Back view of Dell™ PowerEdge™ R640 Server on page 14 of this document.

Before you begin

Warning:

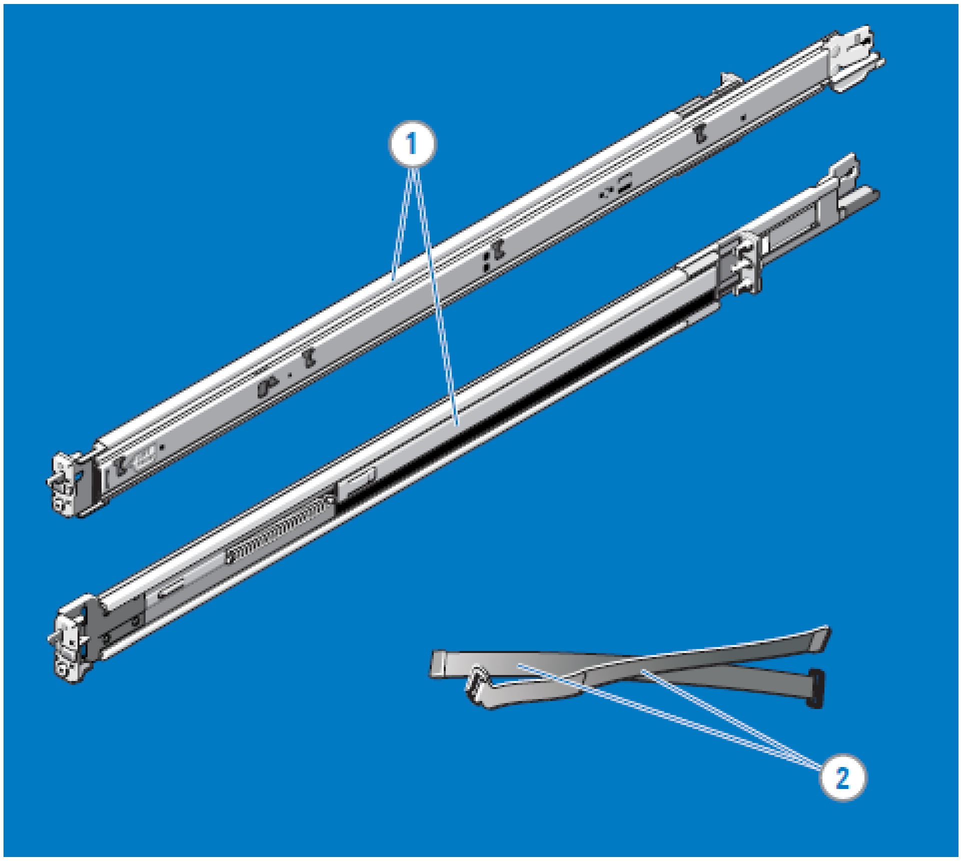
- Before you begin, read and follow the safety instructions in your Enterprise Products Safety, Environmental and Regulatory Information Booklet shipped with your system.
- To avoid injury, do not attempt to lift the system by yourself.
- Verify that the rack is installed according to the manufacturer's 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 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 Dell A7 ReadyRails II sliding rail assembly kit.



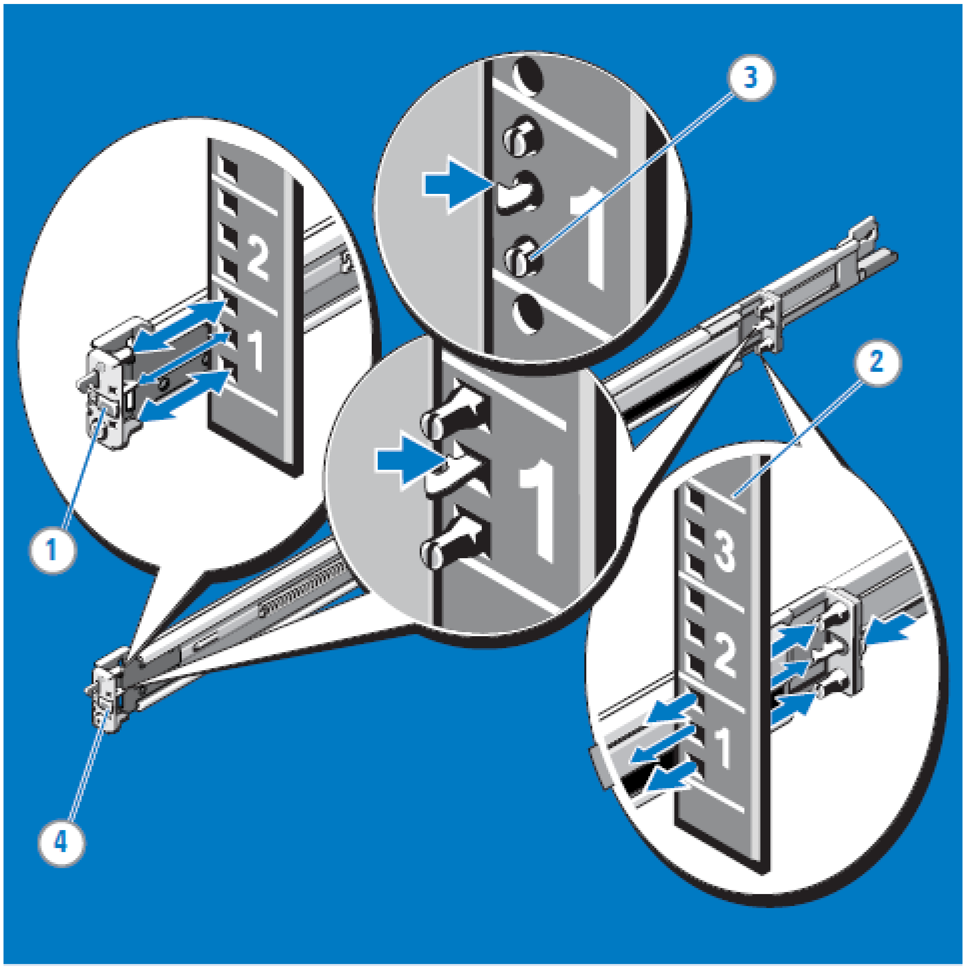
- Two Dell A7 ReadyRails II sliding rail assemblies — (1)
- Two hook and loop straps — (2)

2. Place the kit components within easy reach of your work area.

Important:

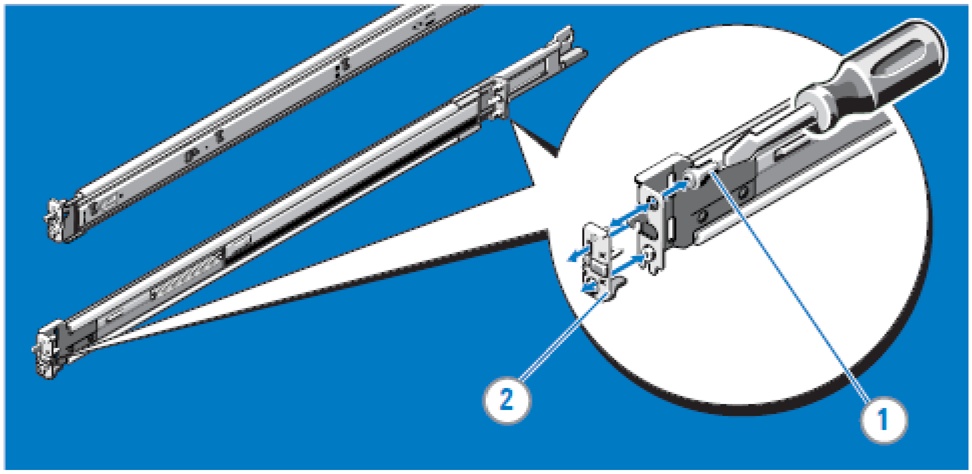
Rail kit installation is performed using either Step 3 or Step 4 depending on the type of rails in use. Read each step carefully and consult your installation environment before proceeding.

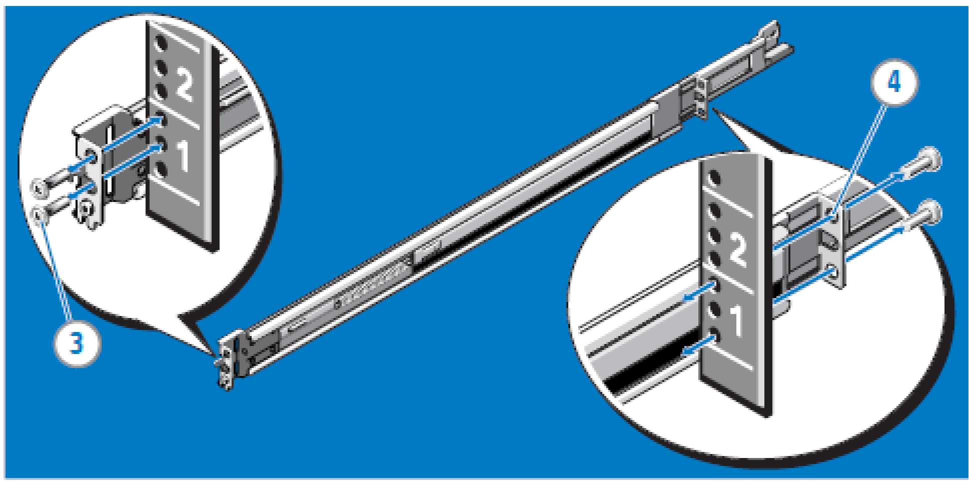
3. Perform the following actions to install toolless rails (Square Hole or Round Hole Racks):



Task order	Task
1	Position the left and right rail end pieces labeled *FRONT* facing inward and orient each end piece to seat in the holes on the front side of the vertical rack flanges.
2	Align each end piece in the bottom and top holes of the desired rack spaces.
3	Engage the back end of the rail until it fully seats on the vertical rack flange and the latch clicks into place.
4	Repeat these steps to position and seat the front end piece on the vertical rack flange.

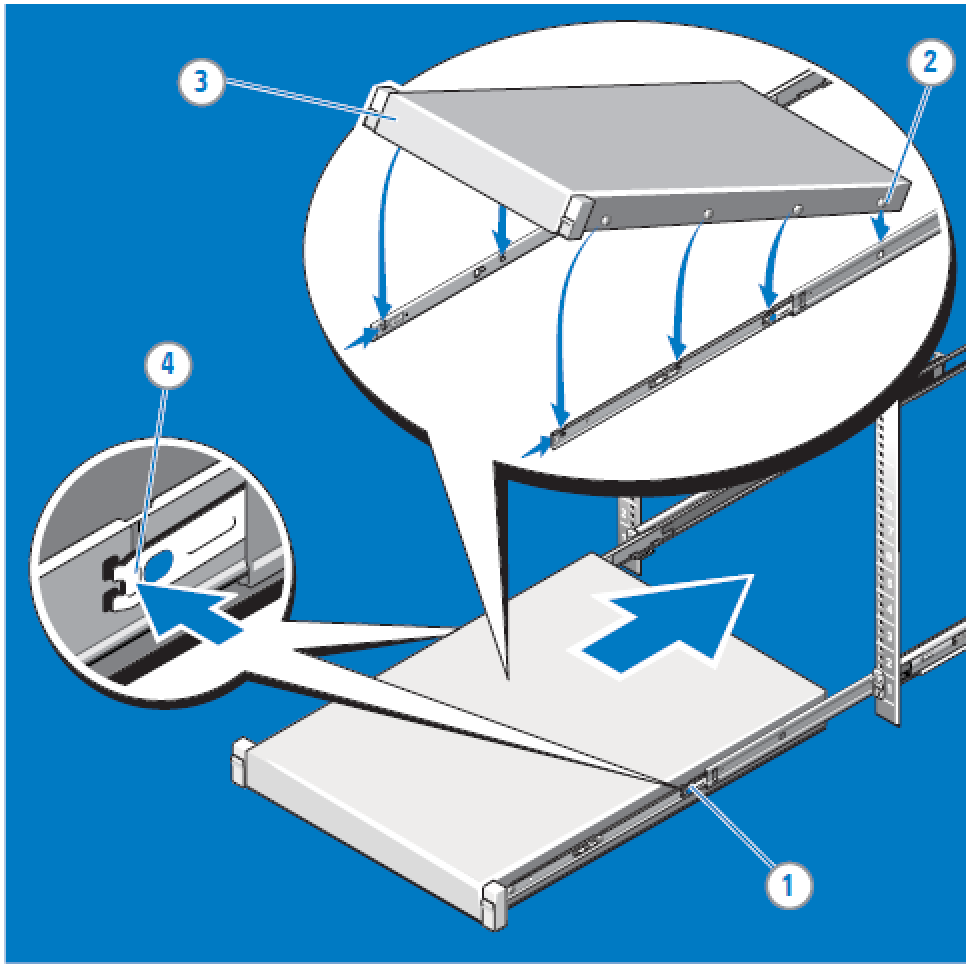
4. Perform the following actions to install toolless rails (Threaded Hole Racks):





Task order	Task
1	Remove the pins from the front and rear mounting brackets using a flat-tipped screwdriver.
2	Pull and rotate the rail latch subassemblies to remove them from the mounting brackets.
3	Attach the left and right mounting rails to the front vertical rack flanges using two pairs of screws.
4	Slide the left and right back brackets forward against the rear vertical rack flanges and attach them using two pairs of screws.

5. 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

Attaching cables

About this task

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

Note:

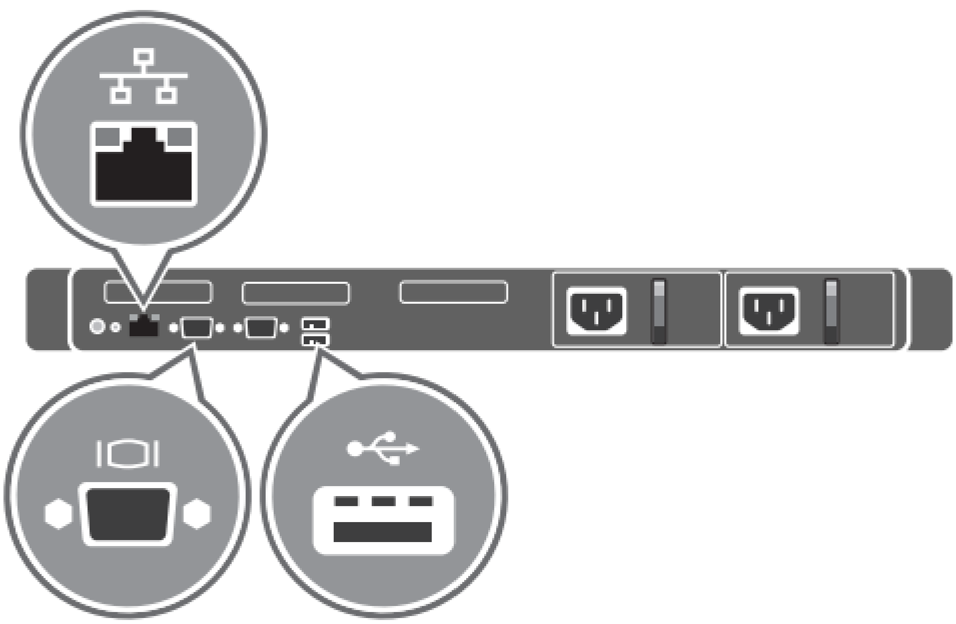
Consult application-specific documentation for information on peripheral and management device connectivity.

Before you begin

Ensure the system has been installed and secured as outlined in Installing the server on page 30 before you attach cables. Ensure you have taken precautions against electrostatic discharge as outlined in Electrostatic discharge on page 28 before you begin.

Procedure

1. Connect the network cables to the appropriate RJ45 ports on the system.
2. Connect optional peripherals using the USB ports on the system. If configuring ESXi 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 ESXi 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 Back view of Dell™ PowerEdge™ R640 Server on page 14.

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.

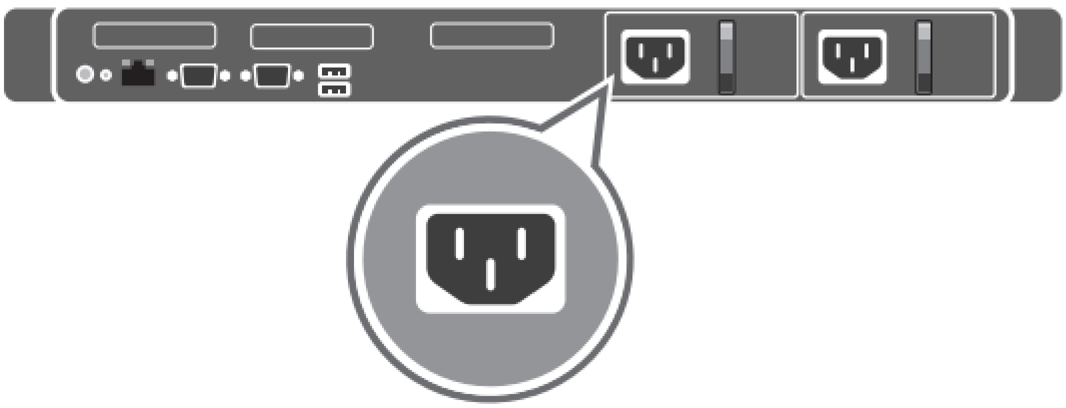
Before you begin

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:

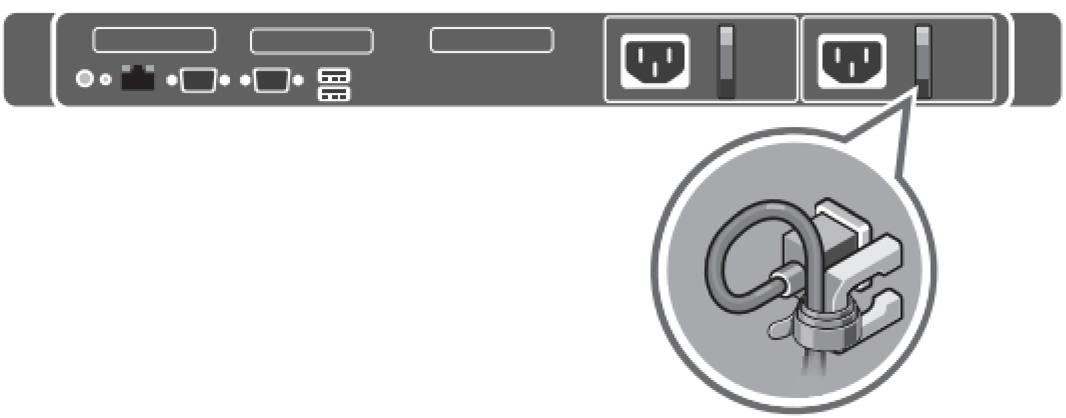
- Installing the server on page 30
- Electrostatic discharge on page 28

Procedure

1. Connect the system to the appropriate power source.

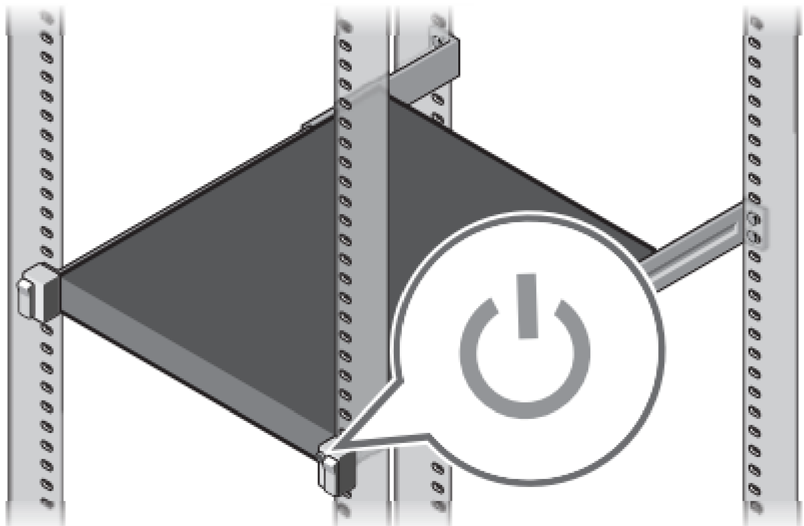


2. Loop and secure the power cable using the retention strap.



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: 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 OVAs.

Dell R640 ESXi Configuration

Overview

The Avaya Solutions Platform 130 (ASP 130) is supported on Dell R640 servers. This section provides the instructions required after physical installation to complete the ESXi configuration with the customer's specific environment information prior to deploying Avaya Application OVAs.

Required items

- Dell R640 server
- console VGA monitor
- USB keyboard

Configuring ESXi Network Settings

About this task

Use this procedure to configure ESXi Network Settings.

Before you begin

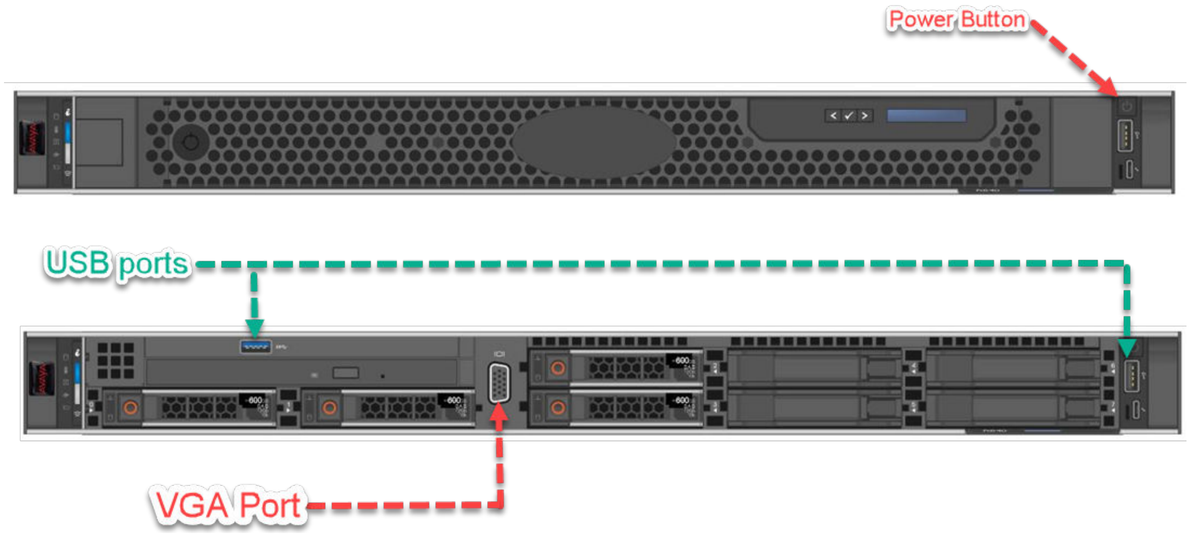
Ensure that you have the following:

- Dell R640 Server
- Console VGA Monitor
- USB Keyboard

Procedure

1. Connect a VGA monitor and USB keyboard to the server. Connections for the VGA monitor and USB keyboard are also located on the rear of the server.

2. Remove faceplate to access front VGA and USB ports.



For quantity of HDDs installed per server profile see “table 2: Skylake CPUs” and “table 3: Cascade Lake CPUs” in Avaya Solutions Platform Appliance profiles on page 16.

3. **Disconnect all Ethernet connections**, including the services port, to the server except vmnic0 (NIC1) and power on the server. If no Ethernet connections are connected to the server that is acceptable also.

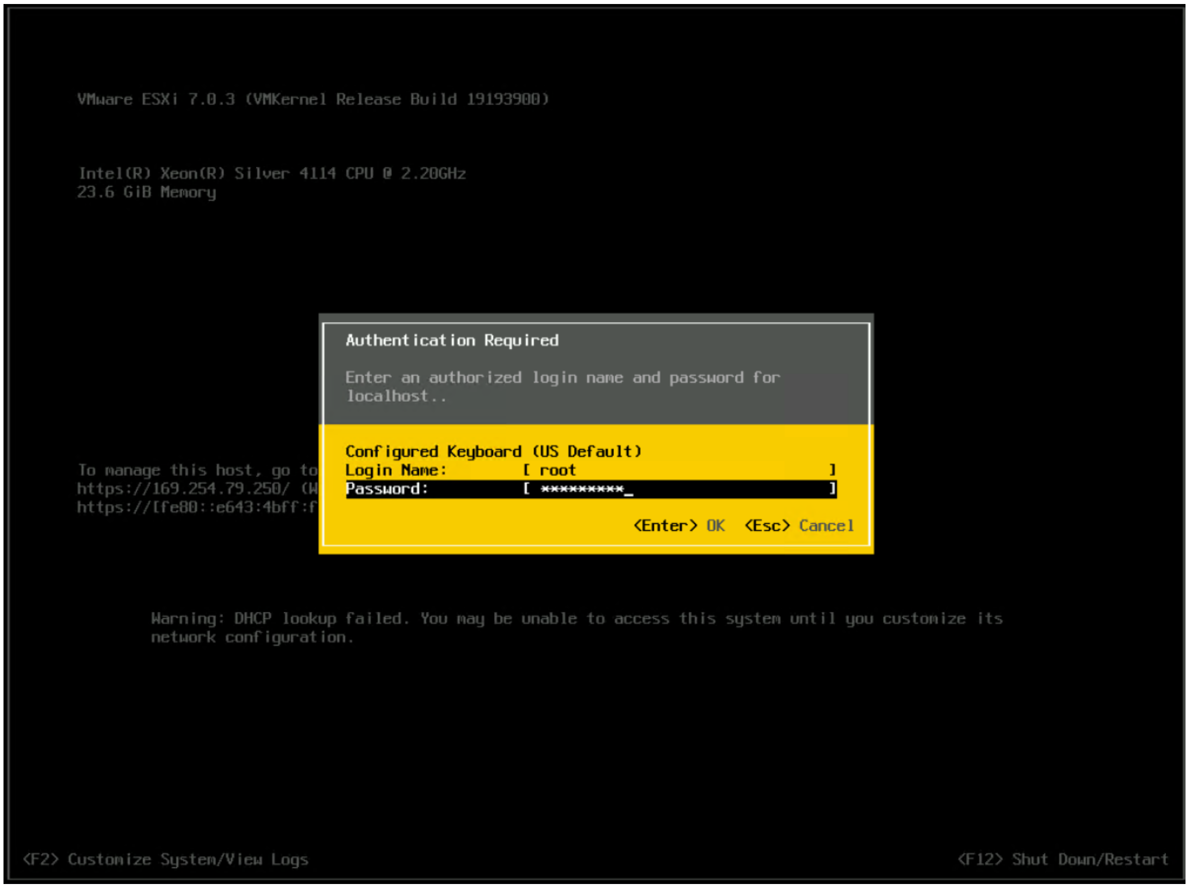
Note:

Best practice is to label all network cables.

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

4. Once ESXi has booted, select **F2** to administer configuration settings. (Build number may vary)

5. Log in as a `root` user, using the password, `ACP130_pw`

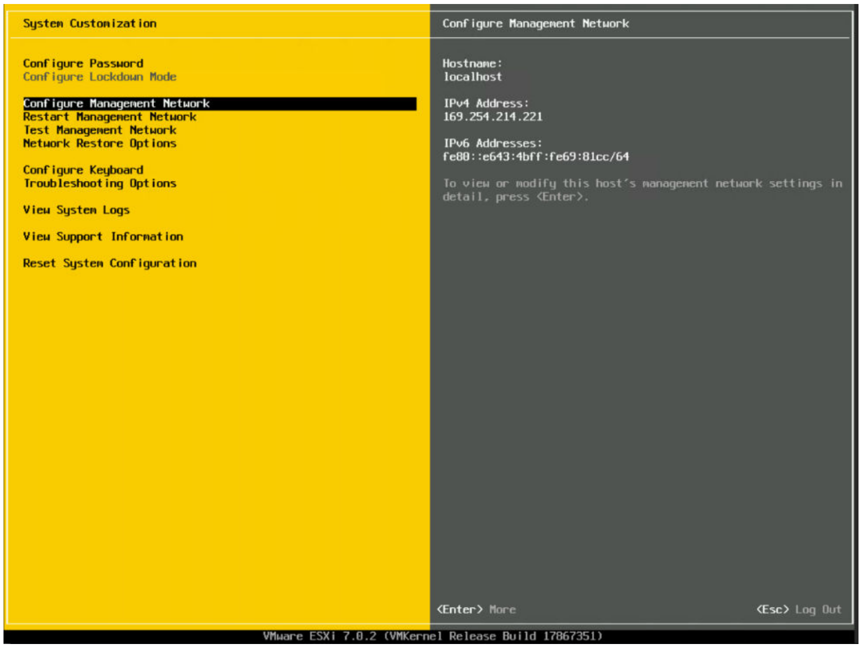


6. From the **System Customization** menu, select **Configure Password**. Create a unique new password to better secure the server, and press **Enter** to submit the change and return to the **System Customization** menu.

Important:

Once a new password is configured, be sure to keep track of the new password. If the new password is lost or forgotten, ESXi will need to be reinstalled.

7. Arrow down and select **Configure Management Network** and press **Enter**.



8. Verify Network Adapters is set to **vmnic0 (NIC1)**. If correct use down arrow key to select **IPV4 Configuration** and progress to step 10 below. If vmnic0 (NIC1) is not selected move to step 9 below.

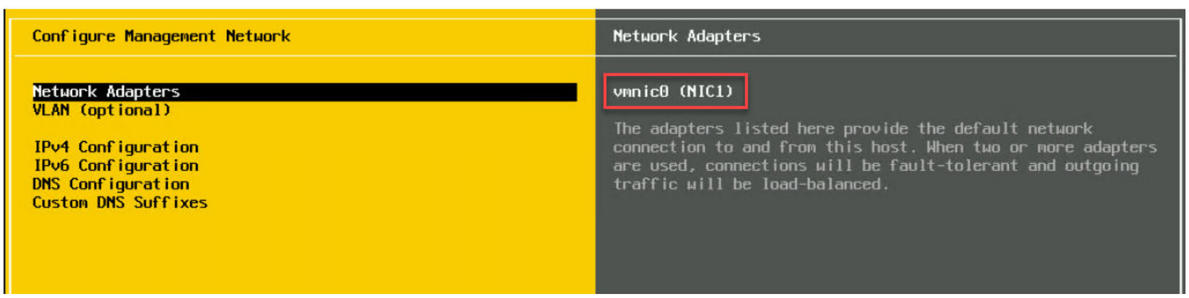


Figure 2: Configuring Management Network

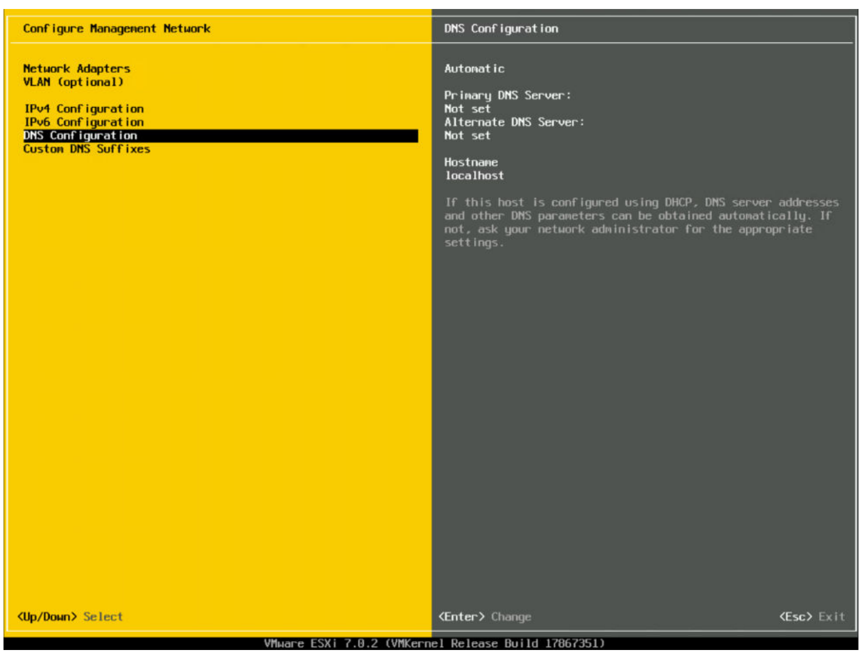
9. If vmnic0 (NIC1) is not selected as shown in step 8 above, then ESXi misconfigured its network interfaces during the install process. The user must remove connections to all of the server's network interfaces except for vmnic0 (NIC1) and reinstall ESXi. User must go to Performing server recovery and/or software remastering on page 86 , move to the **Software remastering** section and reinstall ESXi as instructed.

10. Using arrow keys move cursor to **IPv4 Configuration** and press **Enter**.

11. Press the **down** arrow key to **Set static IPv4 address and network configuration** and press the spacebar to select this option. Press Up/Down arrow key to enter related IP information. When complete, press **Enter**.

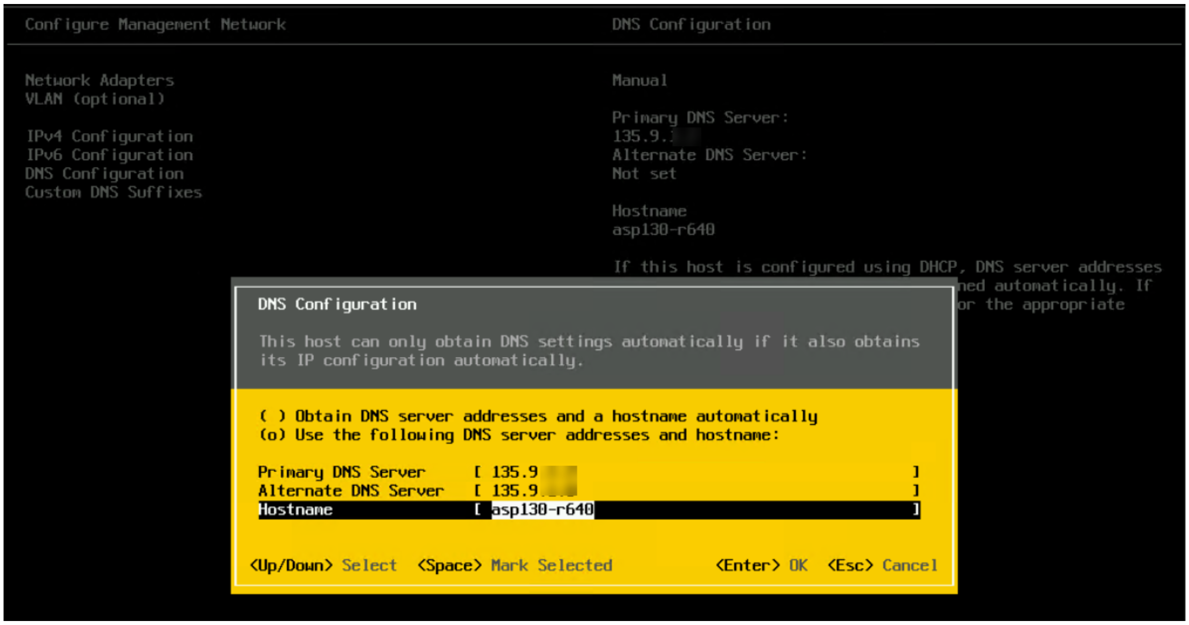
12. The **Manual label** should now be associated with the IP address fields, indicating static addressing mode is configured.

13. Move cursor down to select **DNS Configuration** and press **Enter**.

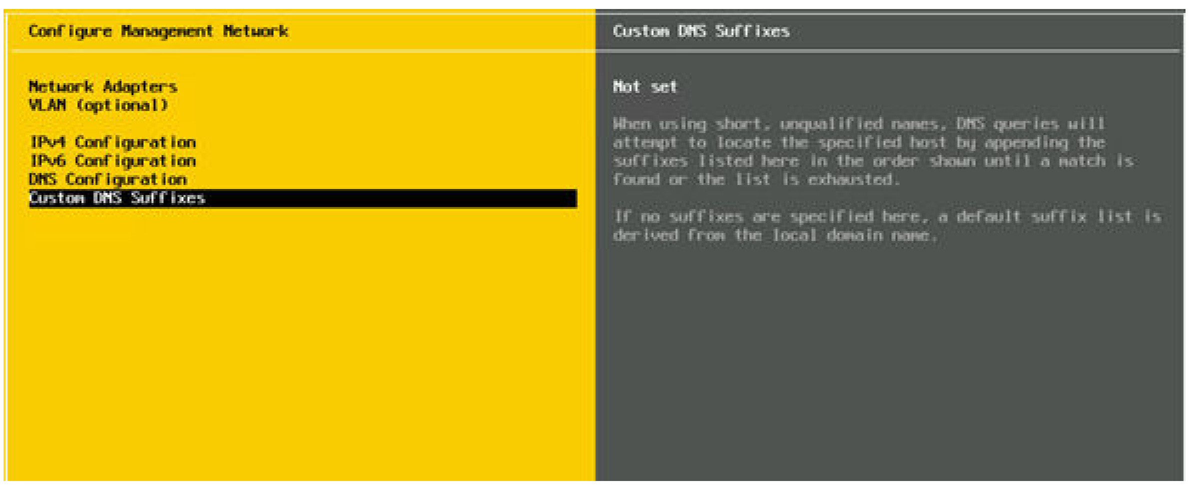


14. The option to **Obtain DNS server addresses and a hostname automatically** is the default. Down arrow to **Use the following DNS server addresses and hostname** and press the spacebar to select it. Up/down arrow to enter the IP address(es) of the DNS

server(s) and the hostname (not the full FQDN) of this server. Do not enter an FQDN in the **Hostname** field. When complete, press **Enter**.

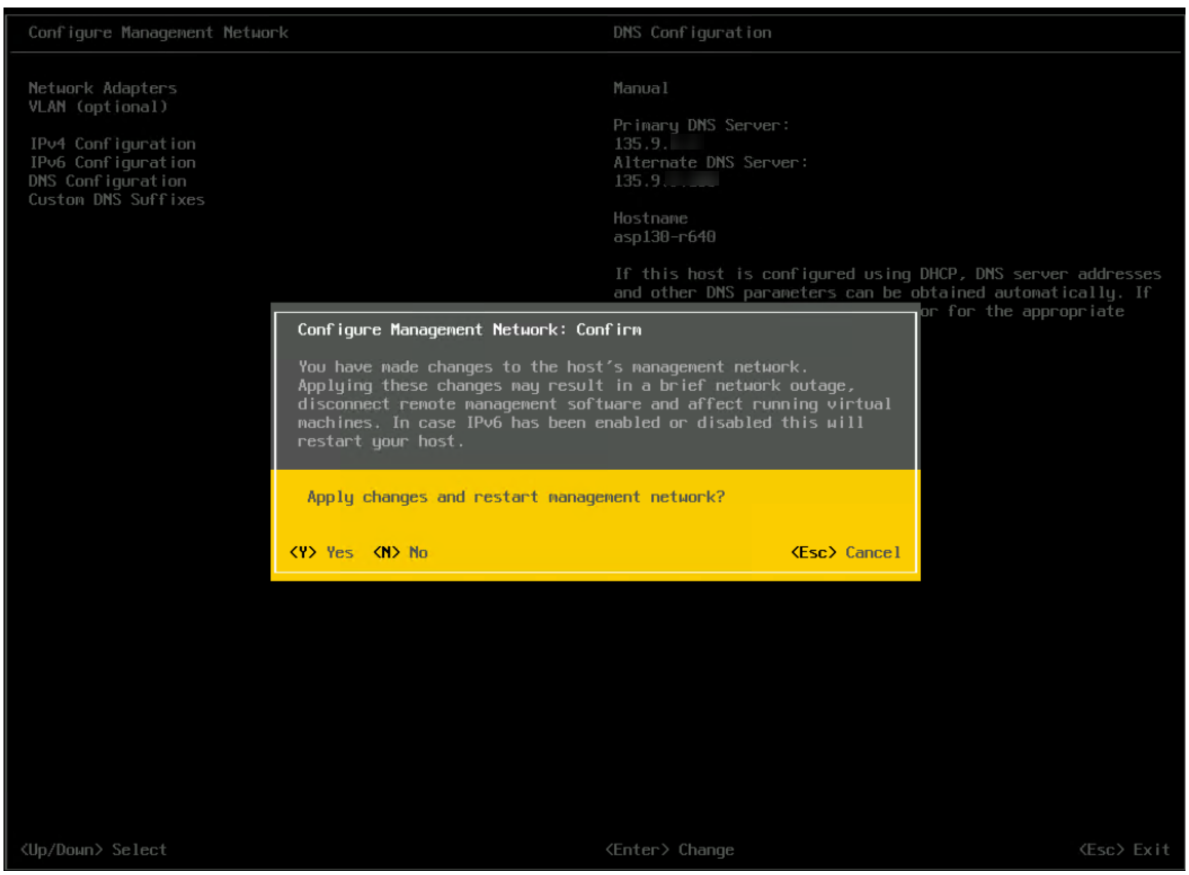


15. Move cursor to **Custom DNS Suffixes** and press **Enter**.



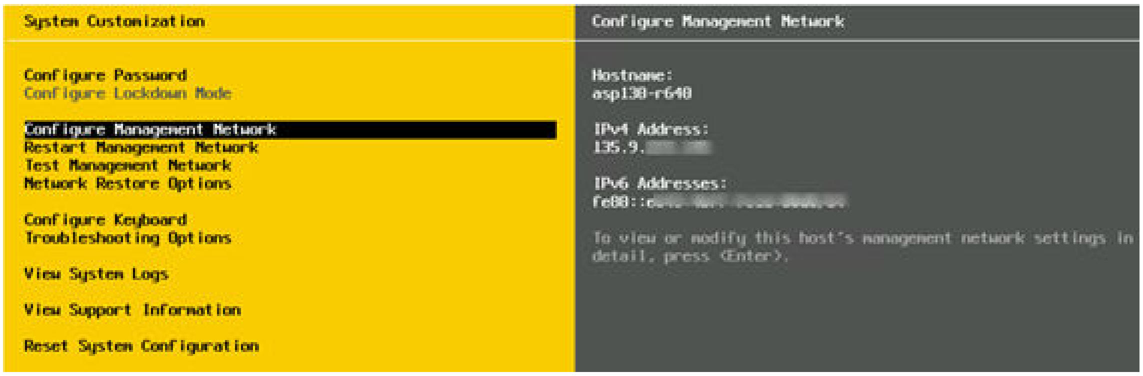
16. Input custom DNS Suffixes and press **Enter** when complete. The FQDN of the server will be created from the DNS hostname and Custom DNS Suffix entries.

17. When all management network information has been entered press **Esc** from the main **Configure Management Network** screen, VMware prompts the administrator to save the configuration. Type `Y` (Yes) to save.



18. The Management Network parameters entered should be saved and displayed as shown below. If correct proceed to the next step.

If the IPV4 address or any other Network parameters are overwritten to different values than entered, then ESXi networking is not configured correctly. The user must reinstall ESXi to ensure internal ESXi networking is configured correctly. The user must remove connections to all of the server's network interfaces except for vmnic0 (NIC1) and reinstall ESXi. User must go to **Chapter 8: Performing server recovery or software remastering**, move to the **Software remastering** section and reinstall ESXi as instructed.



19. From the **System Customization** screen, select **Troubleshooting Options**.

Note:

Use the following steps to enable or disable the ***SSH*** and ***ESXi shell*** services as required to align with customer security policies.

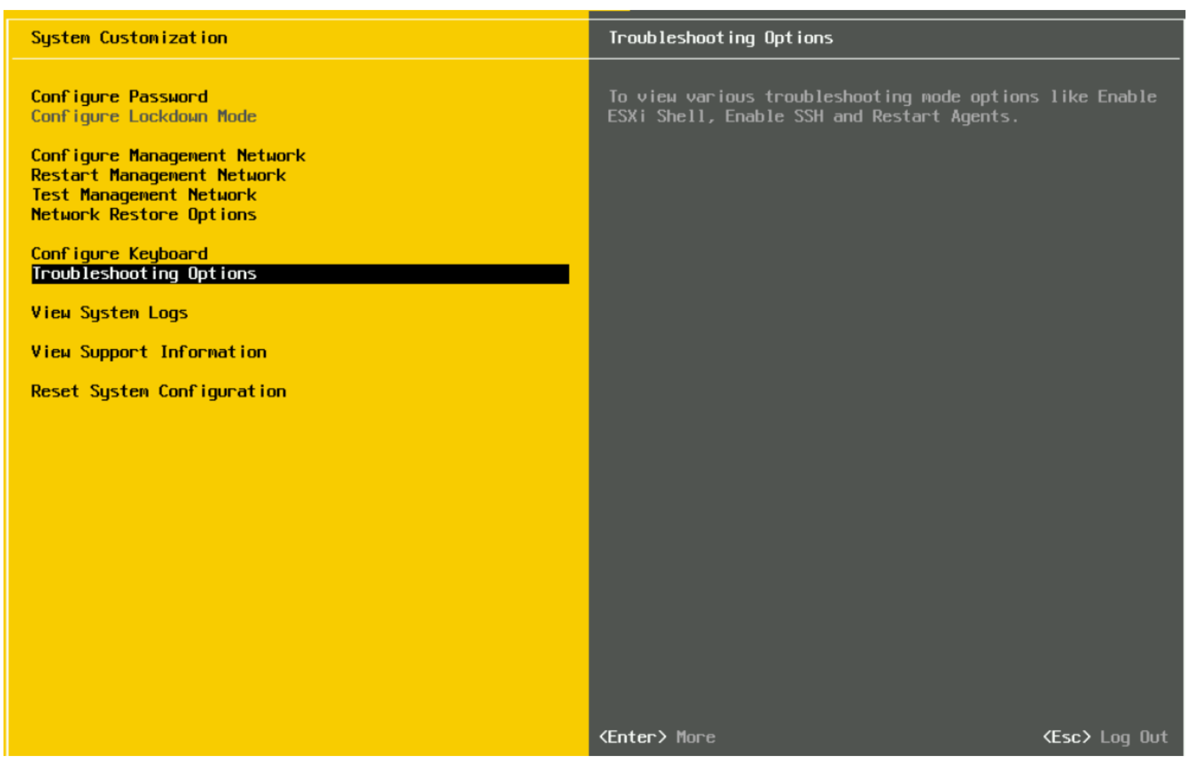


Figure 3: Customizing System

20. From the **submenu**, using the **Up/Down** arrow key, highlight ***ESXi Shell***. Press **Enter** to change the state to **Enabled** or **Disabled**, as seen on the right side of the screen.

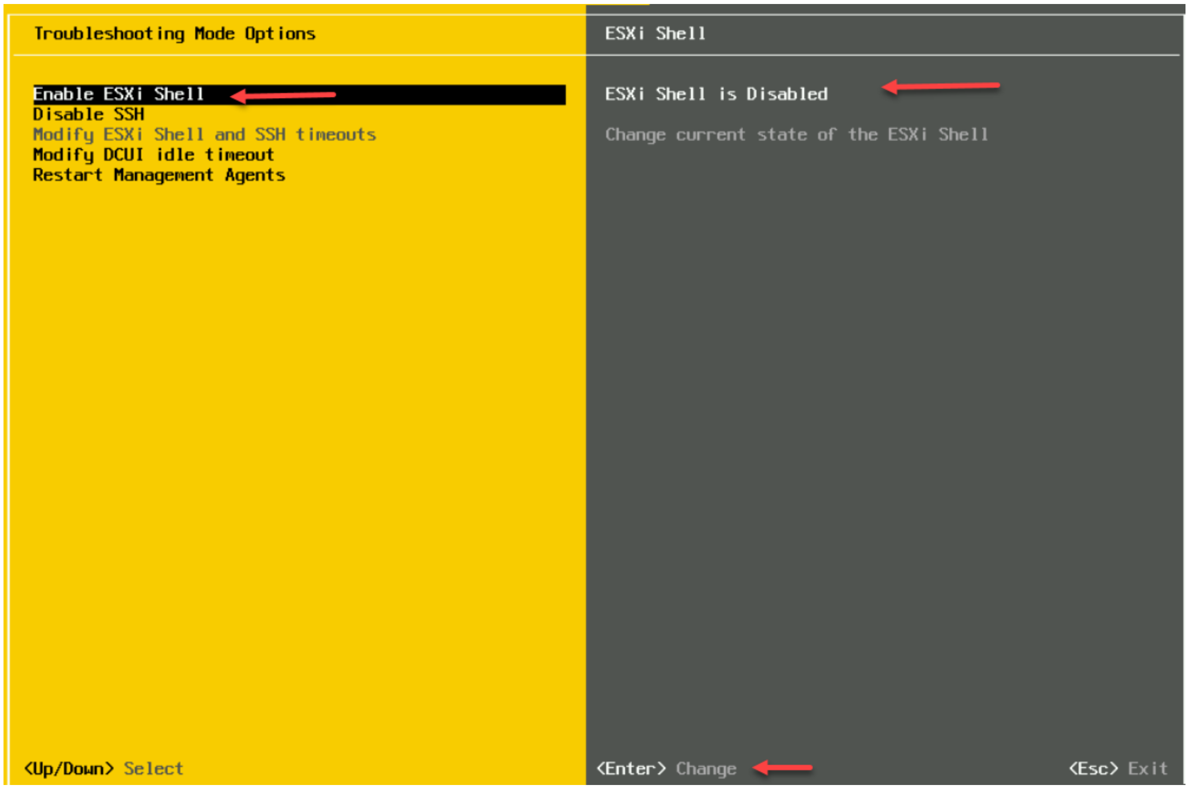


Figure 4: Troubleshooting Mode Options

Note:

The ESXi Shell service will be enabled for all deployments unless otherwise requested by the customer.

21. From the **submenu**, using the **Up/Down** arrow key, highlight ***SSH***. Press **Enter** to change the state to **Enabled** or **Disabled**, as seen on the right side of the screen.

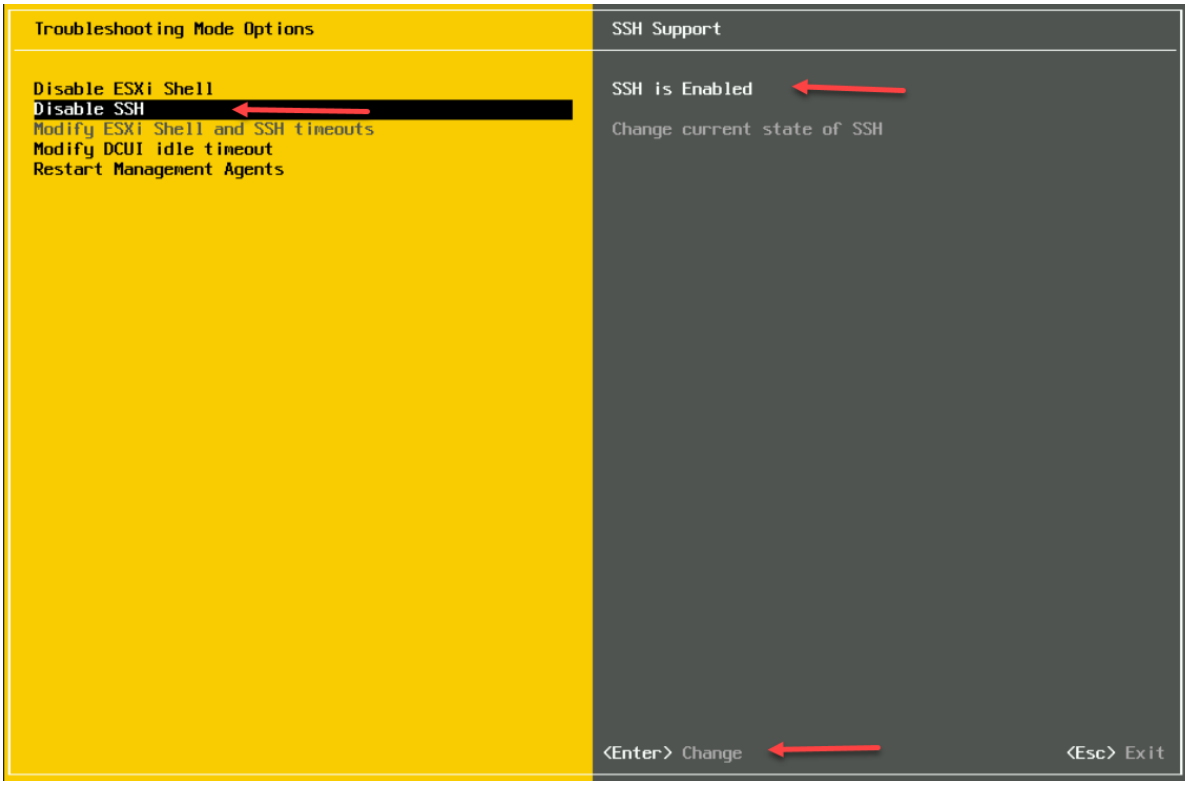


Figure 5: Troubleshooting Mode Options

22. When ready, press **ESC** to exit from the **Troubleshooting Options** submenu. Press **ESC** again to logout from the ESXi Direct Console User Interface (DCUI).
23. If applicable reconnect previously attached network connections.

