



Installing the Avaya Solutions Platform 130 Series

Release 4.0
Issue 8
June 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

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

Licenses

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

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

License types

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	7
Purpose	7
Change history	7
Chapter 2: Overview	9
Avaya Solutions Platform overview	9
Key features	9
Supported software	10
Dell server overview	10
Front view of Dell™ PowerEdge™ R640 Server	11
Back view of Dell™ PowerEdge™ R640 Server	12
Avaya Solutions Platform Appliance profiles	13
Dell PowerEdge R640 server dimensions	14
Environmental requirements	15
Power requirements	17
Chapter 3: Registration	18
Overview	18
HealthCheck tool registration process	18
Registering a new device	19
Viewing the status of your registration request	21
Technical Onboarding Process	22
Chapter 4: Installation	23
Installation checklist	23
Electrostatic discharge	23
Package contents	24
Installing the server	25
Attaching cables	29
Connecting power	30
Chapter 5: Configuration	33
Purpose	33
Dell R640 XL ESXi Configuration	33
Overview	33
Configuring ESXi Network Settings	33
Configuring autostart on ESXi host using Embedded Host Client	46
Configuring SNMP v2c on an ESXi 6.5 host	47
Configuring SNMP v3 on an ESXi 6.5 host	50
Services Port Configuration	53
Management of the TLS protocol configuration for vSphere 6.5 U2 Environment	59
Performing server recovery or software remastering	65
Replacing the host server	71

Adding the license key for server recovery or software remastering.....	72
Dell USB R640 RAID Configuration.....	73
Introduction.....	73
Preparing to configure Dell R640 RAID controller.....	73
Configuring the controller properties.....	76
Creating a virtual disk.....	78
Virtual disk size.....	81
Checking information about the virtual disk.....	82
Dell R640 SNMP trap configuration using iDRAC9.....	83
SNMP alerts.....	83
Configuring SNMP v2c alerts using iDRAC9.....	83
Configuring SNMP v2c traps for Dell R640using iDRAC9.....	86
Configuring SNMP v3 traps for Dell R640 using iDRAC9.....	87
Configuring a user account for SNMP v3 traps.....	92
Chapter 6: Configuration Guidelines.....	94
Preface.....	94
Configuring Core Network Administration.....	95
Default Configuration.....	95
vSwitch Administration.....	95
Configure the Port Groups.....	96
VMkernel NIC Administration.....	97
Application Deployment on the ACP 130.....	98
ACP 130 VLAN Tagging.....	98
ACP 130 NIC Teaming.....	99
Configure ESXi Management Interfaces in the Server for NIC Teaming.....	99
Administer NIC Teaming in ESXi vSphere client.....	103
vSwitch NIC Teaming Administration.....	104
Port Group NIC Teaming Administration.....	106
ACP 130 Host Configuration Backup and Restore.....	108
Backing up the VMware ESXi Configuration.....	108
Restoring the VMware ESXi Configuration.....	108
Log and File Collection to Aid in Troubleshooting.....	109
Collecting the VMware Support Bundle.....	109
Chapter 7: Regulatory information.....	112
Regulatory information.....	112
Chapter 8: Resources.....	113
Documentation.....	113
Finding documents on the Avaya Support website.....	114
Avaya Documentation Center navigation.....	114
Viewing Avaya Mentor videos.....	115
Support.....	116

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
8	June 2021	Added the new “Registration” chapter that includes the information of HealthCheck Tool.
7	November 2020	Updated the following topics: <ul style="list-style-type: none">• “Configuring autostart on ESXi host using Embedded Host Client”• “Application Deployment on the ACP 130”
6	October 2020	Updated the Back view of Dell™ PowerEdge™ R640 Server topic.
5	May 2020	Added a new Chapter Configuration Guidelines, and updated the following topics: <ul style="list-style-type: none">• Configuring SNMP v2c on an ESXi 6DOT5 Host• Configuring SNMP v3 on an ESXi 6DOT5 Host• Configuring SNMP v2c alerts using iDRAC9• Configuring SNMP v2c traps for Dell R640 using iDRAC9• Configuring SNMP v3 traps for Dell R640 using iDRAC9
4	October 2019	Updated the Chapter Configuration to include the installation of ESXi from an ISO for Server Recovery or Remaster of the software.
3	February 2019	Added a new Chapter Configuration.

Table continues...

Issue	Date	Summary of changes
2	January 2019	Added a new Avaya Converged Platform Appliance profiles section.
1	August 2018	Initial release.

Chapter 2: Overview

Avaya Solutions Platform overview

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

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

1. ASP 110: This is a bare metal server used by a few applications. The applications determine if the Operating System (OS) is preloaded at Avnet.
2. ASP 120: This is the Dell R640 shipped from Avnet with Avaya Virtualized Platform preloaded. The ASP 120 is synonymous with AVP. AVP 7.1.3.3 or greater, or AVP 8.0.1 or greater is required.
3. ASP 130: This is the Dell R640 shipped from Avnet with ESXi 6.5 preloaded and with a standard VMware license.

 Note:

On the Avaya Solutions Platform 130 Appliance, VMware Vsphere 6.5 Standard is loaded and the license key is installed.

The license key label is located on the lid of the Avaya Solutions Platform 130 Appliance server.

Key features

The Avaya Dell PowerEdge R640 is the underlying server hardware for the Avaya Solutions Platform 100 series. The PowerEdge R640 is a single/dual socket CPU implementation and 1U 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 will be used as the base platform for all new Avaya offers. The architecture of the R640 is designed to maximize performance and provide flexibility to optimize configurations based on Avaya's applications and customer use cases.

Supported software

The Avaya Solutions Platform 100 series is a hardware platform designed to support many different software solutions. For more information about supported software, consult the individual Avaya solution documentation.

The Avaya Solutions Platform 130 Appliance supports virtualization. The Avaya Solutions Platform 130 Appliance uses VMware vSphere ESXi as the hypervisor.

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 book 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.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third party OEM servers forming part of Avaya's turnkey appliance offers from any source except the Avaya support site. Only consult 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 to this is when an application has provided an upgrade or migration path from an existing server state to a different server state with the appropriate kits, tools, documentation, and training materials.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third party OEM servers forming part of Avaya's turnkey appliance offers from any source except the Avaya support site. Only consult Avaya provided downloads, information and support. All BIOS or firmware updates are provided through Avaya. Go to the Avaya Support website at <http://support.avaya.com> for additional information.
- Avaya Solutions Platform 130 servers must not be updated with BIOS or firmware updates from the vendor's website. Only Avaya provided BIOS/Firmware updates can be used. Updating directly from the vendor's website will result in an unsupported configuration. BIOS/Firmware updates are made available on <http://plds.avaya.com> and are customer installable.
- 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. Note that the OEM server vendor (in this case Dell) provides Avaya with their latest certified package of the ESXi software. This ensures that any updates will be compatible with the underlying hardware, drivers, etc. Once 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 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, brown outs, black outs etc. when the server is connected to standard power mains and has no protection.
- Dell's RAID battery is a consumable item that can be purchased as a part without a Service ticket. Customers are responsible for installing them, the procedure for which is in the Maintaining and troubleshooting document or in appropriate OEM vendor documentation.
- Quality assurance - product integrity testing or environmental international restrictions/ has 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

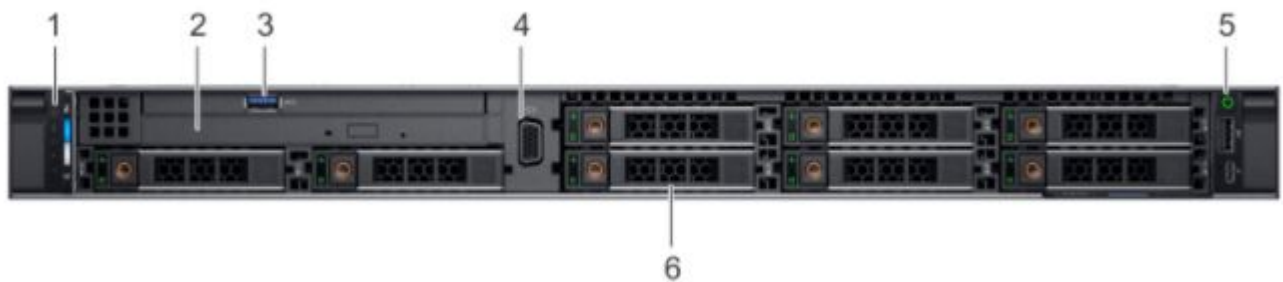


Figure 1: Front view of Dell PowerEdge R640 server

No.	Item	Icon	Description
1	Left control panel	NA	Displays the system health, system ID, and status LED indicators. <ul style="list-style-type: none"> • 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 you to connect a display device to 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	Enable you to install hard drives that are supported on your system.

Back view of Dell™ PowerEdge™ R640 Server

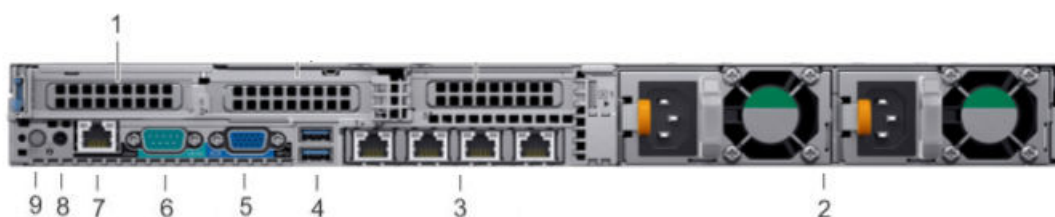


Figure 2: Back view of Dell PowerEdge R640 single CPU server

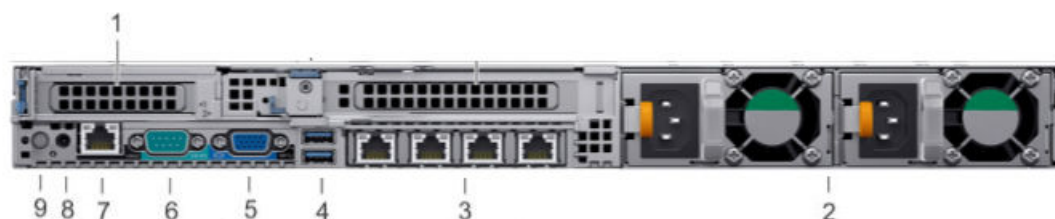


Figure 3: Back view of Dell PowerEdge R640 dual CPU server

No.	Item	Icon	Description
1	PCIe expansion card slot(s)	N/A	Enables you to install PCI Express expansion cards. * Note: Avaya Solutions Platform profiles 2, 3, 4, 5, and 51 are provided with six 1GbE NICs. Avaya does not support the addition of NICs in the field no matter if the server was originally shipped with 4 or 6 NICs in an Avaya Solutions Platform 1XX at this time.
2	Power supply unit (2)	N/A	Voltage type depends on configuration.

Table continues...

No.	Item	Icon	Description
3	NIC port (4)		The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity.
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 Enterprise 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.

Avaya Solutions Platform Appliance profiles

In the Avaya Solutions Platform 100 Series Release 4.0, the server constructs are reduced and shared among Avaya Solutions Platform 110 Appliance, Avaya Solutions Platform 120 Appliance, and Avaya Solutions Platform 130 Appliance.

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
RMU	1U	1U	1U	1U	1U
Intel Skylake CPU	S-4114	S-4114	G-6132	G-6132	G-6132
Number of CPUs Sockets	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 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

Table continues...

Appliance Constructs	Profile #2	Profile #3	Profile #4	Profile #5	Profile #51 (ASP 130 Only)
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-RO Drive	Y	Y	Y	Y	Y

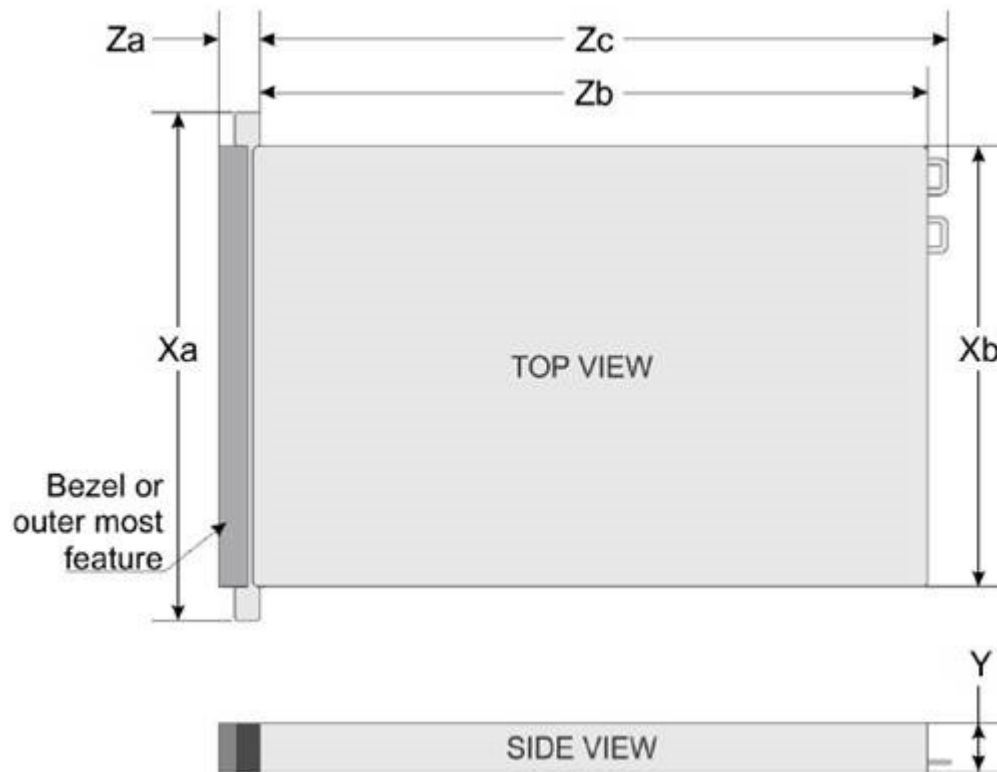
Due to CPU updates from Intel, there is a switch from Skylake CPUs to Cascade Lake CPUs.