    Optional - if iDRAC configuration is desired, it should be done during the next server reboot by pressing **F2**. Refer to the Avaya Solutions Platform130 Series iDRAC9 Best Practices document for details.

    Optional - if **Out of Band Management** is required, see Securing Network Configuration on ASP 130 on page 64. The server is now ready for **OVA** installation. You may now access the system using the network configuration information entered, ***root*** login and your customer specified password.

Verify autostart on ESXi host is enabled using Embedded Host Client

About this task

To start VMs automatically when ESXi host starts up, you can use ESXi Embedded Host Client to verify autostart on the ESXi host.

Procedure

1. Log into the ESXi Embedded Host Client using a web browser.

2. In the Navigator pane on the left, click **Manage**.
3. On the **System** tab, click **Autostart**.
4. Verify that it shows enabled. If it is not enabled follow the steps below.
5. In the Change autostart configuration window, set the autostart configuration as follows:
    a. In the **Enabled** field, select **Yes**.
    b. In the **Start delay** field, type `0`.
    c. In the **Stop delay** field, type `0`.
    d. In the **Stop action** field, click **Shut down**.
    e. In the **Wait for heartbeat** field, select **Yes**.
6. Click **Save**.
7. Click the right mouse button on the host name, and click **Reboot** to restart the server.

    Note:

    If autostart is enabled, all virtual machines running on the host must have open-vm-tools (https://docs.vmware.com/en/VMware-Tools) installed on the guest OS so that the virtual machines can be gracefully shutdown when the host reboots or shuts down. If all VMs do not have tools installed, the host shutdown/reboot will pause until those VMs are manually shutdown prior to the host reboot/shutdown.

Steps required to set Host time and date

Before you begin

The VMware vendor considers as a best practice to have the ESXi hosts configured to an authoritative time (NTP) server. Avaya, for security reasons, recommends synchronizing the ESXi 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.

Procedure

1. Select **Host** > **Manage** > **System** > **Time & Date** > **Edit settings**.

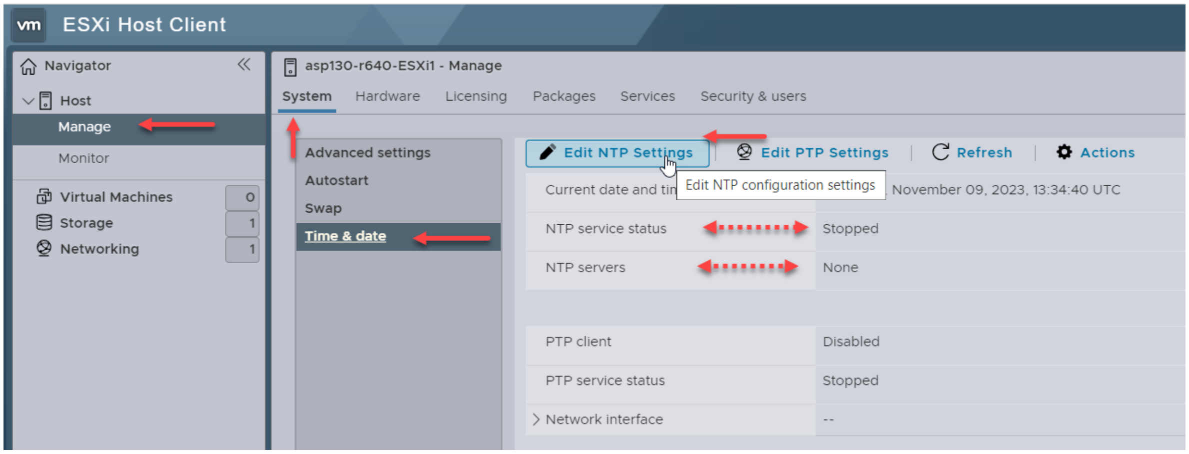


Figure 6: Setting ESXi Host time and date

Perform the following:

a. Select the radio button for **Use Network Time Protocol (Enable NTP Client)**.

b. For NTP service startup policy, select from the drop-down menu: **Start and stop with host**.

c. For NTP servers: Enter customer NTP server IP address. If multiple NTP servers are to be configured, separate these with commas, e.g., *10.31.21.2, 10.31.21.3* etc.

d. When ready, click **SAVE**.

2. Enter Appropriate Information and click **Save**.

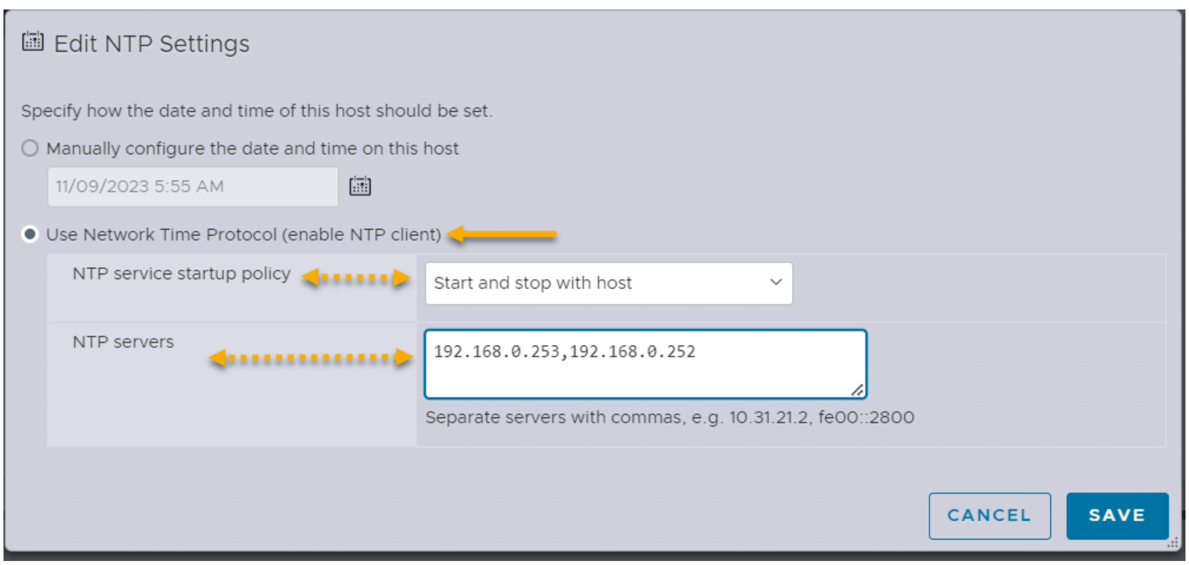


Figure 7: Editing ESXi Host time configuration

Note:

NTP client is configured on the Host, however, the NTP service needs to be started.

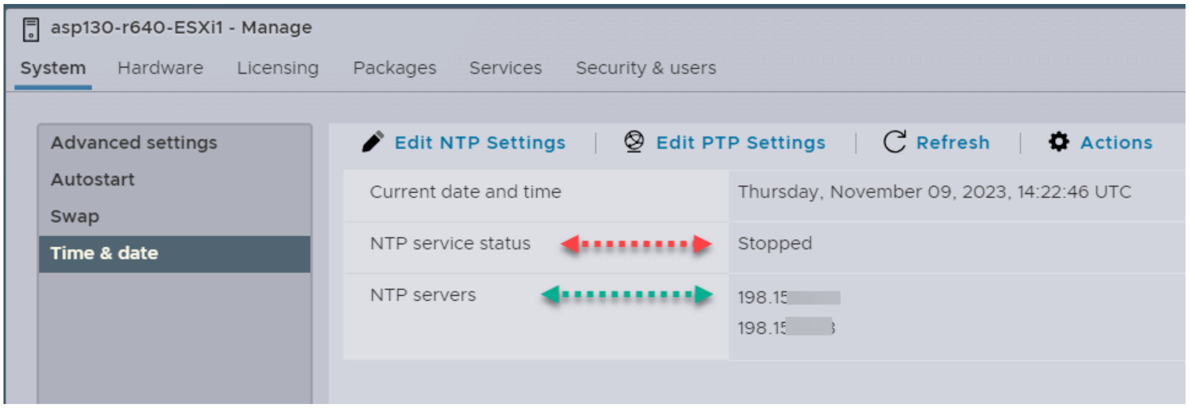


Figure 8: Managing ESXi Host - Time & Date

3. Go to **Services**.
4. Search or locate within the list the **ntpd** service (NTP Daemon).
5. Select **ntpd service** > **Actions** > **Start**.

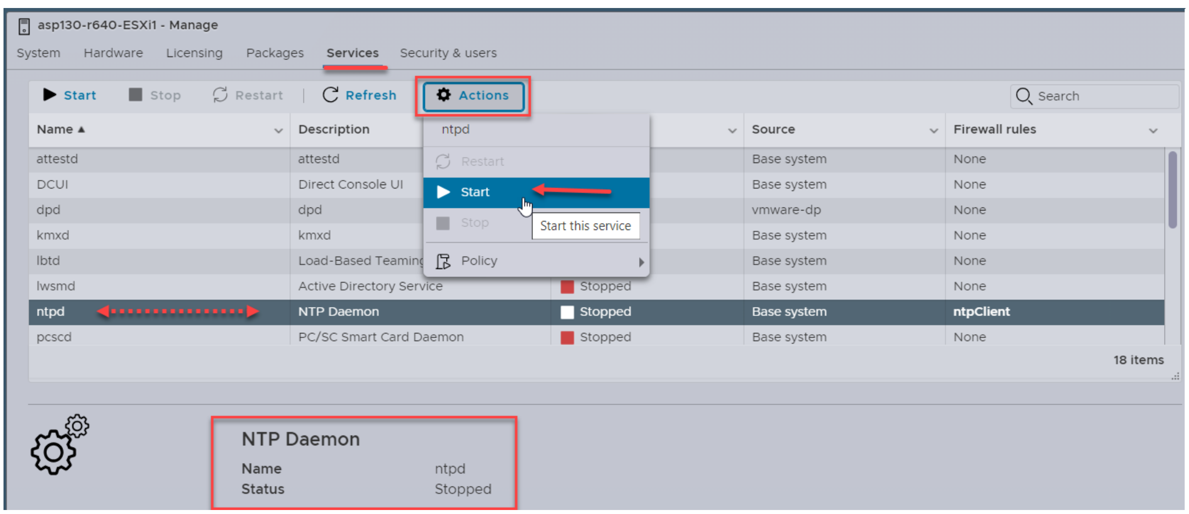


Figure 9: Managing ESXi Host - Services

6. Validate ntpd service is running.

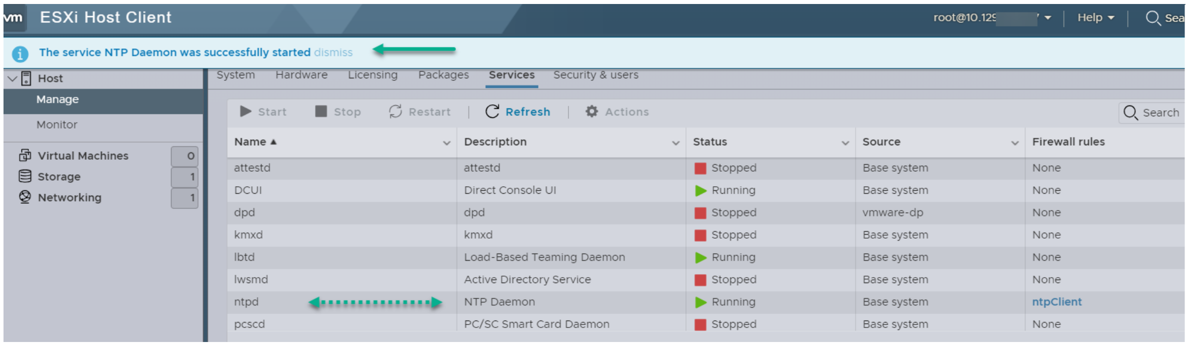


Figure 10: Managing ESXi Host - Services

7. Select **Systems** > **Time & date**.

   Note:

   The NTP service status may not be refreshed immediately and continue to report as stopped. Click the **Refresh** button (not the browser URL) if required, to refresh the screen and get the actual status of the NTP service.

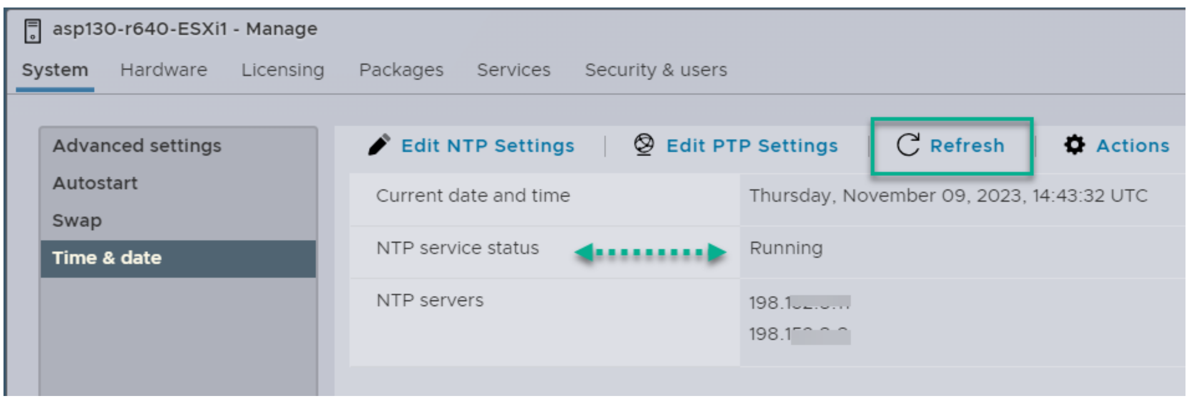


Figure 11: Managing ESXi Host Time & Date - Refresh

Configuring SNMP v2c on an ESXi 7.0 host

About this task

This section provides instructions on how to configure SNMP on the Avaya Solutions Platform 130 server. The Avaya Secure Access Link (SAL) Gateway, as an SNMP trap receiver, can support SNMP v1, v2c and v3. Some trap receivers may only support SNMP v2 and other may require SNMP v3. The ESXi host can support SNMP v2c and v3 simultaneously, if needed.

Note:

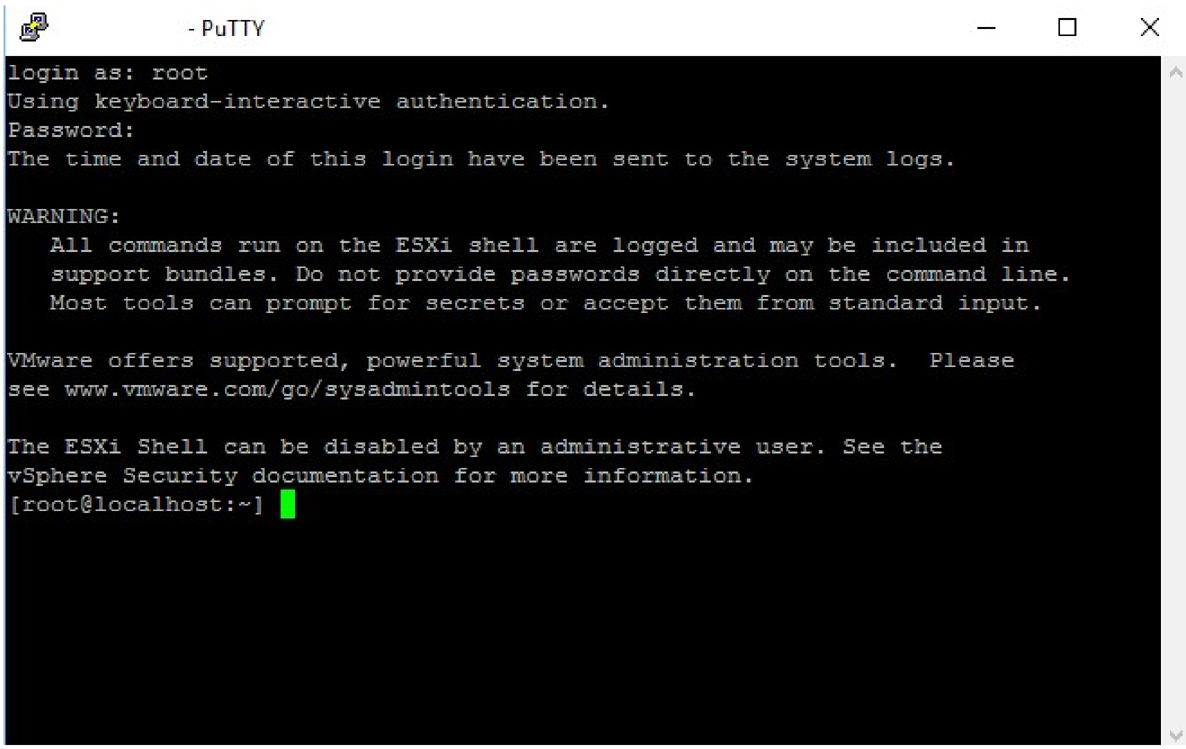
Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Note:

The SSH functionality must be enabled on ESXi. The Avaya installation guidelines direct administrators to enable SSH, so this should not be an issue. If, however, ESXi shell is not enabled, refer to steps 19 to 22 under Configuring ESXi Network Settings on page 38 to enable ESXi shell and SSH.

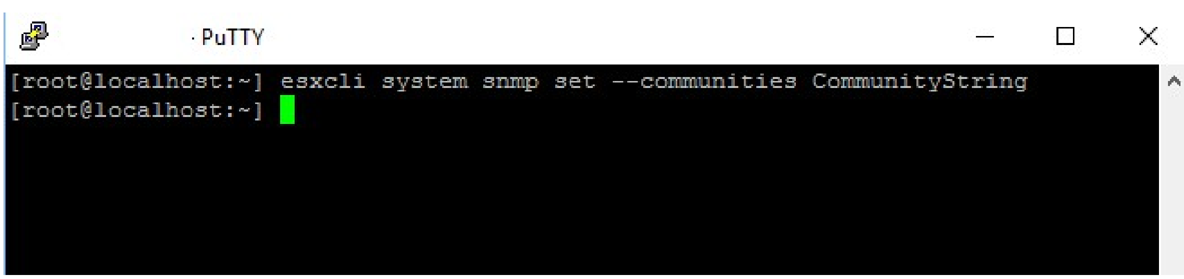
Procedure

1. From a Putty session, via SSH, access the ESXi host. Authenticate using the existing ***root*** credentials.



2. Type the following command to set the community string to be exchanged between the ESXi host and the trap receiver(s):

```
esxcli system snmp set --communities <community string>
```



3. Administer the trap receivers:

```
esxcli system snmp set --targets <SAL_GW_IP_ADDRESS>@<port#>/<community>
```

Example with multiple targets, separated by a comma:

```
esxcli system snmp set --targets 10.1.1.1@162/avaya123,10.1.1.2@162/avaya123
```

Note:

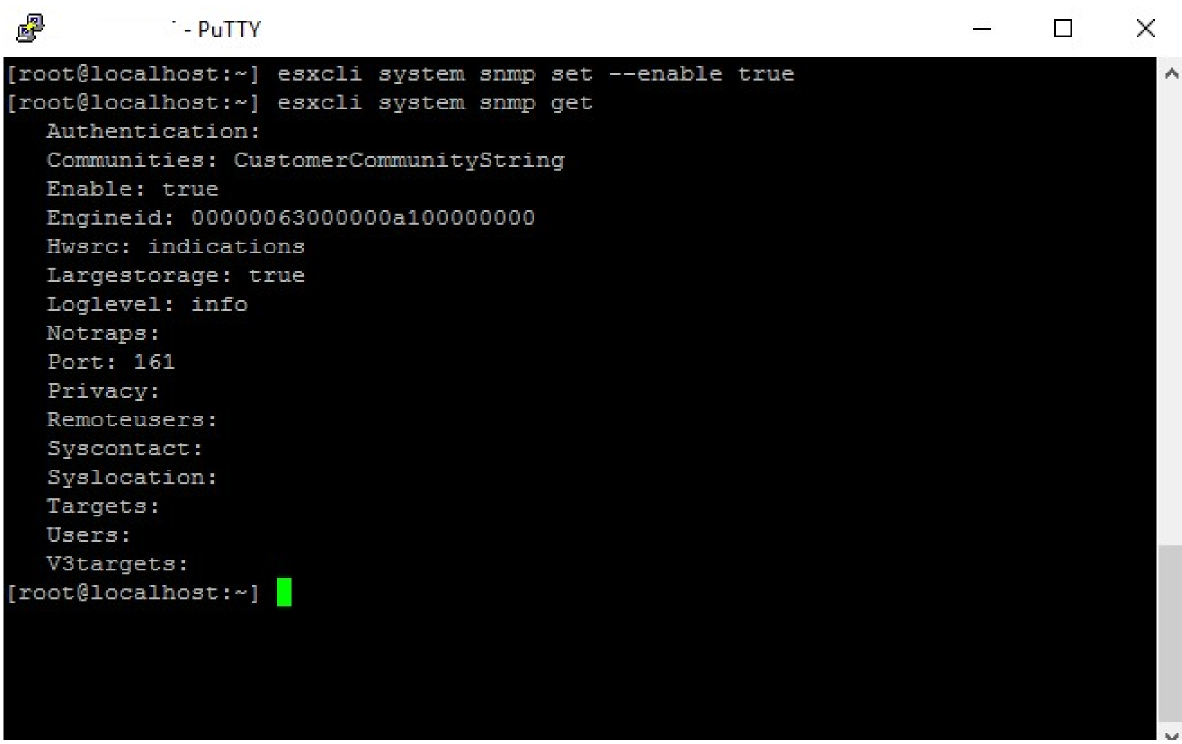
- Port 162 is the standard and default SNMP port for receiving traps, but any port number can be assigned as long as it is matched at both send/receive devices.
- Up to three trap destinations can be administered and must be separated by commas with no subsequent space.
- If sending traps to a System Manager server, the default port that the System Manager uses for trap reception is port 10162.

4. Enable/Disable SNMP on the host using the following command:

```
esxcli system snmp set --enable true (to enable)
esxcli system snmp set --enable false (to disable)
```

5. Confirm the settings with the following command:

```
esxcli system snmp get
```



6. Run the following command to send a test trap and confirm that the administered destination(s) is/are sent SNMP notifications:

```
esxcli system snmp test
```

Note:

The trap sent to the trap receiver(s) may not cause a warning/alarm state change for the ESXi host being administered. The trap will likely be an Informational message variety trap, communicating the ability for the ESXi device to transfer SNMP packets with the administered receiver(s).

7. Use the following command, if you want to remove the SNMP configuration:

```
esxcli system snmp set -reset
```

Configuring SNMP v3 on an ESXi 7.0 host

About this task

The SNMP v3 setting is available on ESXi. This section provides steps on configuring the more secure option of SNMP v3.

Note:

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

Note:

The SSH functionality must be enabled on ESXi. The Avaya installation guidelines direct administrators to enable SSH, so this should not be an issue. If, however, ESXi shell is not enabled, refer to steps 19 to 22 under Configuring ESXi Network Settings on page 38 to enable ESXi shell and SSH.

Note:

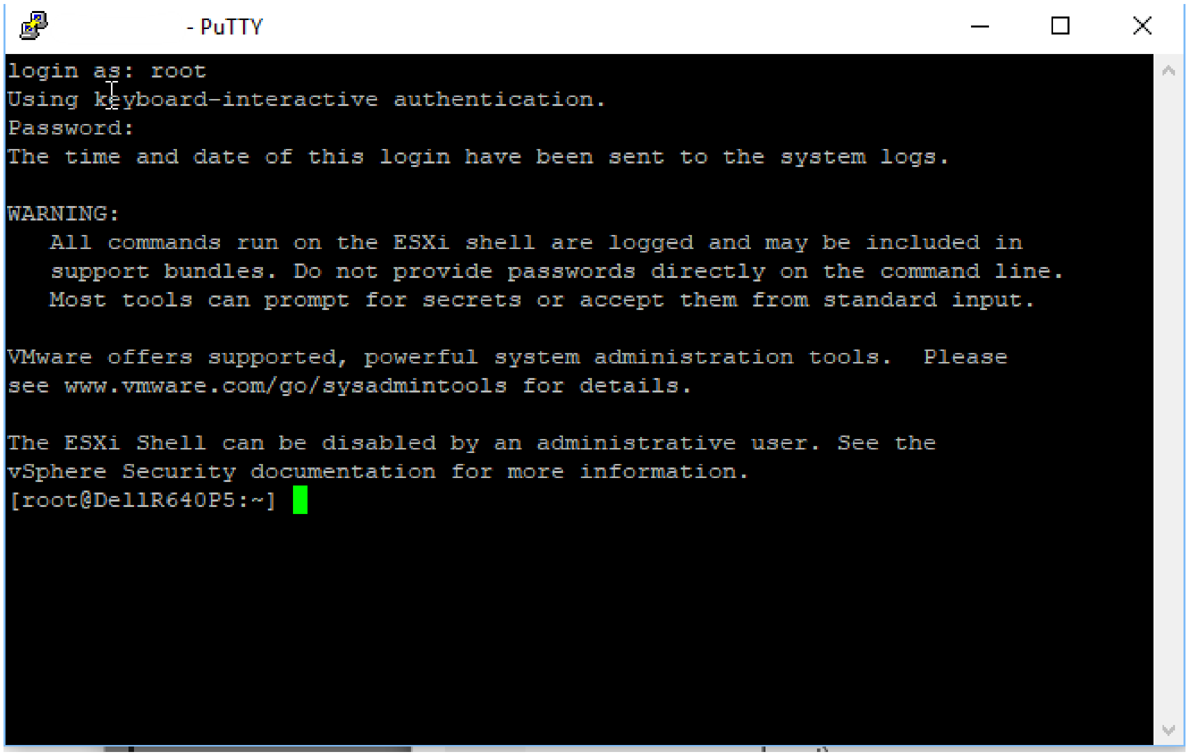
The SAL Gateway does not support Engine ID info exchange; configuring that function has been omitted from this section. For details on creating/supporting Engine ID with other NMS devices, please refer to the following VMware KB article: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-4AF8AA5F-D652-4080-B984-B36A25456A4B.html.

Note:

Starting with ESXi 7.0, MD5 is no longer a supported authenticated method and it has been deprecated due to known weakness on its algorithm. SHA-1 cryptographic hashing algorithm will be deprecated in a future release of vSphere too.

Procedure

1. From a Putty session, via SSH, access the ESXi host. Authenticate using the existing ***root*** credentials.

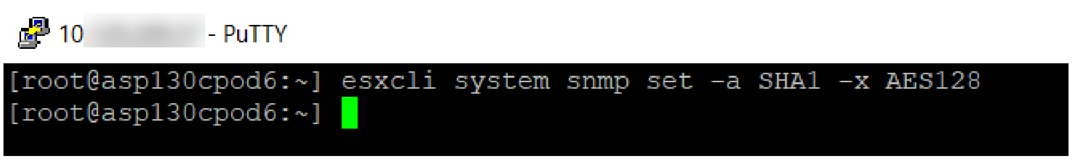


2. Set the *authorization* and *privacy protocols* in ESXi.

```
esxcli system snmp set -a SHA1 -x AES128
```

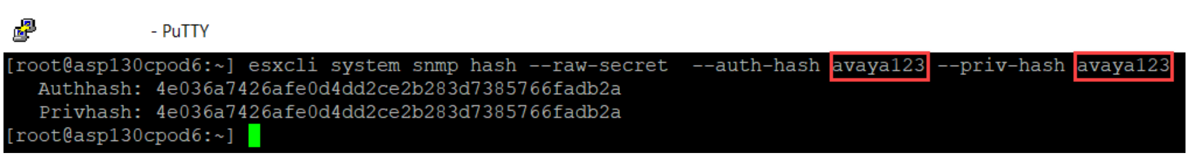
Note:

Syntax is case sensitive.



3. Generate hash values for the privacy and authentication settings.

```
esxcli system snmp hash --raw-secret --auth-hash <authentication password> --priv-
hash <privacy password>
```



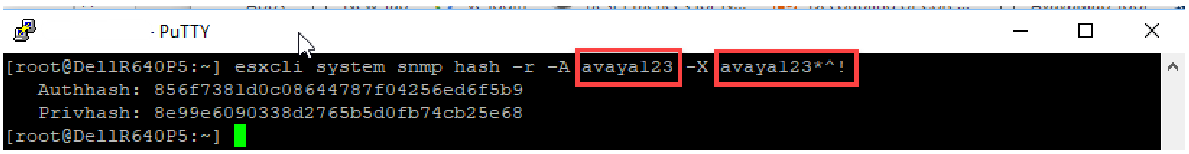
A shorthand method of typing this same command is available:

```
esxcli system snmp hash -r -A <authentication password> -X <privacy password>
```

In the example above, the same avaya123 was used for the authentication and privacy users. This resulted in the same hash key being generated for **`Authhash`** and **`Privhash`**. This method is secure and acceptable.

If even more layers of secure handshake keys are required/desired, unique hash keys foreach element may be generated by selecting unique user secrets for the authentication and privacy elements.

In the example below, the use of unique user secrets, *avaya123* and *avaya123*^!*, produces a unique hash output for each element.



Passwords for ESXi 7.0 must be a minimum of 7 characters long and less than 40 characters.

Characters recommended:

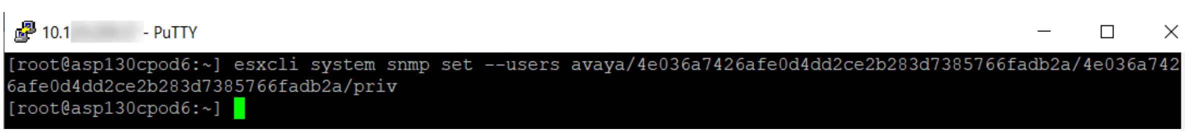
- Lower case and capital letters
- Numbers
- !@ # $ % ^ *

4. Using the hash output values, create a user that will query the SNMP service. The following command will be typed as a line (continuous) command.

```
esxcli system snmp set --users <userid>/authentication hash/privacy hash/model
```

Note:

`model is one of (none|auth|priv).`



In this example, the user is administered as *avaya*. Any user name may be created with a minimum of the same 8 characters that are applied to the hash key secret.

The security option of *priv* provides authentication based on HMAC-MD5 algorithms and AES encryption.

5. Set the SNMP trap receiver(s) for the ESXi host alarms.

```
esxcli system snmp set --v3targets <Receiver IP Address>@162/userid/security-level/message-type
```

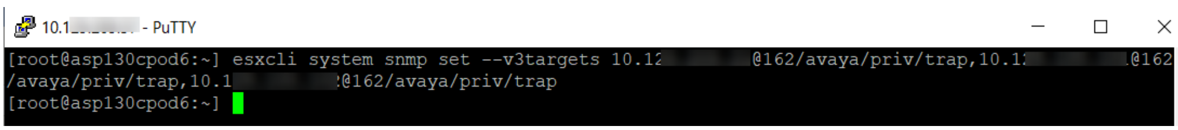
The parameters of the command are as follow

Security-Level: The level of authentication and privacy you have configured. Use *auth* if you have configured authentication only, *priv* if you have configured both authentication and privacy, and *none* if you have configured neither.

Message-type: The type of the messages received by the management system. Use *trap* or *inform*.

Note:

- Port 162 is the standard and default SNMP port for receiving traps, but any port number can be assigned as long as it is matched at both send/receive devices.
- Up to three trap destinations can be administered and must be separated by commas with no subsequent space.



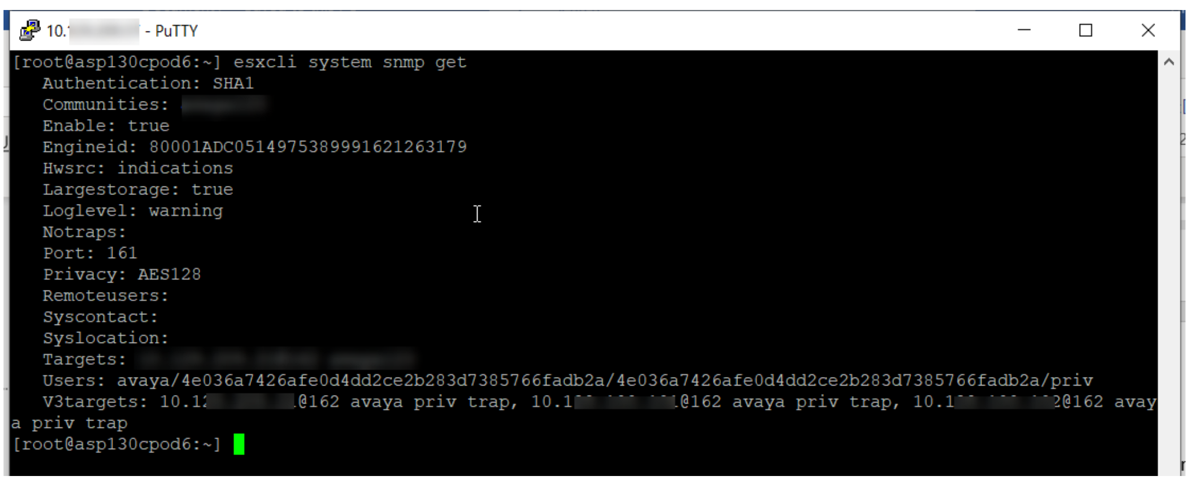
6. Enable SNMP service.

```
esxcli system snmp set --enable true  (to enable)
```

```
esxcli system snmp set --enable false (to disable)
```

7. Review the configuration you have just administered for SNMPv3.

```
esxcli system snmp get
```



8. Once the far end trap receiver has also been configured for SNMPv3, run the following command to send a test trap and confirm that the administered destination(s) is/are sent SNMP notifications:

```
esxcli system snmp test
```

9. Use the following command, if you want to remove the SNMP configuration.

```
esxcli system snmp set --reset
```

Chapter 6: Services Port Verification

Purpose

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation as this may impact integration with other Avaya applications and scripts.

The configuration script for ASP 130 Release 5.1.x is now part of the Avaya tools VIB. When upgrading or performing a fresh install to ASP 130 R5.1.x (7.0 U3c) **and later releases** the services port will be automatically created as part of the first boot and no manual action is required. If this is an ASP 130 4.0 or 5.0 use the *Installing the Avaya Solutions Platform* Release 5.0 document for instructions on running the `ASP130-config-v1.sh` script.

Validating vSwitch1 for Services Port Configuration

About this task

Use this procedure to verify vSwitch1 configuration using the vSphere ESXi host interface under Networking.

Procedure

1. Login into the vSphere Web Client for the ESXi Host.
2. Go to **Networking** > **Port Groups**.

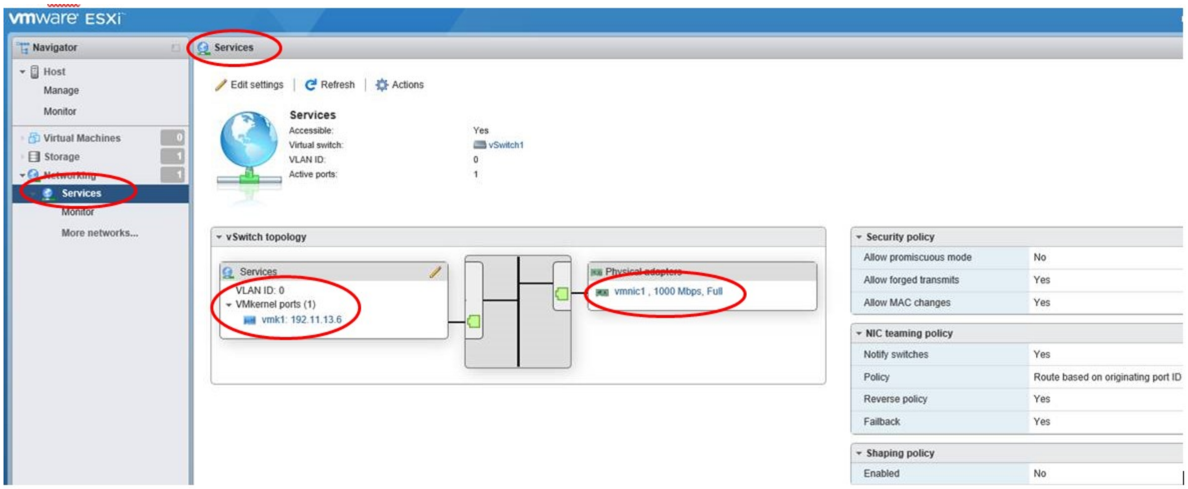
   The Services standard port group should be created and assigned to **vSwitch1**.

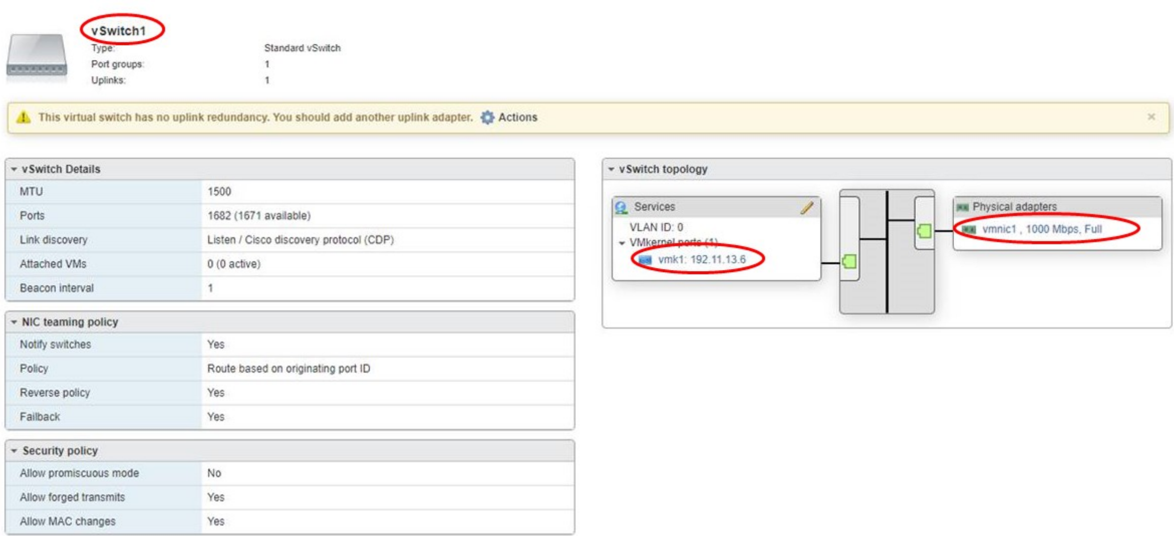
3. Select **Services**.

The Services vSwitch topology should display the following:

- VMkernel port (1): vmk1 should be configured with the **192.11.13.6** IP address
- Physical adapter is vmnic1.
- VLAN ID 0



4. Go to **Networking** > **Virtual Services**.
5. Select **vSwitch1**, and validate the following details:
   - VMkernel port (1): vmk1 should be configured with the 192.11.13.6 IP address.
   - Physical adapter is vmnic1
   - VLAN ID 0

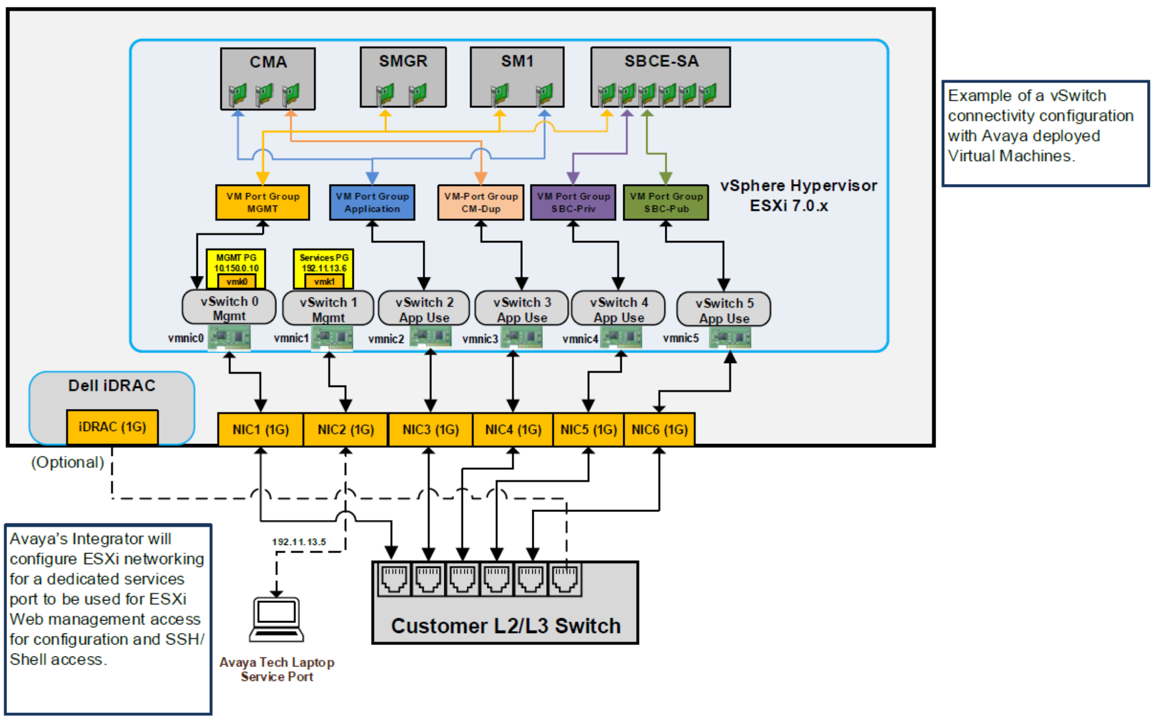


Sample of a typical vSwitch Configuration with a Services Port

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

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

Avaya Solutions Platform 130 - Dell PowerEdge R640 server



Chapter 7: Securing Network Configuration on ASP 130

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

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 rest of the customer network. The OOBM network configuration permits restricted access only to System Administrators.

The Avaya Solutions Platform 130 supports both public and management traffic over the same network interface. On ASP 130, the public network of virtual machines (VM Network) and the management interface of the hypervisor (Management Network) are assigned to vmnic0 as uplink.

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.

Important:

Network configuration on ASP 130 R5.1.x hosts along with deployed applications can either be under Default Mode or OOBM Mode. Configuring management traffic of a few applications on customer's Public Network while the other few on customer's OOBM Network is NOT supported and NOT recommended. Applications that need to be configured in OOBM mode MUST be deployed on ASP 130 hosts with OOBM enabled.

Dell PowerEdge R640 ports

The Avaya Solutions Platform 130 (on PowerEdge R640) supports four NIC ports on its back panel (a maximum of up to three PCIe add-on NIC cards can be installed). The server NIC ports numbering starts from 1 and refers to the external physical NIC ports. The OS VMNIC ports numbering starts from 0 and refers to the NIC ports from the operating system.

NIC port	Server NIC port	OS VMNIC port
First NIC port	Server NIC 1	VMNIC0
Second NIC port	Server NIC 2	VMNIC1
Third NIC port	Server NIC 3	VMNIC2
Fourth NIC port	Server NIC 4	VMNIC3
PCIe Fifth NIC port	Server NIC 5	VMNIC4
PCIe Sixth NIC port	Server NIC 6	VMNIC5

Back 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 occur 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)

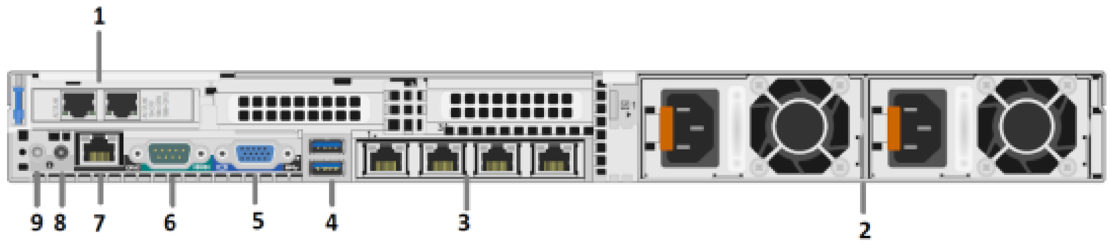


Figure 2: Back View of Dell PowerEdge R640 Single CPU Server with H730P Mini RAID Controller

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

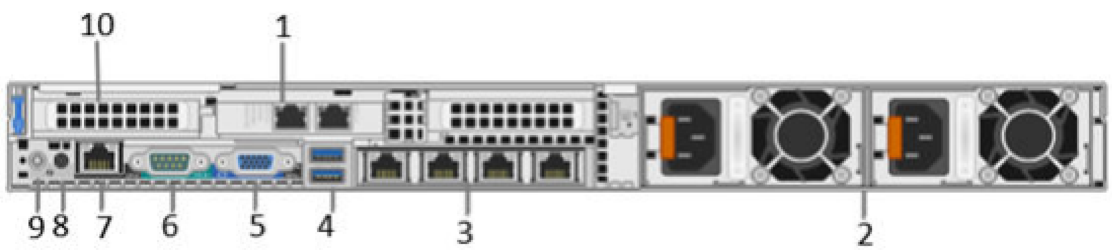


Figure 3: Back View of Dell PowerEdge R640 Single CPU Server with H750 RAID Controller Adapter

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

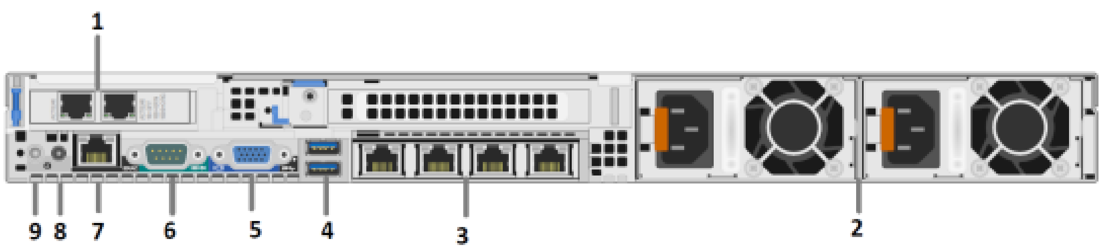


Figure 4: Back View of Dell PowerEdge R640 dual CPU Server with H730P Mini RAID Controller

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

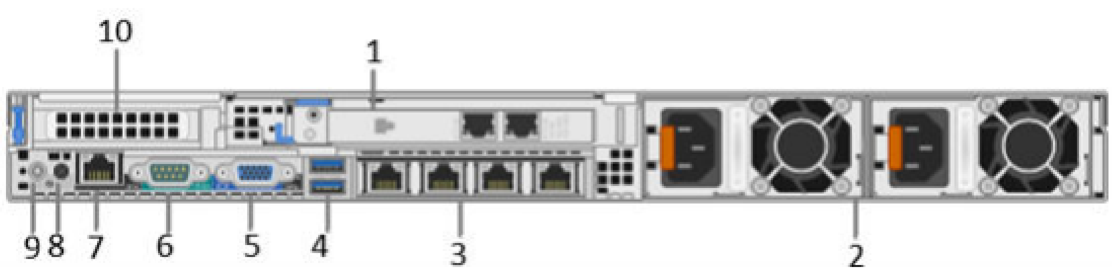
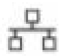


Figure 5: New Configuration of Dual CPU R640 server (H750 and Broadcom 4x1GbE NDC)

Table 12: 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 **vmnic 4&5 are numbered left-to-right.** In **single CPU** configurations the 2x1GbE NIC, located in PCI slot2 has a half-height PCIe faceplate and **vmnic 4&5 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. (vmnic0 – vmnic3 – Left to right viewing from rear of server)
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.

Default mode configuration in ASP 130

The Avaya Solutions Platform 130 installs on the Dell PowerEdge server with the following networking configuration:

- The management traffic of the hypervisor and the management and public traffic of the virtual machines are directed through **vSwitch0** with uplink **vmnic0**, so all IP addresses are on the same network.

- The **SERVICES** port traffic is directed through **vSwitch1** with uplink **vmnic1**.
- No other vmnics are used in this configuration.

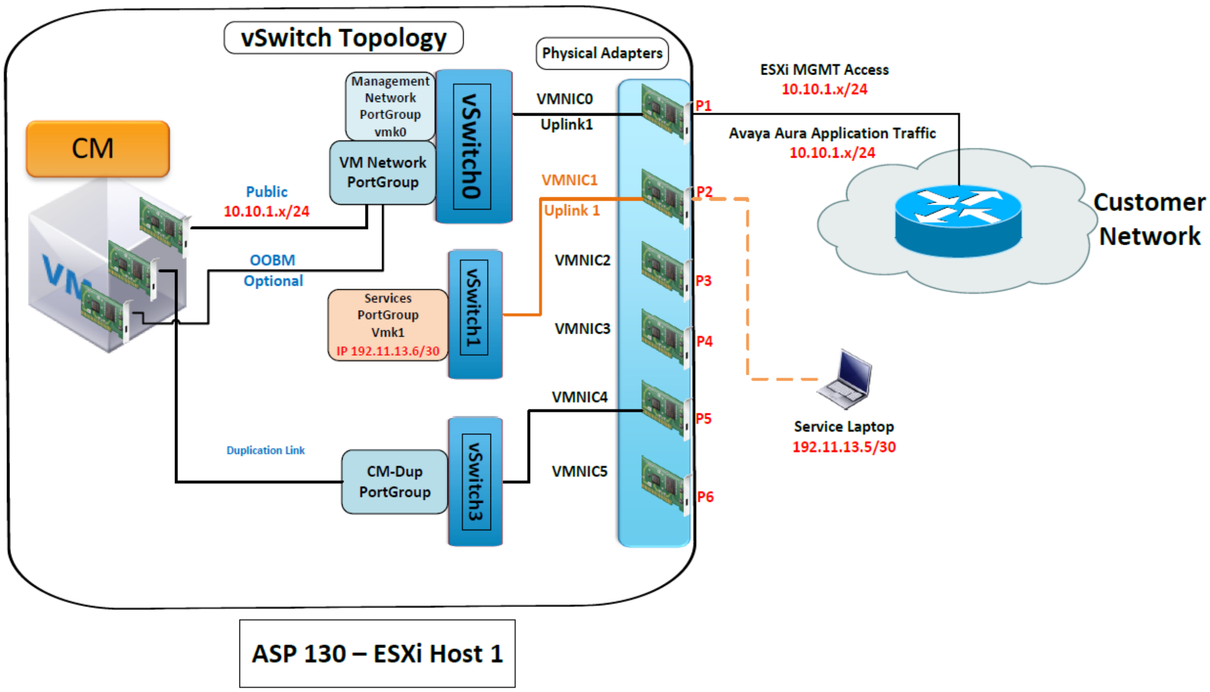


Figure 12: Default mode configuration

This figure is for example purposes only and represents a sample default mode configuration without **OOBM enabled** in Avaya Solutions Platform 130 server. Note that except for the services and OOBM ports, the remaining configuration may vary for each customer environment and applications deployed on each Avaya Solutions Platform 130 server.

OOBM mode configuration in ASP 130

The Avaya Solutions Platform 130 network configuration changes after you enable the OOBM network using the following steps:

- A new virtual switch **vSwitch2** is created with **vmnic2** uplink. The **vmnic2** uplink must be free and available for OOBM configuration.
- The VM Network Port Group remains on **vSwitch0**. However, the Host **Management Network** Port Group label is changed to **OOB Management Network**, and along with the VMkernel **“vmk0”**, these get moved to the newly created **vSwitch2**. When the script completes its job, the user must change the IP address of the VMKernel “vmk0” to an available IP within the Customer Out of Band Management Network to regain access to the host via its new OOBM interface.

Note:

Failure to change the IP address on vmk0 will leave the ESXi host with no Management access.

- A new portgroup **Out of Band Management** is created and added to **vSwitch2**. This is used for Out of Band management traffic of the VMs.
- The **OOB Management Network** Port group assigned to **vSwitch2**, must be configured with an IP address on the same network segment as the customer OOBM network. This network is separated from other subnets/VLANs/IP range, such as what is assigned to **vSwitch0**.
- **vSwitch2** and **vmnic2** separates the OOBM network physically from other customer networks.
- The management traffic of the hypervisor and the virtual machines is directed through **vSwitch2** with uplink **vmnic2**.
- The **SERVICES** port traffic is directed through **vSwitch1** with uplink **vmnic1**.

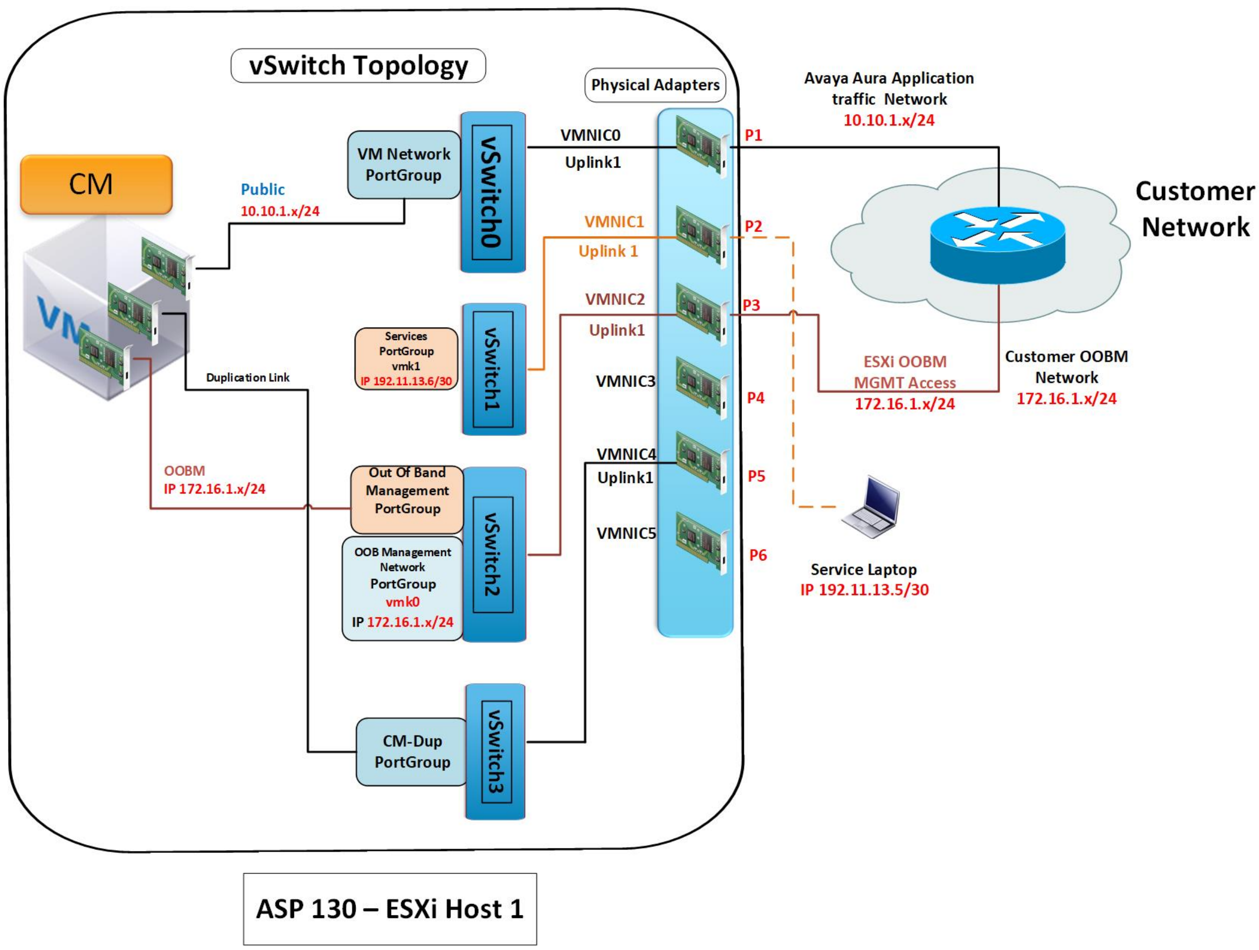


Figure 13: OOBM mode configuration

This figure is for example purposes only and represents a sample default mode configuration with **OOBM enabled** in Avaya Solutions Platform 130 server. Note that except for the services and OOBM ports, the remaining configuration may vary for each customer environment and applications deployed on each Avaya Solutions Platform 130 server.

OOBM configuration on Avaya Solutions Platform 130

You can configure out-of-band management (OOBM) on ASP 130 during one of the following processes:

- Before VM deployment on the ASP 130 host. For example, fresh installation, host remaster, or server recovery/swap.
- After VM deployment on the ASP 130 host. For example, after fresh installation of ASP and migration of hosts from AVP 8.1.x to ASP 130.

Note:

For hosts migrating from previous ASP 130 releases, **vmnic2** must be available for OOBM configuration.

Important:

It is strongly recommended to enable OOBM on a freshly installed ASP 130 server *BEFORE* deploying any VMs on the host. OOBM configuration is service impacting, therefore outage should be planned accordingly for OOBM enablement on hosts that contain deployed VMs. The `asp_oobm_v3.sh` shell script will shut down the VMs before proceeding with OOBM configuration. The VMs have to be manually powered ON after configuring network adapters for OOBM.

For more information on manually powering VMs ON, see Powering VMs ON after disabling OOBM on the host on page 83

Configuring OOBM on ASP 130 before deploying VMs

About this task

OOBM can be configured only through a **SERVICES** port connection to the host. Use the following procedure to configure OOBM on Avaya Solutions Platform 130 before deploying VMs:

Important:

Plan OOBM configuration activity only during maintenance window as it involves network outage thereby resulting in downtime of hosts.

Before you begin

- A secure private network separated from rest of the customer network MUST be available for IP addressing. It is recommended that only System Administrators have access to this network. **MANDATORY**: Connect the LAN cable to the **vmnic2** NIC port (server NIC 3) of the Avaya Solutions Platform 130. Make sure that vmnic2 NIC port is up and accessible before running the script.

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

- Ensure you have one available IP address from the customer's OOBM network.
- To deploy VMs after enabling OOBM on the host, have a System Manager SDM in the same OOBM network, so that the host can be added to the SDM. If you use SDM client on your laptop, then connect to the host through the **SERVICES** port and deploy VMs accordingly.
- Download the `asp_oobm_v3.sh` shell script from the Avaya Support web site or PLDS.

Note:

The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.

- For OOBM specific settings on the deployed VMs, see application specific documentation.

Important:

- To configure OOBM on ASP 130 R5.1.x using `asp_oobm_v3.sh`, **vmnic2** is used as uplink for Out of Band Management traffic of hypervisor. If **vmnic2** is not available, OOBM cannot be configured.
- OOBM configuration should be completed on the host before attempting to configure an application.
- Test OOBM connection to the host before attempting to configure an application.

Note:

When migrating from ASP 120 to ASP 130 the local datastore will retain the AVP "server-local-disk" label. If the available VMFS volume is **server-local-disk** instead of "**datastore1**" it is **OK** to proceed.

Procedure

1. Connect your laptop to **SERVICES** port and configure IP address.
2. Using a SSH client such as WinSCP (Not provided by Avaya), copy the `asp_oobm_v3.sh` shell script to `/vmfs/volumes/datastore1/`.

   You can copy the script using any desire file transfer tool, such us WinSCP (not provided by Avaya).
3. Using a SSH client, login to 192.11.13.6 IP address.
4. In the username field, type `root` and in the password field, type `ACP130_pw` (default) or the password you configured for the root account.
5. Type `cd /vmfs/volumes/datastore1/` and press `Enter` to navigate to the location where you transferred the script.

6. Type `chmod +x asp_oobm_v3.sh` and press `Enter` to grant execute permissions to the shell script.
7. Type `sh asp_oobm_v3.sh` and press `Enter` to view the shell script syntax usage.

   The console displays the following output:

```
Command to configure Out of Band Management on ASP
Management interfaces will be set to vmnic2
Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
Management configuration

WARNING: Contact to the host may be lost due to the movement of ASP host
management connection.
Please make sure you are connected to the host via Services Port before
proceeding with OOBM configuration
```

8. Type `sh asp_oobm_v3.sh enable` and press `Enter` to enable OOBM on the host.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge configuring OOBM on the host.
9. Type `y` and press `Enter` to acknowledge.

```
Performing pre-config checks...
SUCCESS: Hardware Supported for ASP OOBM Configuration
SUCCESS: Platform is ASP, OOBM can be configured

pre-config checks succeeded...
Verifying if vmnic2 is free on ASP130 R5.1...
vmnic2 is free

WARNING: Contact to the host may be lost due to movement of ASP host management
connection. Please make sure you are connected to the host via Services Port. Are
you sure you want to enable Out of Band Management? (Y)es/(N)o: y

Initiated the process of enabling Out of Band Management on the host
```

   The script proceeds to shut down the VMs similar to the following output:

```
Shutting down all the guest VMs deployed on this host

Host has no VMs deployed
Out of Band Management is now enabled on the host

Please change adapter settings of VMs and power on VMs from browser
```

10. There are no VMs deployed now, so ignore the following message:

```
Please change adapter settings of VMs and power on VMs from browser
```

   OOBM is enabled on the host.

   Note:

   During deployment of OVA from SMGR SDM or SDM client, select the **Out of Band Management** portgroup for the VM ethernet interface to connect to the OOBM network.

Next steps

Proceed with changing the vmk0 IP Address settings before deploying VMs. For information on reconfiguring the vmk0 IP Address, see Reconfiguring vmk0 IP Address after enabling OOBM in ASP 130 on page 77.

Configuring OOBM on ASP 130 after deploying VMs

About this task

Use the following procedure to configure OOBM on Avaya Solutions Platform 130 after deploying VMs or after migrating from Avaya Virtualization Platform 8.1.x to Avaya Solutions Platform 130.

Before you begin

- A secure private network separated from rest of the customer network MUST be available for IP addressing. It is recommended that only System Administrators have access to this network.

  MANDATORY: Connect the LAN cable to the **vmnic2** NIC port of the Avaya Solutions Platform 130. Make sure that vmnic2 NIC port is up and accessible before running the script.

  Note:

  Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

- Ensure you have one available IP address from the customer's OOBM network.
- Download the `asp_oobm_v3.sh` shell script from the Avaya Support web site or PLDS.

  Note:

  The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.

- For OOBM specific settings on the deployed VMs, see application specific documentation.

Important:

- To configure OOBM on ASP 130 R5.1.x using `asp_oobm_v3.sh`, **vmnic2** is used as uplink for Out of Band Management traffic of hypervisor. If **vmnic2** is not available, OOBM cannot be configured.
- OOBM configuration should be completed on the host before attempting to configure an application.
- Test OOBM connection to the host before attempting to configure an application.

Note:

When migrating from ASP 120 to ASP 130 the local datastore will retain the AVP "server-local-disk label". If the available VMFS volume is "**server-local-disk**" instead of **datastore1**it is **OK** to proceed.

Procedure

1. Connect your laptop to **SERVICES** port and configure services port IP address for technician's laptop.
2. Using a SSH client such as WinSCP (Not provided by Avaya), copy the `asp_oobm_v3.sh` shell script to `/vmfs/volumes/datastore1/`.

   You can copy the script using any desire file transfer tool, such us WinSCP (not provided by Avaya).
3. Using a SSH client, login to 192.11.13.6 IP address.
4. In the username field, type `root` and in the password field, type `ACP130_pw` (default) or the password you configured for the root account.
5. Type `cd /vmfs/volumes/datastore1/` and press `Enter` to navigate to the location where you transferred the script.
6. Type `chmod +x asp_oobm_v3.sh` and press `Enter` to grant execute permissions to the shell script.
7. Type `sh asp_oobm_v3.sh` and press `Enter` to view the shell script syntax usage.

   The console displays the following output:

   ```
   Command to configure Out of Band Management on ASP
   Management interfaces will be set to vmnic2
   Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
   Management configuration

   WARNING: Contact to the host may be lost due to the movement of ASP host
   management connection.
   Please make sure you are connected to the host via Services Port before
   proceeding with OOBM configuration
   ```
8. Type `sh asp_oobm_v3.sh enable` and press `Enter` to enable OOBM on the host.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge configuring OOBM on the host.
9. Type `y` and press `Enter` to acknowledge.

   If the ASP 130 host was migrated from AVP 8.1.x to ASP 130 and OOBM is being enabled for the first time, the console displays the following output:

   ```
   Performing pre-config checks...

   SUCCESS: Hardware Supported for ASP OOBM Configuration
   SUCCESS: Platform is ASP, OOBM can be configured

   pre-config checks succeeded...
   Verifying if vmnic2 is free on ASP130 R5.1...
   This host is migrated from AVP, therefore OOBM can be configured.
   ```

```
WARNING: Contact to the host may be lost due to the movement of ASP host
management connection. Please make sure you are connected to the host via
Services Port. Are
you sure you want to enable Out of Band Management? (Y)es/(N)o: y

Initiated the process of enabling Out of Band management on the host
```

If the ASP 130 host is freshly installed or if the ASP 130 host was migrated from AVP 8.1.x to ASP 130 and OOBM is being enabled for a second time, the console displays the following output:

```
Performing pre-config checks...
SUCCESS: Hardware Supported for ASP OOBM Configuration
SUCCESS: Platform is ASP, OOBM can be configured

pre-config checks succeeded...
Verifying if vmnic2 is free on ASP130 R5.1...
vmnic2 is free

WARNING: Contact to the host may be lost due to movement of ASP host management
connection. Please make sure you are connected to the host via Services Port. Are
you sure you want to enable Out of Band Management? (Y)es/(N)o: y

Initiated the process of enabling Out of Band Management on the host
```

The script proceeds to shut down VMs similar to the following output:

```
Shutting down all the guest VMs deployed on this host
Shutting down server id: 4
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 1
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 2
serverid: 4 is off
Shutting down server id: 5
Waiting for 20 seconds for serverid: 5 to shut down, attempt: 1
serverid: 5 is off
Shutting down server id: 6
Waiting for 20 seconds for serverid: 6 to shut down, attempt: 1
serverid: 6 is off
Out of Band Management is now enabled on the host

Please change adapter settings of VMs and power on VMs from browser
```

OOBM is enabled on the host.

Next steps

First proceed with changing the vmk0 IP Address settings before enabling OOBM on the VMs. For information on reconfiguring the vmk0 IP Address, see Reconfiguring vmk0 IP Address after enabling OOBM in ASP 130 on page 77.

Once vmk0 IP Address settings are configured, proceed with changing the network adapter settings and enabling OOBM on the VMs. For information on changing the network adapter settings, see Configuring network adapter setting to Out of Band Management on page 76.

Configuring network adapter setting to OOBM

About this task

The VMs are in power OFF state after running the `asp_oobm_v3.sh` shell script as a part of configuring OOBM in the Avaya Solutions Platform 130. Before powering VMs to the ON state, you need to configure the **Network Adapter** setting to **Out of Band Management**.

Before you begin

Connect your laptop to the **SERVICES** port.

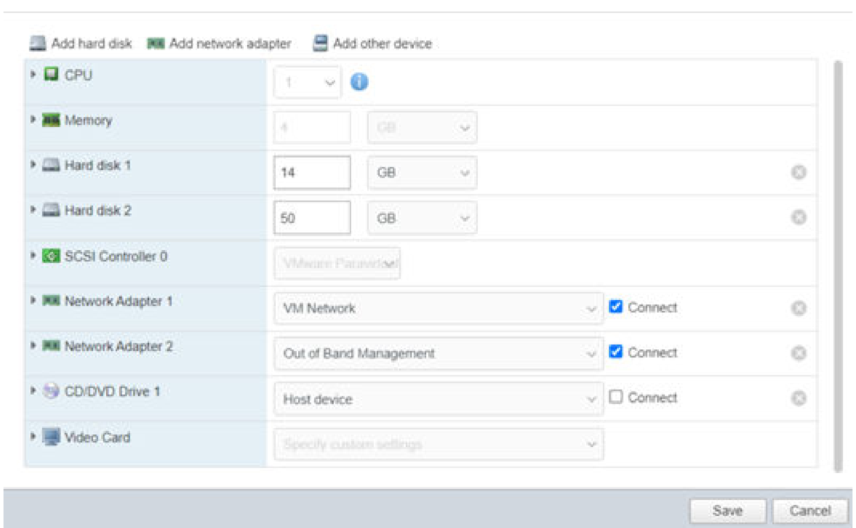
Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
2. In the username field, type `root` and in the password field, type `ACP130_pw` (default) or the password you configured for the root account.
3. Select a VM and navigate to **Actions** > **Edit Settings**.
4. In the **Edit Settings** dialog box, change the **Network Adapter** setting to **Out of Band Management** on the network adpater that will be used for OOBM. The setting change connects the OOBM ethernet interface of the VM to the OOBM Network.

   Important:

   Perform this step for all VMs and follow application specific documentation to fully enable OOBM for each VM.

   For example, the following Communication Manager VM screenshot displays the **Network Adapter 2** or eth1 interface that supports OOBM configuration. This is because the **Network Adapter 2** setting is changed to **Out of Band Management** portgroup. Additional OOBM configuration is required on the CM SMI to complete the OOBM configuration for CM. Refer to respective guides of all products to configure OOBM network for the respective products.



5. After configuring the Network Adapters of all VMs to **Out of Band Management** portgroup you can power ON all the VMs.

   Access management interface of all VMs and host from OOBM network.

   Note:

   During deployment of OVA from System Manager SDM or SDM client, select the **Out of Band Management** portgroup for the VM ethernet interface to connect to the OOBM network. Refer to respective guides of all products to configure OOBM for the respective products.

Reconfiguring vmk0 IP Address after enabling OOBM in ASP 130

About this task

When enabling OOBM in ASP 130 servers, the VMkernel **vmk0** is migrated from vSwitch0 (former in-band Management connection) to **vSwitch2** to become part of the Customer OOBM network and provide Out of band management access to ESXi host. Therefore, vmk0 IP Address must be re-configured to accommodate this change.

Before you begin

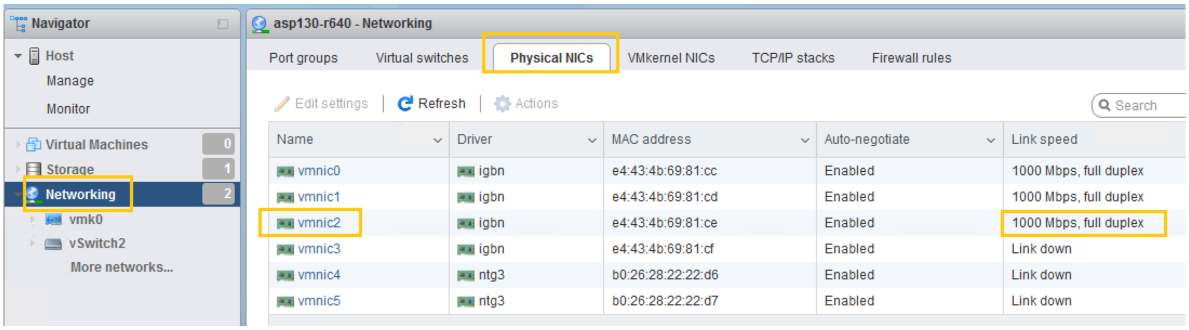
1. Connect your laptop to the **SERVICES** port.
2. Ensure that there is one available IP address from the customer’s OOBM network for each ESXi host.

Procedure

1. Open a web browser and go to `https://192.11.13.6/ui` to open the vSphere HTML client.
2. In the **username** field, type `root` and in the **password** field, type `ACP130_pw` (default) or the password previously configured for the root account.
3. From the menu on the left, navigate to **Networking** > **Physical NICs**.
4. Verify that the **vmnic2** status under link speed is displaying **1000 Mbps, full duplex**.

   Warning:

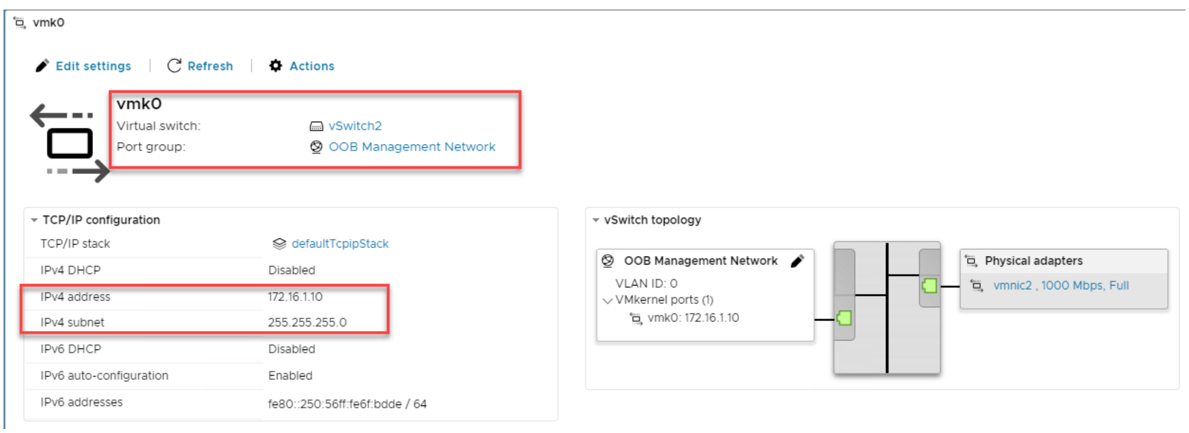
   If the link status is down, ensure that vmnic2 (Server NIC3) is properly wired and connected to the customer switch prior to proceeding.



5. Go to **Networking** > **VMkernel NICs**.
6. Click **vmk0** > **Edit settings**.
7. If required, expand the IPV4 settings view.
8. In the **Address** field, enter the new IP Address to be set that is part of the **customer out of band management network**.

   For example, `172.16.1.10`
9. In the **Subnet mask** field, enter the subnet mask to be set that is part of the **customer out of band management network**.

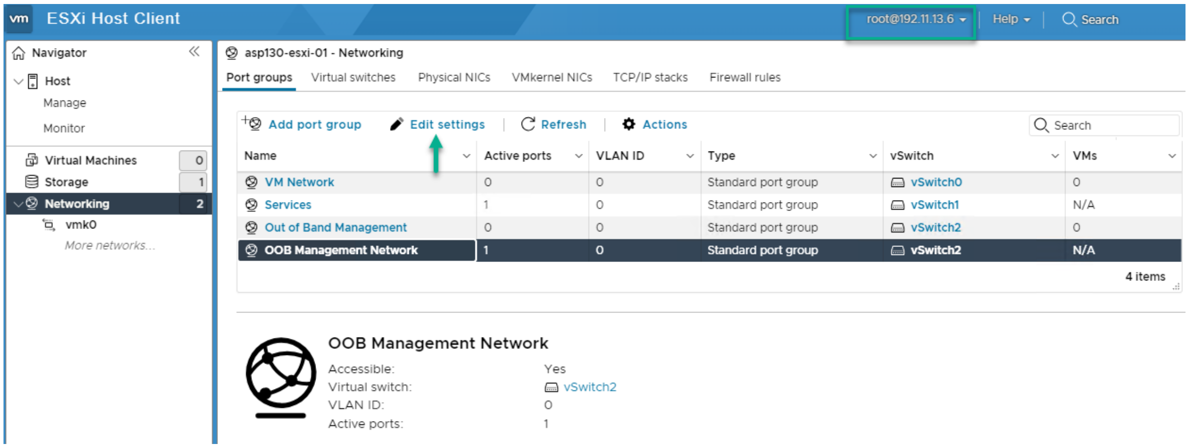
   For example, `255.255.255.0`
10. Click **Save**.



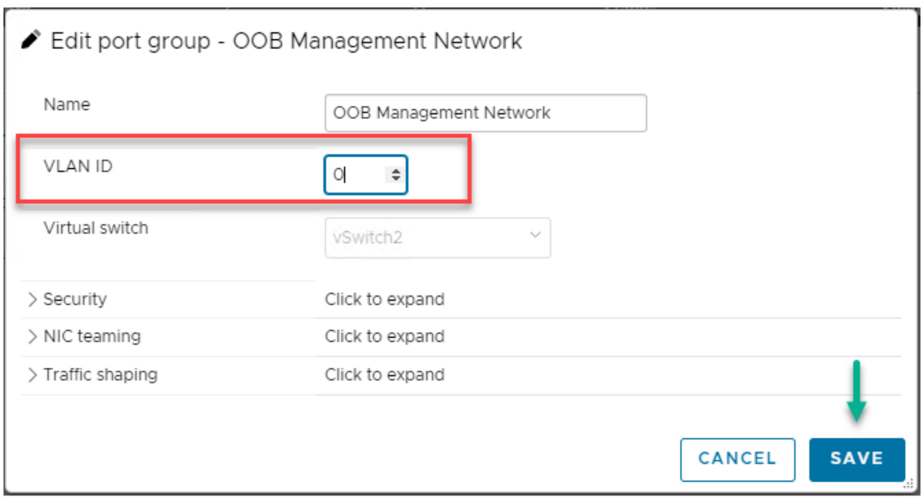
11. Go to **Networking** > **Port Groups**.
12. Select the **OOB Management Network** Port Group and click the **Edit settings** button.

   Note:

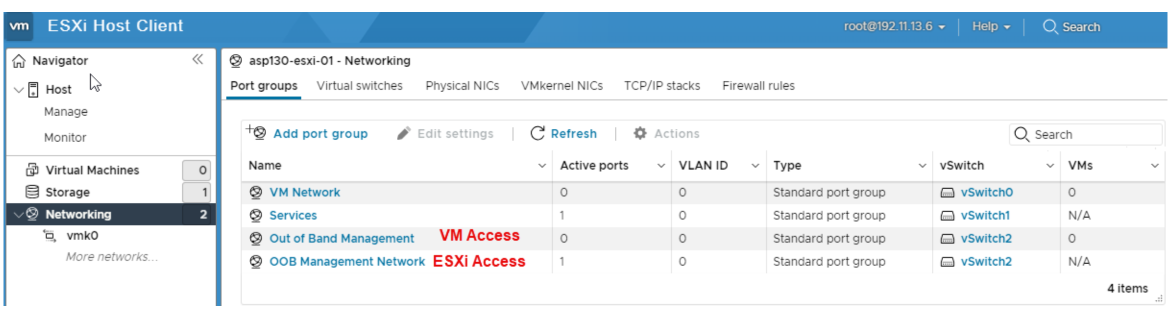
   Management Network Port group is now assigned to **vSwitch2**.



13. If required by the customer network, set the VLAN ID for the customer OOBM subnet. This must be provided by the customer. Otherwise leave 0, to disable VLAN Tagging on the VMkernel port.



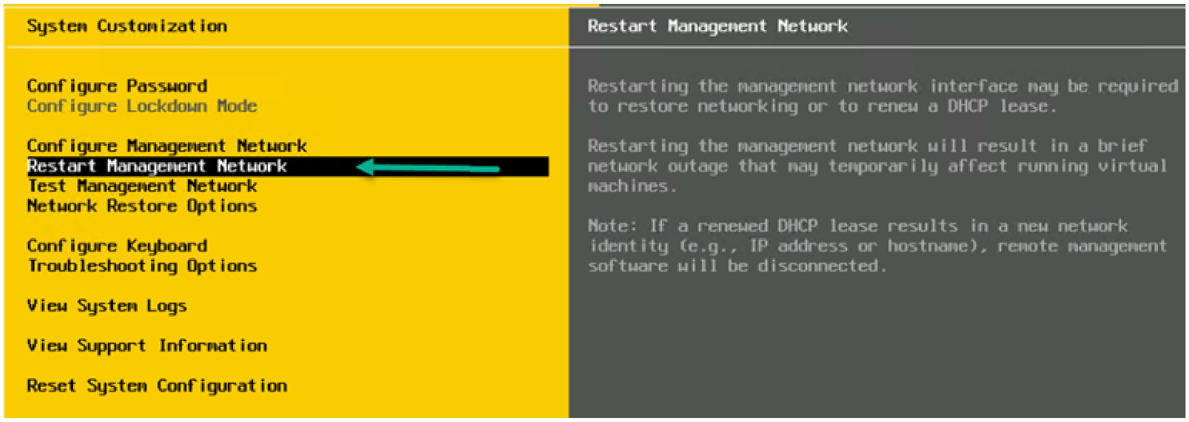
14. When ready, click **Save**.



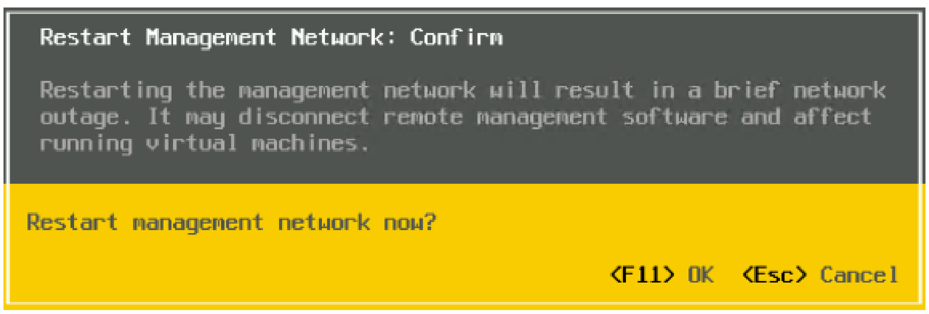
15. Navigate to **Networking** > **TCP/IP stacks**.
16. Click **Default TCP/IP stack** > **Edit settings**.
17. In the **IPv4 gateway** field, enter the default gateway to be set that is part of the **customer out of band management network**.

For example, `10.10.1.1`

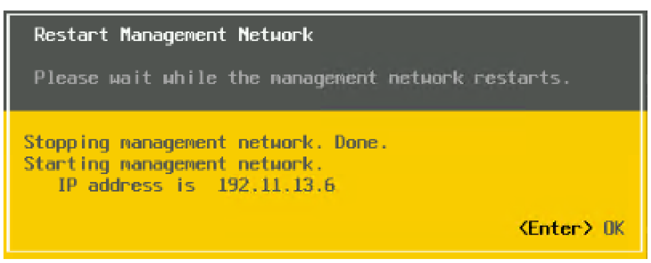
18. Click **Save**.
19. Using a monitor and keyboard, access the ESXi host DCUI.
20. Press **F2** and authenticate using the existing `root` credentials.
21. Using the down arrow key, select **Restart Management Network** and press **Enter**.



22. Press **F11** to restart the management network.

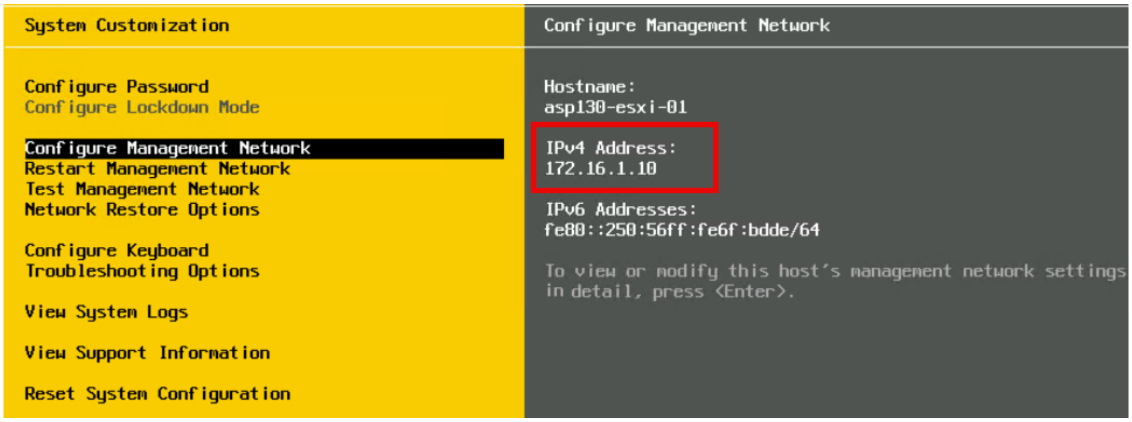


23. Press **Enter** when completed.



24. Press the up arrow key to select **Configure Management Network**.

25. IP Address display is now the one configured for OOBM ESXi access.



26. Repeat steps with remaining ESXi hosts until complete.

Disabling OOBM on Avaya Solutions Platform 130

About this task

The following procedure configures in-band management again on the host.

Important:

- Reconfigure in-band management on the VMs before disabling OOBM on the host.
- An IP MUST be available on the Public Network before disabling OOBM.
- Test Public network access to the host before attempting to configure an application.

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

Note:

When migrating from ASP 120 to ASP 130 the local datastore will retain the AVP "server-local-disk" label. If the available VMFS volume is "**server-local-disk**" instead of "**datastore1**", it is **OK** to proceed.

Procedure

1. Connect your laptop to **SERVICES** port and configure services port IP address for technician's laptop.
2. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
3. In the username field, type `root` and in the password field, type `ACP130_pw` (default) or the password you configured for the root account.

4. Select a VM and navigate to **Actions** > **Edit Settings**.
5. In the **Edit Settings** dialog box, change the **Network Adapter** setting from **Out of Band Management** to **VM Network**. The setting change connects the ethernet interface of VM from OOBM Network back to customer's public network.

   Important:

   Perform this step for all VMs.
6. Using a SSH client such as WinSCP (Not provided by Avaya), copy the `asp_oobm_v3.sh` shell script to `/vmfs/volumes/datastore1/`.

   The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.
7. Type `chmod +x asp_oobm_v3.sh` and press `Enter` to grant execute permissions to the shell script.
8. Type `sh asp_oobm_v3.sh` and press `Enter` to view the shell script syntax usage.

   The console displays the following output:

```
Command to configure Out of Band Management on ASP
Management interfaces will be set to vmnic2
Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
Management configuration

WARNING: Contact to the host may be lost due to the movement of ASP host
management connection.
Please make sure you are connected to the host via Services Port before
proceeding with OOBM configuration
```

9. Type `sh asp_oobm_v3.sh disable` and press `Enter` to disable OOBM on the host.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge disabling OOBM on the host.
10. Type `y` and press `Enter` to acknowledge.

```
Performing pre-config checks...

SUCCESS: Hardware Supported for ASP OOBM Configuration
SUCCESS: Platform is ASP, OOBM can be configured

pre-config checks succeeded...

WARNING: Contact to the host may be lost due to the movement of ASP host
management connection. Please make sure you are connected to the host via
Services Port. Are
you sure you want to disable Out of Band Management? (Y)es/(N)o: y

Initiated the process of disabling Out of Band management on the host
```

   The script proceeds to shut down the VMs similar to the following output:

```
Shutting down all the guest VMs deployed on this host
Shutting down server id: 4
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 1
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 2
```

```
serverid: 4 is off
Shutting down server id: 5
Waiting for 20 seconds for serverid: 5 to shut down, attempt: 1
serverid: 5 is off
Shutting down server id: 6
Waiting for 20 seconds for serverid: 6 to shut down, attempt: 1
serverid: 6 is off
Out of Band Management is now disabled on the host

Please change adapter settings of VMs and power on VMs from browser
```

OOBM is disabled on the host.

Next steps

Before powering on VMs, proceed with Reconfiguring vmk0 IP Address after disabling OOBM in ASP 130 on page 84.

Powering VMs ON after disabling OOBM on the host

About this task

The VMs are in power OFF state after running the `asp_oobm_v3.sh` shell script as a part of disabling OOBM in the Avaya Solutions Platform 130. Before powering VMs to the ON state, check if **Network Adapter** is set to **VM Network**.

Before you begin

Connect your laptop to the **SERVICES** port.

Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
2. In the username field, type `root` and in the password field, type `ACP130_pw` (default) or the password you configured for the root account.
3. Select a VM and navigate to **Actions** > **Edit Settings**.
4. In the **Edit Settings** dialog box, verify if **Network Adapter** is set to **VM Network**.

   Important:

   Perform this step for all VMs.
5. Power ON all VMs.

   Access the management interface of all VMs and the ESXi host from the customer's network to verify connectivity/access.

Reconfiguring vmk0 IP Address after disabling OOBM in ASP 130

About this task

When disabling OOBM in ASP 130 servers, the VMkernel **vmk0** is migrated from vSwitch2 (former out of band Management connection) to **vSwitch0** to become part of the Public network and provide in-band management access to ESXi host. Therefore, vmk0 IP address must be re-configured to accommodate this change.

Before you begin

1. Connect your laptop to the **SERVICES** port.
2. Ensure that there is one available IP address from the Public network for each ESXi host.

Procedure

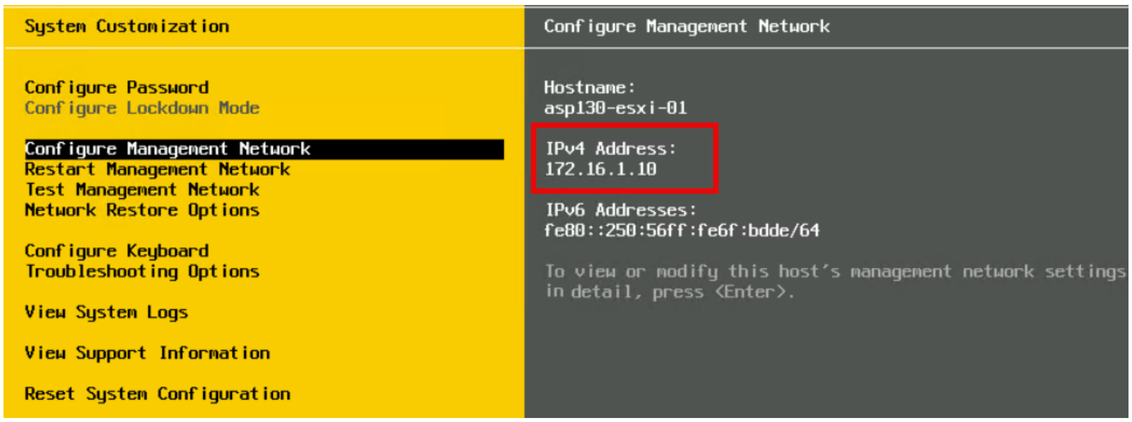
1. Open a web browser and go to `https://192.11.13.6/ui` to open the vSphere HTML client.
2. In the **username** field, type `root` and in the **password** field, type `ACP130_pw` (default) or the password previously configured for the root account.
3. From the menu on the left, navigate to **Networking** > **VMkernel NICs**.
4. Click **vmk0** > **Edit settings**.
5. If required expand the IPV4 settings view.
6. In the **Address** field, enter the new IP Address to be set that is part of the **Public network**.

   For example, `10.10.1.10`
7. In the **Subnet mask** field, enter the subnet mask to be set that is part of the **Public network**.

   For example, `255.255.255.0`
8. Click **Save**.
9. Navigate to **Networking** > **TCP/IP stacks**.
10. Click **Default TCP/IP stack** > **Edit settings**.
11. In the **Routing** > **IPv4 gateway** field, enter the default gateway to be set that is part of the **customer in-band management network**.

    For example, `10.10.1.1`
12. Click **Save**.
13. Disconnect and remove the Ethernet cable from **VMNIC2/NIC3** and the services port network.
14. Using a monitor and keyboard, access the ESXi host DCUI.
15. Press **F2** and authenticate using the existing root credentials.

16. Using the down arrow key,select **Restart Management Network** and press **Enter**.
17. Press **F11** to restart the management network.
18. Press **Enter** when completed.
19. Press the up arrow key to select **Configure Management Network**.
20. IP Address display is now the one configured for ESXi Inbound Management access.



21. Repeat the steps for the remaining ESXi hosts until complete.

Chapter 8: Performing server recovery or software remastering

Note:

Due to changes in our third-party vendor agreement, all NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. A unique standard license key will be provided on a label on the ASP 130 server lid. In the event of a server replacement, the server lid with the ESXi license key must be moved to the new replacement server. Existing ASP 130 servers with a license obtained from PLDS are **not** impacted by this change, only new orders shipped from Avaya's Integrator and warehouses. Existing inventory that was previously sold to Distributors and Partners and is present in their supply chain, will still have the old key. Only when they replenish stock with new orders, post the cutover, will the change take place. *Target cutover is tentatively scheduled for early-mid August, 2024, subject to change. Ensure you are signed up for e-notification.*

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.

Note:

In the case of a hardware failure, if hard disk drives (HDDs) have failed or are not able to be imported to the new server, then both a server replacement and software reinstallation will be required.

Before you begin

Ensure that you have the following:

- Console VGA monitor.
- USB Keyboard.
- Appropriate ESXi software downloaded from PLDS. See PCN2146S Avaya Solutions Platform 130 5.1.x

- 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* 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.
- Best practice would be to not cable out the physical NICs on an ASP 130 R5.1.x.x until ESXi 7.0.x has been loaded and the host IP address assigned.

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. If you are replacing the server, the user should try to import the drives from the failed server. If the import does not work, follow the procedures for Software Remastering below.

Reference *Dell R640 FRU replacement* and *RAID Configuration* chapters of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series* for detailed steps. High level summary of steps is provided below.

Note:

Whether importing of HDDs is successful or not, steps 2 and 3 must be executed.

Procedure

1. Attempt to import the drives (HDDs) from the failed server to the replacement server. Reference *Dell R640 FRU replacement* chapter of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series* document.
   - If importing the drives is successful, reboot the server. Replacement server now has all previous configurations of ESXi
   - If importing the drives is not successful, follow the detailed steps for RAID configuration in *RAID Configuration* chapter of the *Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series* document. Once the RAID configuration is complete, follow the steps in the *Software remastering* section below.
2. 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* and select the latest version of the PSN.
3. Enable and configure iDRAC on the replacement server. For more information, see *Avaya Converged Platform 130 Series iDRAC9 Best Practices*.

Software remastering

About this task

If it is determined that the server hardware is healthy and software needs to be reinstalled, or if importing HDDs into replacement server is not successful, a remaster of the server software is required.

Before you begin

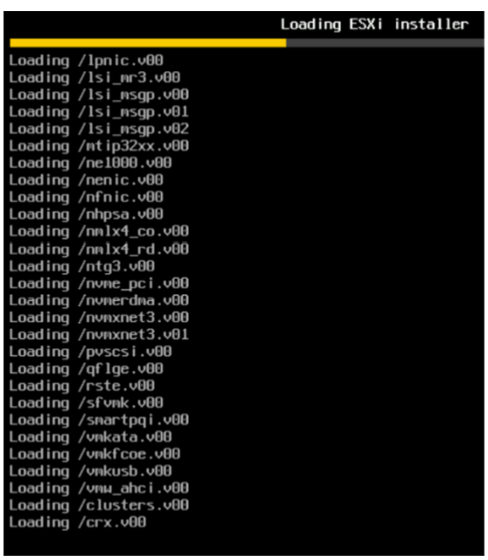
- **Disconnect all Ethernet connections** to the server, including the services port, except vmnic0 (NIC1) and power on the server. It is permissible if the server is not connected to any Ethernet connections.
- During boot, the server will not boot from the DVD drive if the ISO was not correctly burnt to the DVD (issue with physical media or burner) or if the server was set to boot from the HDD first and not the DVD drive.
    1. If latter is the issue, select **F11** during server reboot/power up and access the **Boot Manager**.
    2. On the Boot Manager window, select **One-shot UEFI Boot Menu**.
    3. Select **Embedded SATA Port Optical Drive L: EFI DVD/CDROM1**.

  The server is set to boot from the DVD drive for this current one-time boot instance.

Procedure

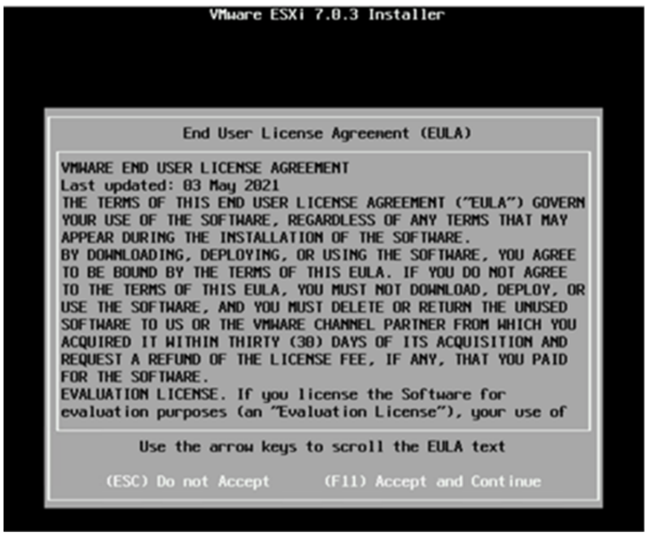
1. Download the ESXi installation ISO file from PLDS.
2. Burn the ESXi installation ISO file on a DVD.
3. Place the ESXi installation DVD in the DVD tray and power up/reboot the server. Server should boot from DVD media.

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

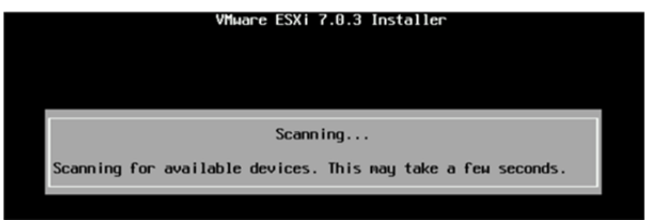
   

4. When this screen appears, press the `Enter` key to continue the installation process.

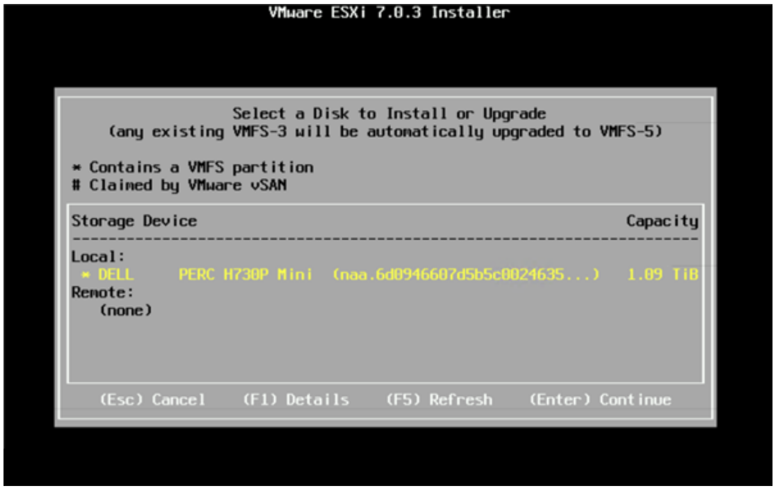
5. VMware provides a 60 day trial license during initial deployment. A permanent license will be deployed post ESXi installation. Press `F11` to accept the licensing conditions and continue the installation.

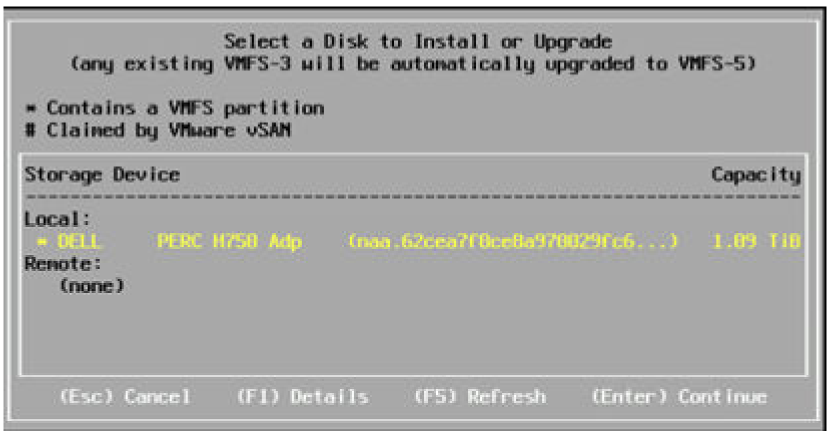


6. The installation program will then scan the server to identify all available drives to accept the software.



7. From the list of options, highlight the local DELL PERC H730P Mini or Dell PERC H750 Adapter Disk (depending on server configuration) and press the `Enter` key.





If the PERC H730P Mini or Dell PERC H750 Adapter (depending on server configuration) is not displayed as a disk for installation, then configure the H730P/H750 RAID Controller first before installation. For more information, see Dell R640 RAID Configuration on page 122. Once the RAID configuration is complete, you can start the installation process again.

8. If the screen below appears and a fresh installation is required then select **Install ESXi, overwrite VMFS datastore** and press **Enter**.

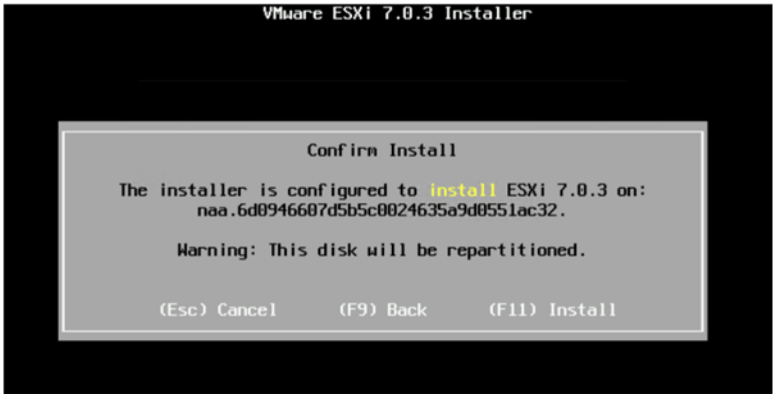
9. Select the language to be used on the ASP 130 solution and press `Enter` to continue.

10. Create a root password of `ACP130_pw`.

Note:

`ACP130_pw` is an example password that is used for Avaya pre-staged servers. Avaya recommends that the customer change the password to a unique, secure password.

11. Press `F11` to continue the installation process for ESXi vSphere 7.0.x.



12. When installation completes, remove media, that is, USB stick or DVD, and press `Enter` to reboot the server and boot ESXi software.

13. Press **Enter** to reboot and boot the ESXi software.

    The server will shutdown and then reboot.

14. Proceed with the next steps.

Next steps

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

- Configure ESXi network settings. For more information, see Configuring ESXi Network Settings on page 38.
- Add the license key and install the license. For more information, see Adding the license key for server recovery or software remastering on page 93.
- If required, install Avaya EASG VIB.
- If required, configure iDRAC and SNMP (iDRAC and ESXi).

Adding the license key for server recovery or software remastering

About this task

To perform server recovery or software remastering, you will need to add the original VMware license key.

Before you begin

Ensure that you:

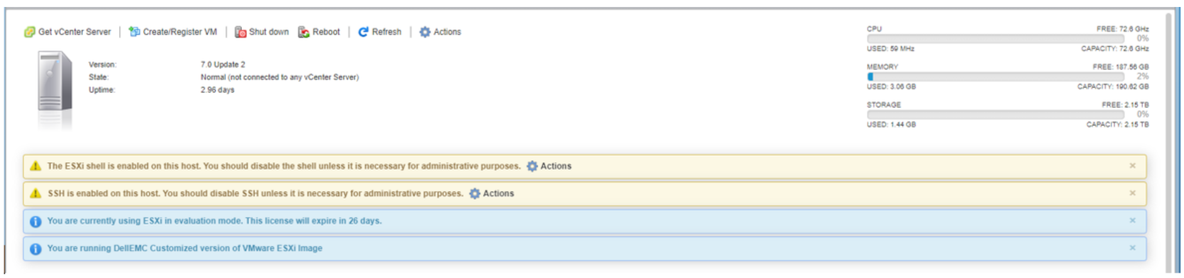
- Acquire the ESXi 7.0 license key from PLDS for the newly installed server.

Procedure

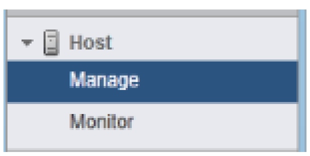
1. Log in to the ESX/ESXi host at the URL `https:// [IP Address of host]/ui`.

   Replace *[IP Address of host]* in the URL with the actual IP address of the host.

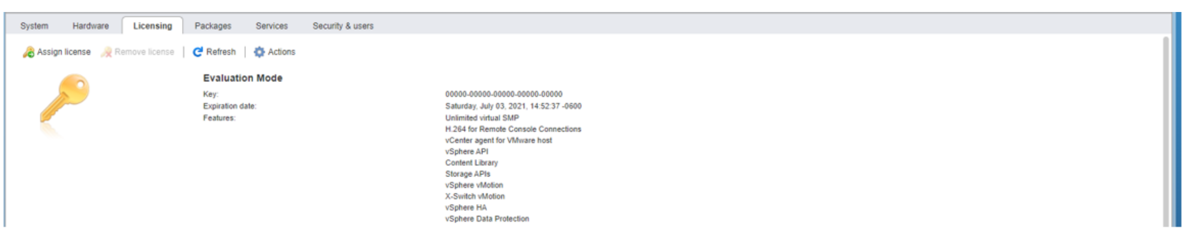
2. From the main ESXi management interface page, there is a notice about the system being in an ESXi evaluation mode for 60 days. Once the customer's license key is assigned to ESXi this warning message will clear.