Table 1: Cascade Lake CPUs

	Profiles 2 and 21		Profile 3		Profile 4		Profiles 5 and 51	
	Old	New	Old	New	Old	New	Old	New
CPU	4114	4210	4114	4210	6132	6226R	6132	6226R
Core Count	10	10	10	10	14	16	14	16
Total Cores	1 X10 = 10	1 X10 = 10	2 X10 = 20	2 X10 = 20	1 X 14 = 14	1 X 16 = 16	2 X 14 = 28	2 X 16 = 32
Clock (Ghz)	2.2	2.2	2.2	2.2	2.6	2.9	2.6	2.9

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	21.9 kilogram
Dell PowerEdge R640	(48.28 lbs)

Environmental requirements

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

Table 2: 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 3: 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 4: 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 5: 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 6: Maximum altitude

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

Table 7: 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 8: 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 9: 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

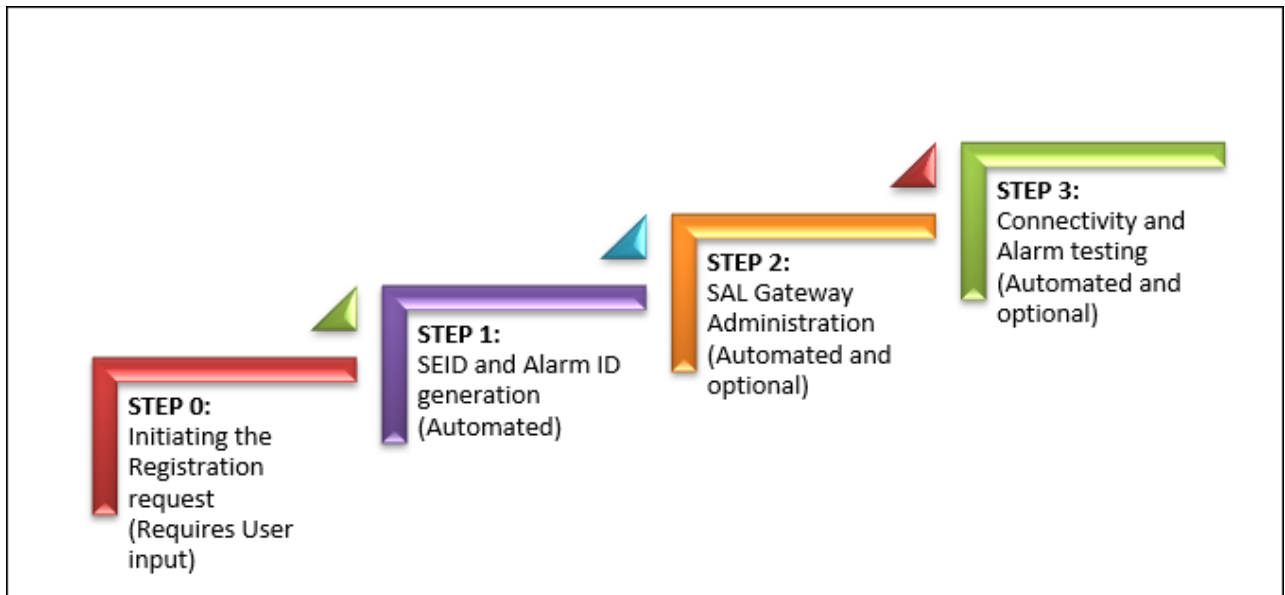
In order to receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in HealthCheck tool.

End user product install base is a prerequisite for services support of Avaya Converged 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 three steps. Only the first step has to be completed by the user manually. The other two 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*.

Before you begin

Ensure that you have the following:

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

 Note:

- US Sold To (functional location) location number format: 000XXXXXXX (000 + 7 digits or can be 00 + 8 digits as well).
- Outside of US (Rest of the World) FL# (Ship To) location number: 00XXXXXXX (always 00 + 8 digits).

- The install base of the device that needs to be onboarded must be created in Siebel.

 Note:

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

- Ensure you have your IP address and host names for iDRAC and the ESXi host.

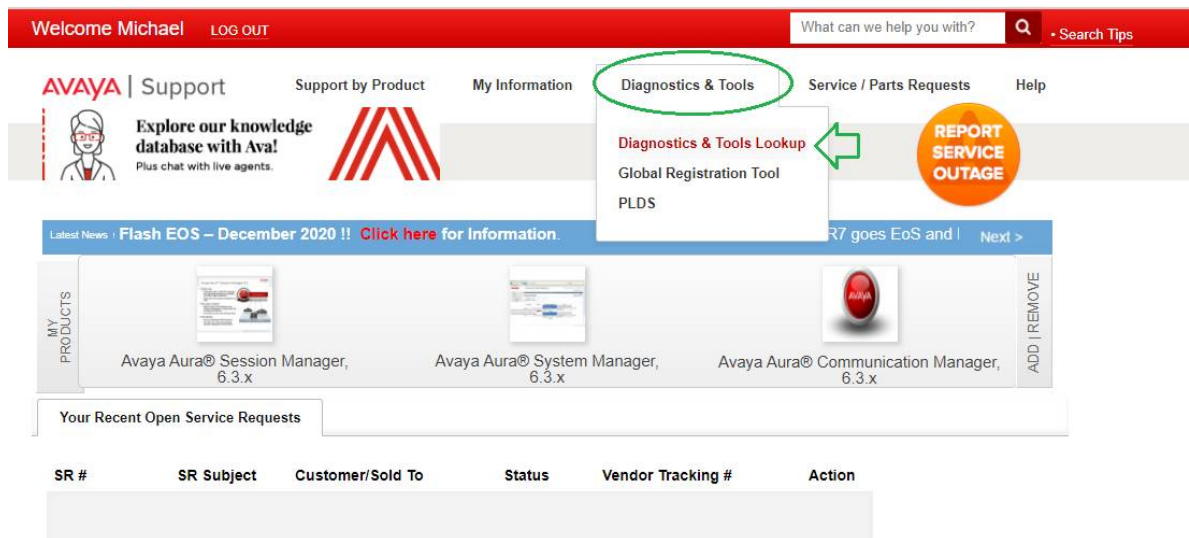
The iDRAC IP address is linked with the Avaya Converged Platform server. The ESXi Host IP address is linked with the Avaya Converged Platform ESXi host.

- 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 Material codes are 700514097 (Profile 2), 700514098 (Profile 3), 700514099 (Profile 4), 700514100 (Profile 5), and 700514579 (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 ACP asset and enter the quantity in the **Location ID** field. Click **Register**.