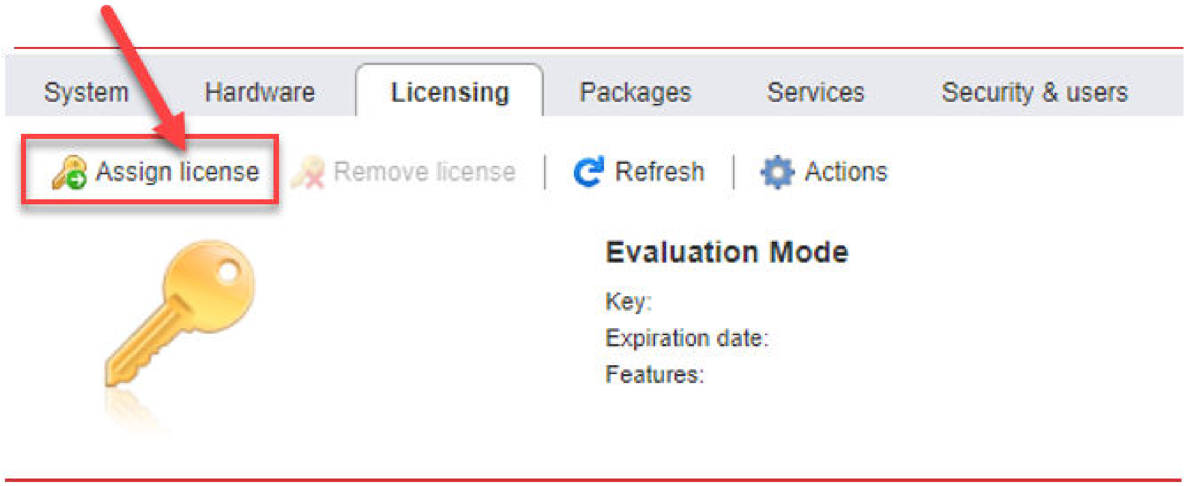
   

3. In the Navigator pane on the left, click **Manage**.

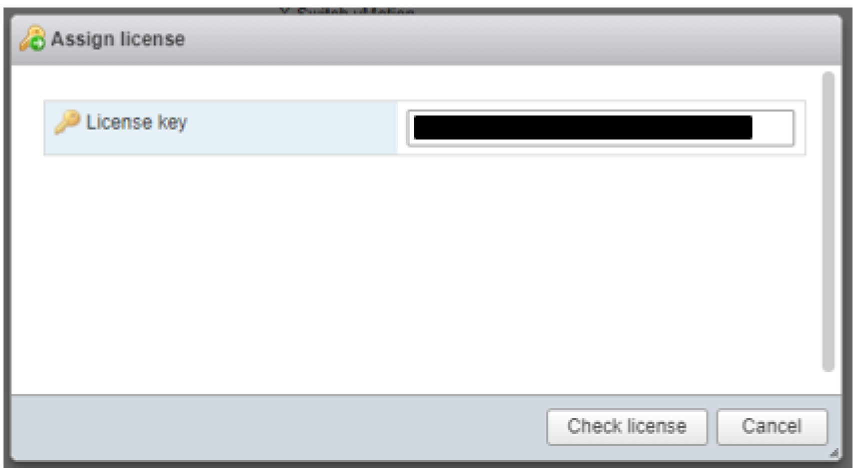
   

4. On the **Licensing** tab, click **Assign license**.

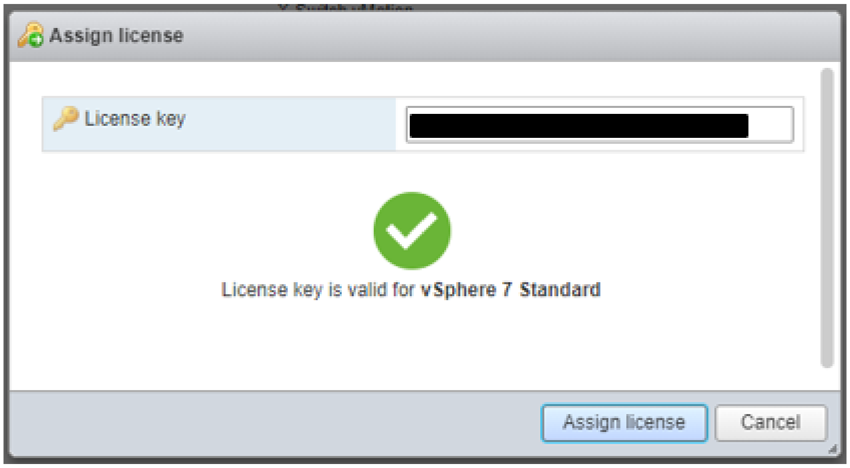
   



5. In the subsequent dialog box, copy and paste in the license key. Click the **Check License** button.



6. VMware will validate the license and return a green check mark, indicating the key is valid. Click **Assign license** to apply it and complete the process.



Installing the Avaya Enhanced Access Secure Gateway

About this task

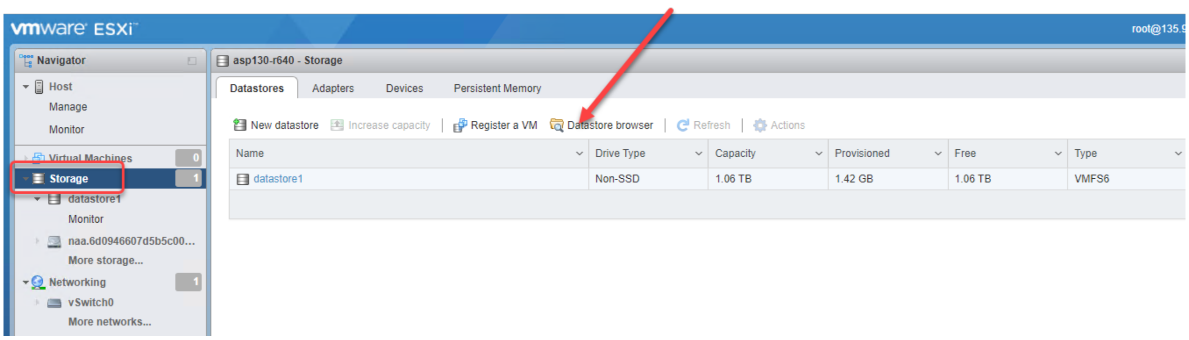
After installing ASP 130 R5.1, install the Avaya EASG VIB zip file.

Before you begin

Download the Avaya EASG zip file from Avaya PLDS and place it in a folder on your local PC. See PCN2146S for the latest version of the Avaya EASG zip file.

Procedure

1. From your local PC, log into the ESXi host at the URL *https:// [IP Address of host]/ui*. Replace *[IP Address of host]* in the URL with the actual IP address of the host.
2. From the main ESXi management interface page, select **Storage** > **Datastore browser**.

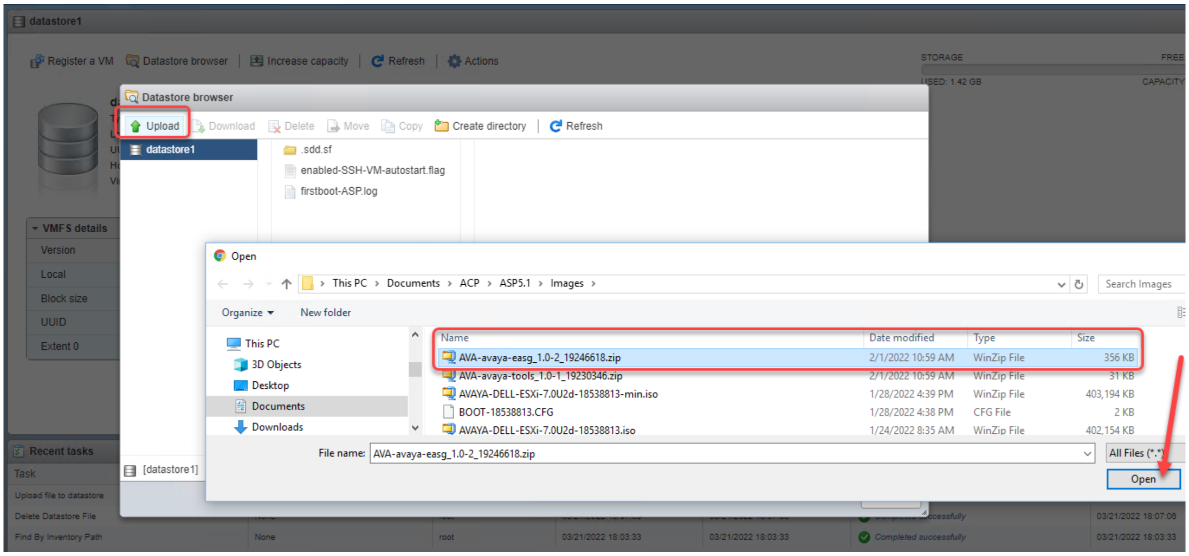


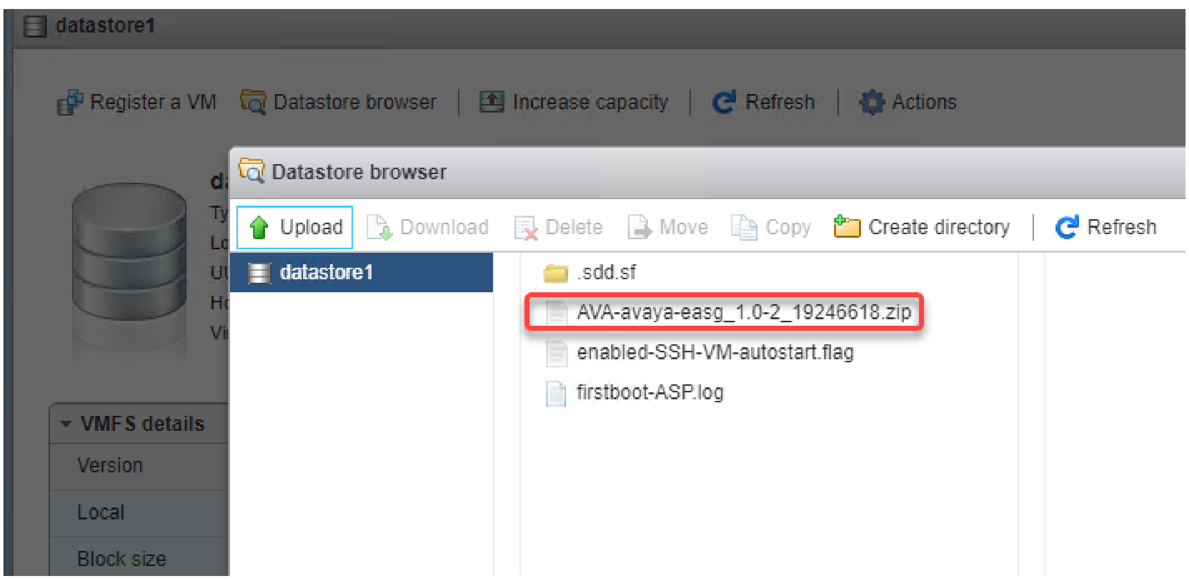
3. Click **Upload**.

4. Select the Avaya EASG file on your local PC and then select **Open**. EASG zip file will copy to VMFS datastore on ESXi host.

   Note:

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





5. From a Putty session, via SSH, access the ESXi host. Accept EULA and `cd` to `vmfs/volumes/datastore1 <Enter>`
6. Type: `ls <Enter>` and verify Avaya EASG zip file is present.

   Note:

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

```
Do you accept the terms of this EULA? Press (Y/y) to accept, (N/n) to decline: ySaving current state in /bootbank
Creating ConfigStore Backup
Locking esx.conf
Creating archive
Unlocked esx.conf
Using key ID
fd1cc2cf-416f-42e3-b831-390ce35c0179 to encrypt
Clock updated.
Time: 00:37:58   Date: 03/22/2022   UTC
[root@asp130-r640:~] cd /vmfs/volumes/datastore1/
[root@asp130-r640:/vmfs/volumes/6238a0c7-e2254ece-025d-e4434b1d80d8] ls
AVA-avaya-easg_1.0-2_19246618.zip  etc
enabled-SSH-VM-autostart.flag      firstboot-ASP.log
[root@asp130-r640:/vmfs/volumes/6238a0c7-e2254ece-025d-e4434b1d80d8]
```

7. Verify the checksum of the EASG zip file matches checksum on PLDS.
8. Type the following command to install the Avaya EASG: `esxcli software vib install -d /vmfs/volumes/datastore1/<Avaya EASG file name.zip> <Enter>`. Avaya EASG VIB should install. See screen shot below for expected output.
9. Type the command **`EASGStatus <Enter>`** to verify EASG is enabled.

Note:

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

```
[root@asp130-r640:/vmfs/volumes/6238a0c7-e2254ece-025d-e4434b1d80d8] esxcli software vib install -d /vmfs/volumes/datastore1/AVA-avaya-easg_1.0-2_19246618.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: AVA_bootbank_avaya-easg_1.0-2
   VIBs Removed:
   VIBs Skipped:
[root@asp130-r640:/vmfs/volumes/6238a0c7-e2254ece-025d-e4434b1d80d8] EASGStatus
EASG is enabled
[root@asp130-r640:/vmfs/volumes/6238a0c7-e2254ece-025d-e4434b1d80d8]
```

Chapter 9: Certificate Administration

Regenerate the SSL self-signed certificates on ESXi 7.0

About this task

During the installation of an ESXi host, the installer generates a self-signed certificate that contains `localhost.localdomain` as the common name. After you configure the hostname of a host, a mismatch between the hostname and the common name in the certificate occurs.

This procedure can be used also when the default self-signed SSL certificate installed on ESXi is about to or has expired.

Note:

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

Note:

ESXi host does not need to be entered in maintenance mode to conduct this activity.

Warning:

Avoid any administrative tasks such as creating back up jobs, taking VM snapshots or making configuration changes to the host when conducting this procedure.

Before you begin

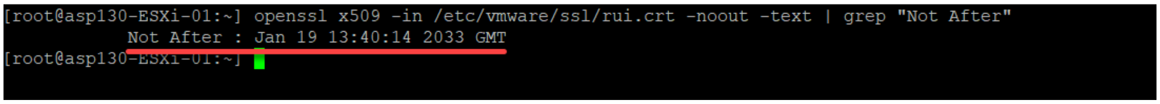
- Access to the ASP 130 server management network either through a SAL Gateway connection (Remotely) or direct service port connection (onsite).
- SSH tool, that is, Putty. (Not provided by Avaya).
- **`root`** password or sroot with EASG enabled.

Procedure

Validating SSL certificate Expiry

1. Log in to the first ESXi host by using a *Secure Shell (SSH)* client, that is, Putty (Not provided by Avaya).
2. Authenticate using the existing **`root`** credentials.
3. Run the following command to validate current SSL certificate expiry:

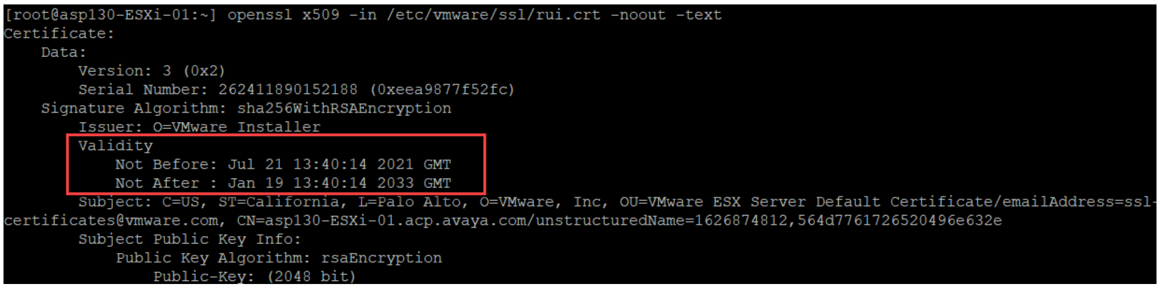
```
openssl x509 -in /etc/vmware/ssl/rui.crt -noout -text | grep "Not After"
```



```
[root@asp130-ESXi-01:~] openssl x509 -in /etc/vmware/ssl/rui.crt -noout -text | grep "Not After"
                Not After : Jan 19 13:40:14 2033 GMT
[root@asp130-ESXi-01:~]
```

or

```
openssl x509 -in /etc/vmware/ssl/rui.crt -noout -text
```



```
[root@asp130-ESXi-01:~] openssl x509 -in /etc/vmware/ssl/rui.crt -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 262411890152188 (0xeea9877f52fc)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=VMware Installer
        Validity
            Not Before: Jul 21 13:40:14 2021 GMT
            Not After : Jan 19 13:40:14 2033 GMT
        Subject: C=US, ST=California, L=Palo Alto, O=VMware, Inc, OU=VMware ESX Server Default Certificate/emailAddress=ssl-
certificates@vmware.com, CN=asp130-ESXi-01.acp.avaya.com/unstructuredName=1626874812,564d7761726520496e632e
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

4. If the Not After date being display is older than the current ESXi host date, proceed with regenerating the SSL Self-signed Certificate.

   Output example:

   ```
   Machine Date:
   Thu Jul 22 13:07:12 UTC 2021
   Validity
        Not Before: Jan 19 13:40:14 2019 GMT
        Not After : Jan 19 13:40:14 2021 GMT
   ```

Regenerating the SSL Self-signed Certificate

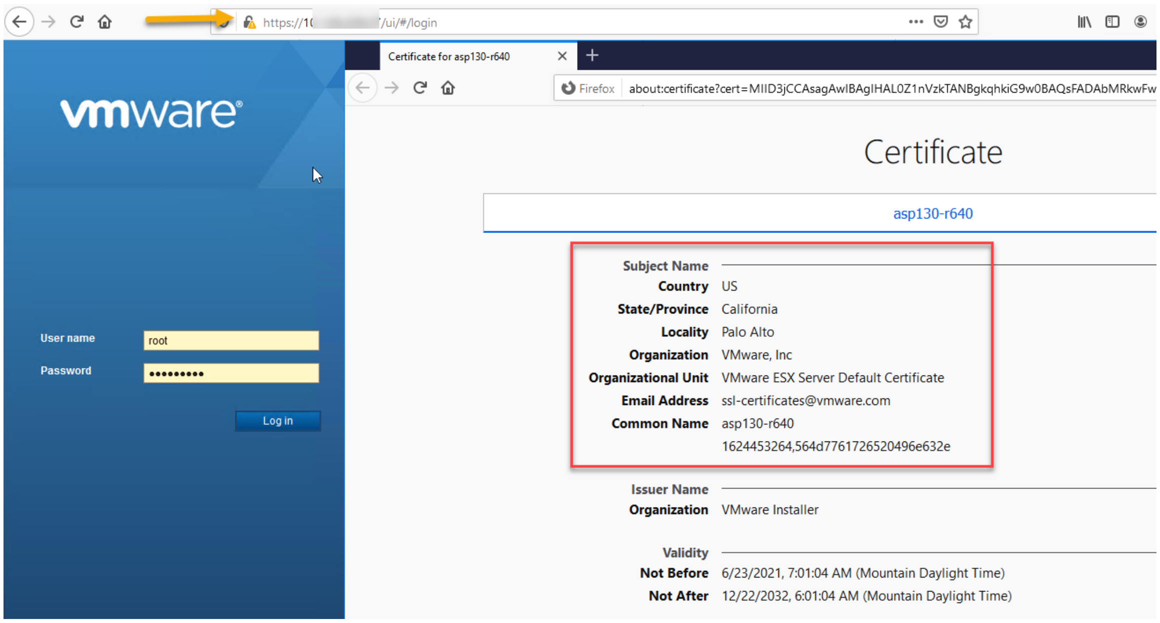
5. Log in to the first ESXi host by using a *Secure Shell (SSH)* client, that is, Putty (Not provided by Avaya).
6. Authenticate using the existing **`root`** credentials.
7. Run the following command to generate the self-signed certificate on the connected ESXi host:

   ```
   /sbin/generate-certificates
   ```

8. Run the following command to restart the **`hostd`** (Management Agent) service on ESXi host.

   ```
   /etc/init.d/hostd restart
   ```

9. Before attempting to re-login to the ESXi host through the web host client to validate the new SSL certificate installed, clear the history, cache and cookies from all previously used browsers. Reference to each browser documentation if needed when doing so.

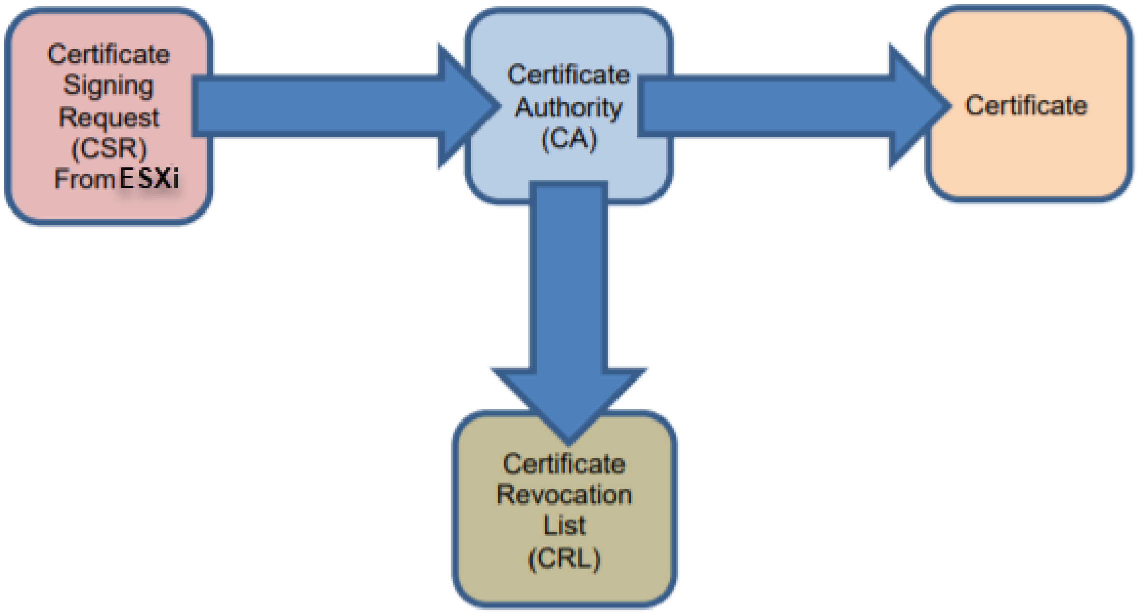


10. Repeat the procedure for all remaining ESXi hosts.

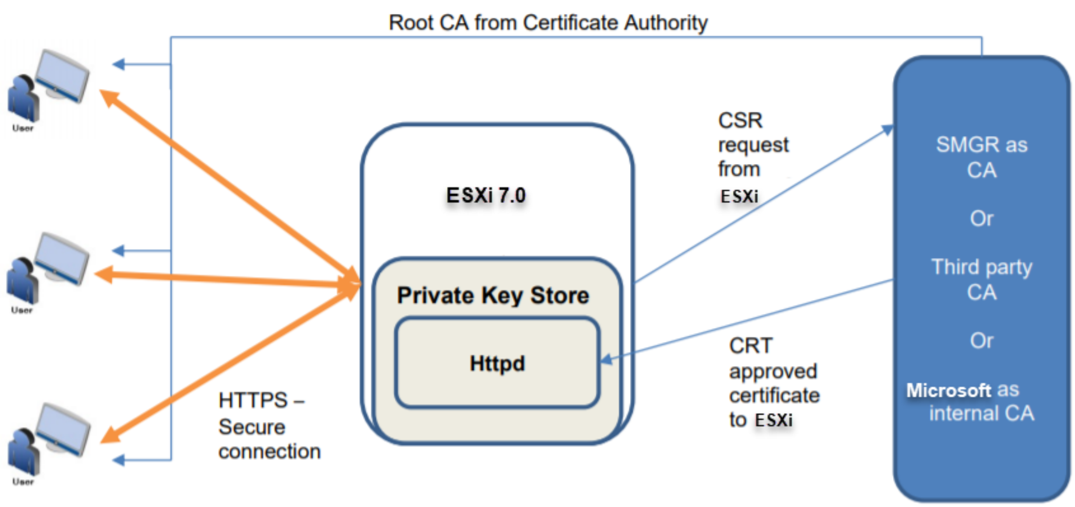
Replacing ESXi SSL certificates and Keys with Custom Certificates

Secure Sockets Layer (SSL):

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 ESXi:



The following figure shows the Certificate Authority in ESXi:



About this task

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

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

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

In an effort 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.

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 ESXi.

Note:

ESXi host does not need to be entered in maintenance mode to conduct this activity.

Warning:

Avoid any administrative tasks such as creating back up jobs, taking VM snapshots or making configuration changes to the host when conducting this procedure.

Before you begin

- Access to the ASP 130 server management network either through a SAL Gateway connection (Remotely) or direct service port connection (onsite).
- SSH tool i.e. Putty. (Not provided by Avaya).
- SFTP / SCP client such as WinSCP. (Not provided by Avaya).
- **`root`** password or sroot with EASG enabled.
- Customer DNS records should be updated with each ESXi FQDN (Hostname + Domain).

Procedure

1. To create the Certificate configuration file for ESXi host, in a text editor of choice (for example, Notepad, WordPad, etc.), copy the following content as is:

```
[ req ]

days = 365

default_md = sha512

default_bits = 2048

default_keyfile = rui.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 = "server.domain.com"

emailAddress= “email Address”

[ alt_names ]

DNS.1 = "ServerName.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.
- **subjectAltName:** Enter the ESXi host FQDN, hostname, IP. For example: `DNS:asp130-ESXi-01.acp.avaya.com`, `DNS:asp130-ESXi-01`, `IP:192.168.220.57`
- **countryName:** Type the two-letter country code without the punctuation. For example, `US`.
- **stateOrProvinceName:** Type the name of the state or province. For example, `Colorado`.
- **localityName:** Type the name of the city. For example, `Denver`.
- **organizationName:** Type the name of the organization. For example: `Avaya Inc.`
- **OrganizationalUnitName:** Type the name of the of the department or organization unit making the request. For example: `IT` , `Engineering`, etc.
- **commonName:** Type the ESXi host Fully Qualified Domain Name. For example: `asp130-ESXi-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, `asp130support@avaya.com`
- **DNS.1:** Type the Fully Qualified Domain Name of the ESXi host. For example: `asp130-ESXi-01.acp.avaya.com`
- **DNS.2:** Type the short, hostname for the ESXi host. For example: `asp130-ESXi-01`
- **IP.1:** Type the ESXi host IP Address. For example: `192.168.200.57`.

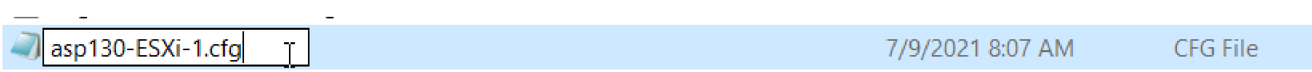
Following image is an example of an edited configuration file:

```
[ req ]

days = 365

default_md = sha512

default_bits = 2048

default_keyfile = rui.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-ESXi-01.acp.avaya.com, DNS:asp130-ESXi-01, IP:192.168.220.57

[ req_distinguished_name ]

countryName = US

stateOrProvinceName = CO

localityName = Denver

0.organizationName = Avaya Inc.

organizationalUnitName = ASP-Engineering

commonName = asp130-ESXi-01.acp.avaya.com

emailAddress = asp130support@avaya.com

[ alt_names ]

DNS.1 = asp130-ESXi-01.acp.avaya.com

DNS.2 = asp130-ESXi-01

IP.1 = 192.168.220.57
```

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

   Note:

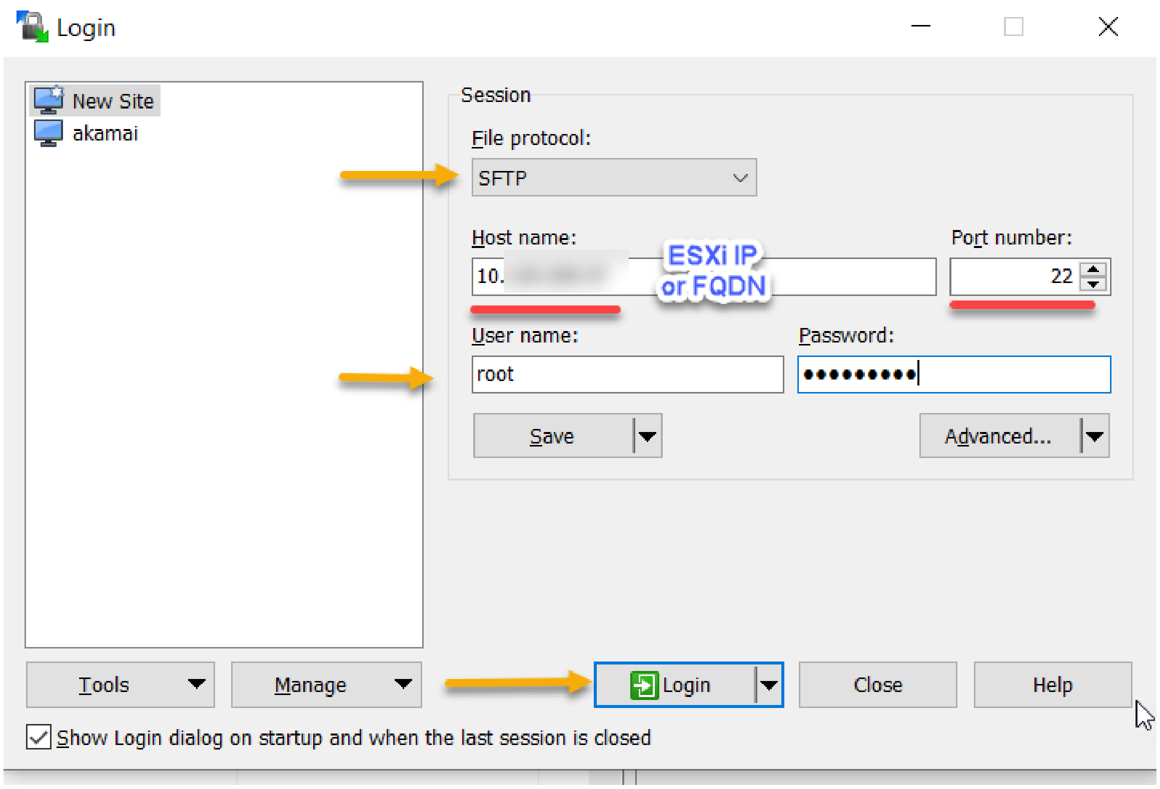
   Depending on the used text editor, the configuration file may have to be saved as a text file first, therefore this will be saved with a `.txt` extension. The newly saved configuration file can then be renamed along with changing the extension from `.txt` to `.cfg`

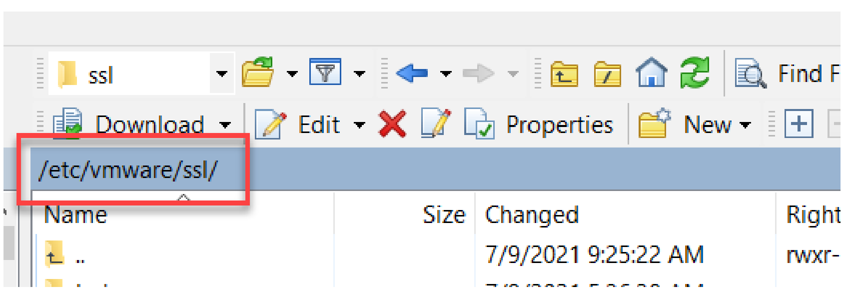
   Note:

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

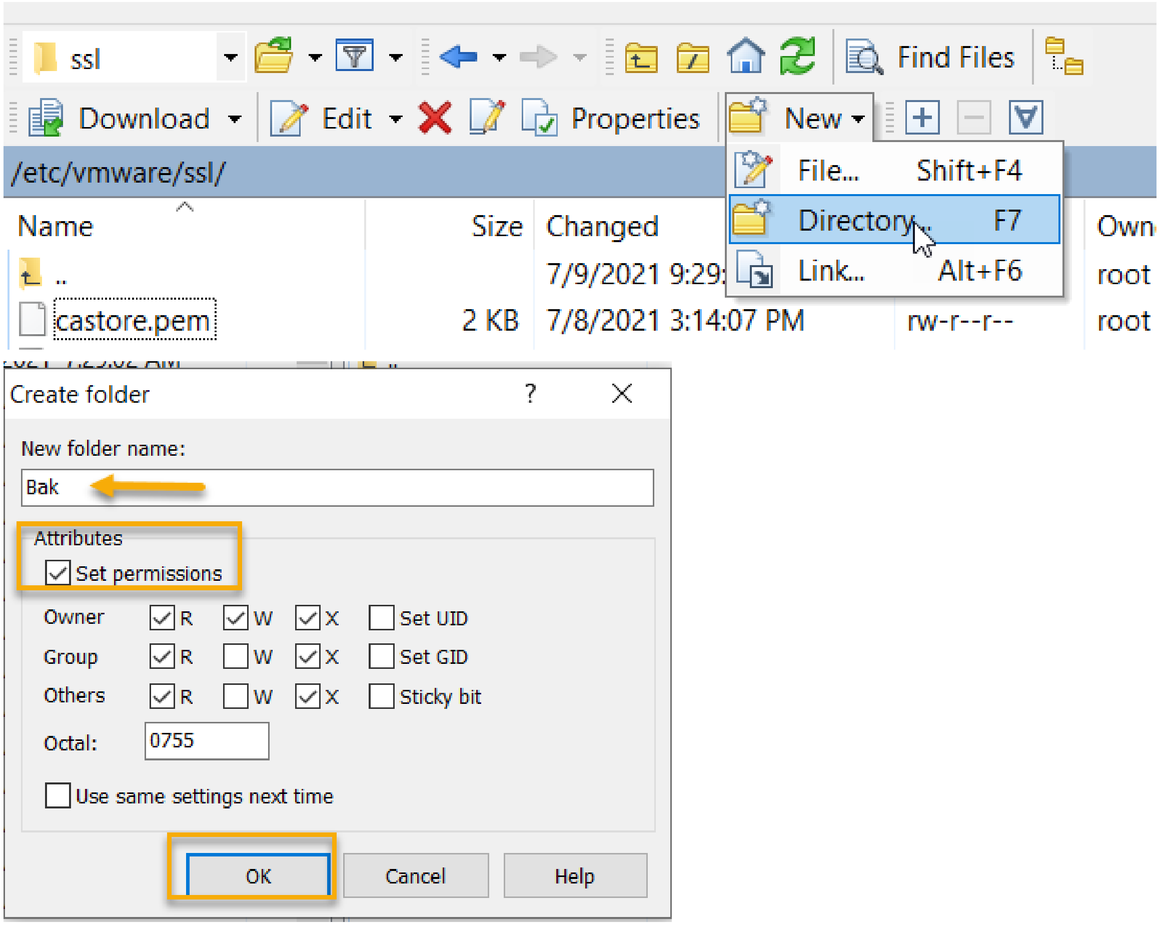
4. Starting with the first, desired ESXi host, open a WinSCP session using the **`root`** credentials.



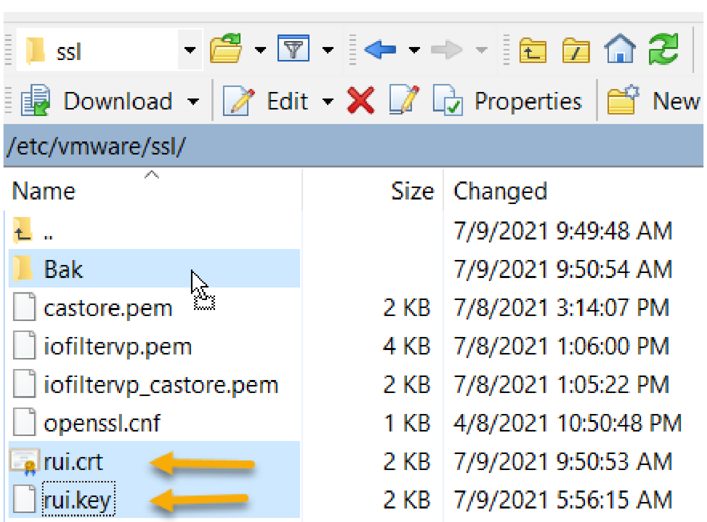
5. From the menu on the right (ESXi directory), navigate to `etc/vmware/ssl/`



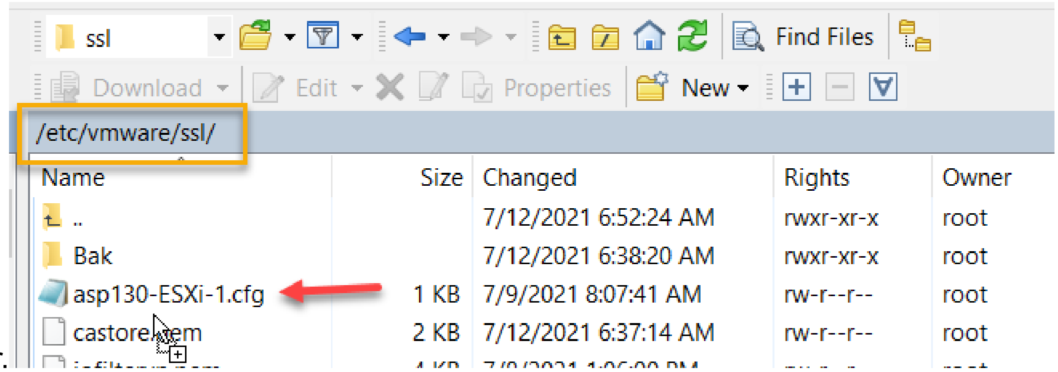
6. Click on **New** > **Directory**... to create a new folder and name it **Bak**.



7. Press and hold the **CRTL** key, then select the files `rui.crt` & `rui.key`, then drag and drop these to the newly created “**Bak**” folder.



8. Using WinSCP transfer the configuration file created in previous steps i.e. `asp130-ESXi-1.cfg` to the same `/etc/vmware/ssl` folder.



Generating the Certificate signing Request in ESXi

Before you begin

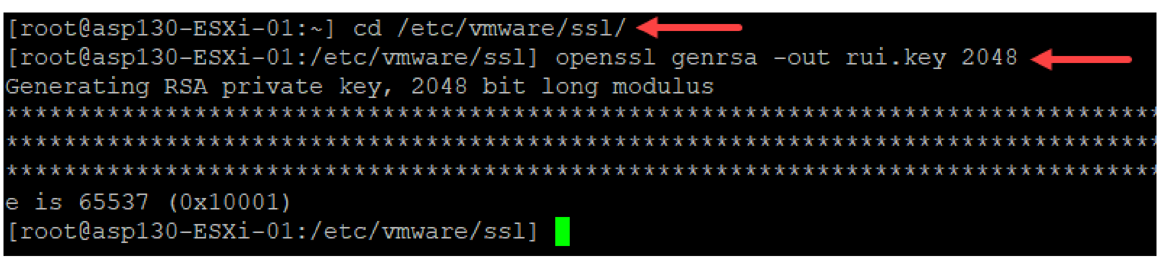
The Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 should be completed before continuing with the following procedure.

Procedure

1. Using Putty or any other SSH tool of desire, open a new SSH session to the selected ESXi host during step 4 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100. Login using the root credentials.
2. Run the following commands:

a. `cd /etc/vmware/ssl/`

b. `openssl genrsa -out rui.key 2048`



c. `openssl req -new -nodes -out rui.csr -keyout rui.key -config <Config_file_name.cfg>`

Note:

The following figure shows an out example using the configuration file previously created and transferred during step 8 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 `asp130-ESXi-1.cfg`. Be aware that configuration files and their name will change per each ESXi host when generating the certificate signing request (CSR).

10.129.209.57 - PuTTY

```
[root@asp130-ESXi-01:/etc/vmware/ssl] openssl req -new -nodes -out rui.csr -keyout rui.key -config asp130-ES
Xi-1.cfg
Generating a RSA private key
*********************************************************************************************************
*********************************************************************************************************
**************************+++++
***************************************************************+++++
writing new private key to 'rui.key'
-----
[root@asp130-ESXi-01:/etc/vmware/ssl]
```

d. `ls -lrt`

```
[root@asp130-ESXi-01:/etc/vmware/ssl] ls -lrt
total 32
-r--r--r--    1 root     root           229 Apr  9 05:50 openssl.cnf
-rw-r--r-T    1 root     root             0 Apr  9 05:54 vsanvp_castore.pem
-r-------T    1 root     root             0 Apr  9 05:54 vsan_kms_client_old.key
-rw-r--r-T    1 root     root             0 Apr  9 05:54 vsan_kms_client_old.crt
-r-------T    1 root     root             0 Apr  9 05:54 vsan_kms_client.key
-rw-r--r-T    1 root     root             0 Apr  9 05:54 vsan_kms_client.crt
-rw-r--r-T    1 root     root             0 Apr  9 05:54 vsan_kms_castore_old.pem
-rw-r--r-T    1 root     root             0 Apr  9 05:54 vsan_kms_castore.pem
-rw-r--r-T    1 root     root          1050 Jul  8 20:05 iofiltervp_castore.pem
-rw-r--r--    1 root     root          3476 Jul  8 20:06 iofiltervp.pem
-rw-r--r--    1 root     root           877 Jul  9 15:07 asp130-ESXi-1.cfg
-rw-r--r--    1 root     root          1050 Jul 12 13:37 castore.pem
drwxr-xr-x    1 root     root           512 Jul 12 13:38 Bak
-rw-r--r--    1 root     root          1704 Jul 12 13:58 rui.key
-rw-r--r--    1 root     root          1281 Jul 12 13:58 rui.csr
[root@asp130-ESXi-01:/etc/vmware/ssl]
```

Note:

2 new files `rui.key` and `rui.csr` will be listed.

e. `openssl req -in rui.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).

```
[root@asp130-ESXi-01:/etc/vmware/ssl] openssl req -in rui.csr -noout -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CO, L=Denver, O=Avaya Inc., OU=ASP-Engineering, CN=asp130-ESXi-01.acp.avaya.com/em
ailAddress=asp130support@avaya.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9d:83:d2:da:02:5c:0c:de:57:fc:b9:75:0f:60:
                    6e:c6:ac:30:f7:fb:4a:fd:2a:aa:9d:0c:0f:40:e4:
                    8f:cb:43:6d:57:37:95:4a:1f:d5:b9:64:57:b8:bc:
                    cd:7d:02:77:50:1c:41:81:d6:b2:e9:5f:f2:a4:c8:
                    d0:bb:f0:20:7b:1b:4c:af:80:40:7e:28:94:41:99:
                    8d:b9:7b:30:5b:29:2f:67:3f:73:8c:0c:51:3f:c2:
```

```
        Attributes:
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:asp130-ESXi-01.acp.avaya.com, DNS:asp130-ESXi-01, IP Address:10.[redacted]
    Signature Algorithm: sha512WithRSAEncryption
         34:18:28:14:60:d2:98:7d:5a:63:d9:da:74:0f:e7:7c:ca:fd:
         f5:85:e2:36:cf:f4:9e:75:cf:56:a8:c7:8b:3d:a0:41:9d:3b:
```

3. Using WinSCP, transfer the `rui.csr` (Certificate Signing Request) file created during step 2 to a local PC and submit it to the CA of choice to have it signed.

   Note:

   The `rui.csr` file is stored under the `etc/vmware/ssl/` location.

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 ESXi during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100. Alternatively, vsphere certificates can be obtained from a Microsoft Certificate Authority (Not included by Avaya). The following VMware KB article 2113926 describes how to submit a certificate request.

Note:

Customers using external CA to sign the CSR files i.e.VeriSign, DigiCert, Symantec can skip and proceed with the next section Replacing SSL certificates in ESXi with a CA Signed certificate on page 116.

Note:

System Manager UI screens shown below may vary slightly based on System Manager software version. Reference the System Manager documentation as necessary.

Before you begin

- The Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 and the Generating the Certificate signing Request in ESXi on page 107 must be completed prior to continuing with the following procedure.
- Access to a System Manager server.
- Transfer the CSR file “`rui.csr`” file in a location accessible to System Manager.
- User account with administrative privileges in System Manager i.e.`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 desire username. For Example, `avaya`

   c. **Password (or Enrollment code):** Enter any desire password. For Example, `avaya123`

   d. **Confirm Password:** `avaya123`

   e. **E-mail address (optional):** Same value used if configured in the certificate configuration file “asp130-ESXi-1.cfg” during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

   Subject DN Attributes

   a. **CN, Common name:** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

   b. **O, Organization:** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

   c. **C, Country (ISO 3166):** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

   d. **OU, Organizational Unit:** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

e. **L, Locality:** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

f. **ST, State or Province:** Same value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

Subject Alternative Name

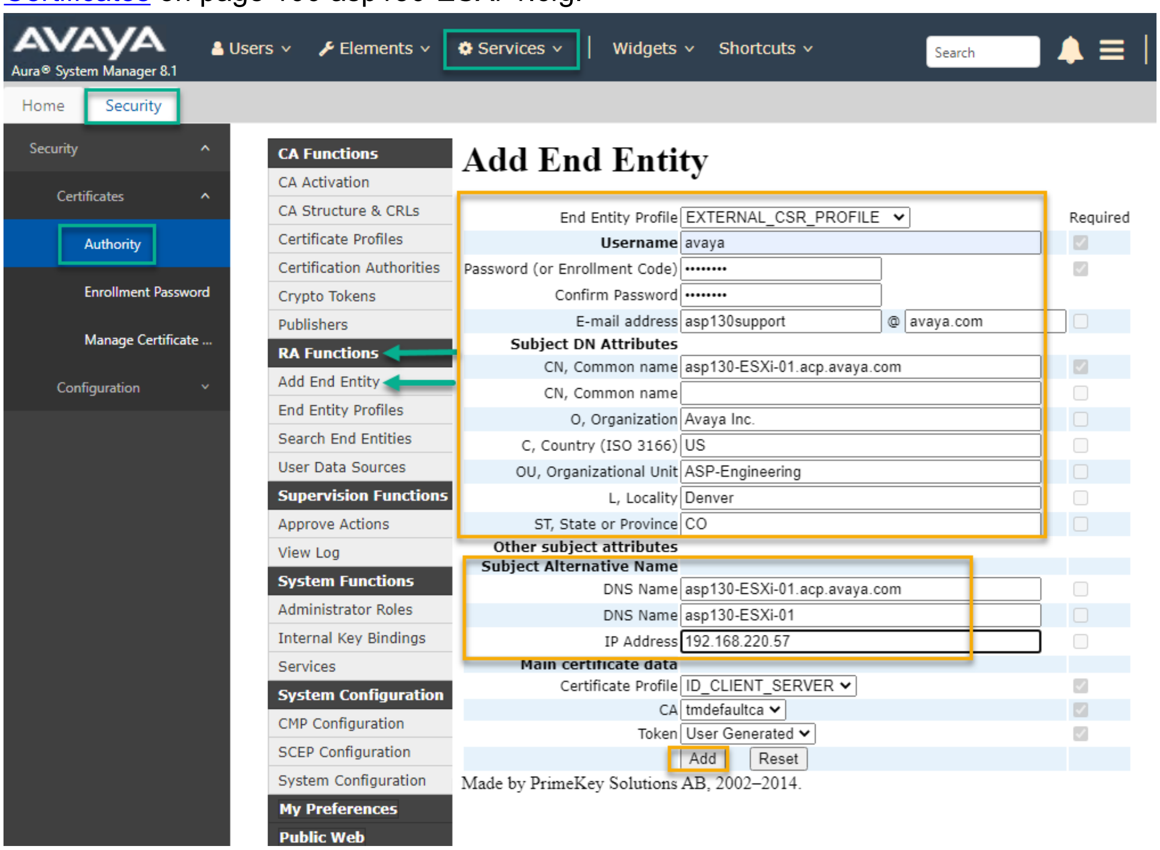
a. **DNS Name:** Enter the DNS.1 value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

b. **DNS Name:** Enter the DNS.2 value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

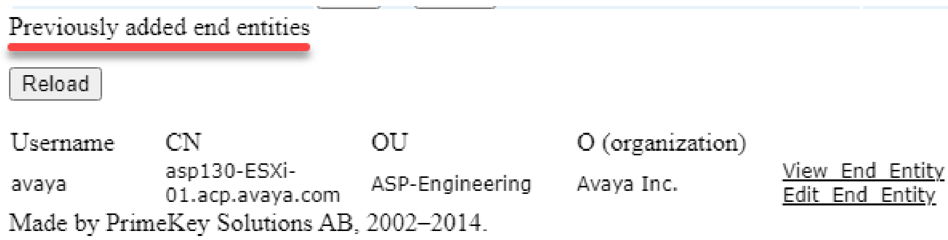
c. **IP Address:** Enter the ESXi host IP address value set in the `asp130-ESXi-1.cfg` configuration file during step 2 of the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100.

6. Review and save:

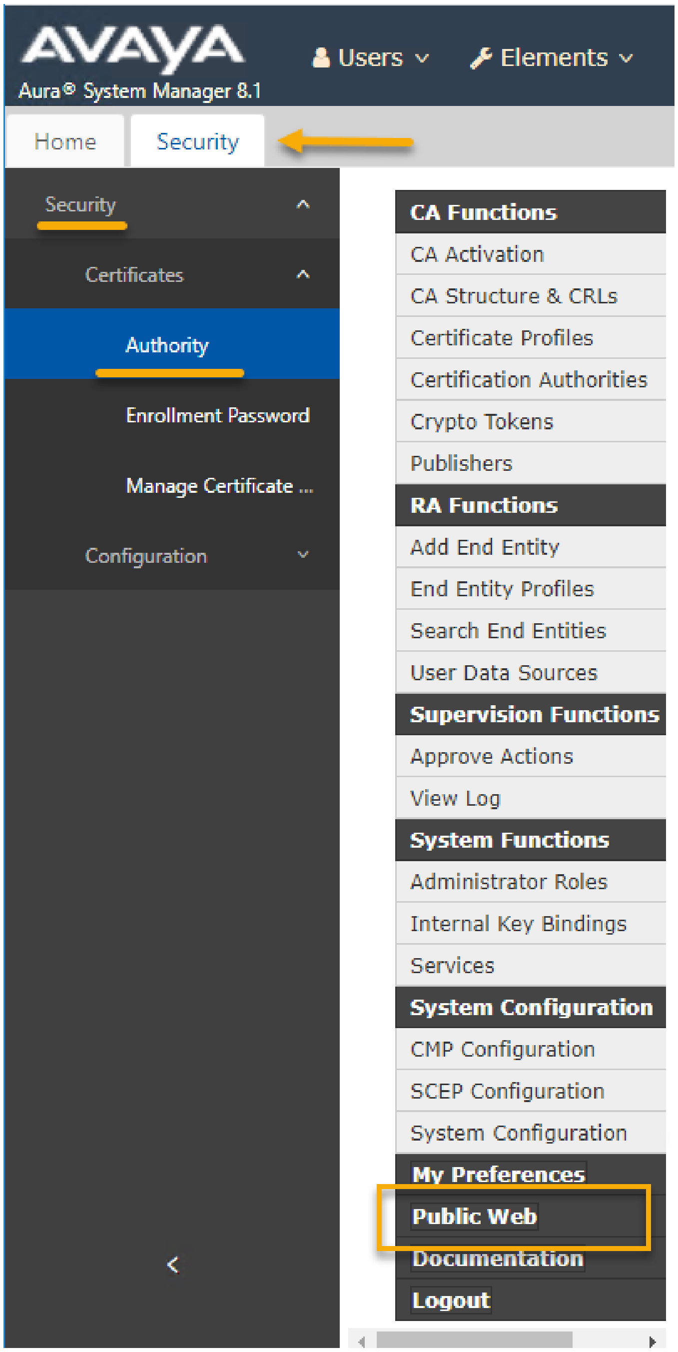
   a. Review and compare the values typed with the ones in the configuration file created during steps in the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 asp130-ESXi-1.cfg.