10. Enter the details in the **ACP**, **ACPEH**, and **SAL Gateway** fields.

▶ SECODE "ACP" = iDRAC

- Enter iDRAC IP Address and Host name in the HealthCheck tool

▶ SECODE "ACPEH" = ESXi Host

- Enter ESXi IP Address and Host name in the HealthCheck tool

▶ SAL Gateway the iDRAC and ESXi Host will be registering

- When you check the SAL ADMIN check box, the best practice is to check the TEST CONN check box. This will test the connectivity to the SAL Gateway you choose.

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*.

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.

Avaya Diagnostics & Tools

REGISTRATION ID: UAR_44475B8C-E03A-4147-8656-6BD21F9CC8B8
CHANGE SEARCH HOME

REGISTRATION SUMMARY

Sold To : 0002788550
Customer Name : AVERY DENNISON
Status : Completed
Submitted Date : 2020-04-30 09:59:33

Search:

	MATERIAL CODE	SECODE	SEID	ALARM ID	SEID CREATION STATUS	SAL ADMINISTRATION RESULT	TESTING RESULT	SR#
	385416	PD3VCE	(628)089-9559					

Showing 1 to 3 of 3 entries

About Avaya | Contacts | Careers | Site Map
Terms of Use | Privacy Statment | © 2013-2015 Avaya Inc.

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](#).

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 23.		
2	Inspect package contents.	See Package contents on page 24.		
3	Install the server using the rail kit.	See Installing the server on page 25.		
4	Attach cables.	See Attaching cables on page 29.		
5	Connect power.	See Connecting power on page 30.		

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.

Before you begin

Warning:

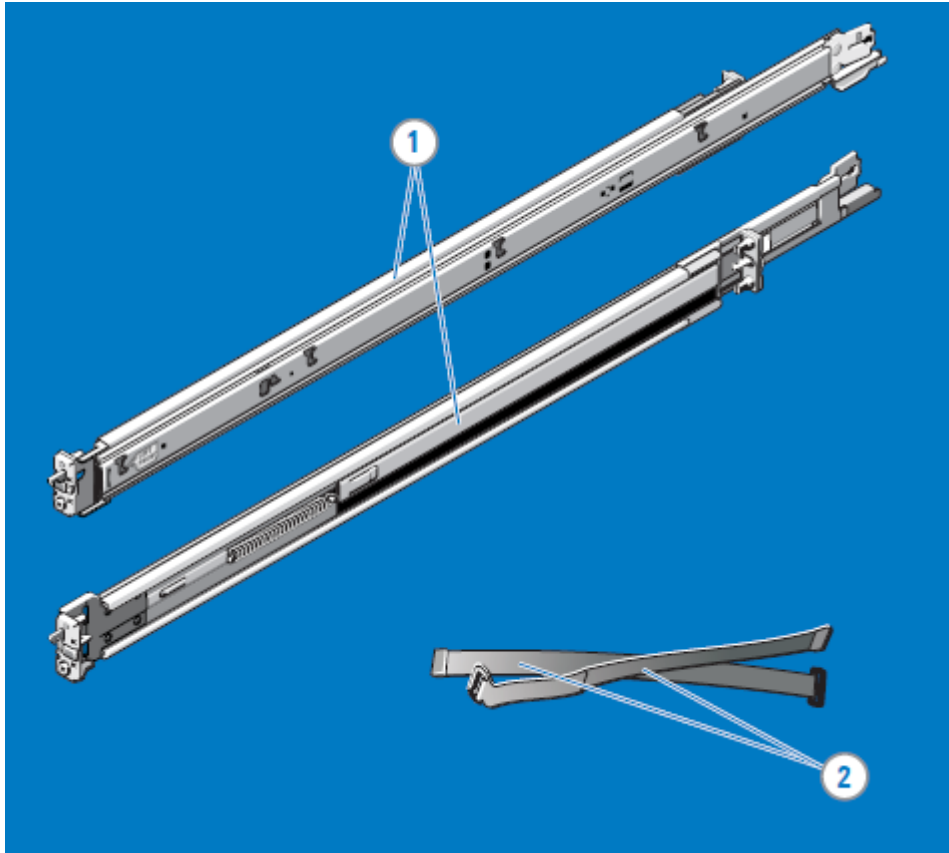
- Before you begin, read and follow the safety instructions in your Safety, Environmental, and Regulatory information document shipped with your system.
- To avoid injury, do not attempt to lift the system by yourself.
- Verify that the rack is installed according to the manufacturer's instructions and 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.



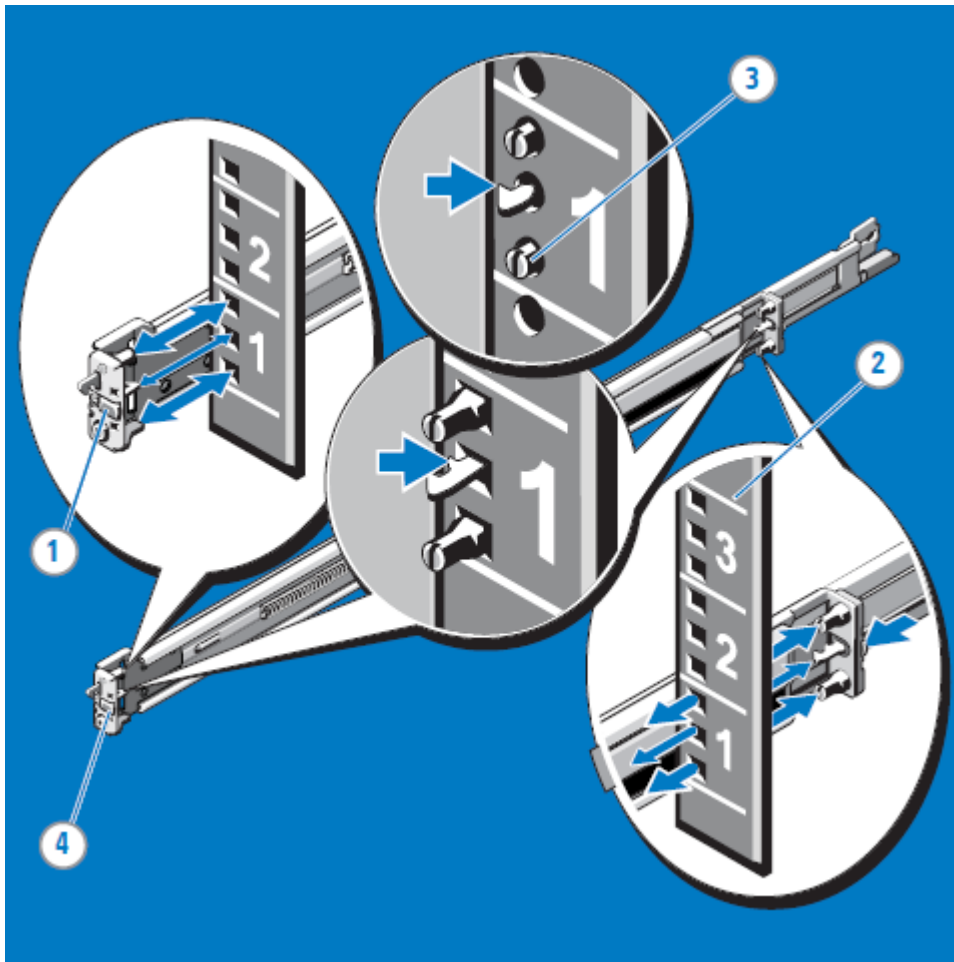
- Two Dell A7 ReadyRails II sliding rail assemblies — (1)
- Two hook and loop straps — (2)