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



7. From the menu on the left pane, select **Public Web**. A new tab opens.



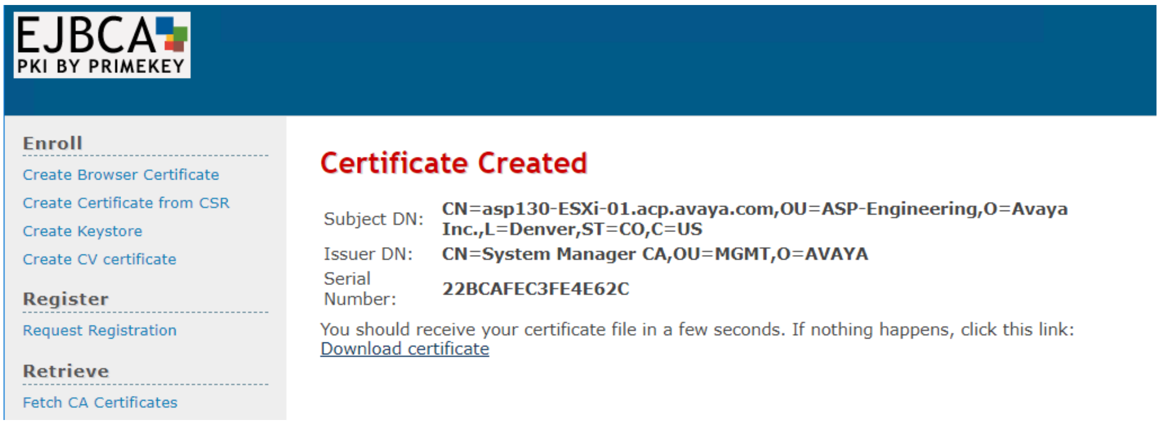
8. From the **EJBCA** webpage, select **Create Certificate from CSR** under **Enroll**.
9. Enter the following information:
    a. **Username:** The one configured when creating the entity during step 5 i.e. `avaya`
    b. **Enrollment Code:** The one configured when creating the entity during step 5 i.e. `avaya123`

c. **Request file:** Select **Choose File** to import the "`rui.csr`" file previously saved locally in the computer used during [Signing the Certificate Signing Request (CSR) by an Organizational CA](#) on page 109 procedure.

d. **Result type:** From drop-down menu, select **PEM-certificate only**.

e. Select **OK** to generate the certificate.

10. A certificate with a `PEM` format is created and automatically downloaded to the computer used to issue the sign request.

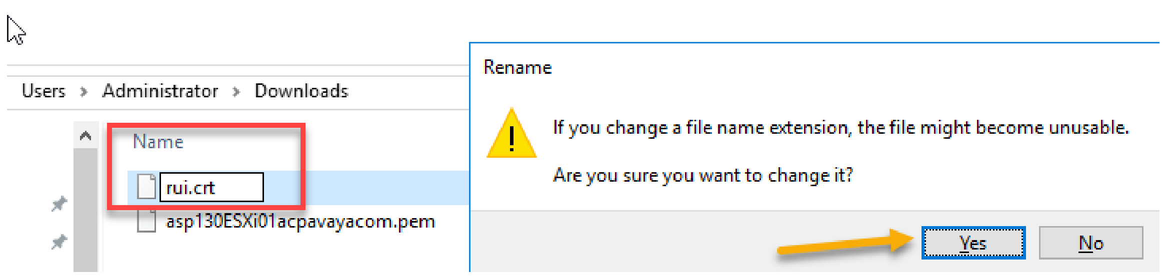


11. Navigate to the location where certificate is downloaded.

12. Create a copy of the pem file i.e `asp130ESXi01acpavaya.com.pem` and rename it to `rui.crt`.

Note:

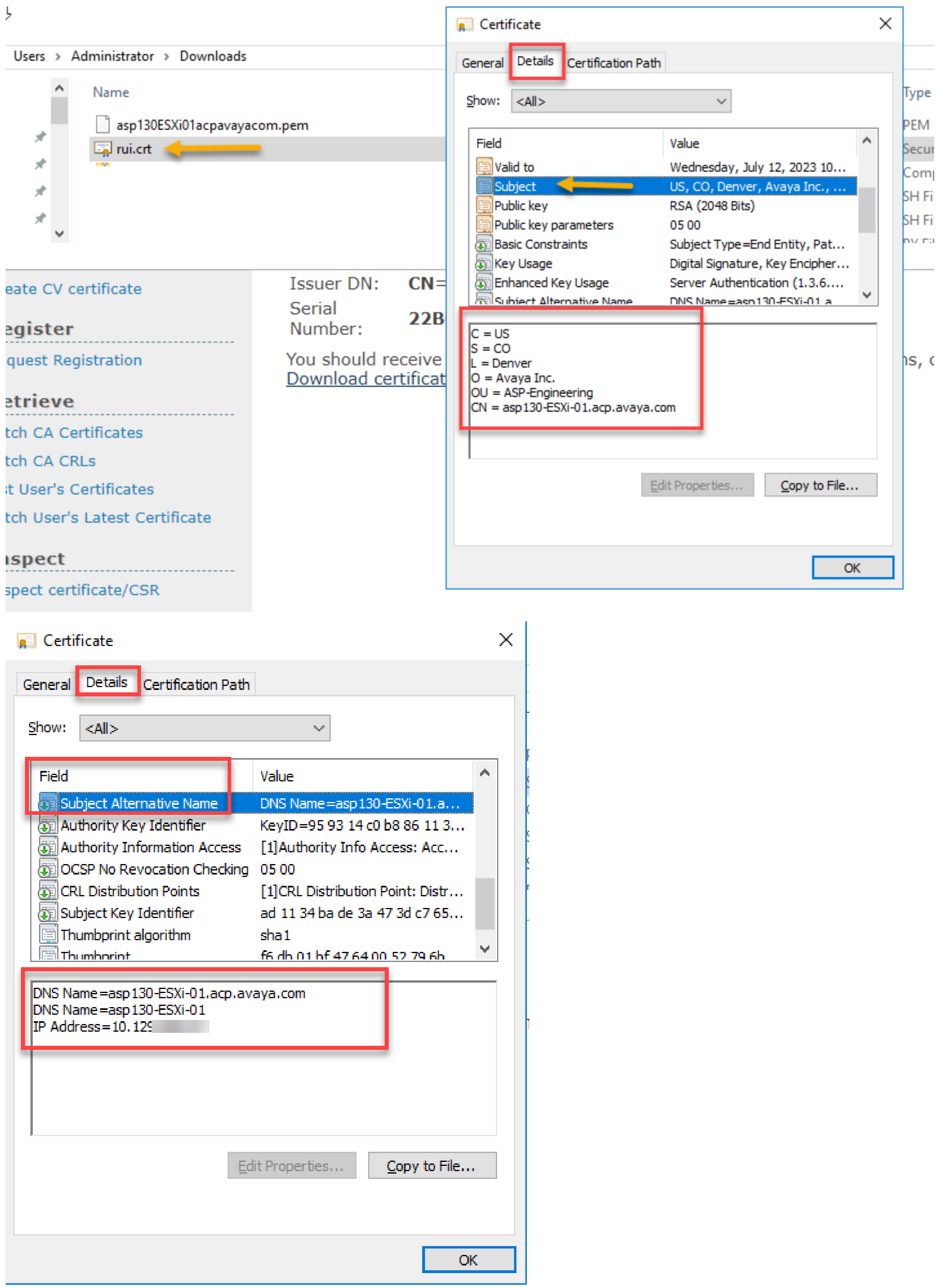
The file name must be named `rui.crt`.



13. Double-click the `rui.crt` file and validate the information in the certificate to ensure that the information is correct before proceeding.

Note:

These steps validate the input entered by the user when generating the CSR.



14. Once the validation is complete, click **OK** to close the file.

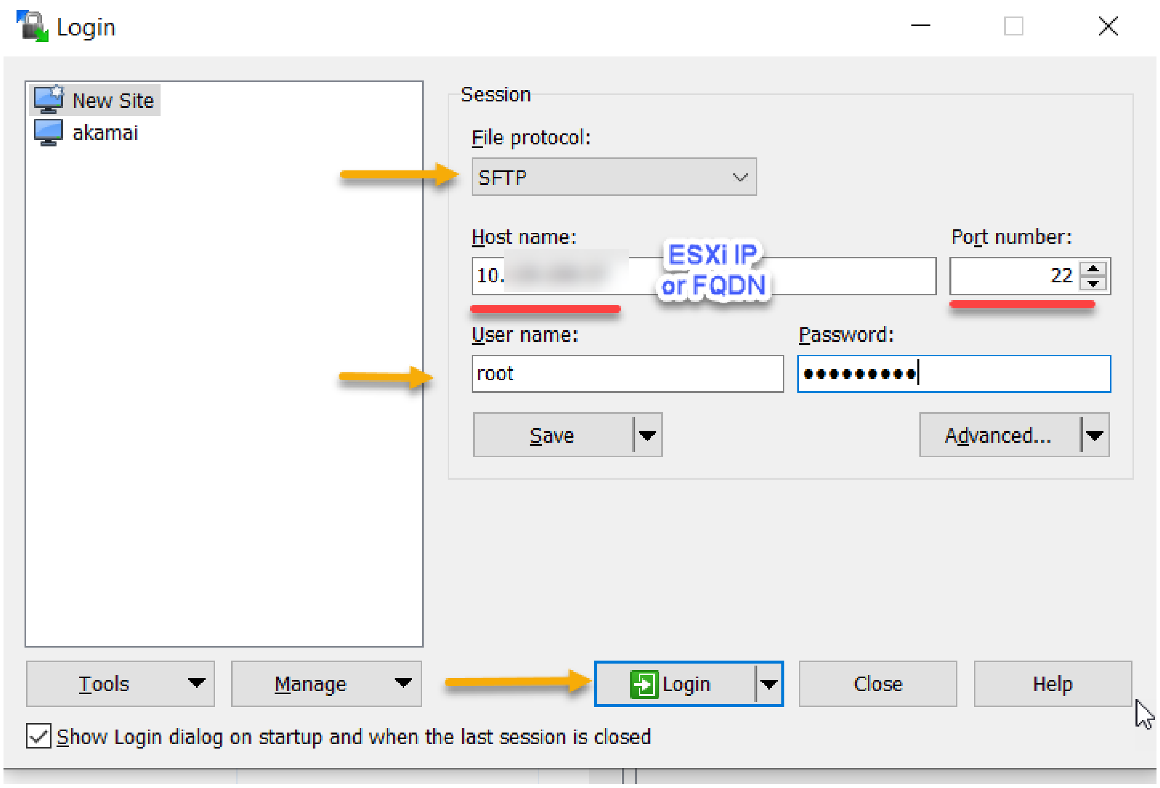
Replacing SSL certificates in ESXi with a CA signed certificate

Before you begin

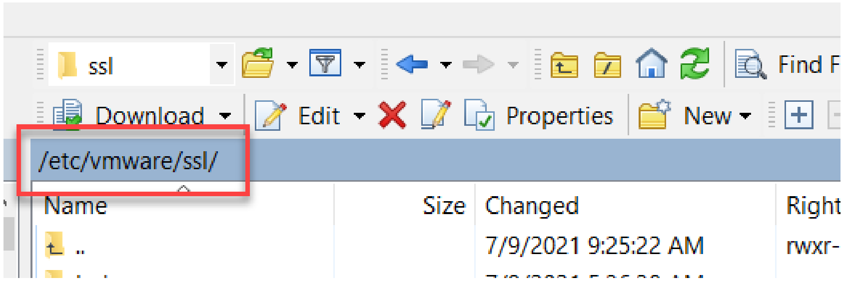
- The Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100, Generating the Certificate signing Request in ESXi on page 107 and Signing the Certificate Signing Request (CSR) by an Organizational CA on page 109 must be completed prior to continuing with the following procedure, if using System Manager.
- Customers using an external CA or any other organizational CA such us Microsoft CA should have by now the signed certificate in `CRT` format and renamed to `rui.crt` and CA `root` certificate.

Procedure

1. Open a WinSCP session using the **`root`** credentials to the ESXi selected in the Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 procedure.



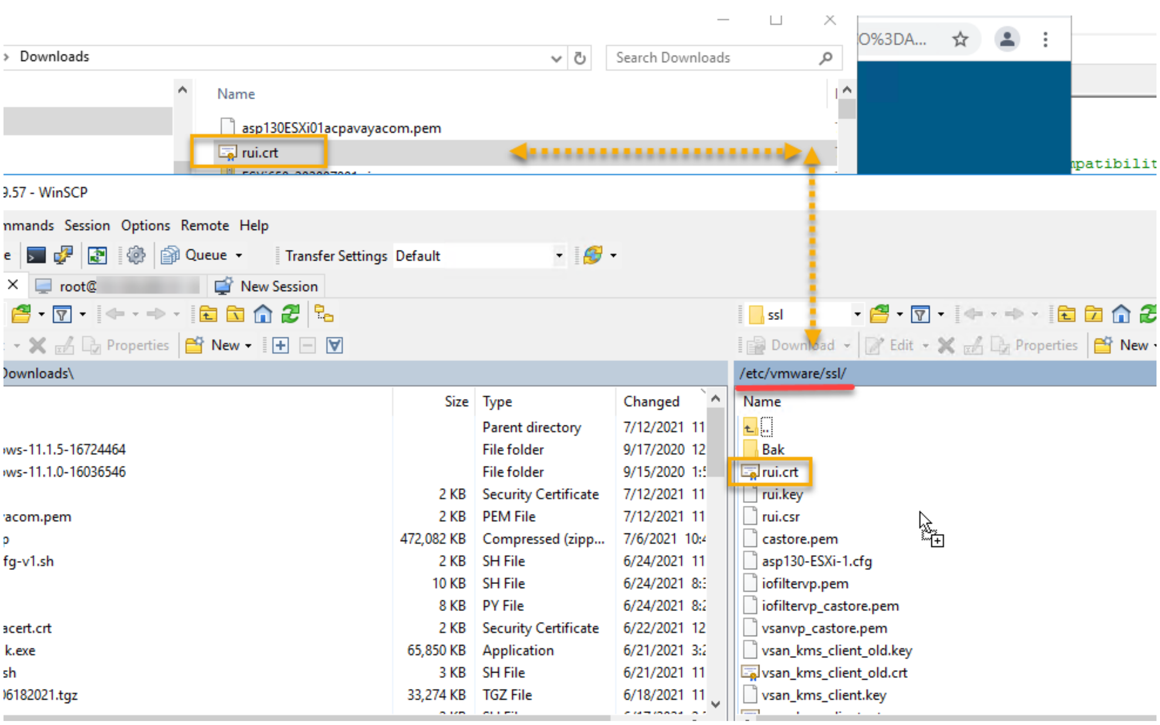
2. From the menu on the right (ESXi directory) navigate to `etc/vmware/ssl`



3. Transfer to ESXi the generated signed certificate by the Certificate Authority (CA) in `CRT` format.

Note:

In this example the `rui.crt` certificate has been signed and generated by the System Manager application as documented in the Signing the Certificate Signing Request (CSR) by an Organizational CA on page 109. Procedures already take into account the renaming of the original file produced by the CA to the one expected by ESXi. When using an external CA such us: VeriSign, DigiCert, Symantec, etc. ensure to rename the return signed certificate to `rui.crt`



4. Log in to the selected ESXi host during Replacing ESXi SSL certificates and Keys with Custom Certificates on page 100 by using a *Secure Shell (SSH)* client i.e. Putty (Not provided by Avaya).
5. Authenticate using the existing `root` credentials.

6. Run the following command to restart the **`hostd`** (Management Agent) service on ESXi host: `/etc/init.d/hostd restart`

Adding the CA root certificate to a Web browser

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 will be used. Customers using an external CA or a Microsoft CA can skip steps 1 through 6 and proceed with the root certificate installation.

For Browsers not listed in this section, reference to each browser vendor documentation to import `CRT` certificates.

Users (Client PC) with other OS apart from Windows such as Mac OS, RedHat, CentOS etc, 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.

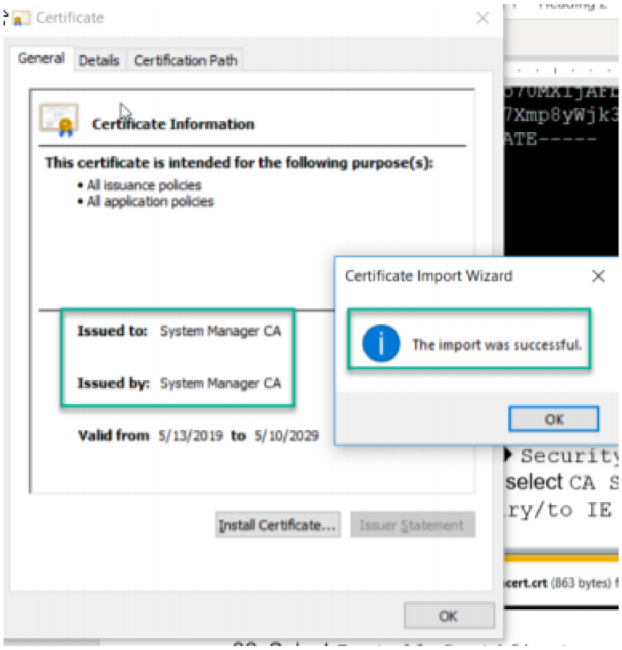
Procedure

The following procedure can be performed using either *Microsoft Edge* or *Chrome* browser.

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**.



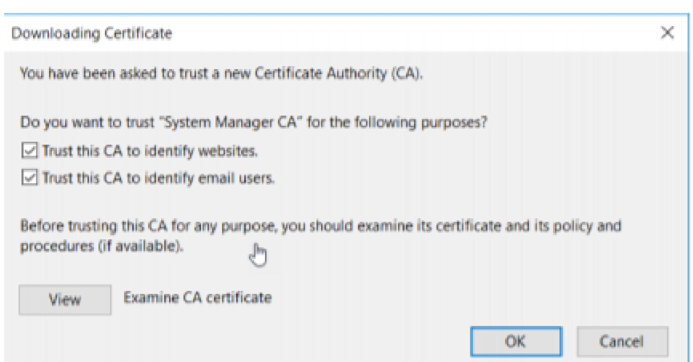
Related links

[Procedure for Firefox Browser](#) on page 119

Procedure for Firefox Browser

Procedure

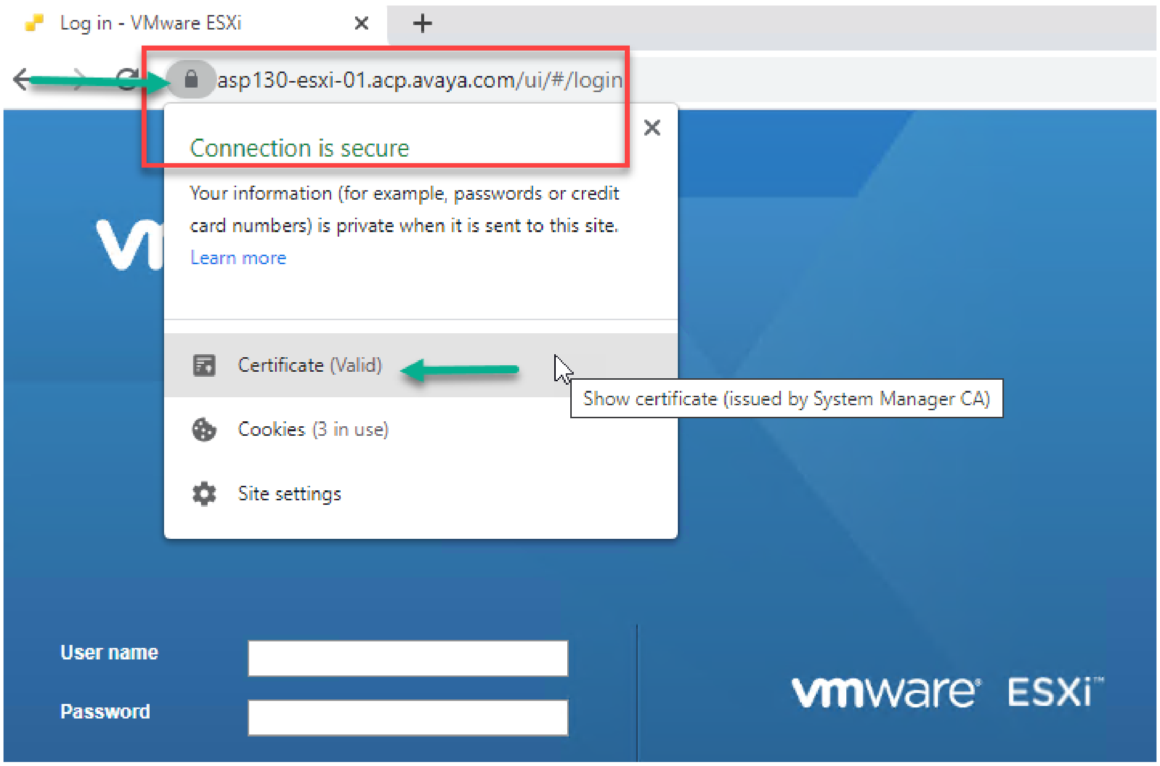
1. Open *Firefox* and access Avaya Aura® System Manager.
2. Login with administrative credentials. For example, `admin`.
3. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
4. Under **CA Functions**, select **CA Structure & CRLs**.
5. Select **Download to Firefox**.
6. Check both selections and click **OK**.

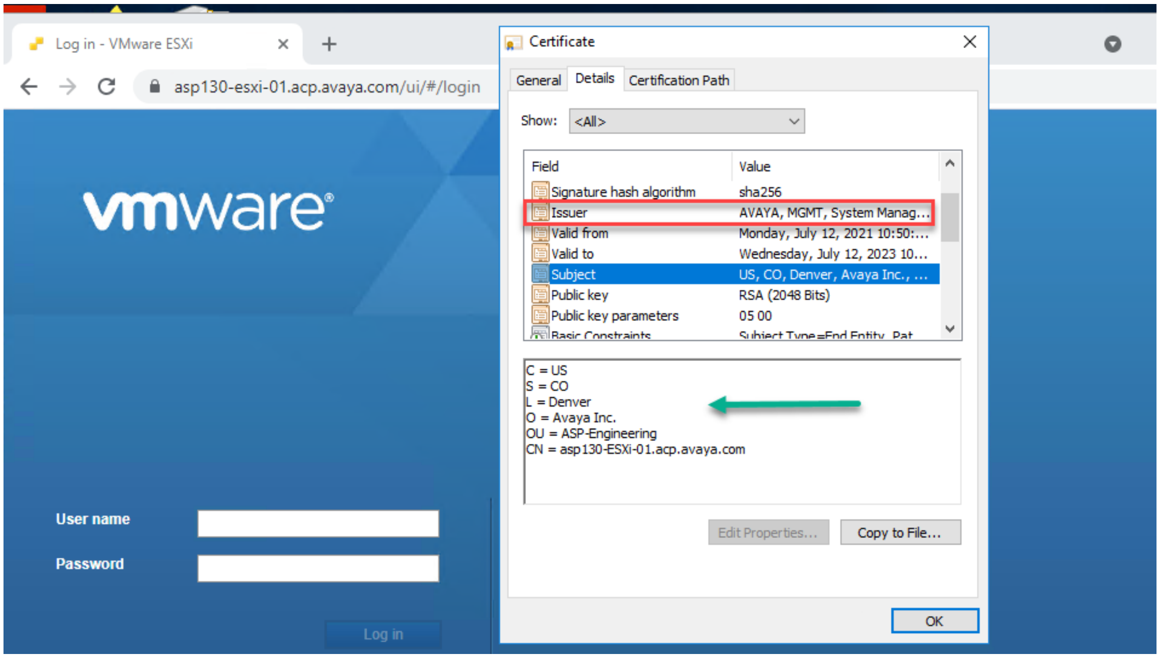


7. Clear the history, cache and cookies from all previously used browsers. Reference to each browser documentation if needed when doing so.
8. Open a new Web browser to the ESXi selected throughout steps 1 through 5 by either using the FQDN or IP Address.

   Note:

   Connection at this point will show as secure. Optionally by clicking on Certificate, one can review the certificate information.





Related links

Adding the CA root certificate to a Web browser on page 118

Chapter 10: Dell R640 RAID Configuration

Introduction

The Dell R640 RAID controller (H730P Mini or H750) is an enterprise-class controller providing a robust infrastructure to maximize server uptime.

This section describes the procedures to configure the Dell R640 RAID controller (H730P Mini or H750) for Avaya Solutions Platform (ASP) 1XX RAID Array configurations.

Note:

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

Preparing to configure Dell R640 RAID controller

About this task

Use this procedure to configure the Dell R640 RAID controller (H730P Mini or H750) for ASP ESXi software installation. To do that the user must first delete all the existing configurations from the controller. The controller configuration process for creating ASP 130 RAID configurations for profiles 2,3,4,5 and 51 is the same whether the server has an H730P or H750 controller. The top level menu of the H750 has one additional level that requires selection vs the H730P. That additional level selection is designated where necessary in the steps shown below.

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.

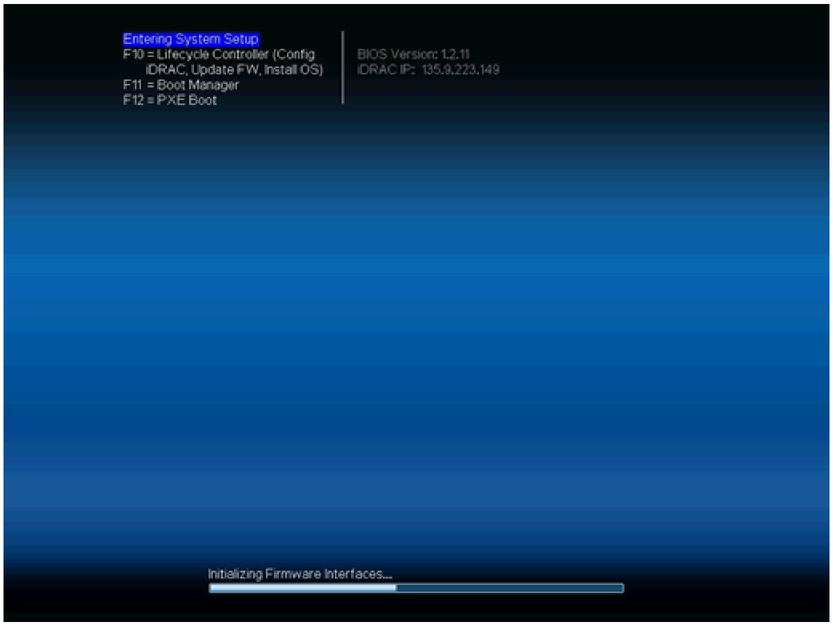
Before you begin

- Ensure the server has the correct number of HDDs installed for the server profile.
- Connect your VGA monitor, USB keyboard, and USB mouse to the server.
- Power up the server.

Procedure

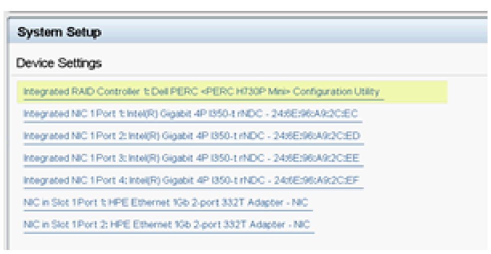
1. When the hardware boot screen appears, select **<F2>System Setup**.

   Blue highlight indicates that the user selected the **System Setup** Menu.



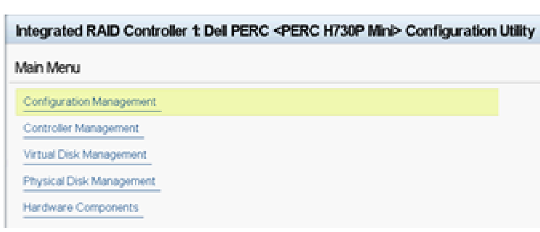
2. Clear all existing arrays by doing the following:
    a. Click **Device Settings** > **Integrated RAID Controller 1: Dell <PERC H730P Mini> Configuration Utility** or for the H750 select **Device Settings/RAID Controller in Slot 1: Dell PERC H750 Adaptor Configuration Utility/Main Menu**.

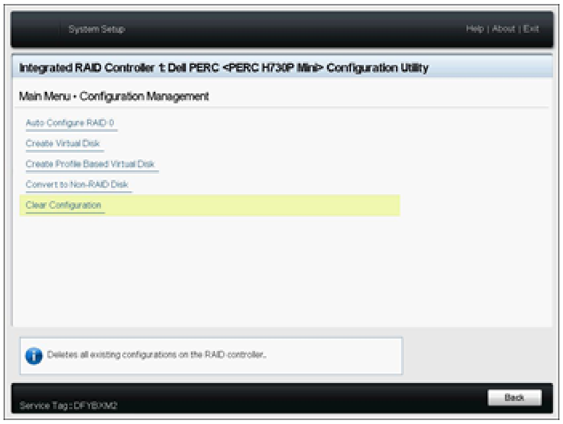
    

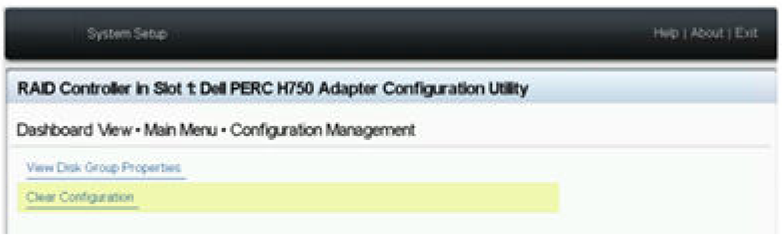
    

    b. On the Main Menu, click **Configuration Management** > **Clear Configuration**.

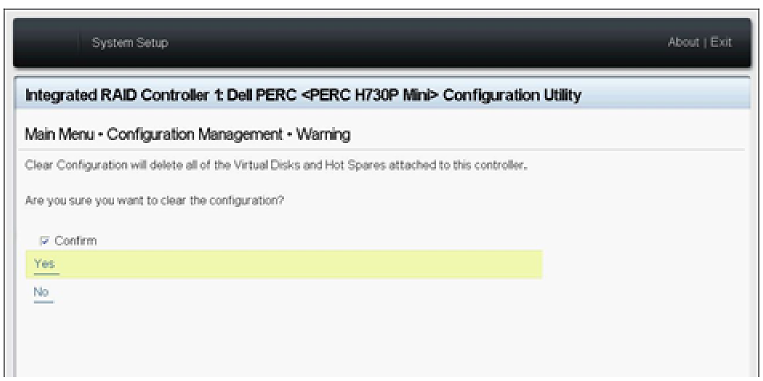
    This command deletes all existing configurations from the RAID controller.

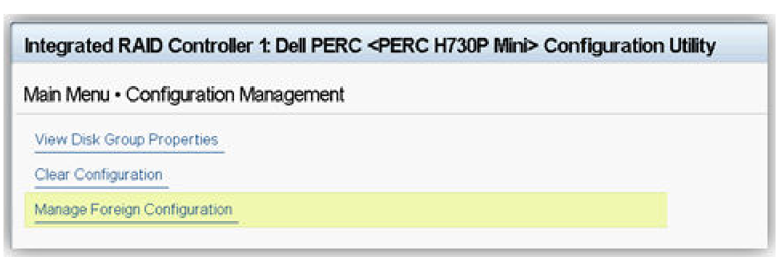


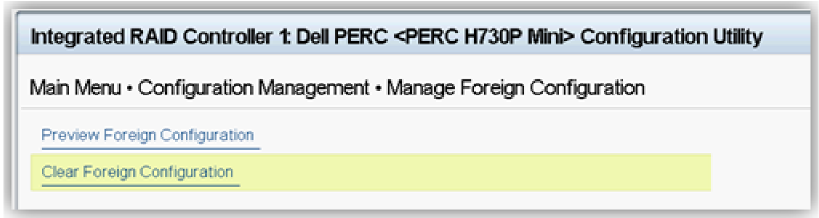


c. Check the **Confirm** box, select **Yes**, and click **OK**.

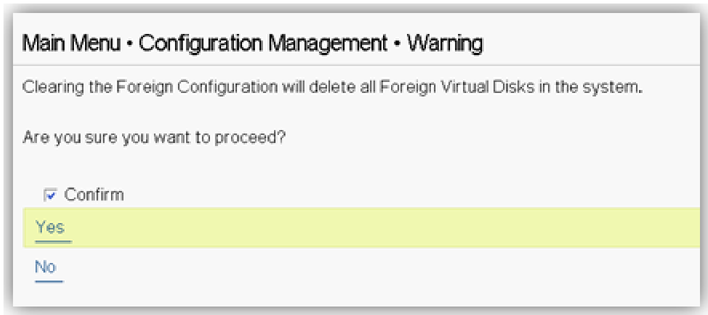


d. **(Optional)** On the Configuration Management window, if you see the **Manage Foreign Configuration** link, then click **Manage Foreign Configuration** > **Clear Foreign Configuration**.





e. Check the **Confirm** box, select **Yes**, and click **OK**.



3. Click **Back**.

Next steps

Proceed to Configuring the controller properties on page 125 for the steps to manage the controller and configure its advance properties.

Configuring the controller properties

About this task

Use this procedure to manage the controller and configure its advance properties.

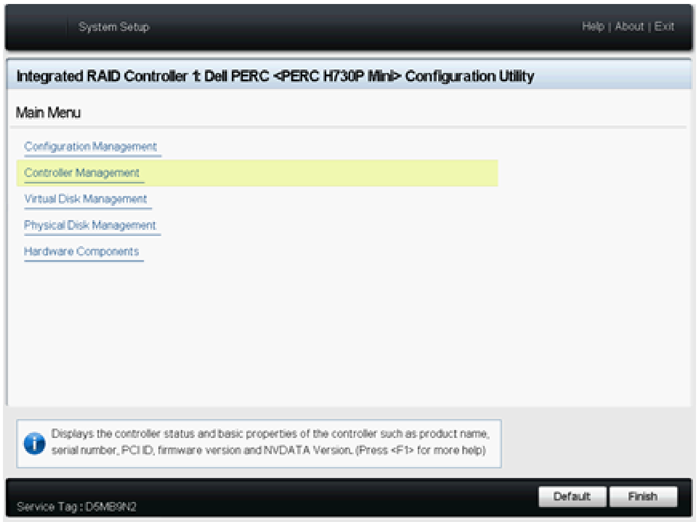
Before you begin

Delete all existing configurations on the RAID controller.

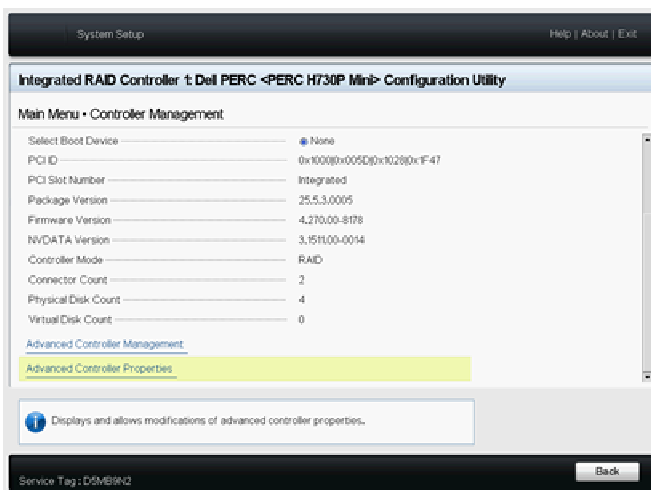
Procedure

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

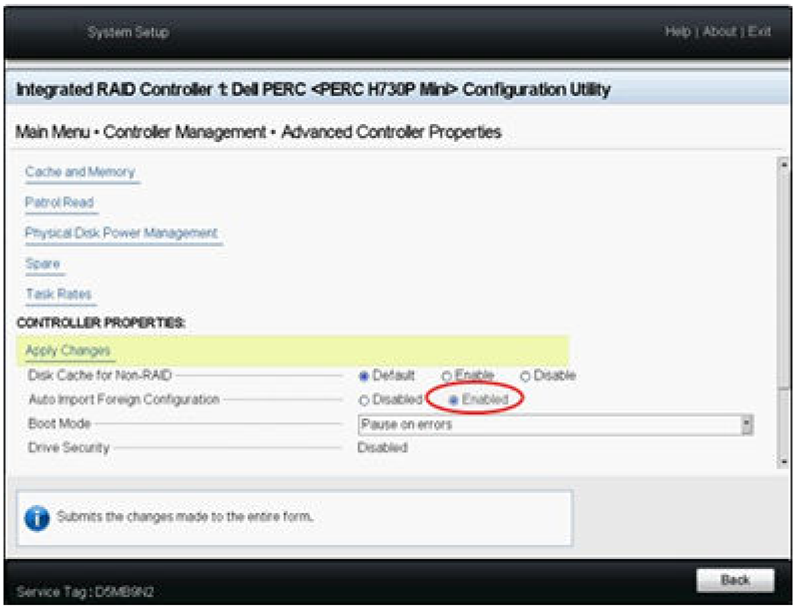
   This section displays and allows modifications of the advance controller properties.



2. Scroll down and click **Advanced Controller Properties**.



3. Under Controller Properties, set **Auto Import Foreign Configuration** to **Enabled**. If this setting is already set to **Enabled** select **Back** and go to Next steps below.



4. Click **Apply Changes**.
5. Scroll down and click **OK**.
6. Click **Back**.

Next steps

Proceed to Creating a virtual disk on page 127 for the steps to create a virtual disk by selecting the RAID level, physical disks, and virtual disk parameters.

Creating a virtual disk

About this task

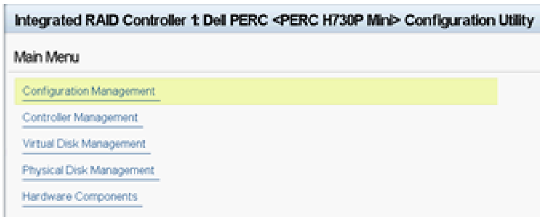
Use this procedure to create a virtual disk by selecting the RAID level, physical disks, and virtual disk parameters.

Before you begin

- Delete all existing configurations on the RAID controller.
- Configure the controller properties.
- Ensure that **Auto Import Foreign Configuration** is set to **Enabled**.

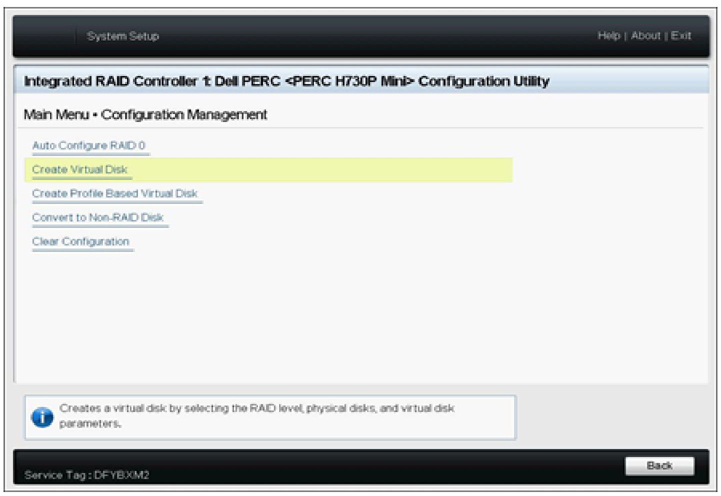
Procedure

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

2. Click **Create Virtual Disk**.

   If there is no option to create a virtual disk, then all disks in the system must already be assigned to an array. You must delete all the existing configuration before creation of a new virtual disk. Go back to the beginning of this section to delete/clear existing arrays if necessary.

3. Configure the virtual disk parameters as follows:

   a. In **Select RAID Level**, select the RAID level specified by the appropriate Avaya Solutions Platform configuration.

      Following are the RAID configurations for Avaya Solutions Platform.

      Avaya Solutions Platform 1XX Profile 2 = 3x600 GB > RAID5

      Avaya Solutions Platform Profiles 3&4 = 4x600 GB > RAID6

      Avaya Solutions Platform Profile 5 = 6x600 GB > RAID6

      Avaya Solutions Platform Profile 51 = 8x600GB > RAID6

   b. For **Virtual Disk Name**, ensure name is set to **VD0**. If it is not then change to VD0 unless application specific documentation instructs otherwise.

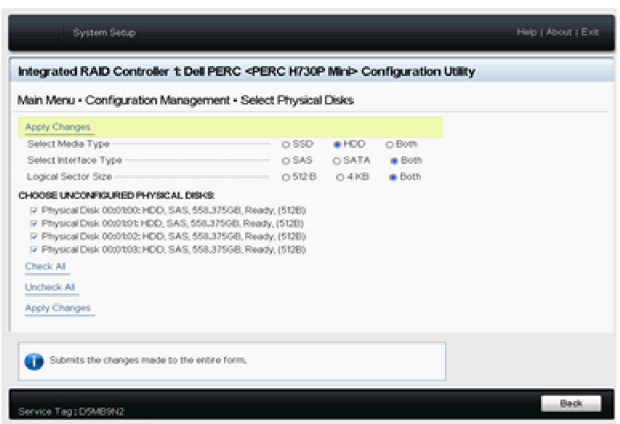
c. Under **Configure Virtual Disk Parameters**, set the **Strip Element Size** value to `256 KB`.

d. Scroll down and select **Fast Default Initialization**.

The following is an example of configuring the virtual disk parameters:

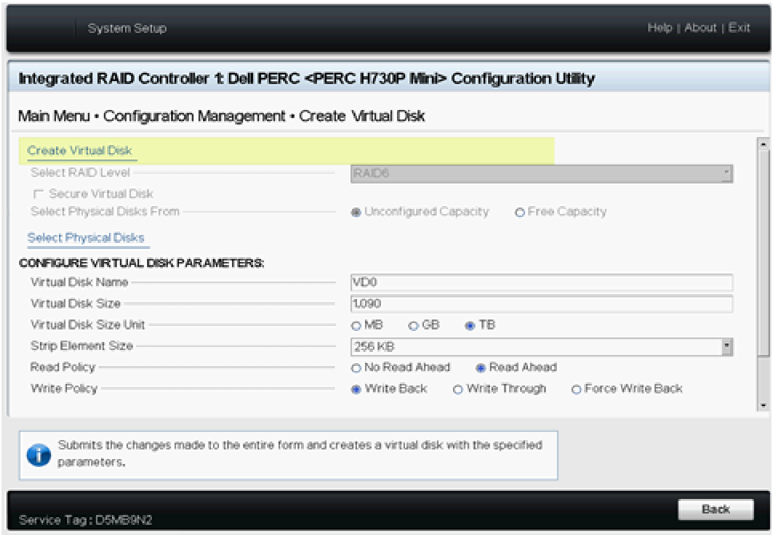
4. On the **Create Virtual Disk** screen, click **Select Physical Disks**.
5. Under **Choose Unconfigured Physical Disks**, select all the unconfigured physical disks for the Avaya Solutions Platform profile configuration, as mentioned in step 3.

   The following is an example with 4 physical disks selected.



6. Click **Apply Changes**, then click **OK**.
7. Check that the virtual disk size is approximately of the expected size as shown in [Virtual disk size](#) on page 130.

8. Click **Create Virtual Disk**.



9. Check the **Confirm** box, select **Yes**, and click **OK**.

   The system creates a new virtual disk.

10. Click **Back**.

Next steps

Proceed to Checking information about the virtual disk on page 131 for the steps to check the basic properties of a specific virtual disk.

Virtual disk size

The following table provides the expected virtual disk sizes for the RAID configuration.

RAID configuration	Raw Storage	Usable Capacity in Terabytes	Usable Capacity in Tebibytes	ASP Base Profile (no optional HDDs)
5	3x600 GB = 1.8 TB	1.2	1.09	2
6	4x600 GB = 2.4 TB	1.2	1.09	3, 4
6	5x600 GB = 3.0 TB	1.8	1.64	N/A
6	6x600 GB = 3.6 TB	2.4	2.18	5
6	7x600 GB = 4.2 TB	3.0	2.73	N/A
6	8x600 GB = 4.8 TB	3.6	3.27	51

Note:

The table provides the usable capacity both in Terabytes and Tebibytes, as operating systems may calculate data storage space in Tebibytes.

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 the same for both the H730P and H750.

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.

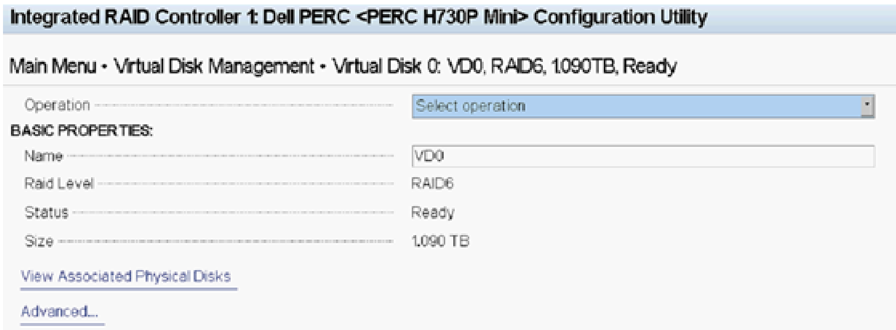
   

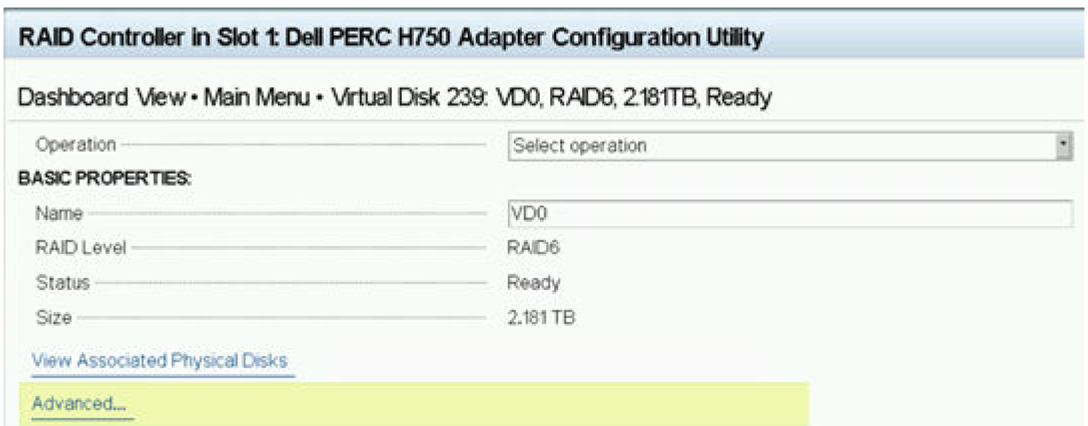
2. Click the virtual disk name.
3. Under Basic Properties, check the information about the virtual disk. You can see the following parameters of the virtual disk:
   - Name
   - RAID Level
   - Status

- Size

Note:

Notice that the H730 RAID Controller creates its first Virtual Disk starting as number 0 and increments up. Whereas the H750 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 86 for information on installation of ESXi Software.

Chapter 11: Dell 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:

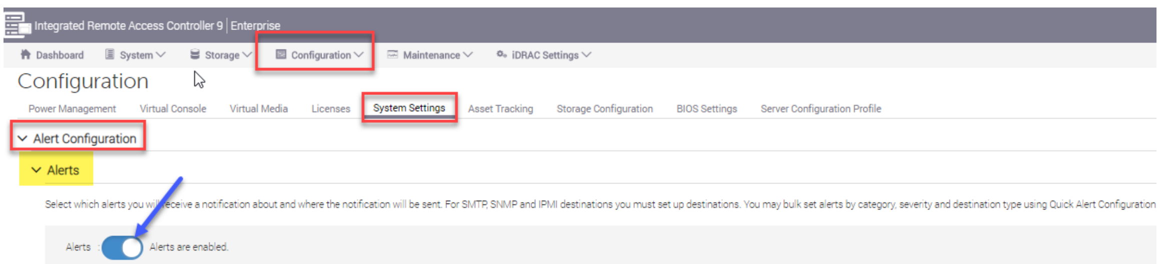
Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Before you begin

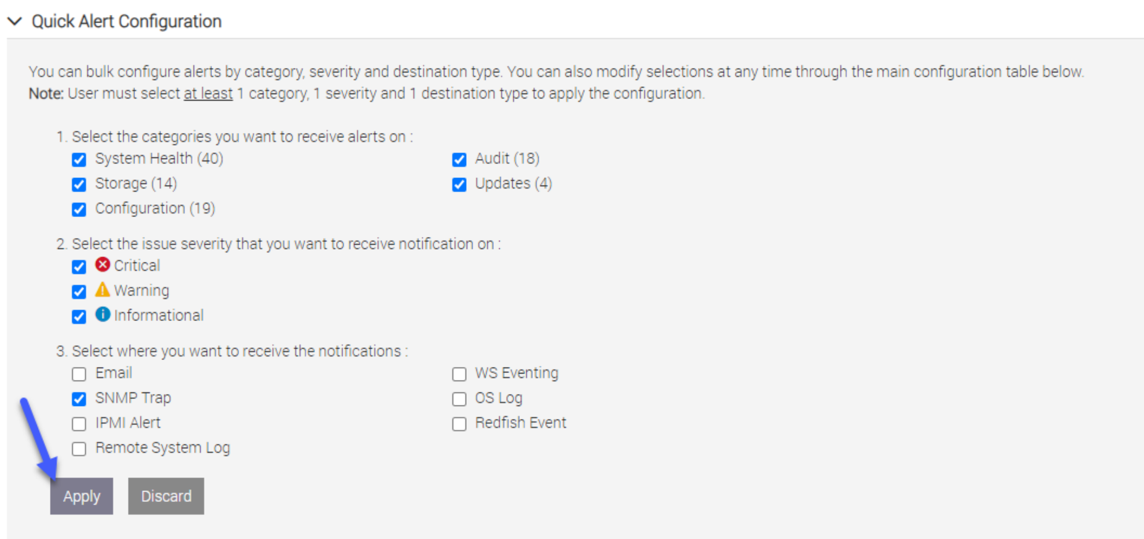
Log into the iDRAC9 web interface using the IP address and login details that were specified while configuring the iDRAC. See the Avaya Solutions Platform 130 Series iDRAC9 Best Practices document for configuring the iDRAC.

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.

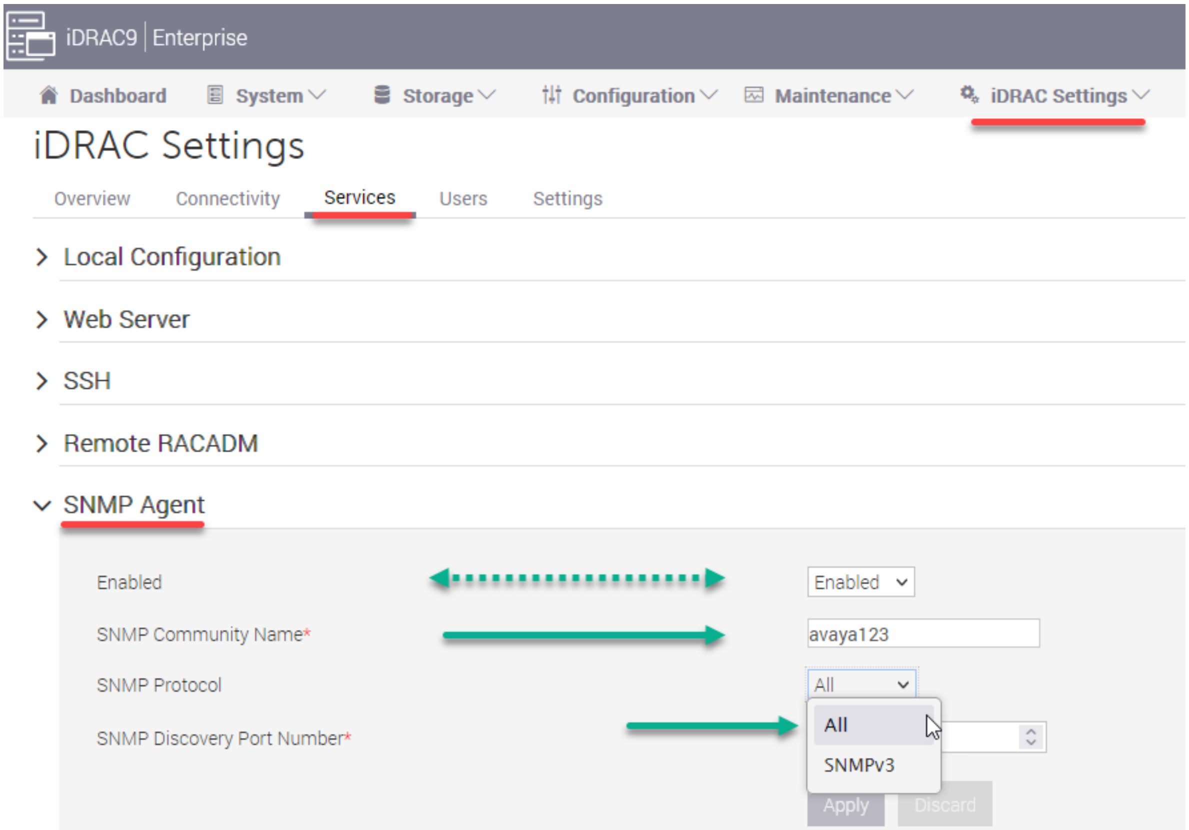


Figure 14: Configuring SNMP v2c using iDRAC9

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.

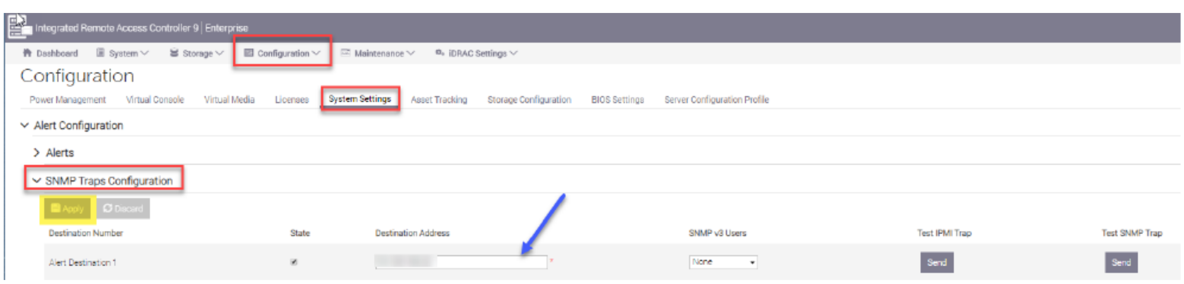
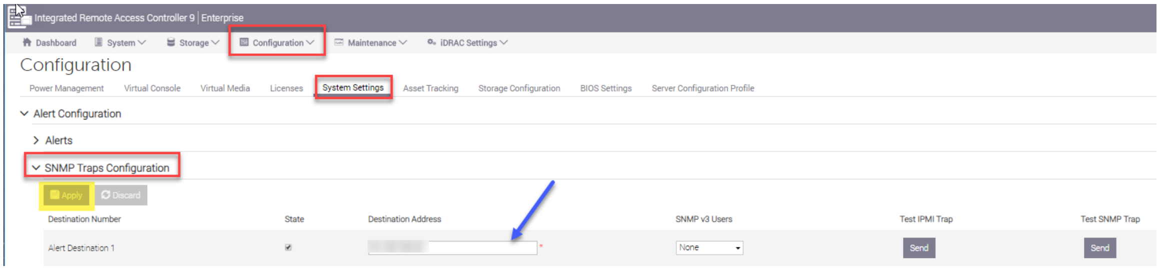


Figure 15: Configuring SNMP Traps

- 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.

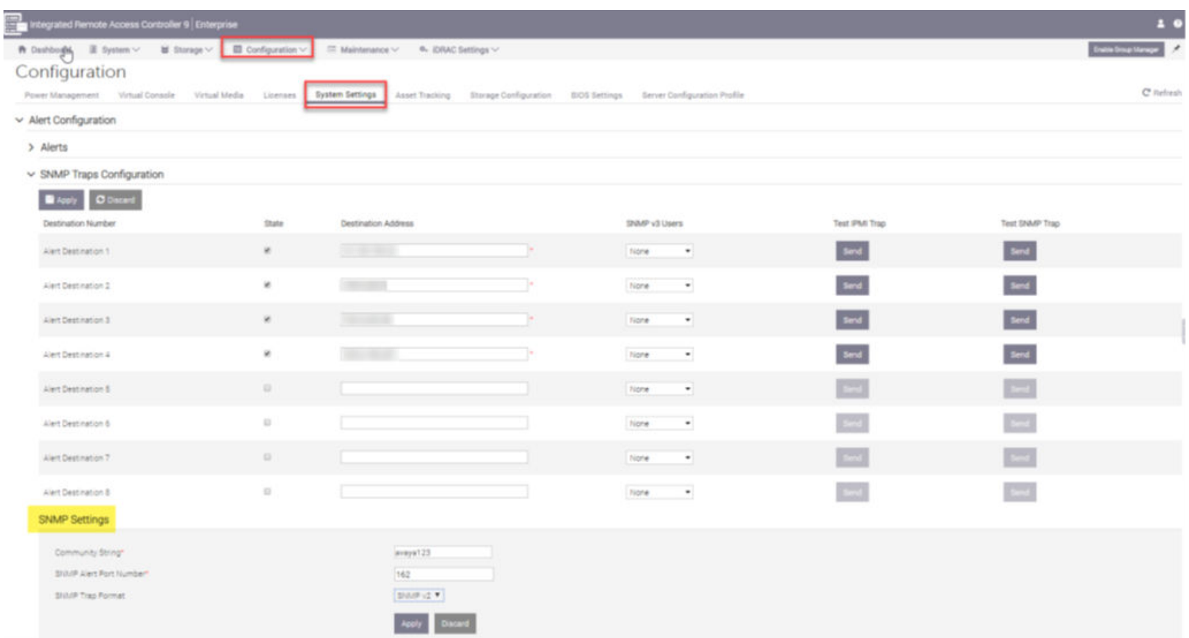


Figure 16: Configuration

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.

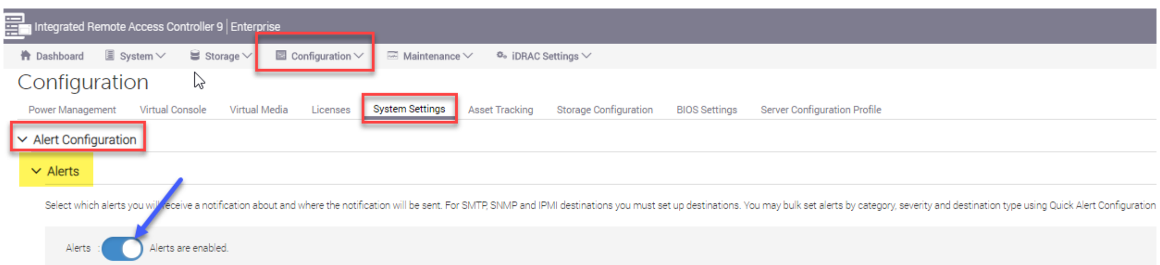
Before you begin

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.

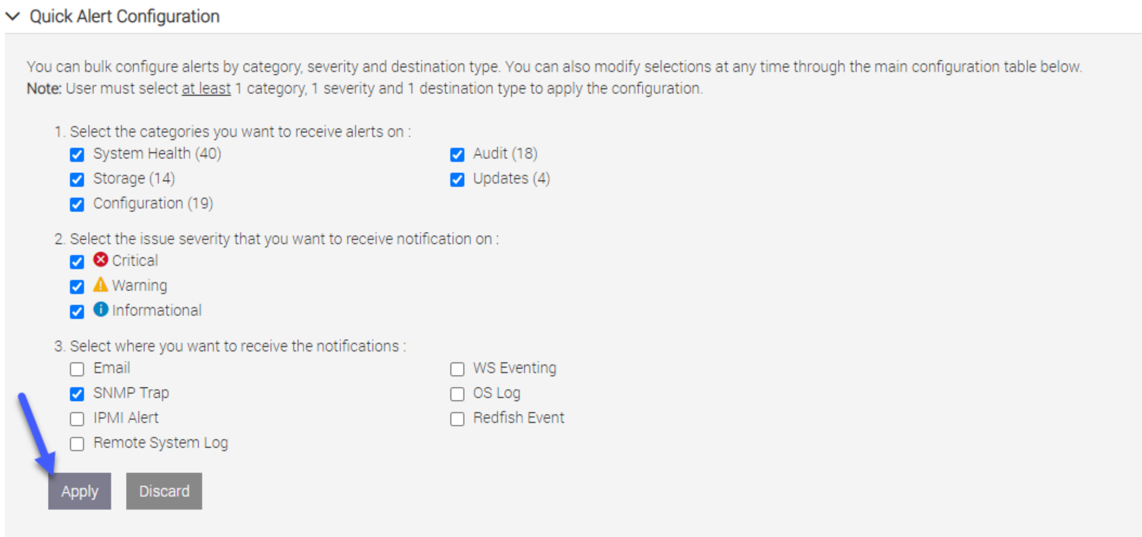
Procedure

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:

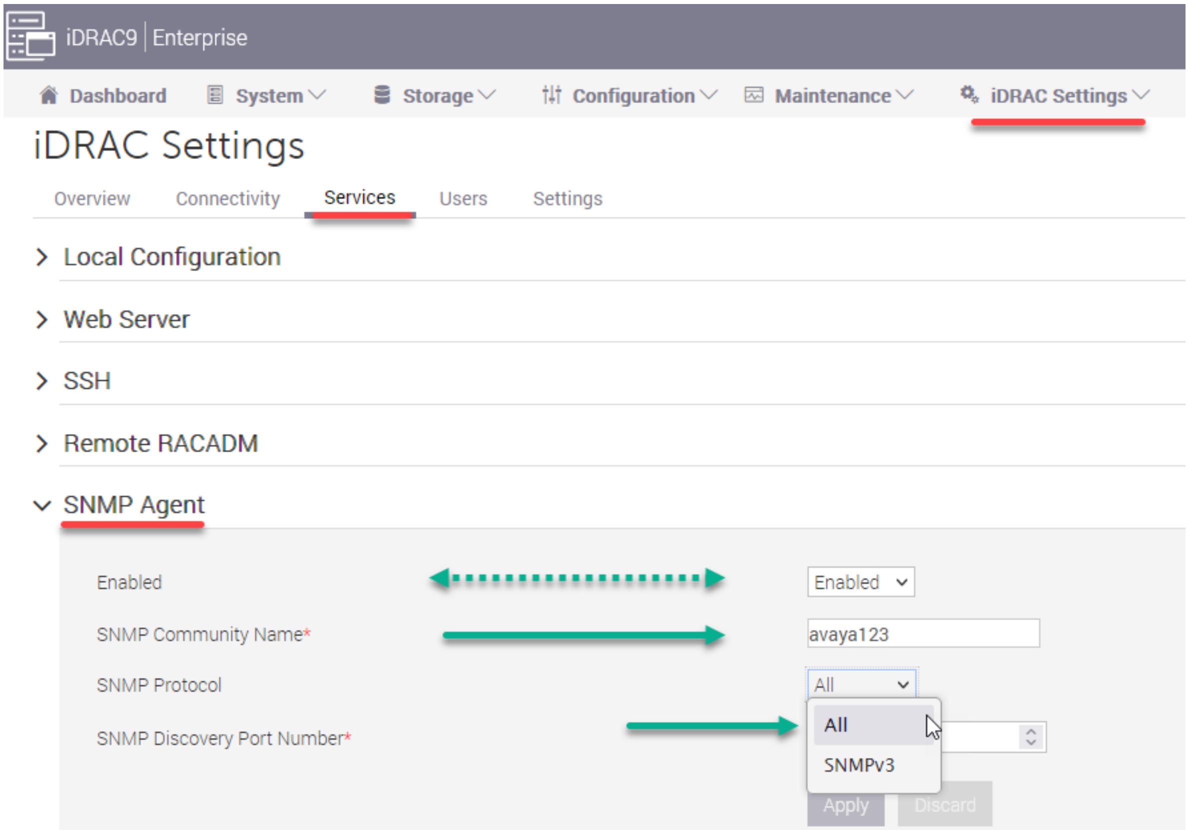
   Avaya strongly recommends changing the SNMP community name to a non-standard name for security purposes.

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

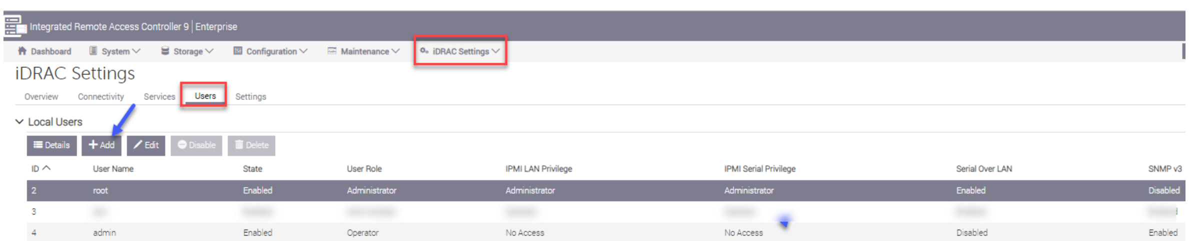
   Note:

   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.



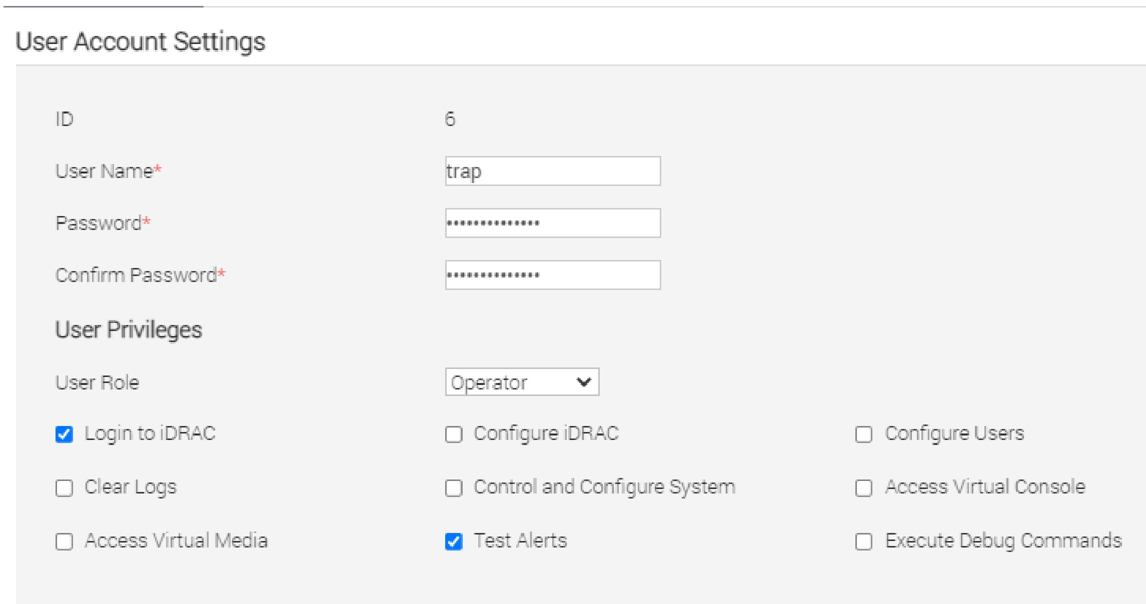
Note:

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 will be 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**.

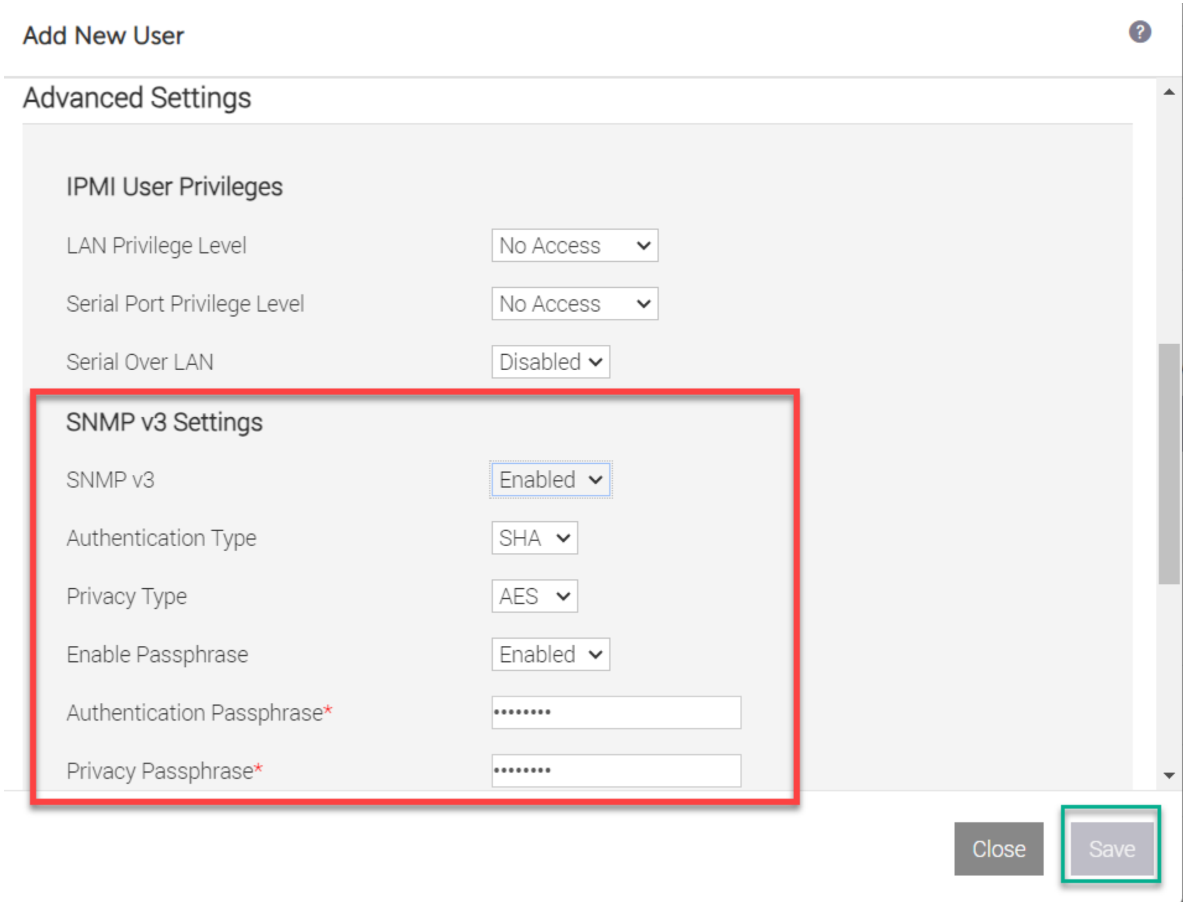
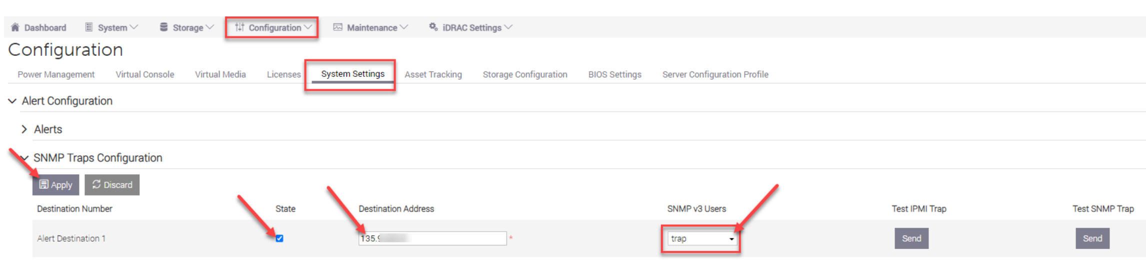


Figure 17: Adding a New User

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.

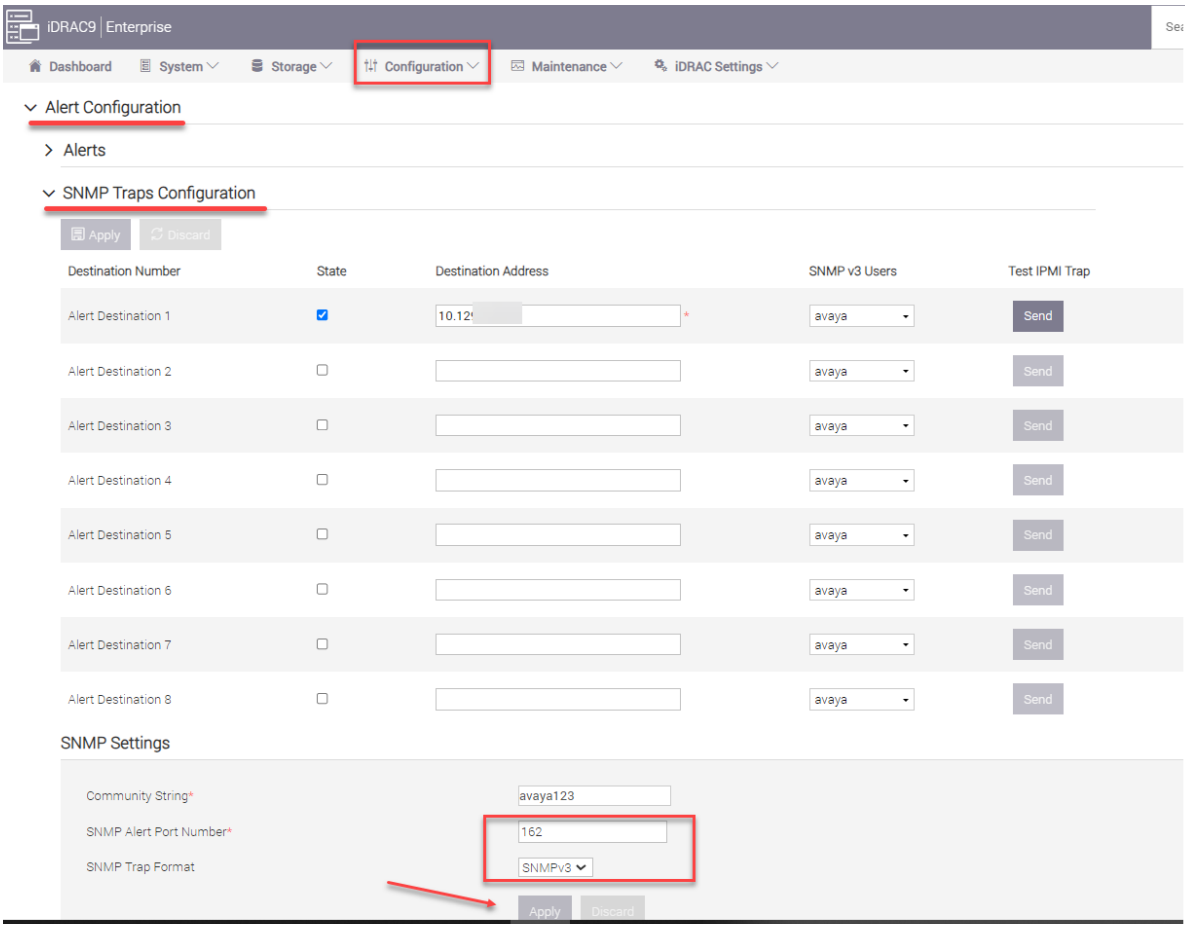


Figure 18: Configuring SNMP Traps

9. 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.

How to Query for SNMP EngineID

About this task

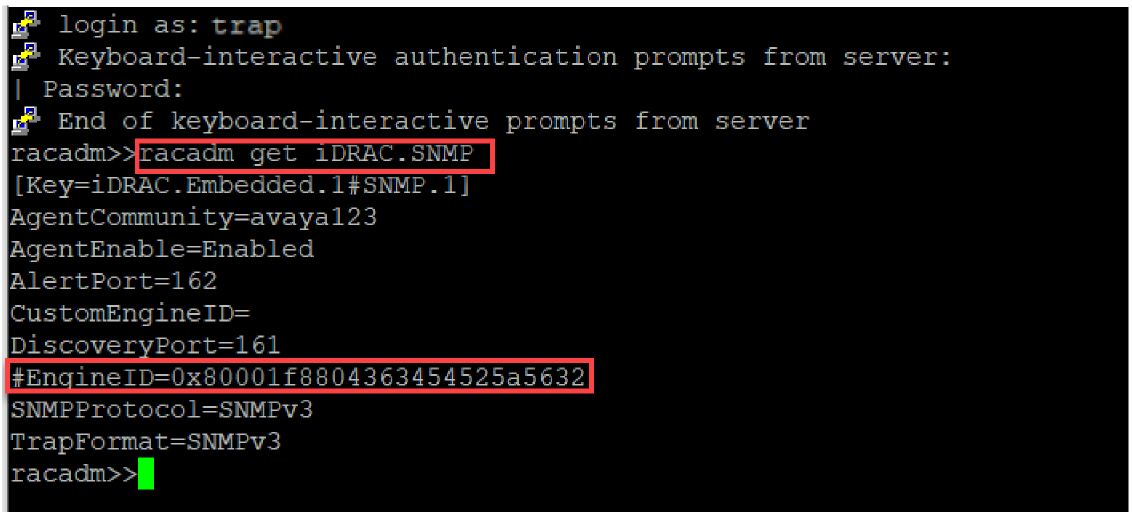
When configuring an SNMPv3 destination device the Engine ID from the source device may be required. To acquire the iDRAC EngineID the user must open an SSH session into the iDRAC interface and query for the EngineID.

Before you begin

Open an SSH session into the iDRAC9 interface using the IP address that was specified when configuring the iDRAC. See Avaya Solutions Platform 130 Series iDRAC9 Best Practices document for configuring the iDRAC.

Procedure

1. Login to the iDRAC using the user id associated with the SNMPv3 user account.
2. Type the command racadm get iDRAC.SNMP <ENTER>



```
login as: trap
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
racadm>>racadm get iDRAC.SNMP
[Key=iDRAC.Embedded.1#SNMP.1]
AgentCommunity=avaya123
AgentEnable=Enabled
AlertPort=162
CustomEngineID=
DiscoveryPort=161
#EngineID=0x80001f8804363454525a5632
SNMPProtocol=SNMPv3
TrapFormat=SNMPv3
racadm>>
```

Figure 19: Querying for SNMP Engine

3. The EngineID along with other SNMP information is displayed.
4. Use the EngineID if required for the SNMPv3 destination device.
5. Type exit <ENTER> to close the SSH session.

Chapter 12: Additional Configuration Guidelines

This section describes additional configuration guidelines while performing installation for Avaya Solutions Platform 130.

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 5.1.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.

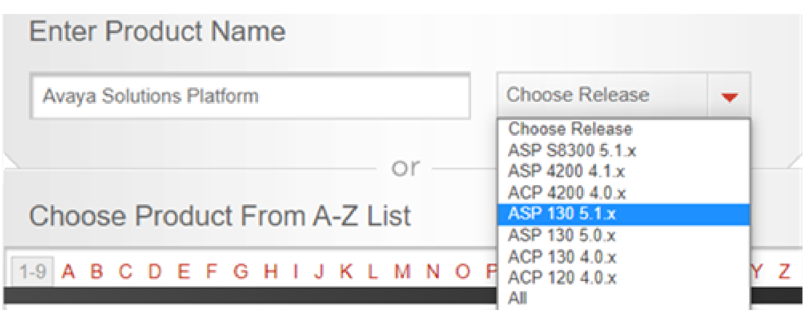
Scope

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

Expected Results

Provide additional information to optimize and utilize additional features and configurations for better usability, manageability, security, or performance to promote improved customer satisfaction.

This chapter will be evolving along with the ASP 130 offer. It is advised that users refer to the http://support.avaya.com/ website for the latest version of all ASP 130 documentation.



Configuring Core Network Administration

Default Configuration

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation as this may impact integration with other Avaya applications and scripts.

All ASP 130s ship with 6 physical NIC ports. The first NIC will be associated with your VM and management traffic. This is assigned to vSwitch0. The second NIC port is assigned to vSwitch1 and is reserved for the Services Port. This port will be assigned IP address 192.11.3.6. It will be used for on-site installers and repair to access the ESXi shell and web. The other 4 NIC ports can be used for Virtual Machines that require their own network segment or they can be used for NIC Teaming. Avaya recommends that vSwitch2-5 be assigned to the other 4 NIC ports.

Note:

If you are using NIC Teaming, you will lose a physical NIC port for each vSwitch you will be teaming with.

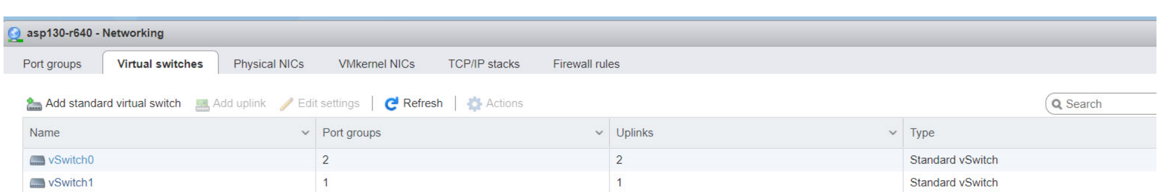
Administer the foundational network configuration.

A deployment with multiple network segments requires appropriate planning. Avaya recommends that each network segment be associated with a single physical NIC port. The network segments will be associated with a vSwitch and a Port Group. It is best practice to configure the hosts vSwitches and Port Groups prior to deploying the OVA.

vSwitch Administration

There will be 2 Standard vSwitch entities administered in the delivered ASP 130 server.

- vSwitch 0
  - Assigned to all VM and ESXi management packet traffic
  - The VMkernel, vmk0 will be associated with vmnic0 for ESXi IP support
- vSwitch 1
  - Exclusively assigned to the direct-connect services port
  - No VM traffic should be assigned to this vSwitch
  - The VMkernel, vmk1 will be associated with vmnic1 for ESXi IP support. This provides a direct-connection between the services laptop and the ESXI host.



Note:

If Out of Band Management (OOBM) is desired in the configuration, an additional vSwitch (vSwitch2-5) should be created to carry the non-management traffic. It is recommended that the Virtual machine port group associated with this new vSwitch be named *Public*. It is also recommended that VMkernel port groups are never associated with vSwitch2-5 for ASP 130.

Configuring a Standard vSwitch

About this task

Use this procedure to create a standard vSwitch in ESXi 7.0 to provide network connectivity for hosts, virtual machines and to handle VMkernel traffic. Application design considerations must be taken into account if performing additional ESXi networking configurations.

Note:

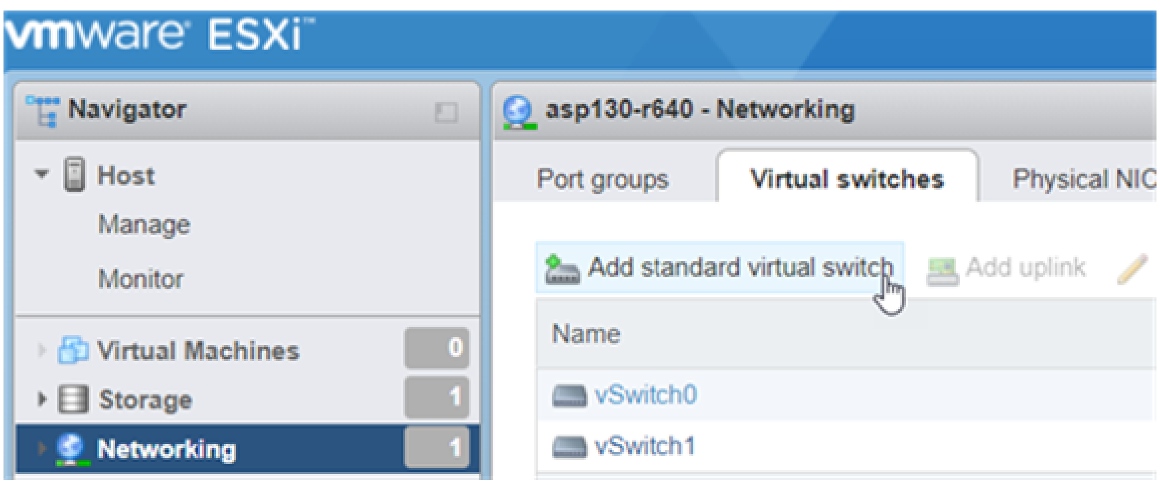
vSwitch0 and **vSwitch1** will come pre-configured in the delivered ASP 130 server.

Before you begin

- Access to the ASP 130 server management network either through a SAL Gateway connection (remotely), the customer network or direct service port connection (onsite).
- Obtain root credentials (root or sroot if EASG is enabled).

Procedure

1. Open a web browser and connect to the desired ESXi host using the existing root credentials i.e. `https://ESXi_IP_or_FQDN/ui`.
2. In the vSphere client, from the menu on the left, select **Networking** and then the **Virtual Switches** tab.
3. Click-on the **Add standard virtual switch** to create the new standard vSwitch.



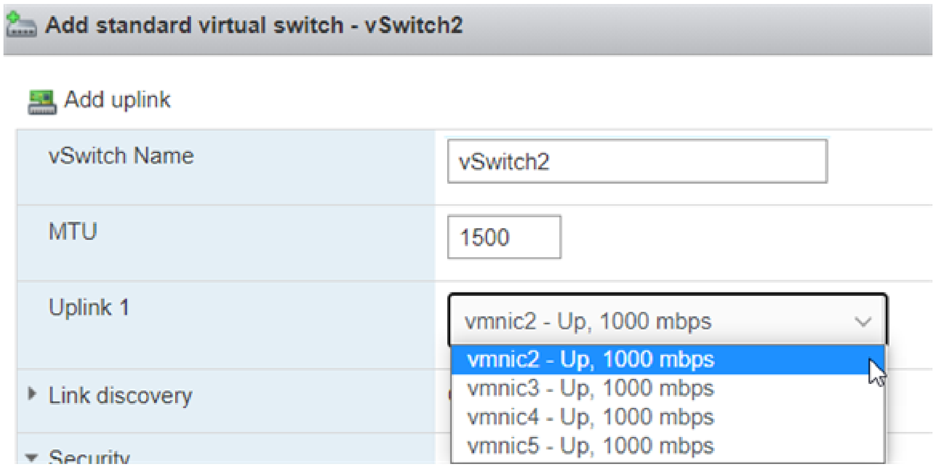
4. A new pop-up configuration window will open. Complete the following fields:
   a. **vSwitch Name**: Only vSwitch2 through 5 are supported due to the Physical NIC limitation with ASP 130 servers, enter a value of vSwitch2, vSwitch3, vSwitch4 or vSwitch5.

b. **MTU**: Leave default value

c. **Uplink 1**: From the drop-down menu, select one of the available vmnics

Note:

In this example, vmnic2 will be selected for vSwitch2. The already assigned vmnics i.e. vmnic0/vmnic1 which by default gets assigned to vSwitch0/1 respectively, will not be displayed from the selection menu.



d. (Optional) Click **Add uplink** to add an additional physical uplink to a virtual switch. Then select an available vmnic from the drop-down menu same as with step c.

Note:

To provide network redundancy, configure at least two physical network adapters (uplinks) in a vSwitch.

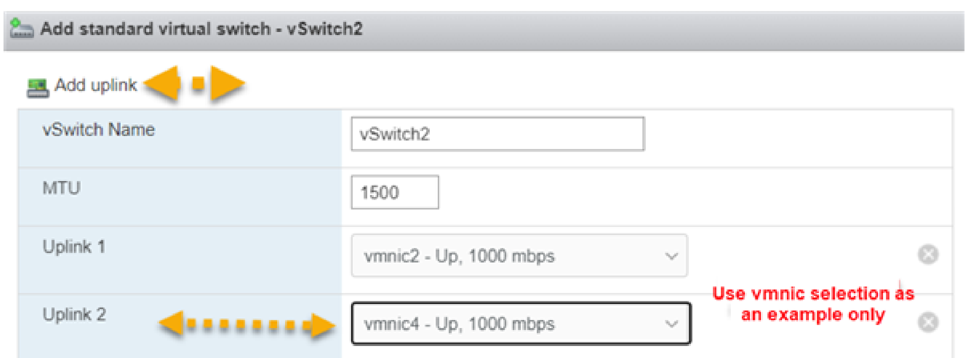


Figure 20: Adding Standard Virtual Switch

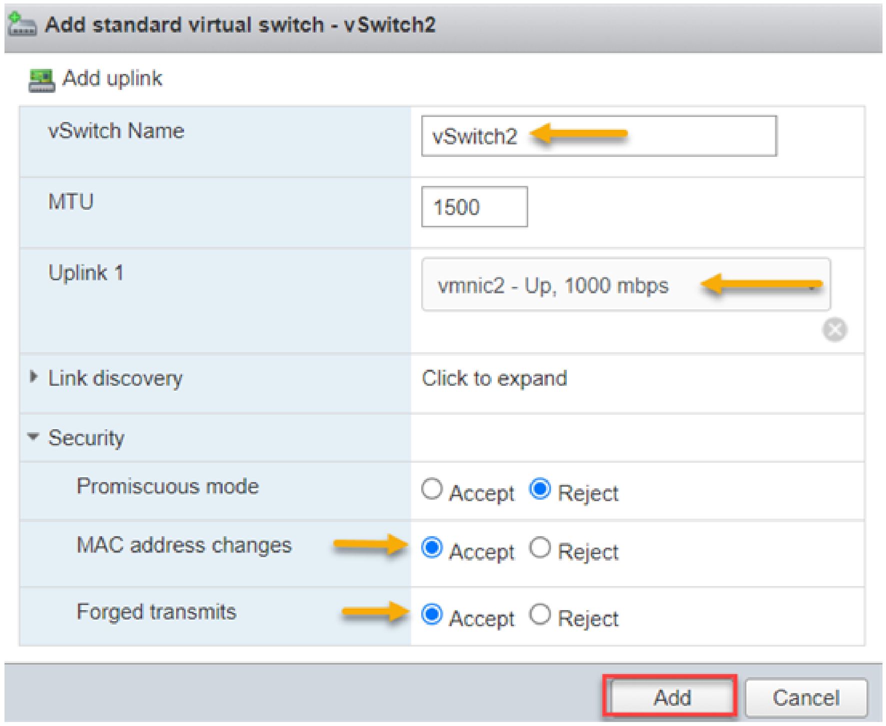
e. **Link discovery**: Leave default values.

f. **Security**: values should match the ones configured in vSwitch0

- **Promiscuous mode** -> Reject
- **MAC address changes** -> Accept

- **Forged transmits** -> Accept

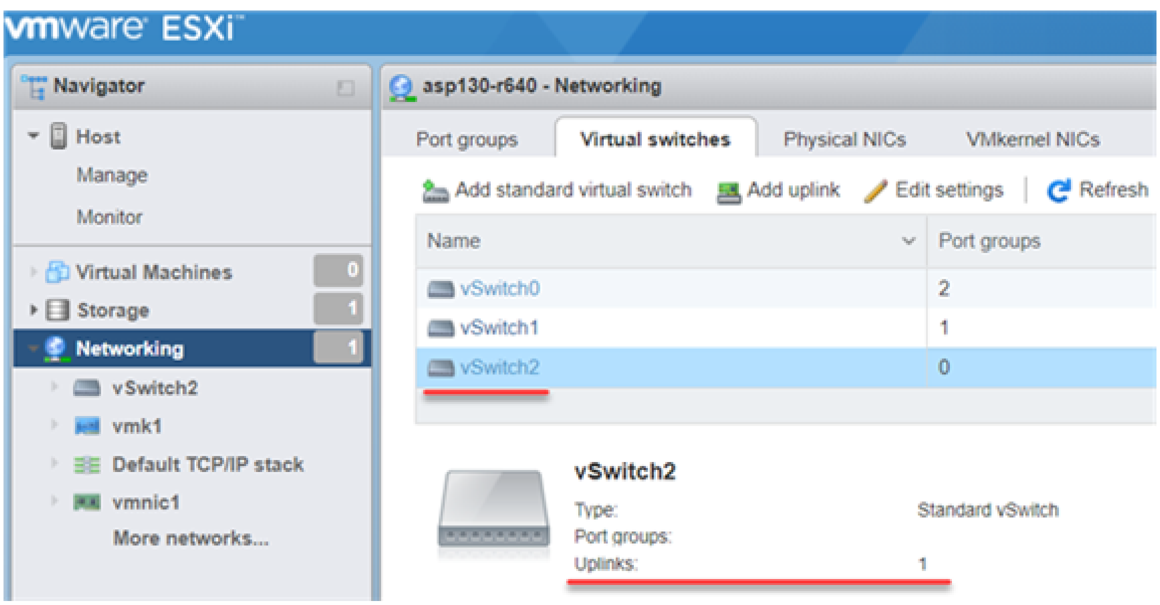
g. Review selections and when ready, click the **Add** button to create the new vSwitch.



5. Pop-up configuration window gets closed and newly created vSwitch is now displayed.

Note:

The **Uplinks** number will reflect the selections made through steps c – d.



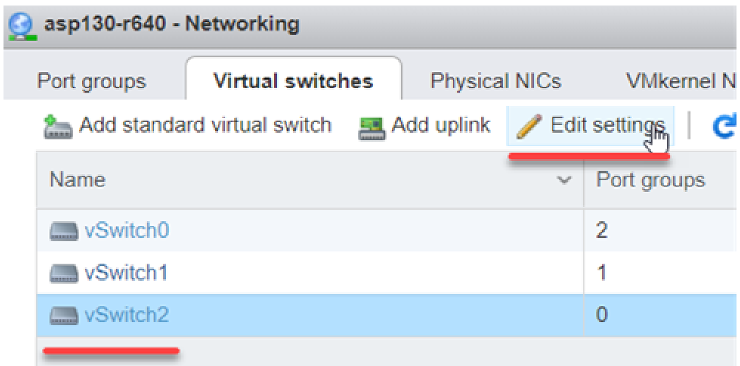
6. Repeat steps 1-4 when creating vSwitch3 through 5.

Mandatory steps for standard vSwitch configured with 2 Uplinks

Note:

Standard vSwitch with a single uplink configuration can skip steps 7-9.

7. Select the newly created standard vSwitch i.e. **vSwitch2** and click on the **Edit Settings** button.

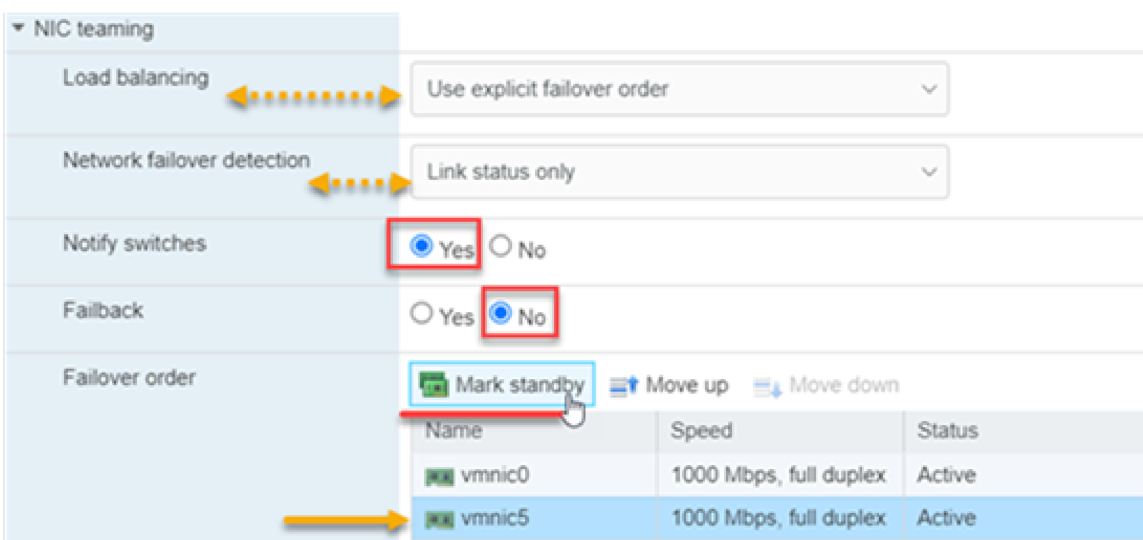


8. Expand the **NIC teaming** view and proceed with the following configuration:

Note:

By default, the second uplink vmnic will be set to *Active*. This second uplink vmnic must be changed to *standby* as *Active-Active* is not supported.

- **Load balancing**: **Use explicit failover order**
- **Network failover detection**: **Link status only**
- **Notify switches**: Leave default selection (**Yes**)
- **Failback**: **No**
- **Failover order**: Select vmnic from step 4 i.e. **vmnic5** and click on **Mark standby**.

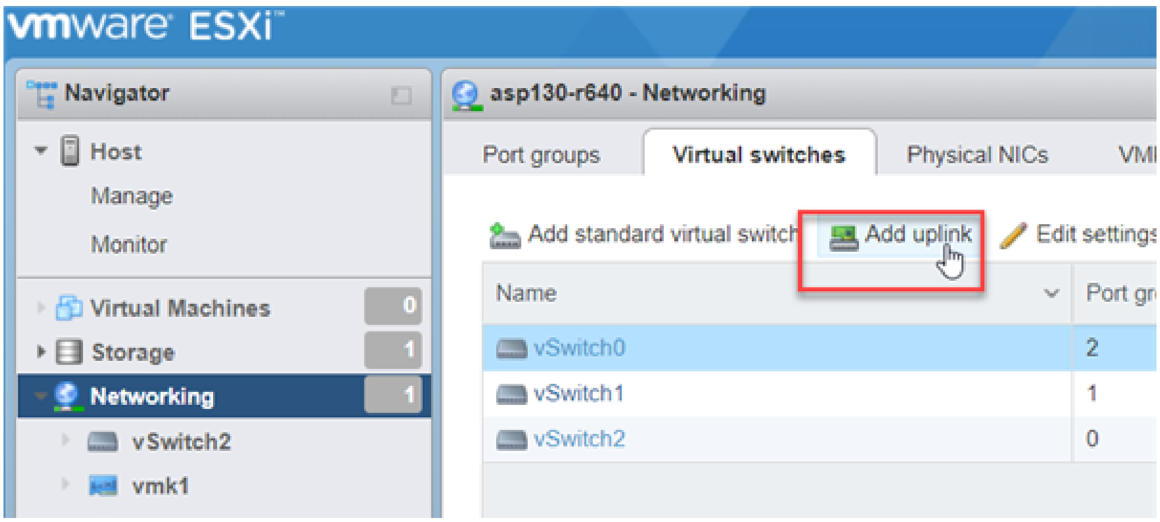


9. Review selections when ready click on the **Save** button to permanently save new settings.

Adding Uplink to an existing standard vSwitch

Procedure

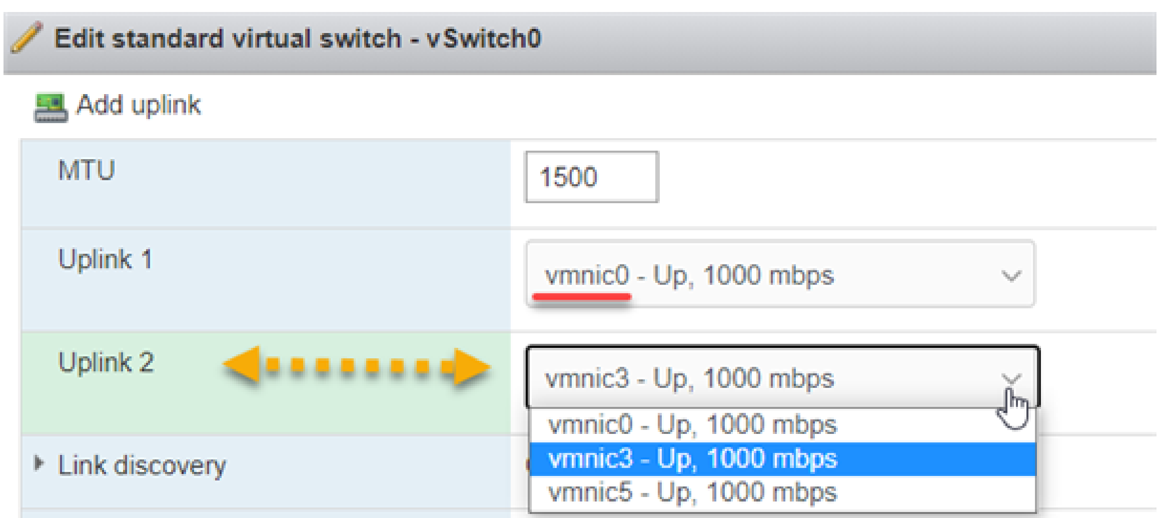
1. If not already, open a web browser and connect to the desire ESXi host using the existing root credentials i.e. `https://ESXi_IP_or_FQDN/ui`.
2. In the vSphere client, from the menu on the left, select **Networking** and then the **Virtual Switches** tab.
3. Select one of the existing standard vSwitch previously configured, such as **vSwitch0**, and click on the **Add uplink** button.



4. Select a unique, unassigned **vmnic** from the **Uplink 2** drop-down menu.

Note:

Do not select the same **vmnic** that has been previously assigned to **Uplink 1**.

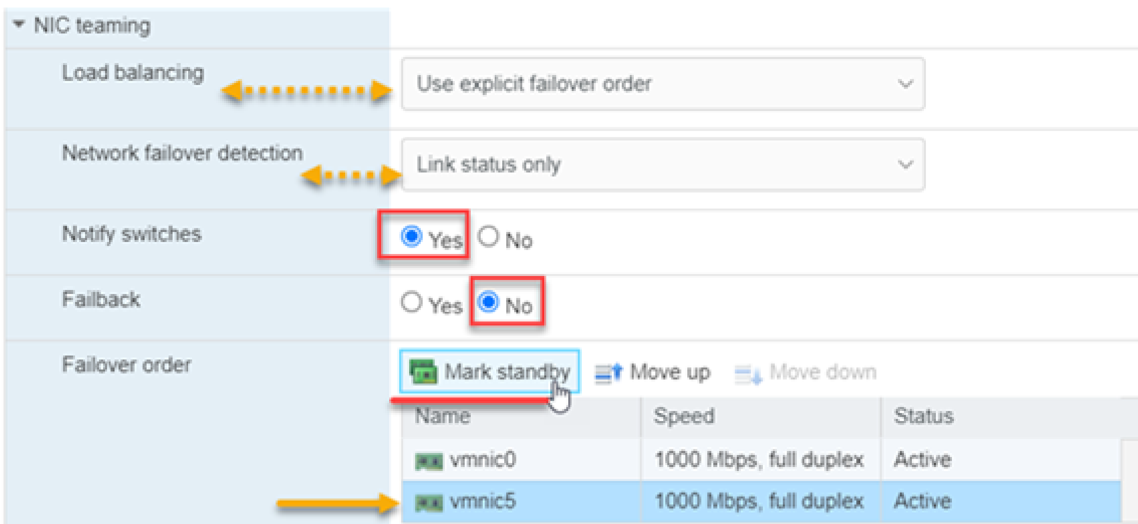


5. Expand the **NIC teaming** view and proceed with the following configuration:

   Note:

   By default, the second uplink vmnic will be set to *Active*. This second uplink vmnic must be changed to *standby* as *Active-Active* is not supported.

   - **Load balancing**: Use explicit failover order
   - **Network failover detection**: Link status only
   - **Notify switches**: Leave default selection (Yes)
   - **Failback**: No
   - **Failover order**: Select **vmnic** from step 4 i.e. **vmnic5** and click on **Mark standby**



6. Review selections when ready click on the **Save** button to permanently save new settings.

Add a Virtual Machine Port Group

About this task

Use this procedure to add a port group to a standard virtual switch. Port groups provide networking for virtual machines. Application design considerations must be taken into account if performing additional ESXi networking configurations. For example, when deploying CM Duplex the CM duplication link needs to be on a separate, dedicated virtual machine port group with VLAN tagging off.

Note:

VM Network, **Management Network** and **Services Port Groups** will come pre-configured in the delivered ASP 130 server.

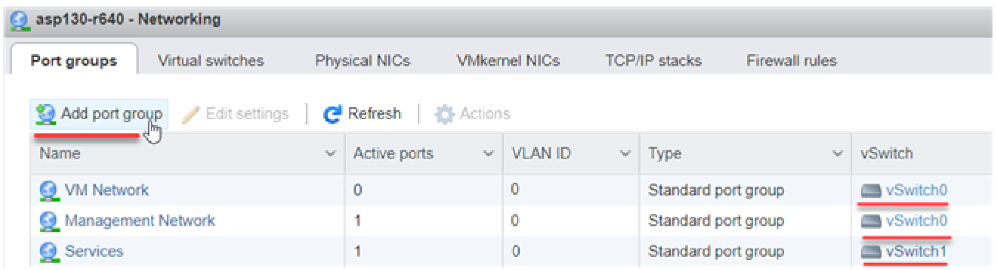
Before you begin

- Access to the ASP 130 server management network either through a SAL Gateway connection (Remotely) or direct service port connection (onsite).

- `root` password.
- Standard vSwitch must be configured prior to this activity.

Procedure

1. Open a web browser and connect to the desire ESXi host using the existing root credentials i.e. `https://ESXi_IP_or_FQDN/ui`.
2. In the vSphere client, from the menu on the left, select **Networking** and then the **Port Groups** tab.
3. Click on the **Add port group** button.