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

! Important:

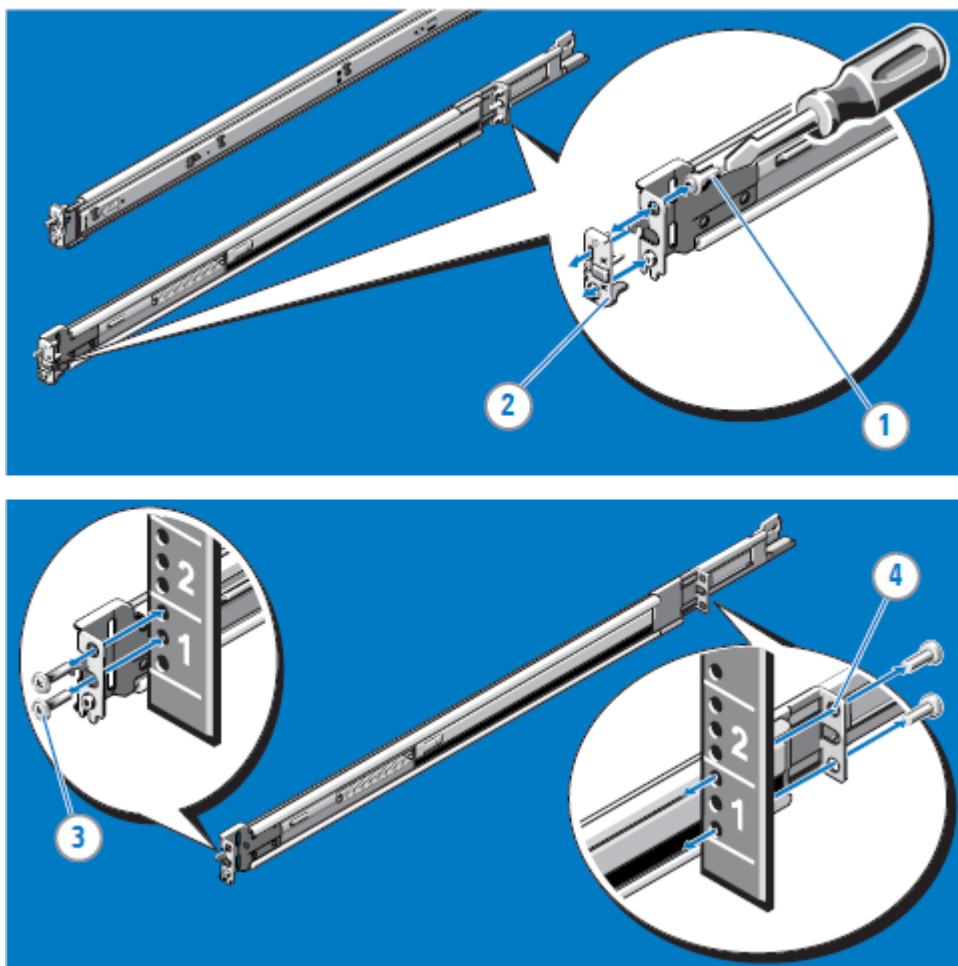
Rail kit installation is performed using either Step 3 or Step 4 depending on the type of rails in use. Read each step carefully and consult your installation environment before proceeding.

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



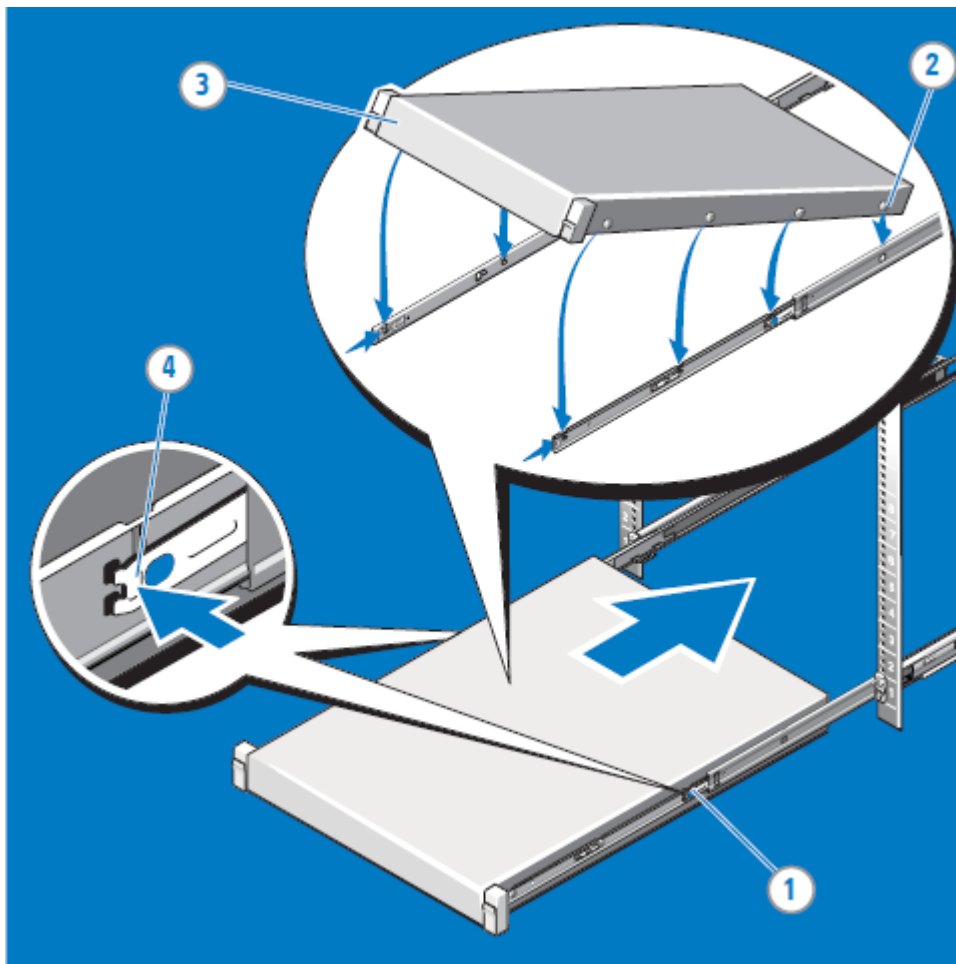
Task order	Task
1	Position the left and right rail end pieces labeled FRONT facing inward and orient each end piece to seat in the holes on the front side of the vertical rack flanges.
2	Align each end piece in the bottom and top holes of the desired rack spaces.
3	Engage the back end of the rail until 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:**