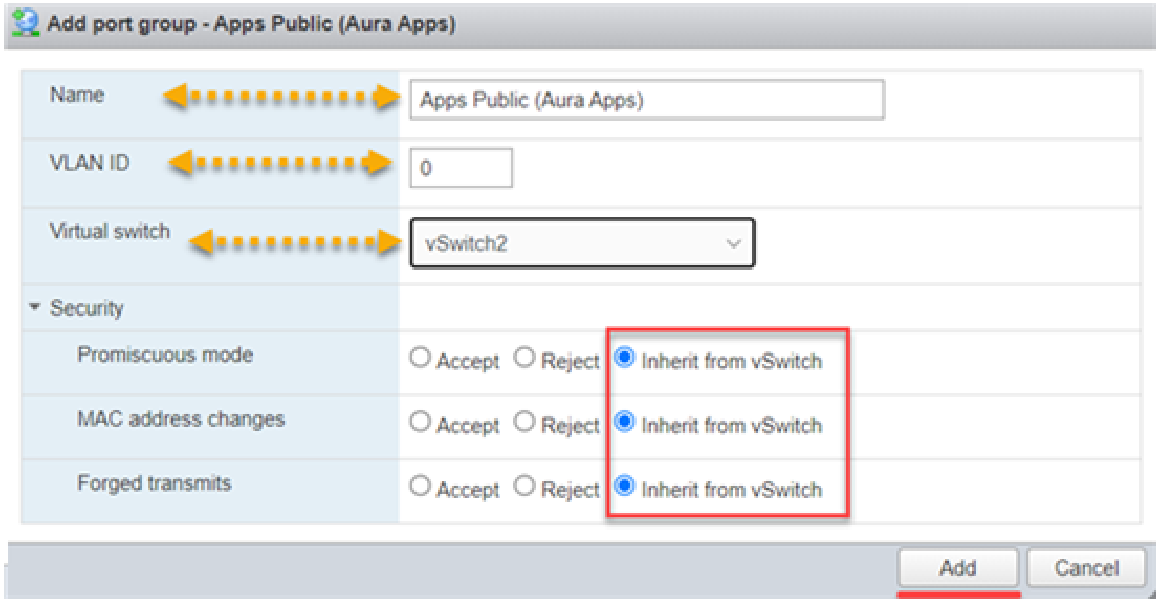


4. A new pop-up configuration window will open. Complete the following fields:
   a. **Name**: Enter a descriptive name for the new port group i.e. Apps Public (SM, SMGR, CM), CM-Duplication etc.
   b. Set the VLAN ID to configure VLAN handling in the port group. The VLAN ID also reflects the VLAN tagging mode in the port group.

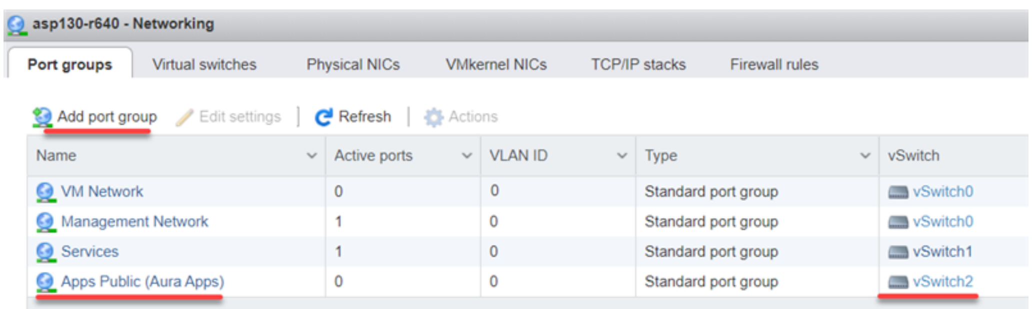
VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN. (ASP 130 recommended)
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that is entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN. (This is not supported by ASP 130).

   c. Select one of the existing standard virtual switches from the drop-down menu i.e. **vSwitch2** for the Avaya Aura® application traffic.
   d. Expand **Security** view and validate selections are set to receive values from **vSwitch** *inherit from vSwitch*

e. Review values and when ready click the **Add** button to add the new vSwitch.

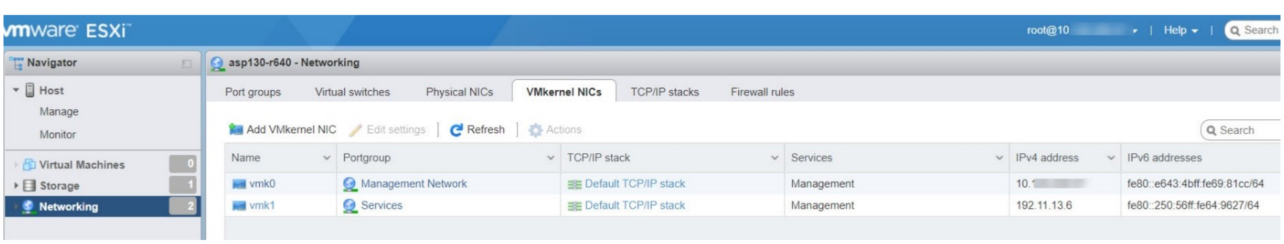


f. Pop-up configuration window will close, and the **Port groups** tab will refresh with the newly created Port group.



VMkernel Port Administration

VMkernel ports have been configured in the delivered ASP 130 server. The required VMkernel ports are pre-configured by Avaya's Integrator. Below are the two administered values that come as part of the standard configuration. VMkernel ports are assigned for the services and ESXi management to allow remote access into the server via specific IP addresses.



Warning:

The Avaya assigned VMkernel port configuration should not be altered. Any changes will not be supported.

ASP 130 VLAN Tagging

Due to the complexities and coordination between ESXi network configuration and the customer network switch Avaya does not recommend the use of VLANs in ESXi.

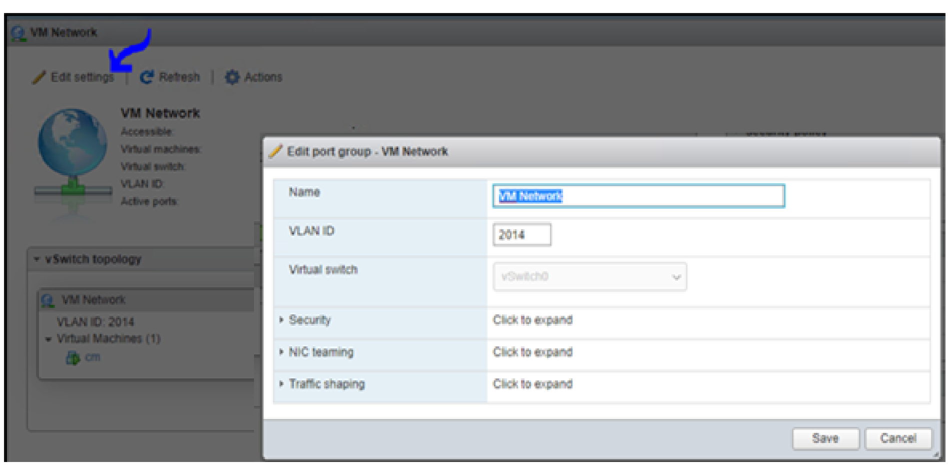
By default, the ESXI management NIC interface will be **vmnic0**. Since the packet traffic for ESXi management activities is minimal, users may opt to also use **vmnic0** to also support application traffic.

While the use of VLAN tagging will help support the network port-trunking infrastructure, this will require extensive coordination with the customer's network engineering team.

The VLAN tagging administrative fields are found in **Networking** > **Port groups**, and these settings need to match the VLAN configuration of the physical ethernet switches the ASP 130 is connected to. Click on the port group needing to be assigned a VLAN, and then **Edit settings** to administer the desired VLAN ID. Setting VLAN ID to any value other than 0 will enable VLAN tagging. By default VLAN ID is set to 0.

The table below reflects the supported entries for ESXi. The VLAN ID also reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN. (ASP 130 recommended)
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that is entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN. (This is not supported by ASP 130).



Note:

It is recommended that VLAN tags not be used in order to keep network configuration and troubleshooting as simple as possible.

ASP 130 NIC Teaming

NIC teaming provides a redundant path for the management and Application traffic.

NIC Teaming is a VMware feature, not an Avaya feature. Customers wishing to configure NIC Teaming on the ASP 130 are required to use Avaya's instructions.

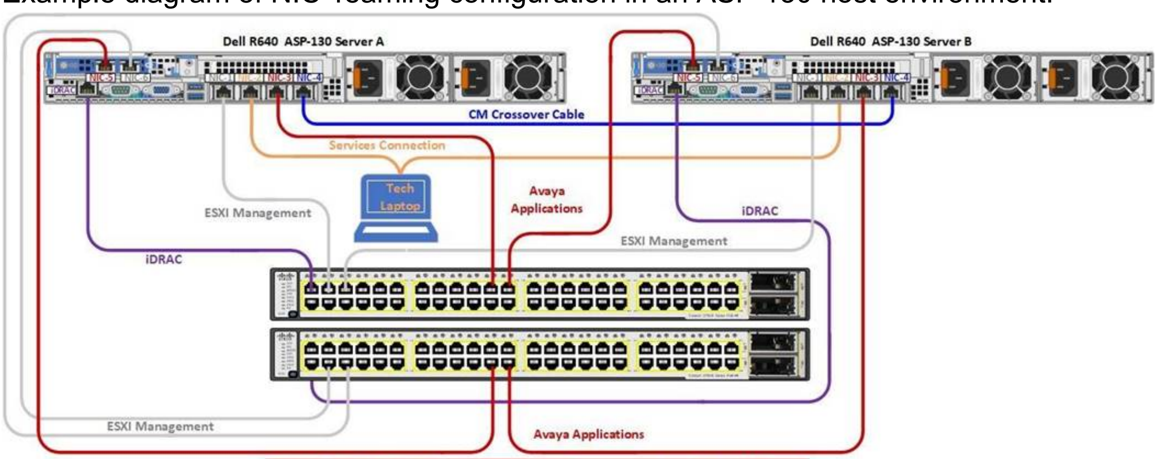
Note:

The only supported NIC teaming configuration within the ASP 130 solution is *Active*/*Standby*.

Administer NIC Teaming in ESXi vSphere client

The administration for NIC Teaming is addressed in both the vSwitch and Port Group levels. To keep a streamlined and consistent behavior the vSwitch will be the primary reference point for NIC Teaming behaviors and expectations.

Example diagram of NIC Teaming configuration in an ASP 130 host environment:



Pysical	Virtual	vSwitch	Usage	Native VLAN
NIC 1	vmnic0	vSwitch0	ESXI Management Primary	Management VLAN
NIC 2	vmnic1	vSwitch1	Avaya Services Port	Direct Connected VLAN
NIC 3	vmnic2	vSwitch2	Avaya Applications Primary	Voice VLAN
NIC 4	vmnic3	vSwitch3	CM Duplication Link (Crossover Cable)	Direct Connected VLAN
NIC 5	vmnic 4	vSwitch2	Avaya Applications Secondary	Voice VLAN
NIC 6	vmnic 5	vSwitch0	ESXI Management Secondary	Management VLAN
iDRAC	iDRAC	N/A	iDRAC	iDRAC Subnet

Configure ESXi Management Interface in the Server for NIC Teaming

The ESXi 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.

vSwitch1 is a dedicated services vSwitch, it will never be associated with NIC Teaming. Leave this vSwitch administration, associated VM Kernel and Port Group administration in the original deployed state as it is used by Avaya Services Technicians to connect to the host locally if problems arise with the server.

In this configuration example, vSwitch0 is configured with a new uplink. For updating the NIC teaming configuration on a vSwitch that has been previously configured with a redundant uplink go to Updating the NIC Teaming configuration on a standard vSwitch on page 159.

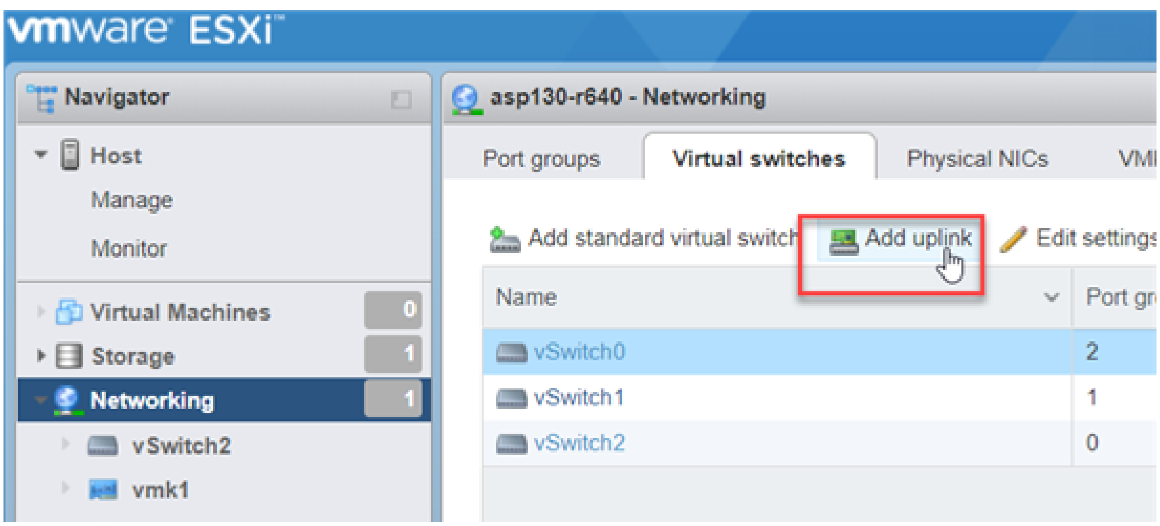
Note:

Following the same steps and referencing to the image in the Administer NIC Teaming in ESXi vSphere client on page 156, NIC teaming can be configured on the vSwitch created for the Aura Application traffic, for example: On vSwitch2, pairing NIC3 (vmnic2) with NIC5 (vmnic4).

Adding Uplink to an existing standard vSwitch

Procedure

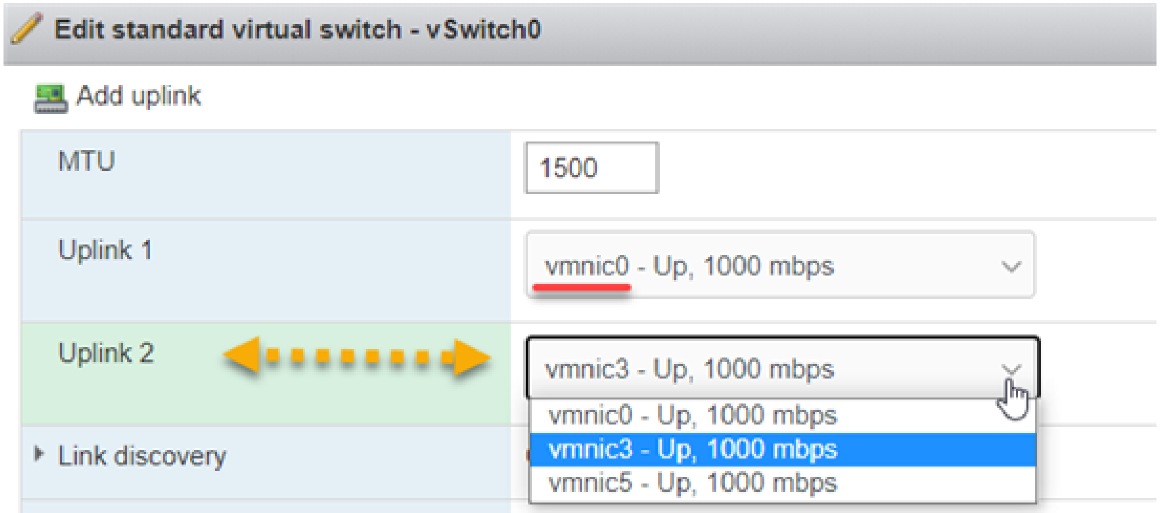
1. If not already, open a web browser and connect to the desire ESXi host using the existing root credentials i.e. `https://ESXi_IP_or_FQDN/ui`.
2. In the vSphere client, from the menu on the left, select **Networking** and then the **Virtual Switches** tab.
3. Select one of the existing standard vSwitch previously configured, such as **vSwitch0**, and click on the **Add uplink** button.



4. Select a unique, unassigned **vmnic** from the **Uplink 2** drop-down menu.

   Note:

   Do not select the same **vmnic** that has been previously assigned to **Uplink 1**.

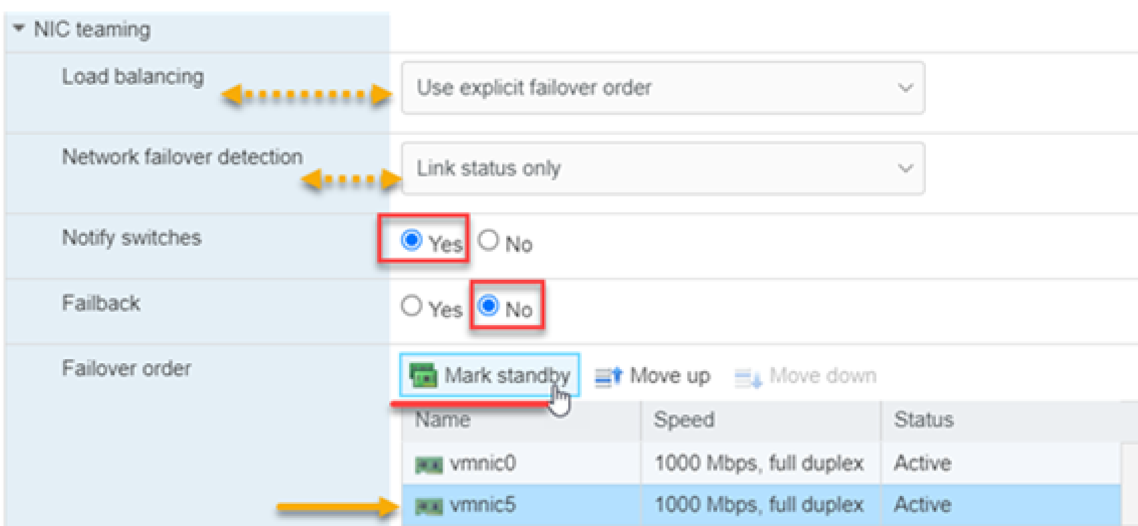


5. Expand the **NIC teaming** view and proceed with the following configuration:

Note:

By default, the second uplink vmnic will be set to *Active*. This second uplink vmnic must be changed to *standby* as *Active-Active* is not supported.

- **Load balancing**: Use explicit failover order
- **Network failover detection**: Link status only
- **Notify switches**: Leave default selection (Yes)
- **Failback**: No
- **Failover order**: Select **vmnic** from step 4 i.e. **vmnic5** and click on **Mark standby**



6. Review selections when ready click on the **Save** button to permanently save new settings.

Updating the NIC Teaming configuration on a standard vSwitch

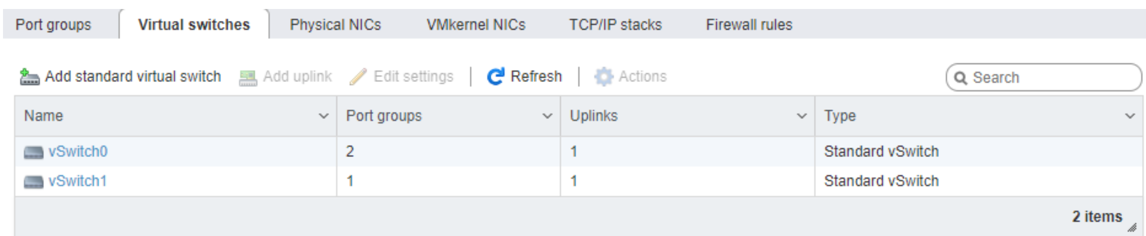
About this task

vSwitch1 is a dedicated services vSwitch, it will never be associated with NIC Teaming. Leave this vSwitch administration, associated VM Kernel, and Port Group administration in the original deployed state as it is used by Avaya Services Technicians to connect to the host locally if problems arise with the server.

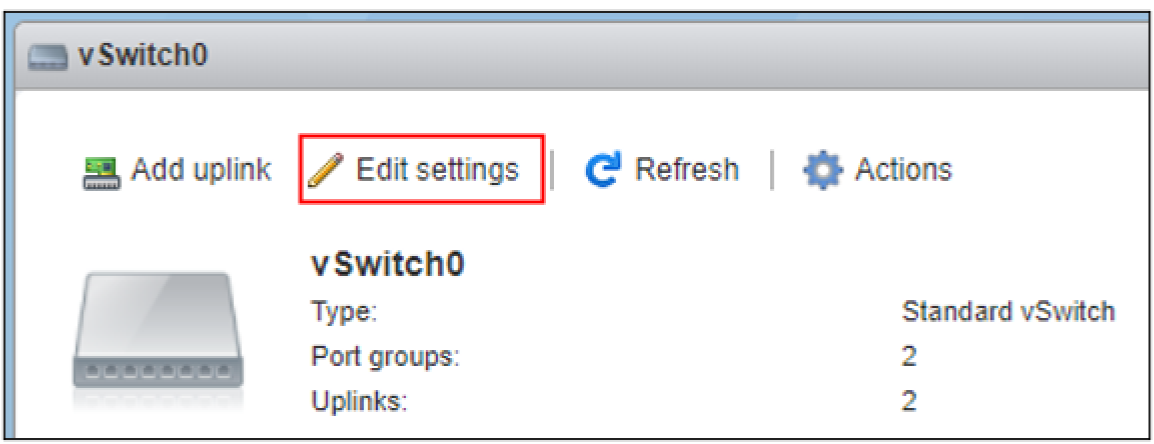
In this example, vSwitch0, supporting ESXi management and VM management traffic has already been configured with a redundant uplink, however, the NIC teaming configuration settings are updated to the values currently supported by the ASP 130 solution. The NIC1 port, vmnic0 is paired with the NIC6 port, vmnic5 to provide additional network redundancy by distributing the backup functionality across 2 different NIC cards.

Procedure

1. From the Networking menu option, select the **Virtual switches** tab and click **vSwitch0**:



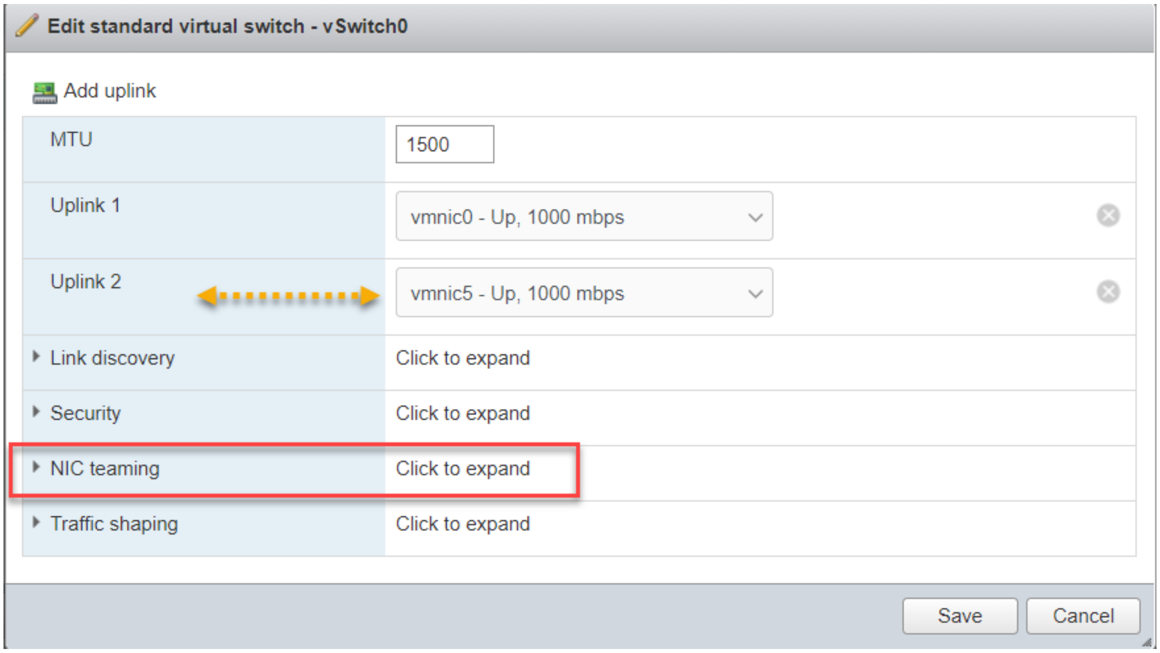
2. From the vSwitch0 submenu, select **Edit settings**:



3. From the **Edit settings** options, click the **NIC teaming** drop-down arrow:

   Note:

   By default, when adding an additional uplink to a vSwitch, the associated vmnic will be set to *Active*. This second uplink vmnic must be changed to *standby* as *Active-Active* is not supported.

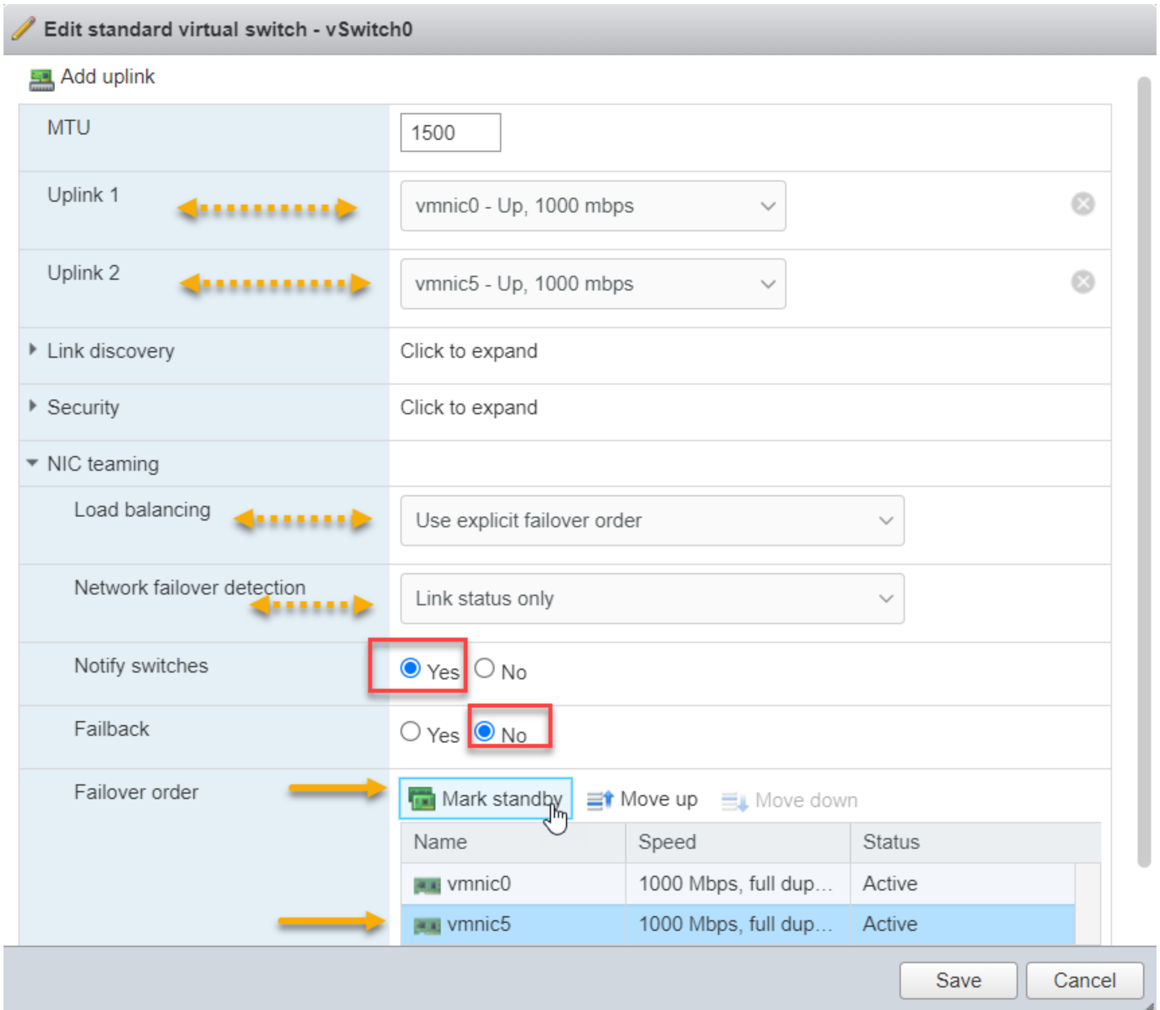


4. Administer the options noted in this example.

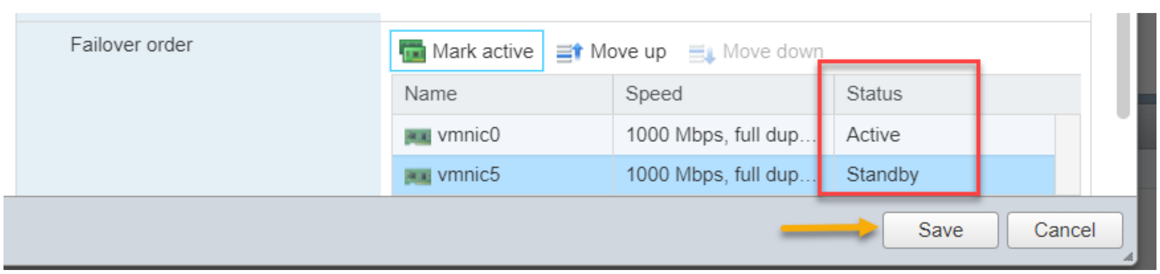
   Deviations from the recommended settings could have negative impacts to the performance and stability of Avaya applications on the ASP 130 server and are not guaranteed.

   a. Load balancing will be set to **Use explicit failover order**.
   b. Network failover detection will be set to **Link status only**, supporting Layer 1 failure.
   c. Notify switches is set to **Yes** to alert the network devices of the change in MAC address termination point, for vSwitch0 traffic, through the use of Reverse Address Resolution Protocol (RARP).
   d. Failback is set to **No**. This prevents a double fault condition by causing all packet traffic to return to using the primary NIC interface once it recovers from whatever caused it to fail.

e. Failover order if not already set, select the vmnic set in uplink 2 i.e. **vmnic5** and click on **Mark standby**.



f. Confirm **vmnic5** status changes from **Active** to **Standby**.



5. When ready, click the **Save** button.

Port Group NIC Teaming Administration

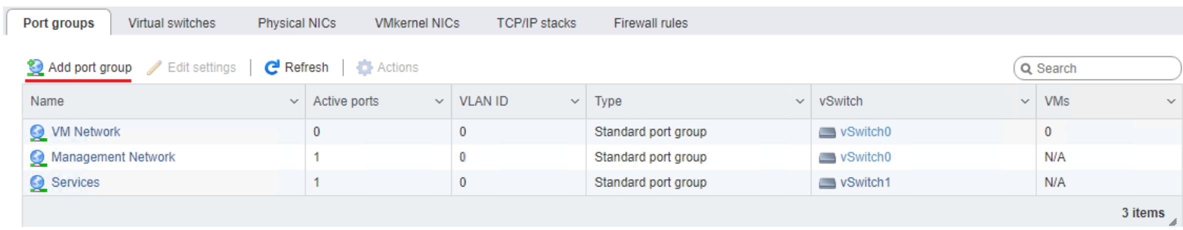
About this task

Note:

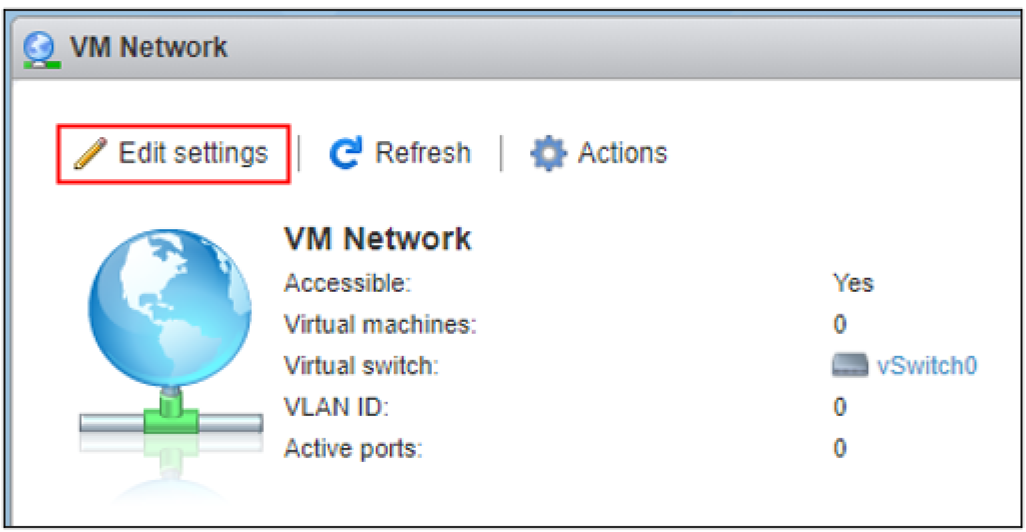
NIC teaming configuration in the VM port groups will be inherited from the vSwitch configuration.

Procedure

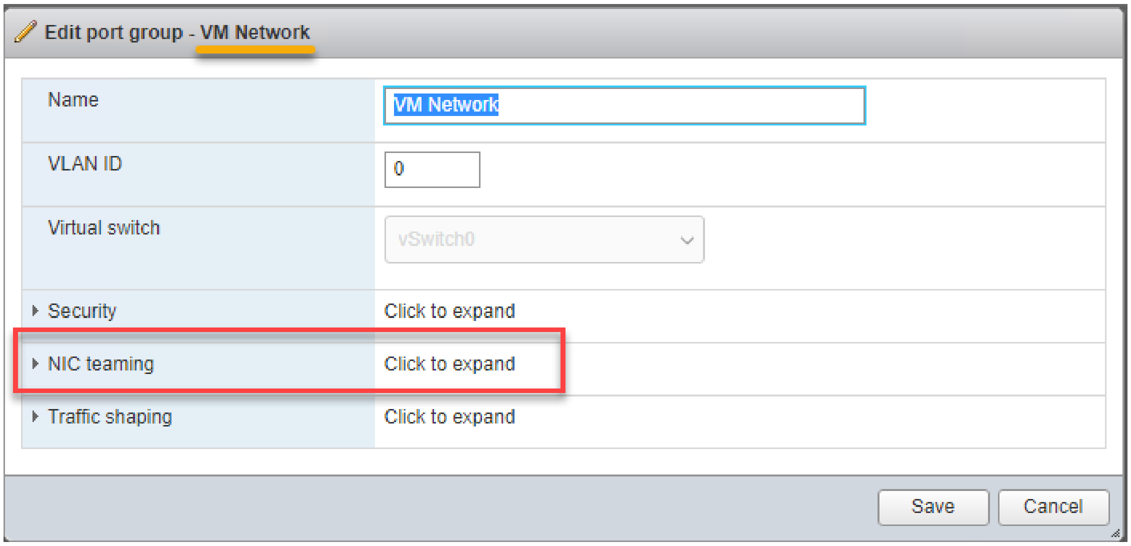
1. From the Networking menu option, select the **Port groups** tab, and click **VM Network**:



2. From the VM Network submenu, select **Edit settings**:



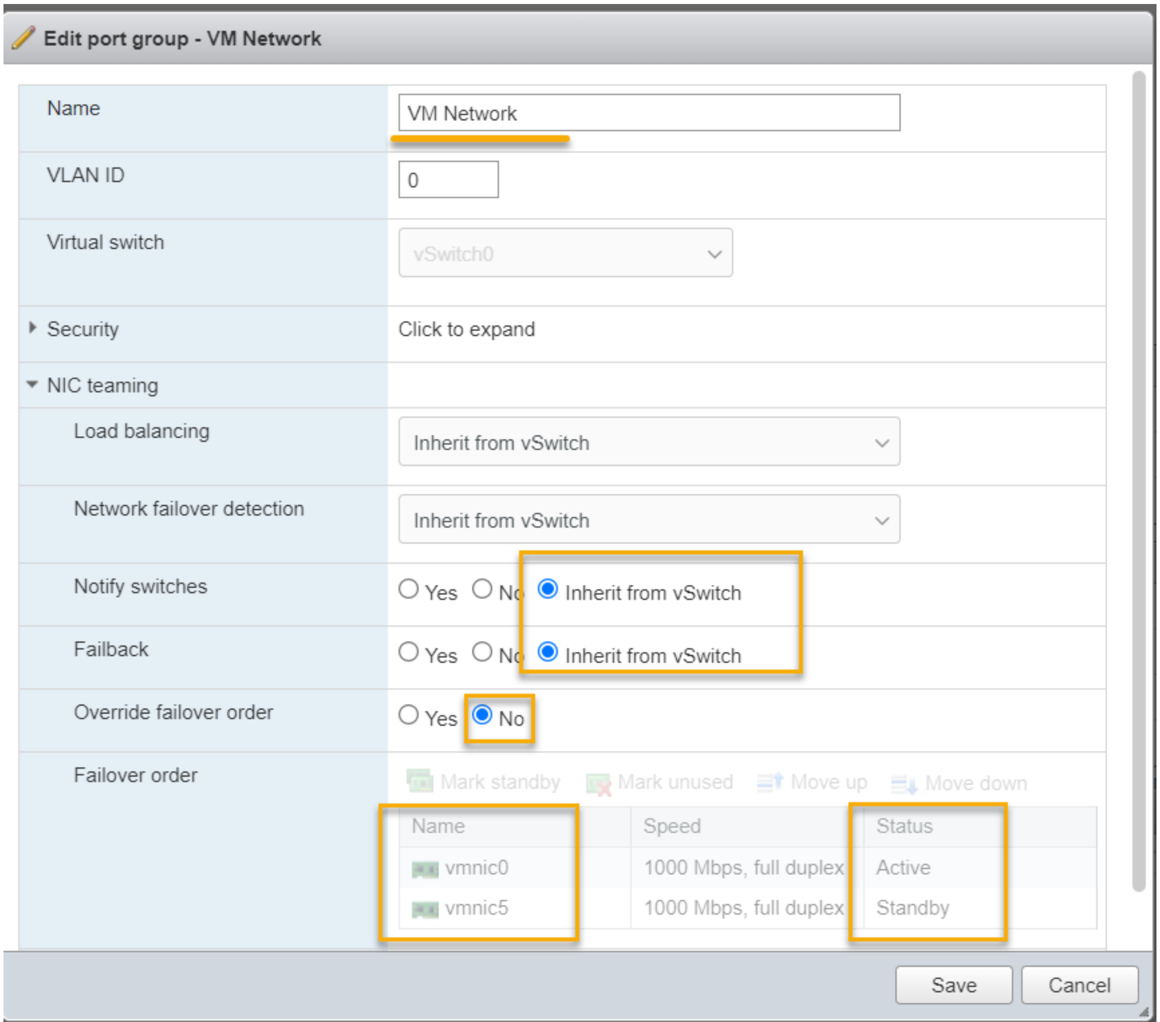
3. From the **Edit settings** options, click the **NIC teaming** drop-down arrow:



4. Administer the options noted in this example.

   Deviations from the recommended settings could have negative impacts to the performance and stability of Avaya applications on the ASP 130 server.

   a. Load balancing is set to **Inherit from vSwitch**. This will keep the configuration between both vSwitch and the VM Port Groups equivalent.
   b. Network failover detection is set to **Inherit from vSwitch**.
   c. Notify switches is set to **Inherit from vSwitch**.
   d. Failback is set to **Inherit from vSwitch**.
   e. Override failover order is set to **No** to continue the port group adherence to administration of the vSwitch assigned to this port group.



5. Click the **Save** button when finished.
6. Return to the **Networking** > **Port groups** tab and select **Management Network**.
7. Repeat the administrative process as previously documented for the VM Network port group. Both port groups must have their NIC Teaming administration configured.

ASP 130 TLS protocol configuration for vSphere 7.0 Environment

VMware ESXi 7.0 disables TLS v1.0 and TLS v1.1 by default. Only TLS 1.2 is enabled. This is true for fresh installations of 7.0 and upgrades from ESXi 6.5.

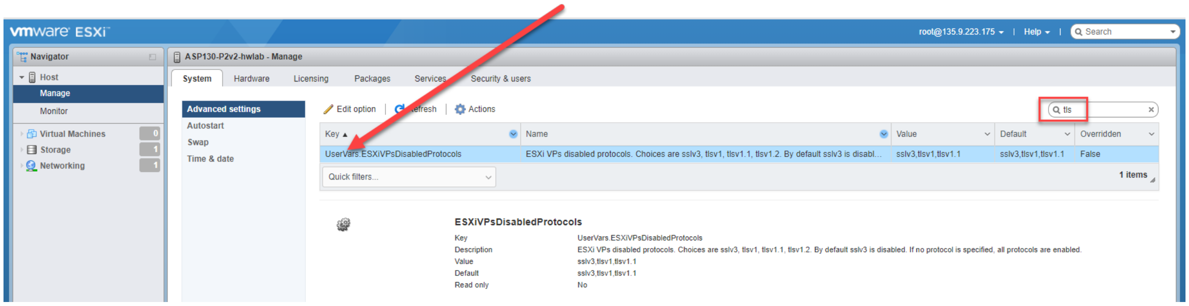
Viewing TLS settings

About this task

Use the following procedure to identify the TLS versions enabled on an ESXi Host and to modify TLS settings if required.

Procedure

1. Log into the ESXi host's Web interface.
2. Go to **Manage** > **System** > **Advanced settings**.
3. In the **search** field enter **tls** and click in the **UserVars** field. ESXi disabled Protocols will be displayed.



Chapter 13: 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.

Before deploying any virtual machines, refer to the *Policies for technical support of the Avaya Solutions Platform (ASP) 130* at https://download.avaya.com/css/public/documents/101062774.

SMGR/SDM or SDM Client is the preferred deployment method when deploying Avaya Aura® VMs.

Note:

OVA deployment using vCenter is not supported on ASP 130 servers.

Deployment of application OVA's must follow the A1S configurator host assignment and application footprint.

Related links

Deploying supported Avaya Application OVA's on an ASP 130 using the Solution Deployment Manager (SDM) on page 166
Deploying an OVA using the ESXi VMware Host Client on page 167
Setting Autostart values on VMware Host Client deployed VMs on page 171

Deploying supported Avaya Application OVA's on an ASP 130 using the Solution Deployment Manager (SDM)

The Solution Deployment Manager (SDM) is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® specific applications. There are two instances of SDM available for use, one is the System Manager Solution Deployment Manager, which is embedded into System Manager and the other is the standalone SDM client. Both instances can be used to deploy supported Application OVA's in the Avaya Solutions Platform server environment.

Note:

Only System Manager SDM can be used for applying Feature Packs, Service Packs and patches. The SDM client only supports the initial deployment of OVA's.

See the *Administering Avaya Aura® System Manager* for Release 10.1.x or 10.2.x and the *Using the Solution Deployment Manager Client* release 10.1.x or 10.2.x documents for details and procedures to configure the Solution Deployment Manager and to link the ASP 130 R640 (ESXi host) servers.

Administering Avaya Aura® System Manager

- Release 10.1.x: https://download.avaya.com/css/public/documents/101079155
- Release 10.2.x: https://download.avaya.com/css/public/documents/101087661

Using the Solution Deployment Manager client:

- Release 10.1.x: https://download.avaya.com/css/public/documents/101079109
- Release 10.2.x: https://download.avaya.com/css/public/documents/101087665

See the corresponding application deployment guides for details on deploying the applications on an ASP 130 (ESXi host) using SDM. Go to the *Deploying Avaya Aura® 'Application Name' in Virtualized Environment* documents for procedures and instructions per supported Avaya Application.

Example of ESXi OVA deployment

Note:

Application-specific deployment guides take precedence over the example deployment below.

Related links

Application Deployment on the ASP 130 on page 166

Deploying an OVA using the ESXi VMware Host Client

About this task

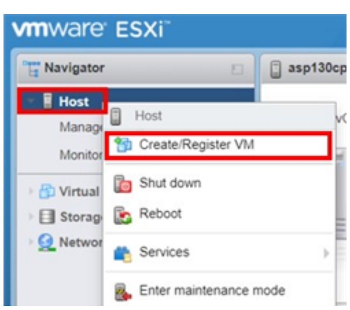
Use the following procedure to deploy a supported virtual machine on the Avaya Solutions Platform 130 series.

Before you begin

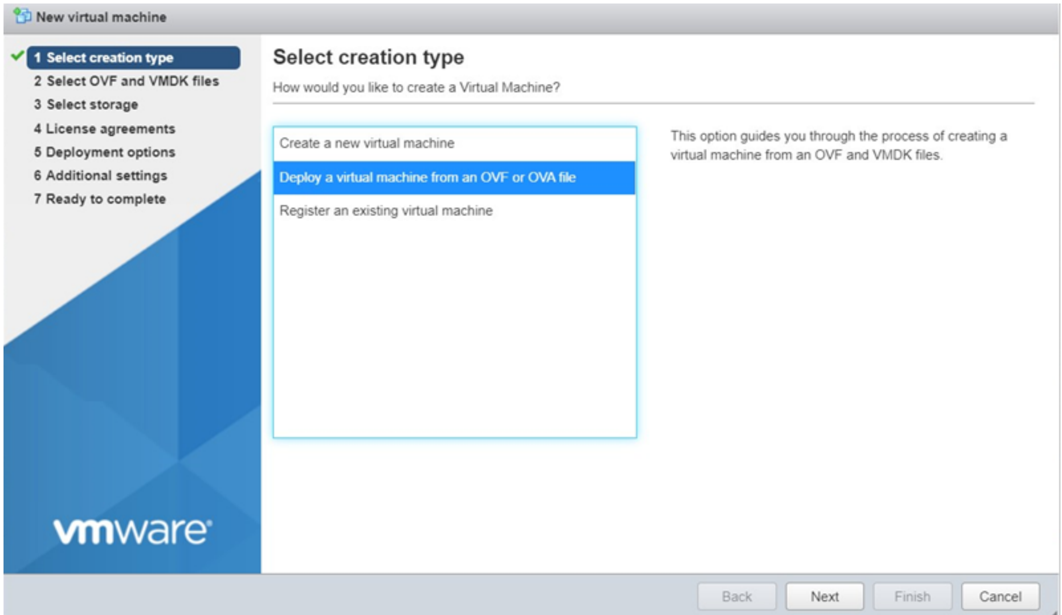
All vSwitches and port groups should be created prior to OVA deployment so that VM traffic can be supported.

Procedure

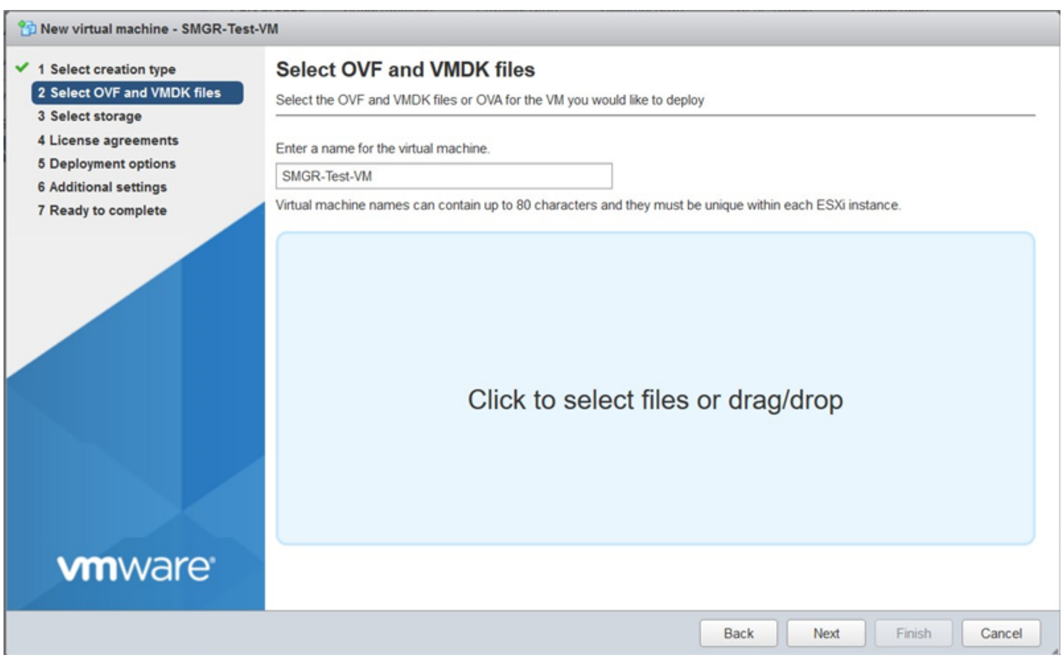
1. Login to the ESXi embedded host client with the root credentials.
2. Select and right-click **Host** > **Create/Register VM**



3. Select **Deploy a virtual machine from an OVF or OVA file**



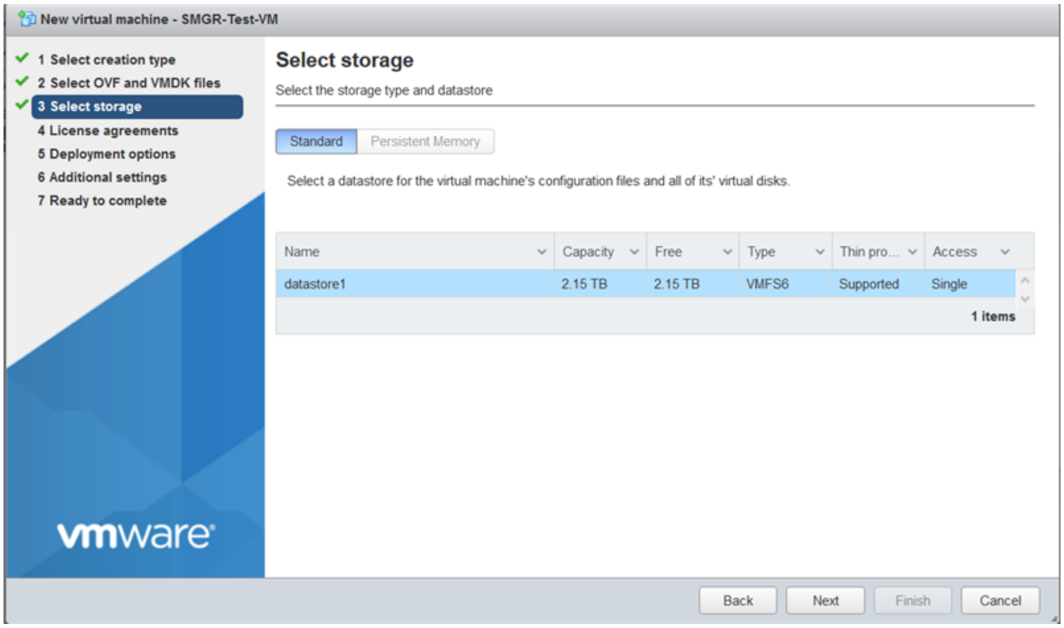
4. Click **Next**.
5. Do the following under **Select OVF and VMDK Files**:
   a. Enter the desired name for the virtual machine.
   b. Browse to and select the OVF/OVA file. Click **Open**.



6. Click **Next**.
7. Select **datastore1** for the storage.

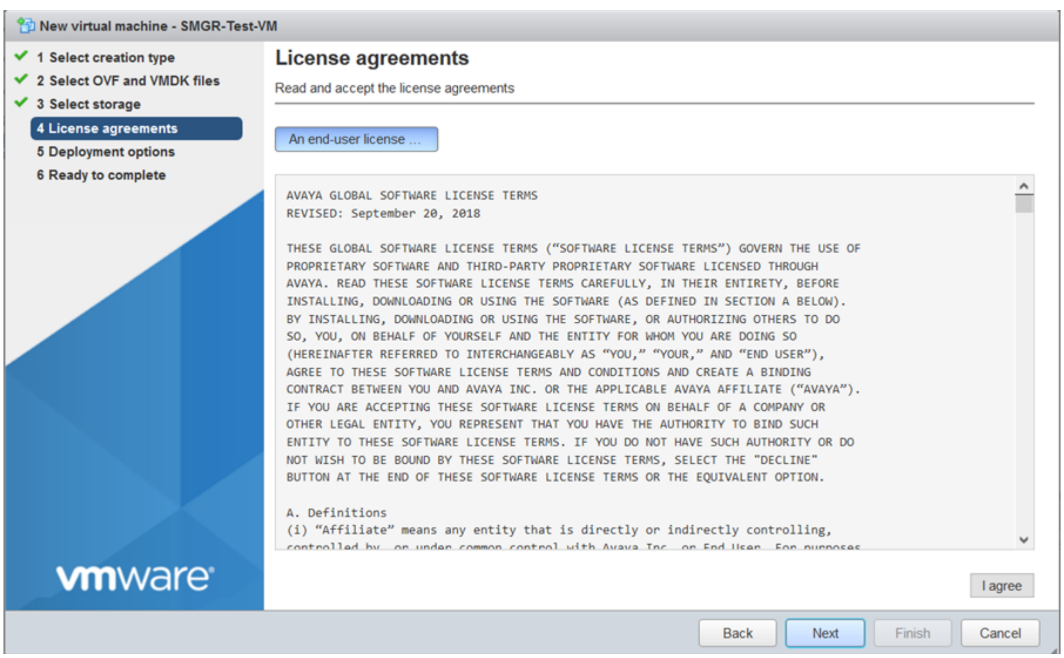
Note:

If the available VMFS volume is **server-local-disk** instead of **datastore1** it is **OK** to proceed.



8. Click **Next**.
9. Scroll down and click **I agree** to accept the License agreements.

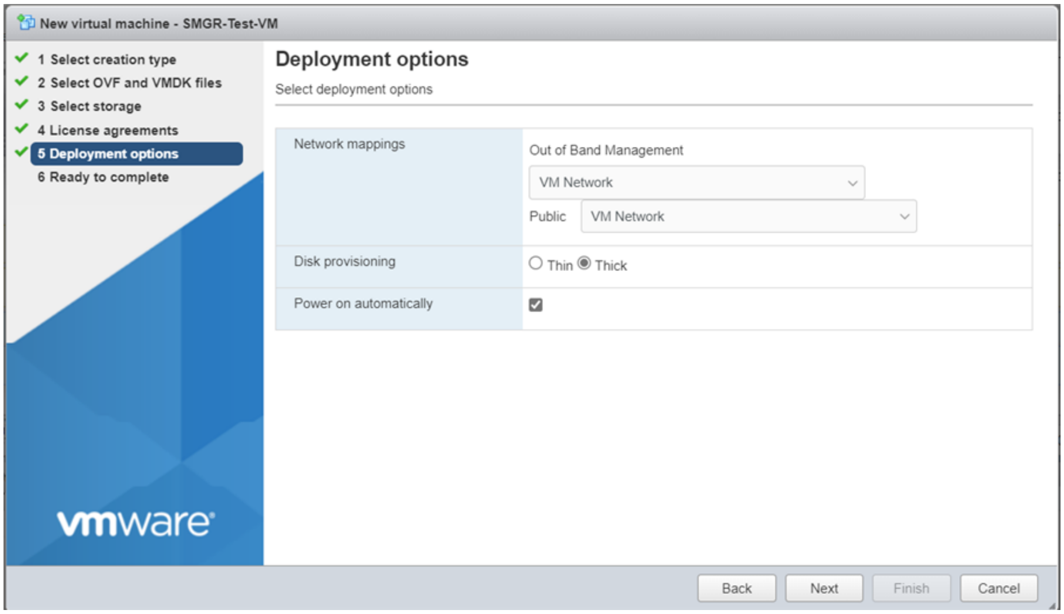
   Use the following image as an example only.



10. Click **Next**.
11. On the **Deployment options** tab select the recommended settings as supported by the Application. See the *Avaya Application documentation* as a reference. Options here will differ depending on the Application deployed, screenshot below is an example of SMGR option fields.

    Note:

    The only supported ASP 130 Disk provisioning option is **Thick**.



12. Click **Next**.
13. Additional settings:

    If additional settings appear before selecting **Next**, check specific application deployment documentation for any additional entries.

    These additional settings may not be accepted in this phase so verification should be performed after OVA deployment completion. If that is the case then these settings will need to be configured manually during first log in process.
14. Review the settings selection. Click **Finish** to deploy the OVF/OVA file.

    The progress will be displayed in the ESXi Host Client's recent tasks.
15. Refer to the Application documentation for steps to complete the configuration if required.

Related links

Application Deployment on the ASP 130 on page 166

Setting Autostart values on VMware Host Client deployed VMs

About this task

For VMs deployed using the ESXi VMware Host Client, the autostart values must be set manually or the VMs will not start automatically after a reboot of the ASP 130 ESXi host. VMs that are deployed using SDM or SDM Client have autostart configured and will start automatically after a ESXi host reboot.

Important:

A best practice is to always set autostart settings manually regardless of how the VMs are deployed.

Do the following steps to manually set Autostart values for a VM deployed using the VMware Host Client:

Procedure

1. Go to **Navigator** > **Manage** > **System**.
2. Click **Autostart**.

   The system default settings are set to the following values. **Do not change these values**:

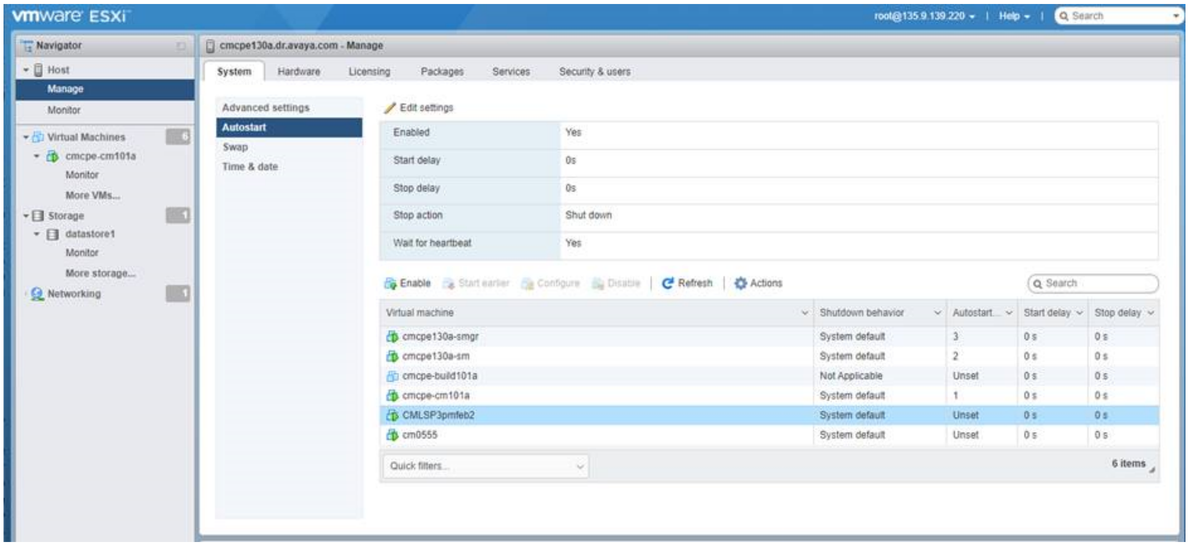
   - Enabled = Yes
   - Start delay = 0s
   - Stop delay = 0s
   - Stop action = Shut down
   - Wait for heartbeat = Yes
3. Navigate to the table below that lists the virtual machines.

   To change **Autostart** values of a VM, change values of **Shutdown behavior** and **Autostart** for the appropriate VM listed in this table.

   Note:

   For a VM by default, the **Shutdown behavior** displays **Not Applicable** and the **Autostart** displays **Unset**.
4. Right click on the VM.
5. Select **Autostart** on the pop-up window and click **Enable**.

   This selection resets the **Shutdown behavior** setting to **System default** and populates a startup order setting in the **Autostart** column.
6. After **Autostart** is enabled for the VMs, select **Autostart** on the pop-up window to change the startup order. The startup order is initially set to the order in which autostart is enabled on the virtual machines.



Select **Start earlier** or **Start later** option for a VM as required.

Related links

Application Deployment on the ASP 130 on page 166

Chapter 14: ASP 130 Host Configuration Backup and Restore

Backing up the VMware ESXi Configuration

About this task

Note:

This procedure assumes that *no DHCP* was used for assigning IP addresses to the ASP 130 host, that it is still in the same configuration originally deployed and shipped by Avaya.

You need to have a current backup of the VMware ESXi host configuration data in case a server fails and needs to be replaced. Use the procedure in this section to back up the VMware ESXi host configuration using the ESXi command line.

Note:

For additional information and procedures, see VMware Knowledge Base article 2042141: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042141.

The following is a list of some of the key ESXi items and configurations that are backed up during the procedure:

- ESXi host details (Hostname, IP address, FQDN, domain)
- Network configurations (vSwitches, VMkernel's, Port groups, NIC teaming, tagging)
- Certificates (self-signed and third-party)
- Licensing
- Enabled services (SSH, Shell)
- User accounts and credentials for access (DCUI, root, custom accounts)
- List of VM's configured for AutoStart
- Logs and log file directory locations
- The /etc/hosts file contents
- TLS/SSL protocols enabled/disabled

Procedure

1. Log in to the ESXi host by using a Secure Shell (SSH) client e.g., PuTTY.
2. Authenticate using the existing *root* credentials or *sroot* EASG if enabled.

3. Use the command **`vim-cmd hostsvc/firmware/backup_config`** to back up the ESXi host configuration.

   A URL will be displayed in the command line similar to the following example:

   `http://*/downloads/52c08d7e-3f2a-6156ec7c-8f9cb8f77911/configBundle-esxi1.sv.avaya.com.tgz`

4. Copy and paste the URL into a browser and in place of the `*` in the URL enter the ESXi host IP or FQDN. Press **Enter**.

   Example:

   `http://<IP address or FQDN of ESXi host>/downloads/52c08d7e-3f2a-6156ec7c- 8f9cb8f77911/configBundle-esxi1.sv.avaya.com.tgz`

   Note:

   The backup will automatically be downloaded to the local laptop as soon as you press **enter**.

Restoring the VMware ESXi Configuration

About this task

Use the procedures in this section to restore ESXi host configuration in case of server failure or replacement through the ESXi command line.

Note:

When restoring configuration data, the build number of the ESXi host must match the build number of the host backup file and UUID (can be obtained using the command "**`esxcfg-info -u`**") of the host should match the UUID of the host on backup file.

For additional information and procedures, see VMware Knowledge Base article 2042141:

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042141.

Before you begin

- The ESXi host network settings will be required to be configured first in order to access the ESXi host to run the restore procedure. See Configuring ESXi Network Settings on page 38.
- Enable SSH access on the ESXi host. See steps 19 to 22 under Configuring ESXi Network Settings on page 38.
- The `configBundle-HostFQDN.tgz` backup file should be renamed as `configBundle.tgz` before initiating the restore command. If not changed the restore command will fail.

Procedure

1. Connect to the ESXi host using SSH with PuTTY.
2. Log in using the local administrative credentials.
3. Use the command `vim-cmd hostsvc/maintenance_mode_enter` to put the host into Maintenance Mode.
4. Use WinSCP to copy the backup configuration file to the `/tmp` directory on the host.

   Important:

   Using the command in the next step reboots the host after completion. You will not be warned or asked to defer the reboot.
5. Use the command `vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz` to restore the configuration.
6. The server will automatically reboot to restore the ESXi configuration from the backup after command completion.
7. Once the server is back online, if not done automatically, use the command `vim-cmd hostsvc/maintenance_mode_exit` to exit the host from Maintenance Mode.

   All configuration data including the vSwitches/VMkernels/Licensing is restored.

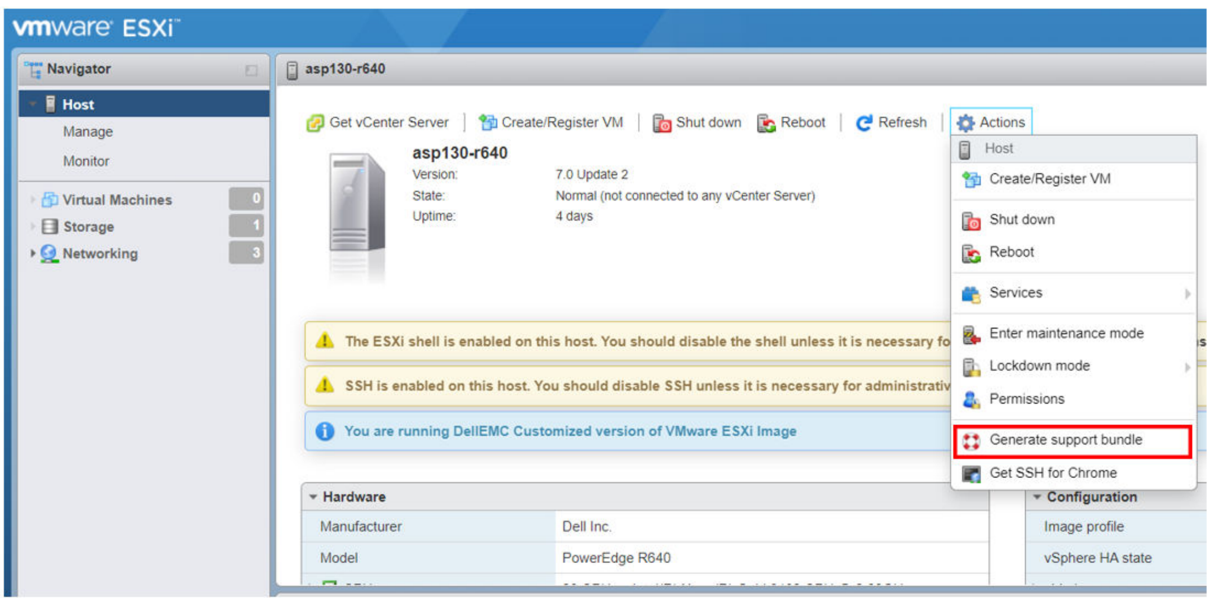
Chapter 15: Log and File Collection to Aid in Troubleshooting

Collecting the VMware Support Bundle

About this task

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 support bundle logs so that the information related to the incident timeframe is not lost in log rotation.

- Option 1: through web interface
  1. From the vSphere Navigator menu, select **Host**.
  2. From the Host options, select **Actions**.
  3. From the Actions drop-down menu, select **Generate support bundle**:



- Option 2: via CLI
  1. Using an SSH session, log in to the ESXi host using the **`root`** credentials.
  2. From the command line, type `vm-support`.

     The log file construction will commence.

```
[root@asp130-r640:~] vm-support
/bin/vm-support v4.1: 15:01:40, action threads 4
15:01:40: Gathering output from /usr/lib/vmware/vm-support/bin/encryption-prolog
15:01:40: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa get-metrics
15:01:40: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa get-status
15:01:40: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa trace-info
15:01:40: Gathering output from vmware -vl
15:01:40: Gathering output from /usr/sbin/localcli system version get --alternat
15:01:40: Gathering output from /sbin/vsi_traverse -s
15:01:40: Gathering output from /usr/sbin/localcli system coredump partition get
15:01:41: Gathering output from /sbin/vsi_traverse -s
15:01:41: Gathering output from /usr/sbin/localcli system coredump partition lis
15:01:41: Gathering output from /usr/sbin/esxcfg-info -a |
15:01:42: Gathering output from /usr/sbin/localcli --plugin-dir /usr/lib/vmware/
15:01:42: Gathering output from /usr/sbin/esxcfg-info -a -F xml -
15:01:47: Gathering output from /bin/localcli hardware ipmi sel get -p -i -n all
15:01:47: Gathering output from /sbin/vsi_traverse -s \
15:01:47: Gathering output from /bin/localcli hardware ipmi sel list -p -i -n al
15:01:47: Gathering output from /sbin/vsi_traverse -s -l 0 /
15:01:48: Gathering output from /bin/localcli hardware ipmi sdr get -p -i -n all
15:01:48: Gathering output from /sbin/vsi_traverse -s -l 0 -
15:02:02: Gathering output from /bin/localcli hardware ipmi sdr list -p -i -n al
15:02:02: Gathering output from /sbin/vsi_traverse -s -l 0 /
```

When completed, ESXi will report `Done` and will provide the location of the support bundle file.

```
15:04:12: Gathering output from /bin/cat /var/log/vvold.log
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/spherelet
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/hostd.0.g
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/hostd.log
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/vmkernel.
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/vmkernel.
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/vmkernel.
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/vmkwarnin
15:04:12: Adding /vmfs/volumes/60d0f953-40b16dc2-2828-e4434b6981cc/log/vpxa.0.gz
15:04:12: Gathering output from /sbin/localcli --formatter=json storage nfs list
15:04:12: Gathering output from /usr/lib/vmware/vm-support/bin/encryption-epilog
15:04:12: Done.

Non-fatal errors encountered during the run:
   Cmd "localcli software baseimage get" failed with exit code 1
Please attach this file when submitting an incident report.
To file a support incident, go to http://www.vmware.com/support/sr/sr_login.jsp
To see the files collected, check '/vmfs/volumes/60cccb07-ea586794-0dce-e4434b69
81cc/esx-asp130-r640-2021-06-28--15.01-2151824.tgz'
```

3. Note the ESXi host IP or FQDN, the bundle file name and time the file was created for Avaya services team member(s). A screen capture like the one below provides all that is needed:

```
[root@asp130-r640:/vmfs/volumes/60cccb07-ea586794-0dce-e4434b6981cc] ls -l
total 47160
-rwxr-xr-x    1 root     root          1901 Jun 17 20:30 ACP130srvprt-cfg.sh
-rwxr-xr-x    1 root     root          1791 Jun 24 17:01 ASP130-vswitch2-5-cfg-v1.sh
-rwxr-xr-x    1 root     root          2645 Jun 21 17:45 ASP130srvprt-cfg-v2.sh
drwxr-xr-x    1 root     root           420 Jun 18 17:34 VMware-VMvisor-Installer-7.0.0.update02-17867351
-rw-r--r--    1 root     root      47405661 Jun 28 15:04 esx-asp130-r640-2021-06-28--15.01-2151824.tgz
-rw-r--r--    1 root     root          1403 Jun 22 18:10 rui.crt
-r--------    1 root     root          1704 Jun 22 18:10 rui.key
d-w-r-xr-T    1 root     root           420 Jun 18 16:45 vmkdump
```

4. Use SCP to copy the file from the ESXi host to a local machine.

   Note:

   Customers and Business Partners should not contact VMware for support. All support for the underlying hypervisor/ESXi on the ASP 130 must be through Avaya.

Collecting an iDRAC Support Assist file

About this task

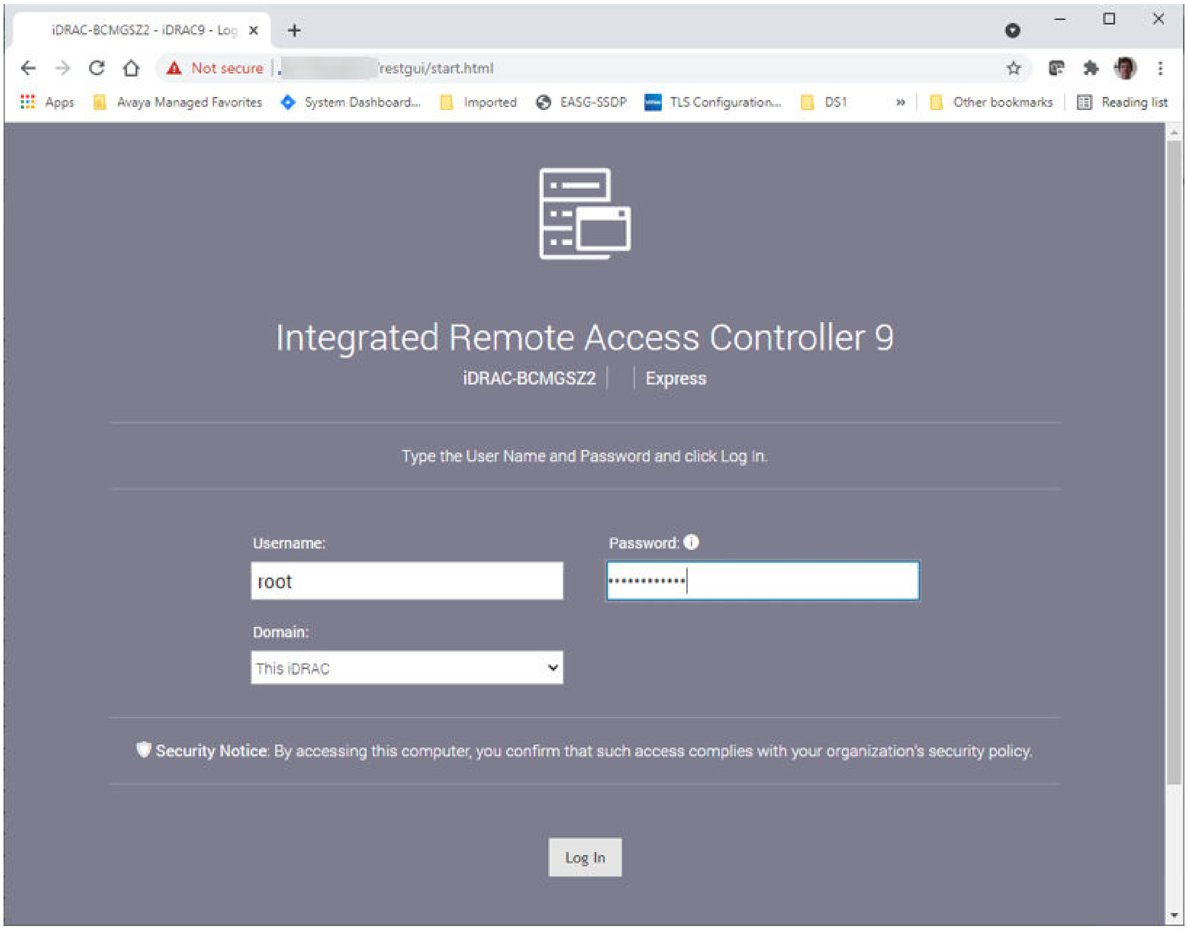
When there is an issue with the ASP 130 server a Support Assist file may need to be generated for debugging purposes. When opening a service request with Avaya this file may be required.

Before you begin

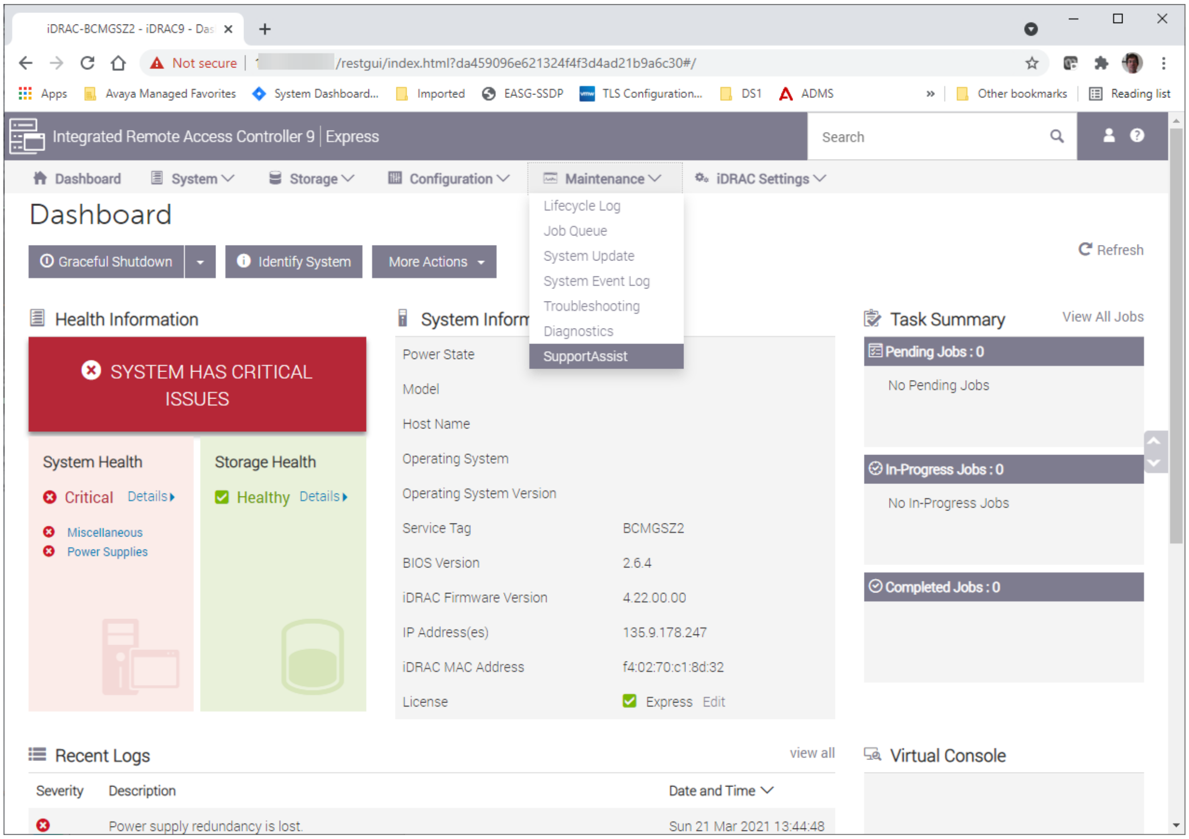
- iDRAC should be enabled and network settings configured accordingly.
- iDRAC should be reachable over the customer's network or an on-site resource available for direct connect to the iDRAC.

Procedure

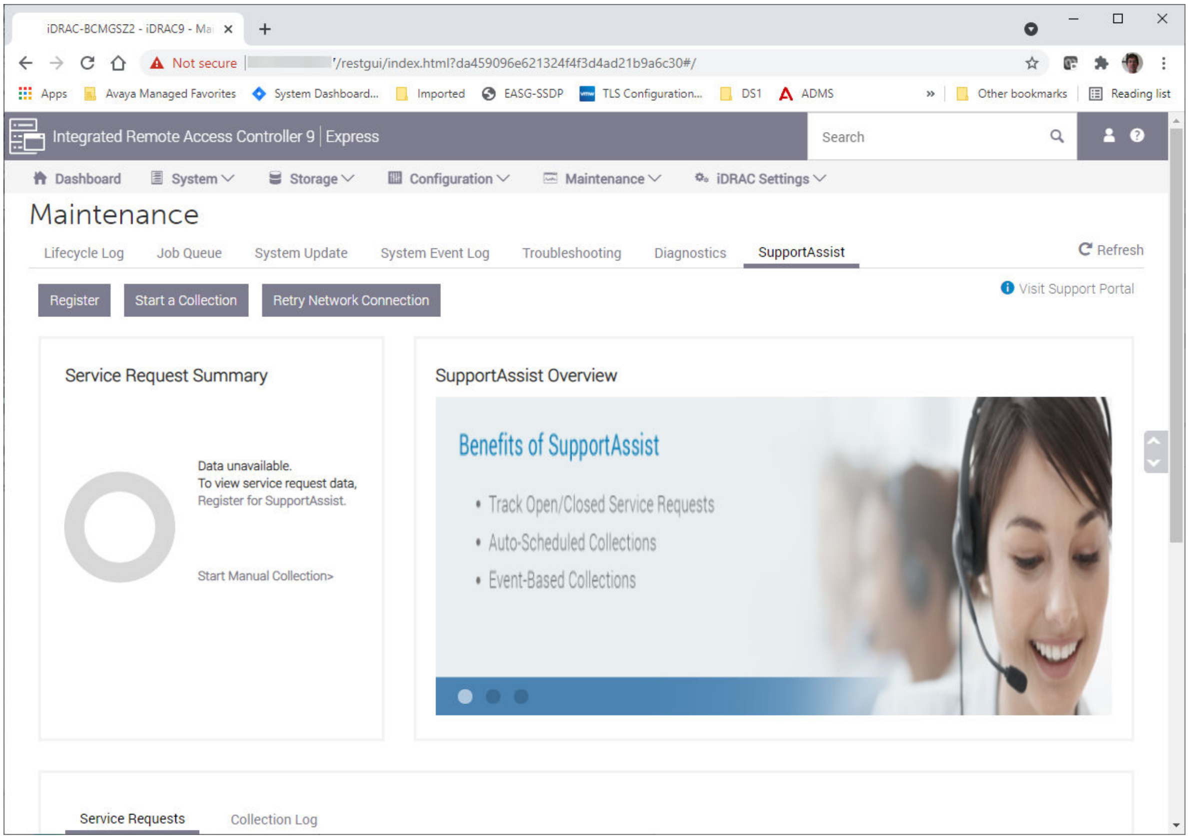
1. Open a browser and login to the iDRAC web interface using the `root` or equivalent account:



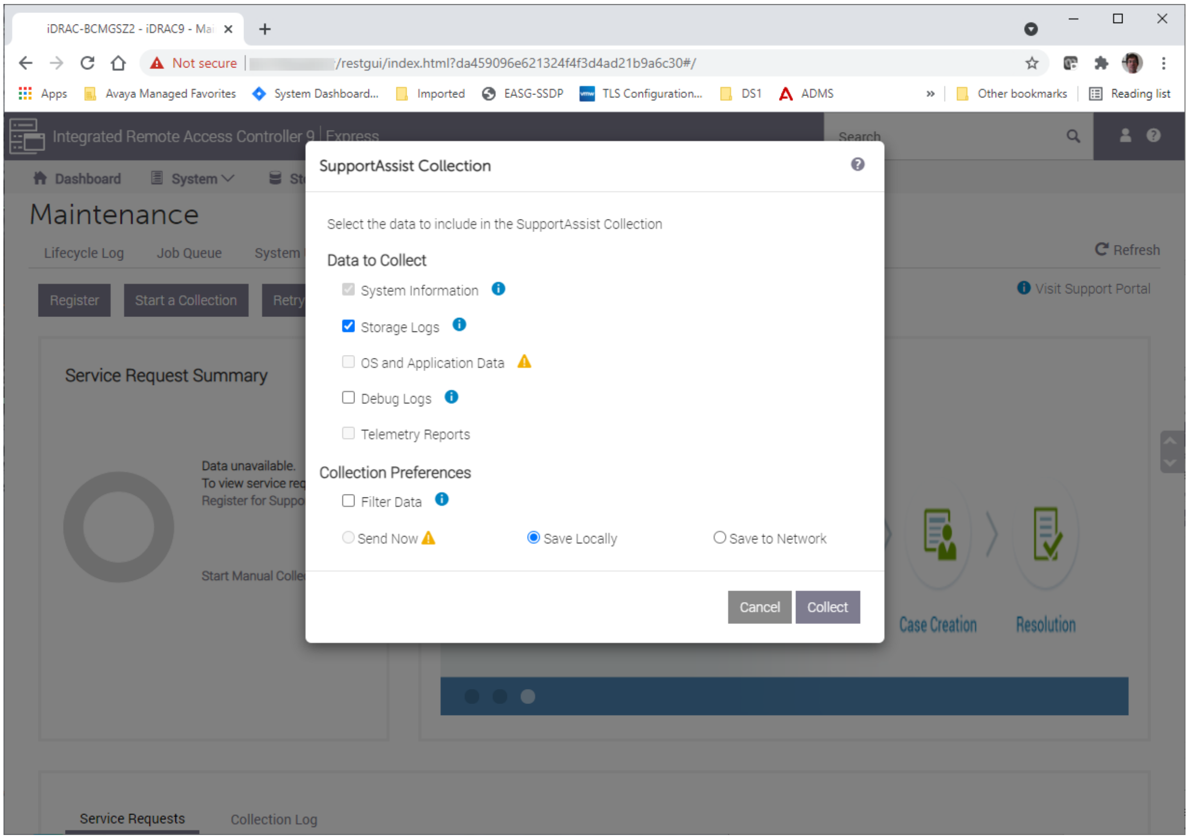
2. Select **Maintenance** > **SupportAssist** from the main screen:



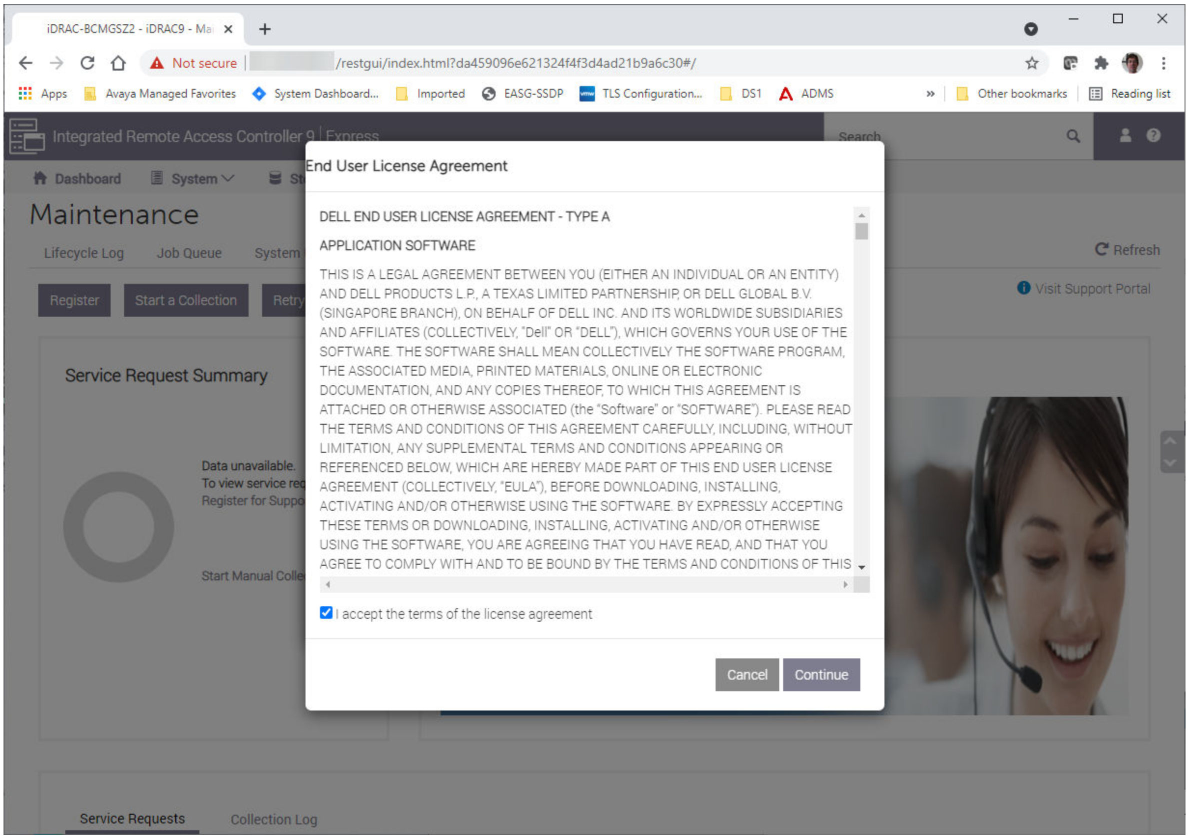
3. In the **SupportAssist** screen, select **Start a Collection**:



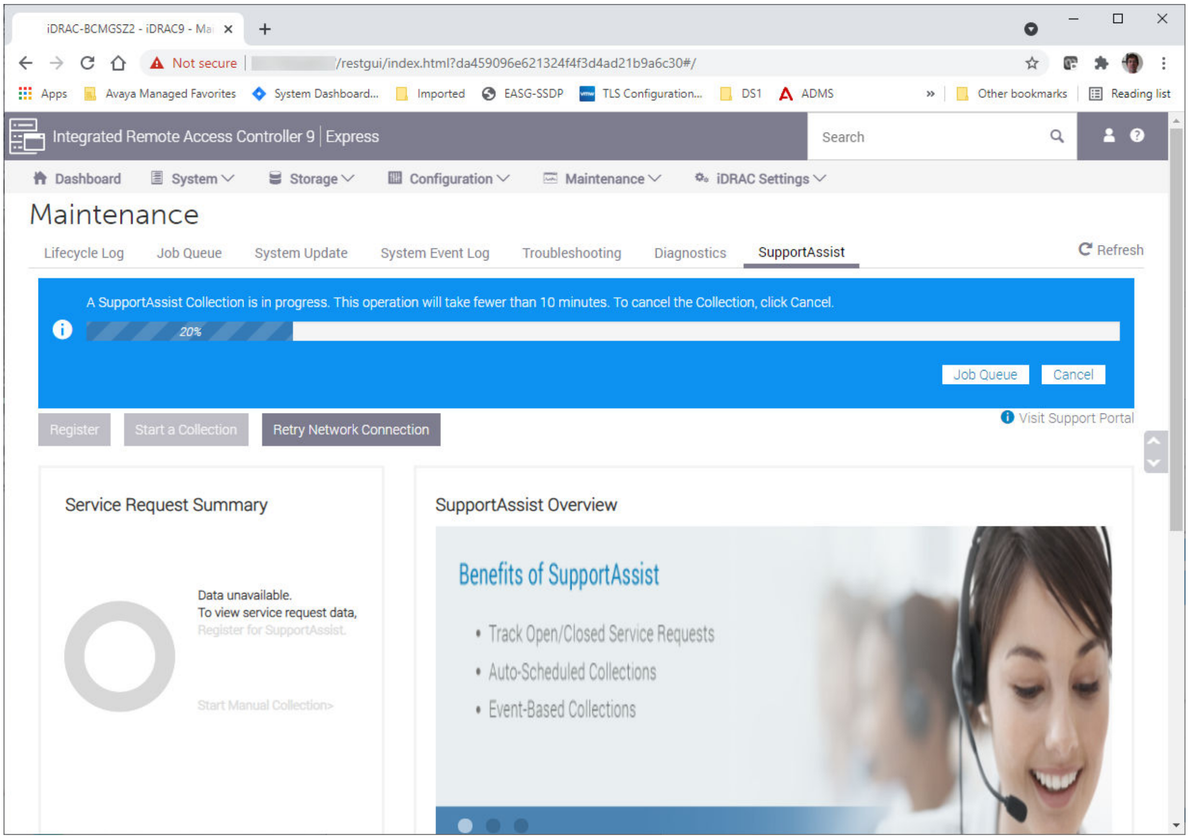
4. In the Collection pop-up, keep the defaults of **System Information** and **Storage Logs** and save locally unless instructed otherwise by Avaya support. Then click on the **Collect** button.



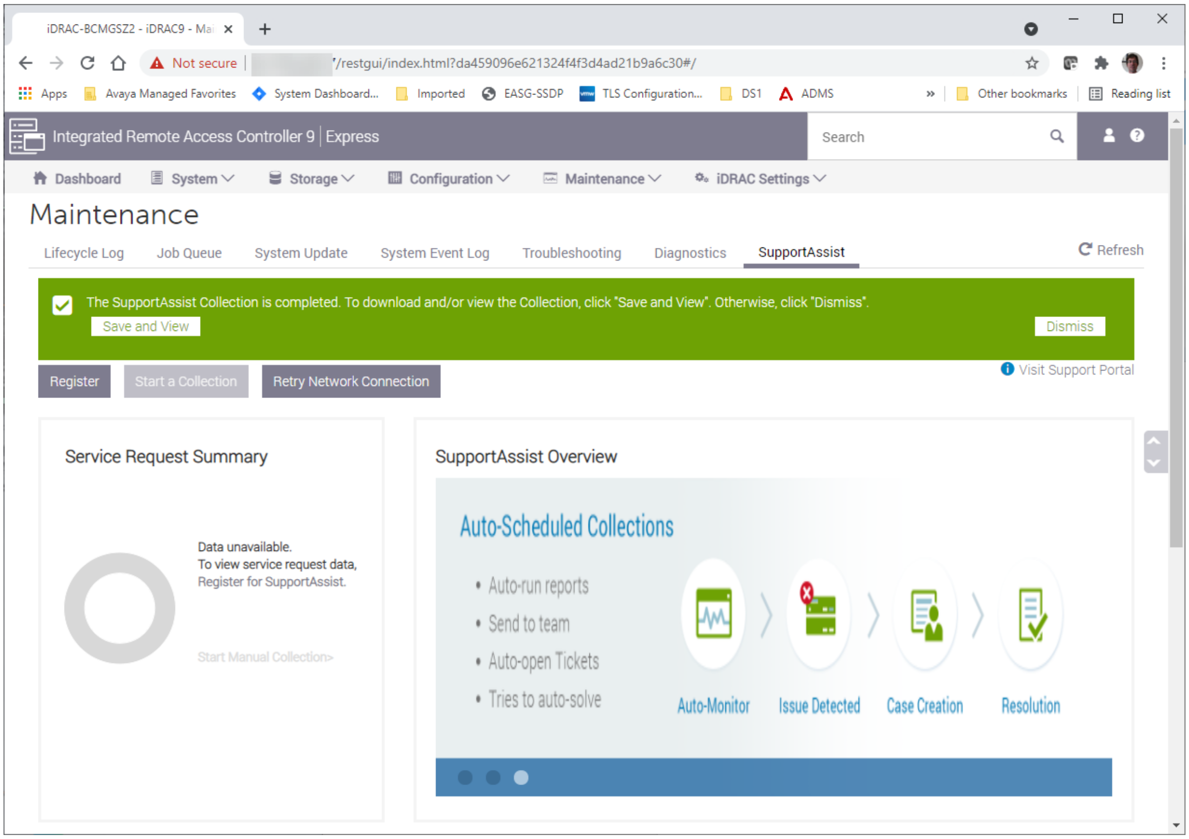
5. Accept the terms of the License Agreement and click **Continue**:



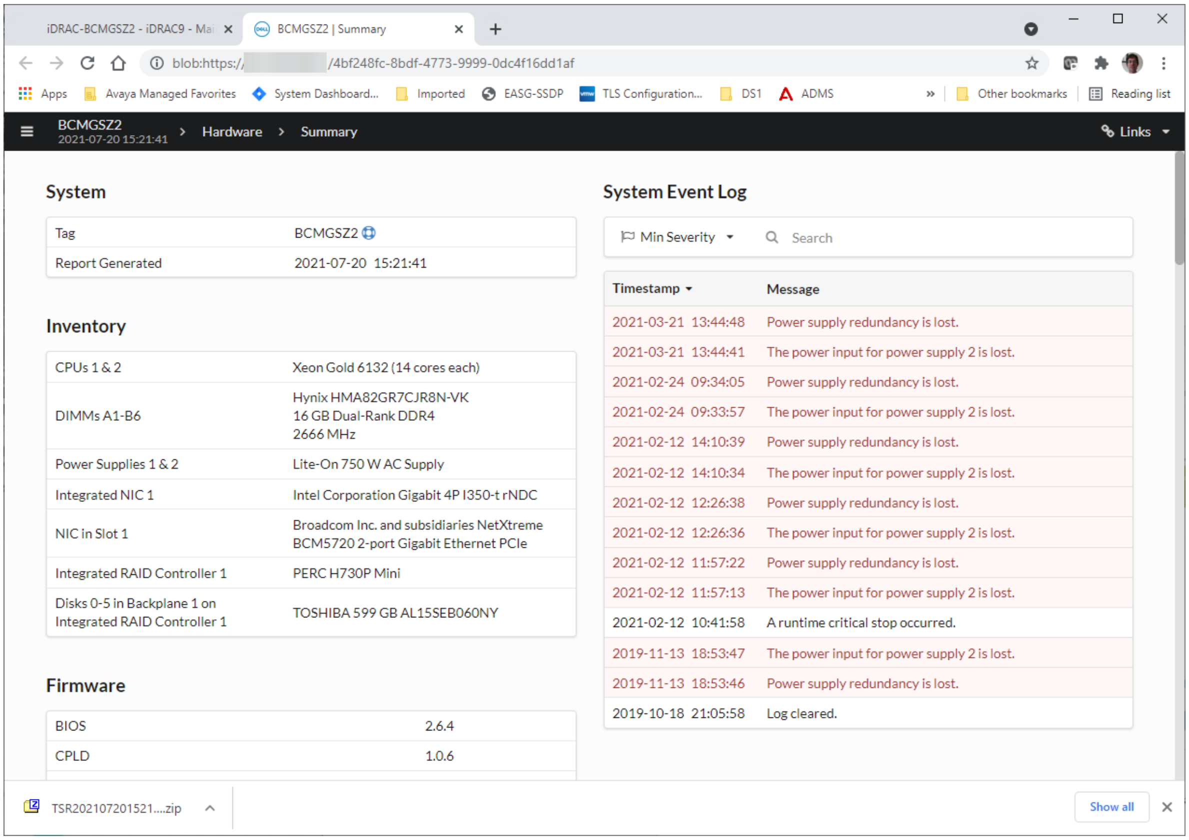
6. This will start the collection and show the progress of the data collection:



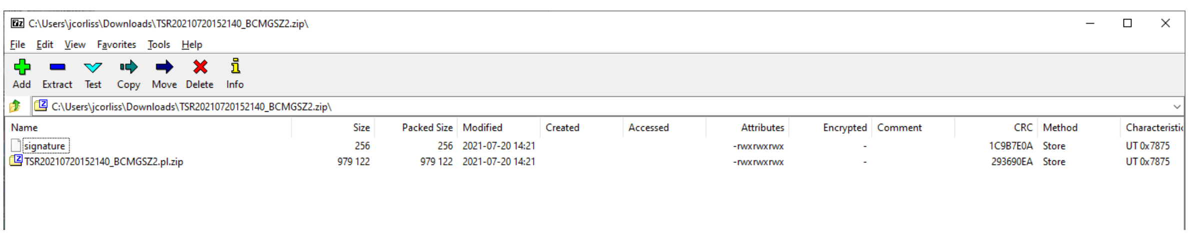
7. When completed you can save the file to your PC – select **Save and View**:



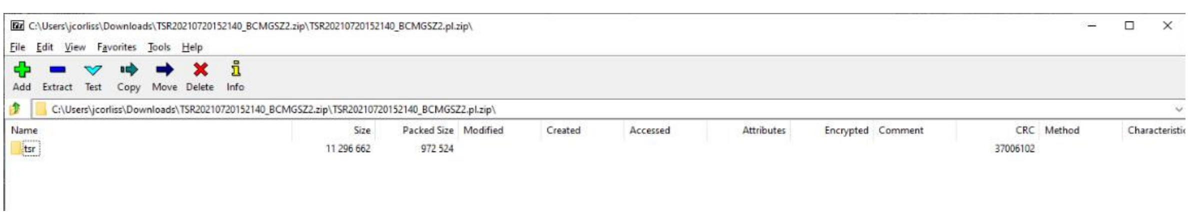
8. This will open a new tab and allow you view the data in a GUI format. It will also download a .zip file of the same information for later viewing:



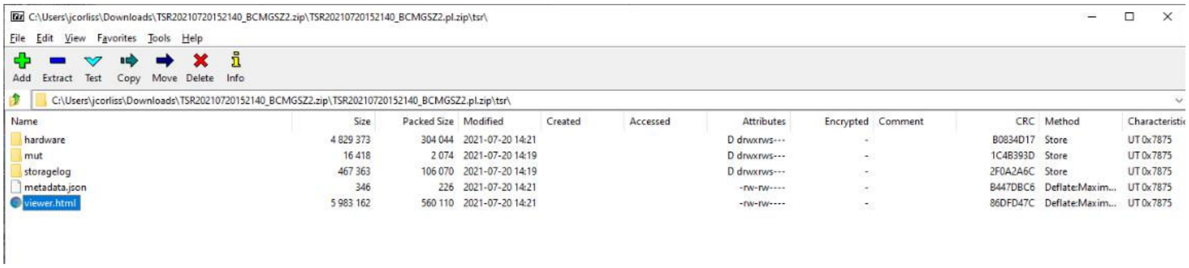
9. To view the same data at a later time from the zip file open the zip file in an archive manager such as 7z:



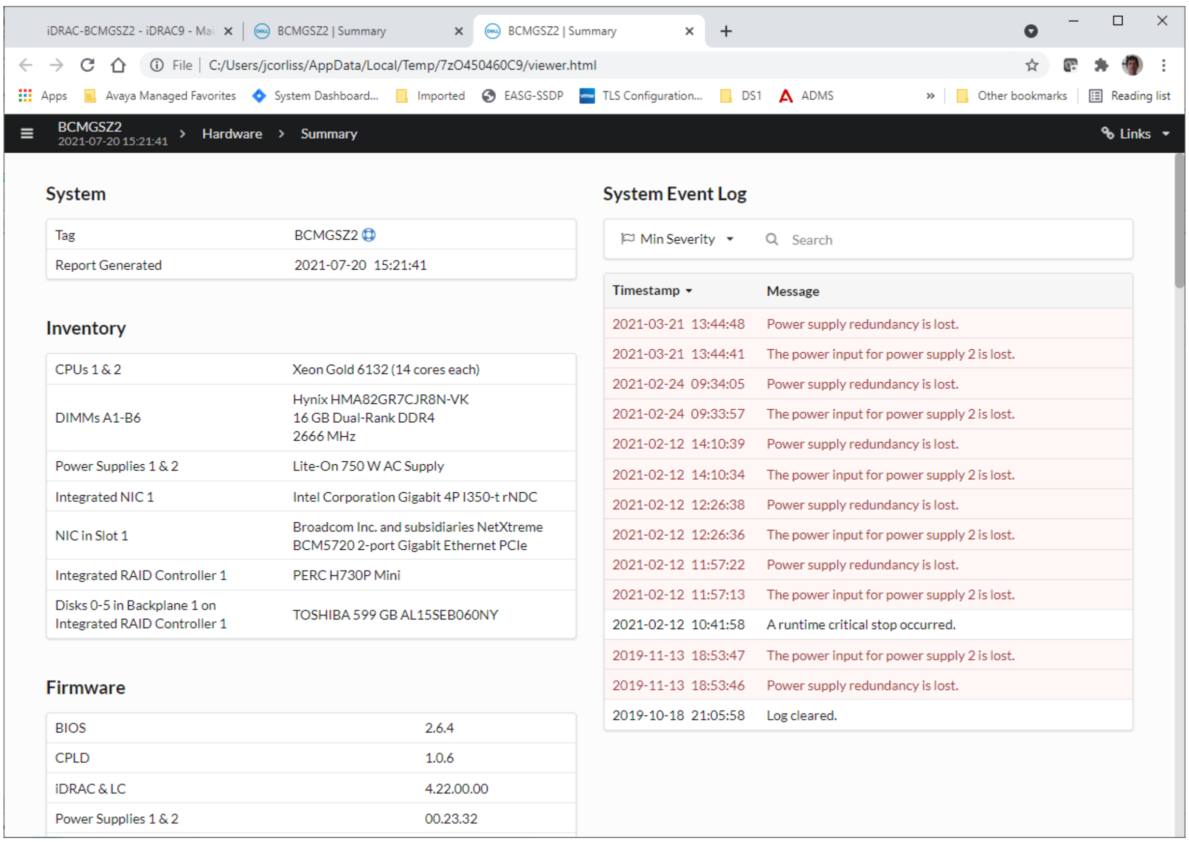
10. In the archive manager, click on the embedded zip file to extract that data. This will present a folder named **tsr**:



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 16: Regulatory Information

Regulatory Information

For a complete listing of the DELL PowerEdge R640 regulatory information, navigate to 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 17: 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
Avaya Solutions Platform 130 Series - Updating to R5.1.0.5 (ESXi 7.0 U3q) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.5.0 release from earlier ASP 130 5.1.x releases.
Avaya Solutions Platform 130 Series - Updating to R5.1.0.4 (ESXi 7.0 U3p) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.4.0 release from earlier ASP 130 5.1.x releases.
Avaya Solutions Platform 130 Series - Updating to R5.1.0.3.0 (ESXi 7.0 U3o) from R5.1.x (ESXi 7.0 U3x)	Describes procedure to perform upgrade to ASP 130 5.1.0.3.0 release from earlier ASP 130 5.1.x releases.
Upgrading to R5.1.0.2 (ESXi 7.0 U3i) from R4.x (ESXi 6.5.x) or R5.x (ESXi 7.0.x)	Describes procedure to perform upgrade to ASP 130 5.1.0.2.0 release from earlier ASP 130 5.1.x or 4.x releases.
Upgrading to R5.1.0.1.0 (ESXi 7.0 U3d) from R4.x (ESXi 6.5.x) or R5.x (ESXi 7.0.x)	Describes procedure to perform upgrade to ASP 130 5.1.0.1.0 release from ASP 130 5.1.x or 4.x releases.
Installing the Avaya Solutions Platform 130 Series 5.1.x	Describes how to install Avaya Solutions Platform 130 Series 5.1.x.
Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series 5.1.x	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series 5.1.x.
Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300	Describes how to install, maintain, and troubleshoot Avaya Solutions Platform S8300.
Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.1	Describes procedure to migrate from AVP to latest ASP 130 R5.x release.
Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300	Describes migration procedure from AVP to Avaya Solutions Platform S8300.

Table continues…

Title	Description
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes the best practices of using Integrated Dell Remote Access Controller (iDRAC).
PSN027109u - Avaya Solutions Platform 100 series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 14.0	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update. For reference, search the Avaya support web site for: *Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update* and select the latest version of the PSN.
PCN2146S Avaya Solutions Platform 130 5.1.x	This is a Product Correction Notice about the availability of ASP 130 R5.1.x and Avaya's Customized Image of VMware ESXi 7.0.
Avaya Solutions Platform 130 5.1.x_Release_Notes	Release Notes.
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 R4.x, R5.x and ASP S8300 R5.1	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 based on supported and tested configurations.

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

V

W