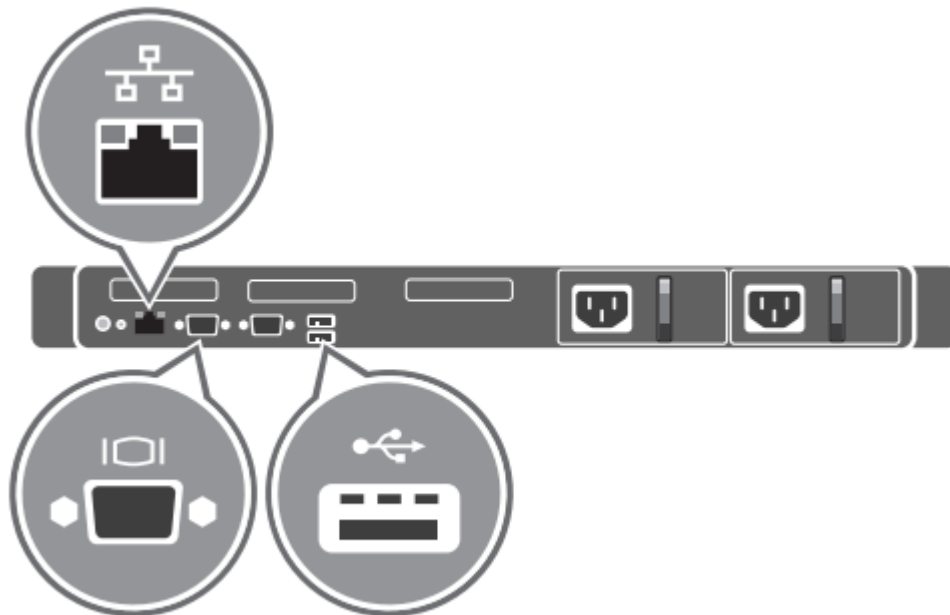
Consult application-specific documentation for information on peripheral and management device connectivity.

Before you begin

Ensure the system has been installed and secured as outlined in [Installing the server](#) on page 25 before you attach cables. Ensure you have taken precautions against electrostatic discharge as outlined in [Electrostatic discharge](#) on page 23 before you begin.

Procedure

1. Connect the network cables to the RJ45 port 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.



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.

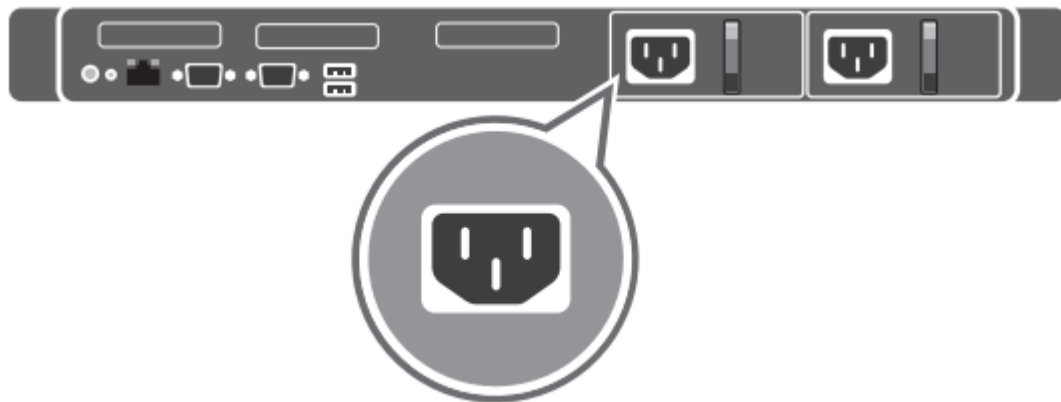
Before you begin

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

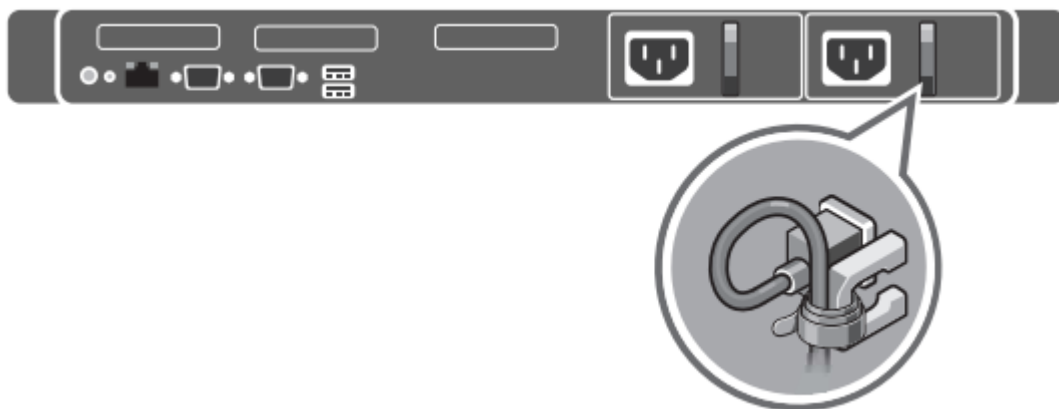
- [Installing the server](#) on page 25
- [Electrostatic discharge](#) on page 23

Procedure

1. Connect the system to the appropriate power source.

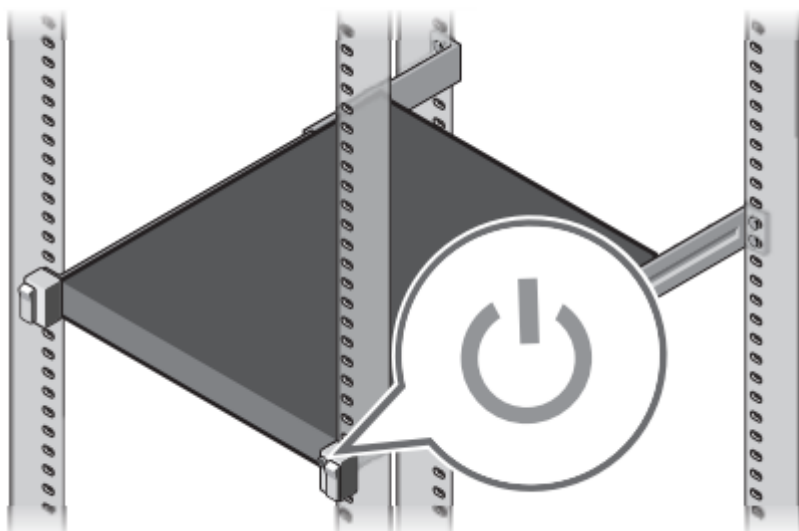


2. Loop and secure the power cable using the retention strap.



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. This chapter also includes instructions to disable TLS 1.0 and 1.1 and to configure SNMP v2 settings for ESXi.

Dell R640 XL ESXi Configuration

Overview

The Avaya Solutions Platform130 (ACP 130) is initially supported on Dell R640 servers. This section provides the instructions required after physical installation to complete the system setup 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.

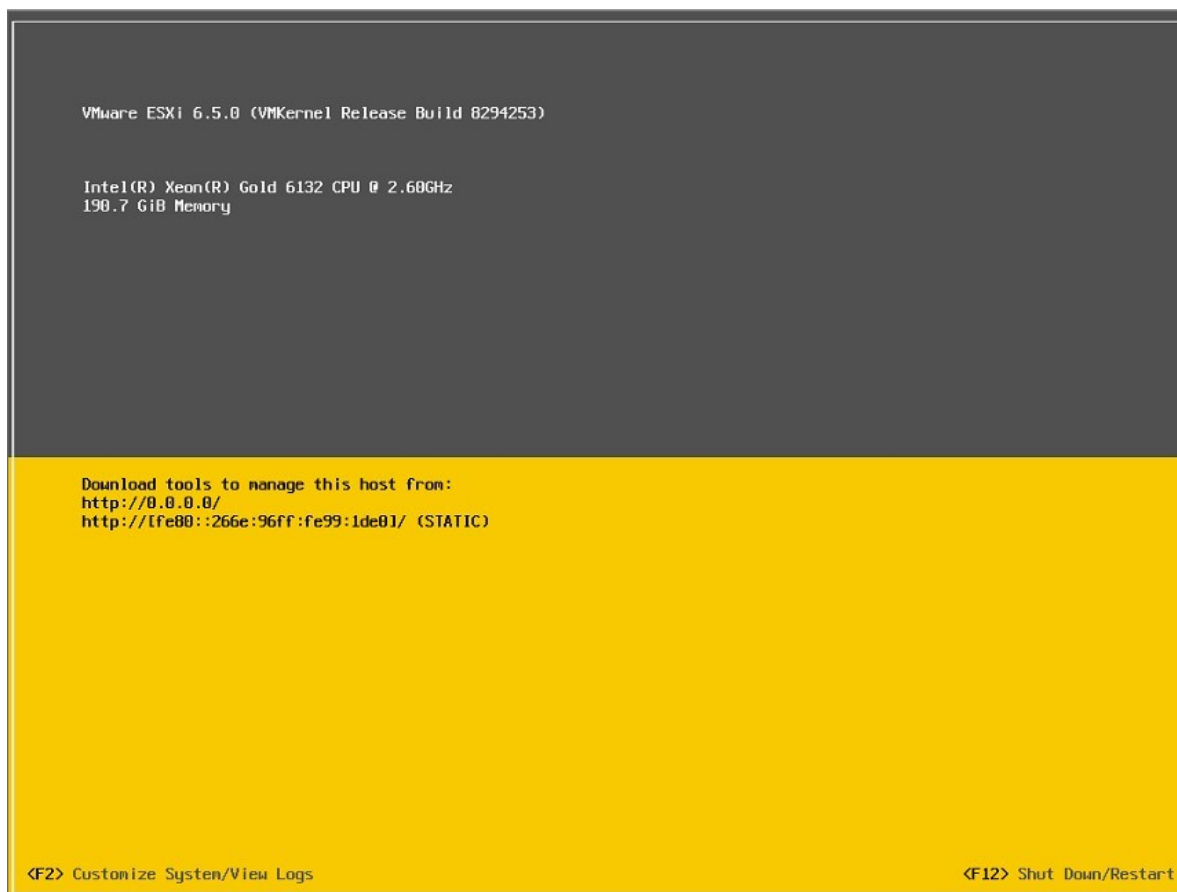


Connection points for VGA monitor and USB keyboard are also on the rear of the server.

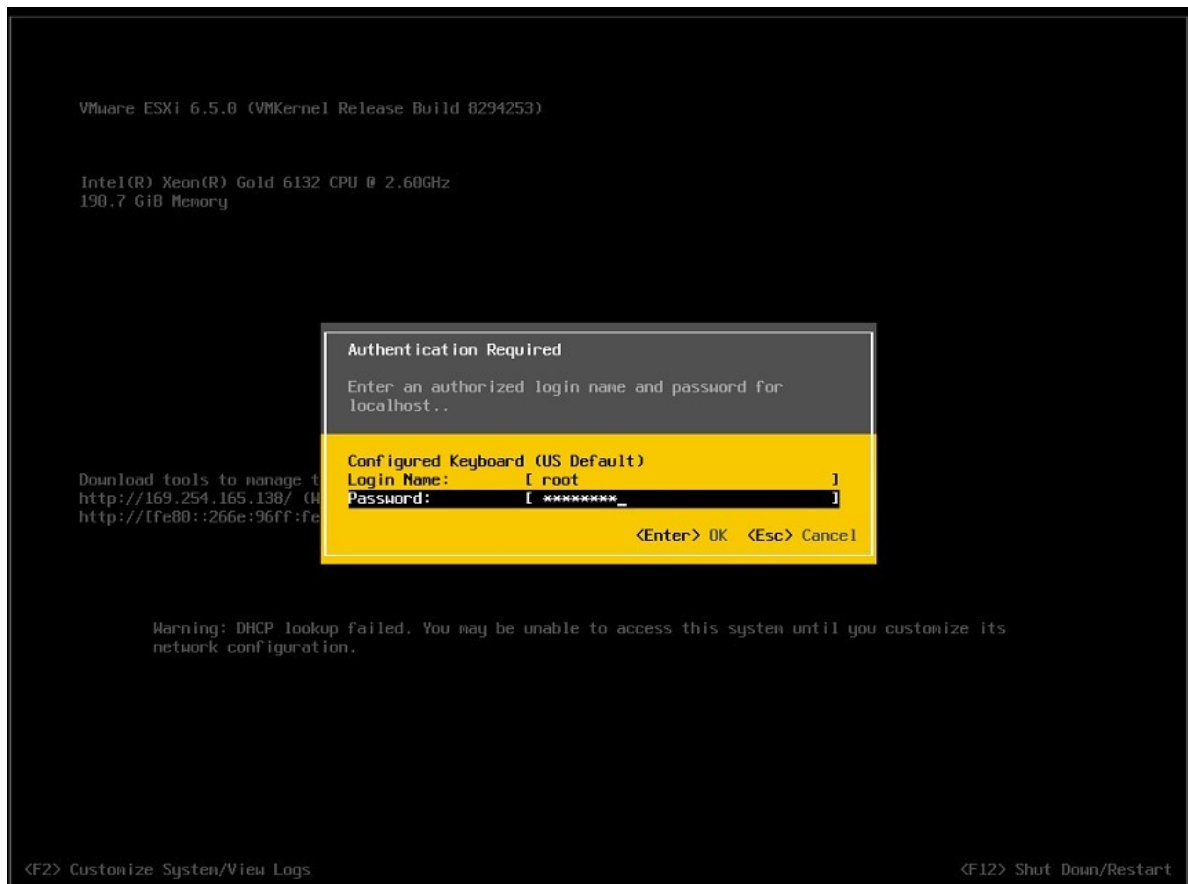
2. Power on the server.

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

3. Once ESXi has loaded, select F2 to administer configuration settings.



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

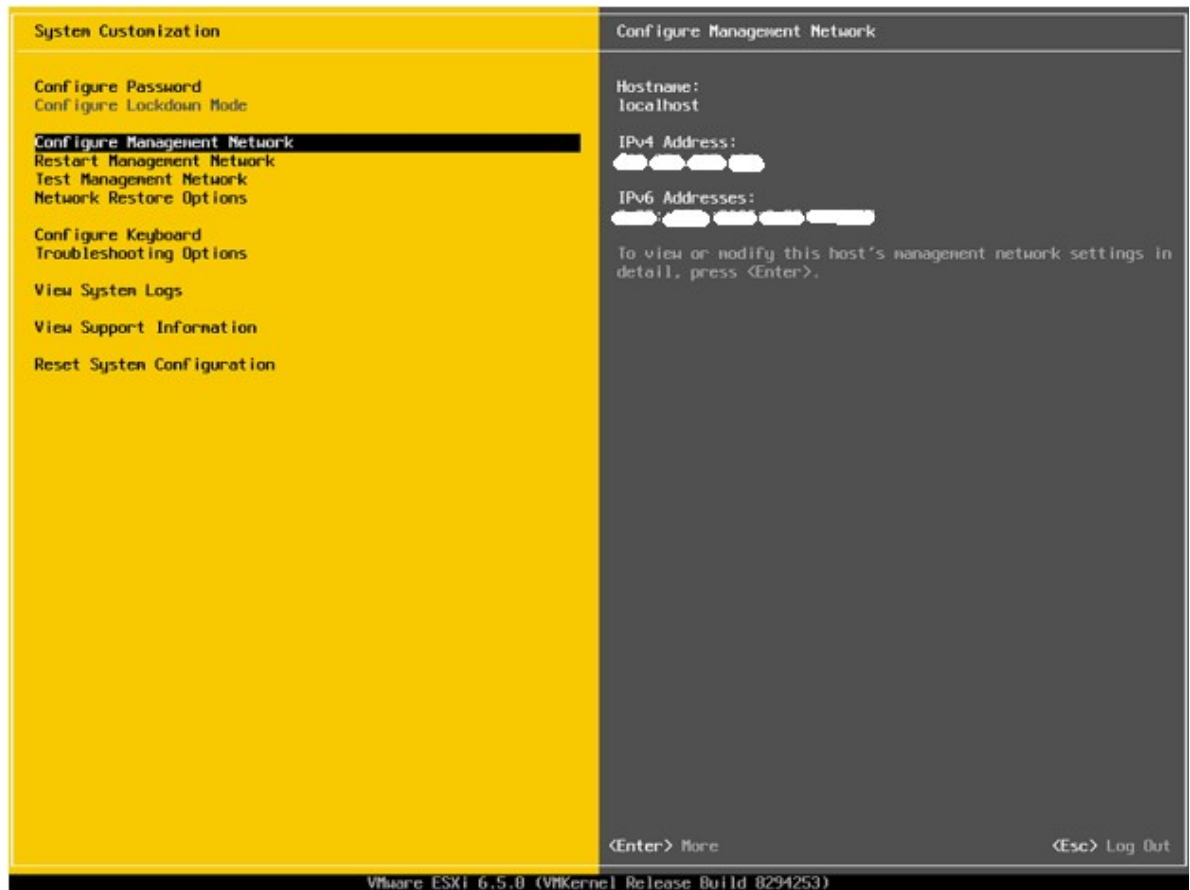


5. From the **System Customization** menu, select **Configure Password**. Create a unique new password to better secure the server, and press **Enter** to submit the change and return to the **System Customization** menu.

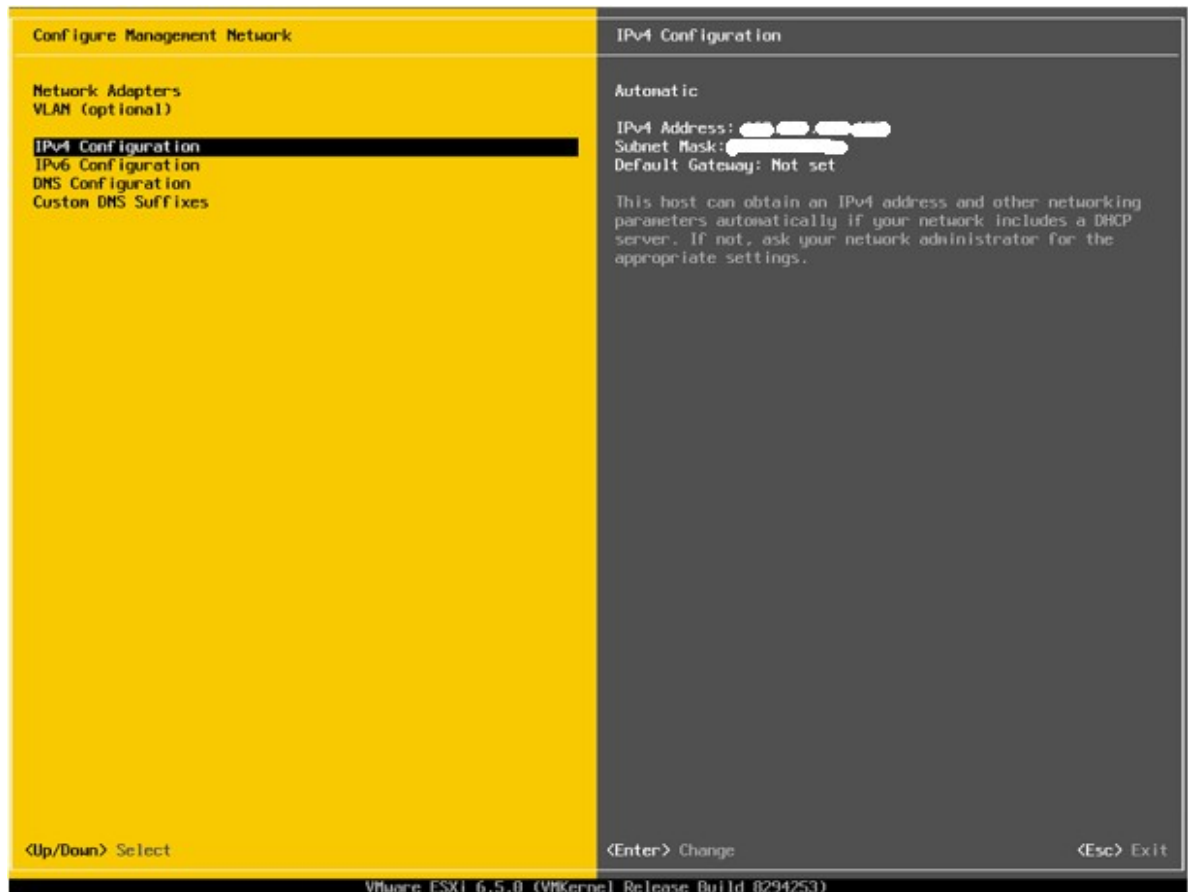
! Important:

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.

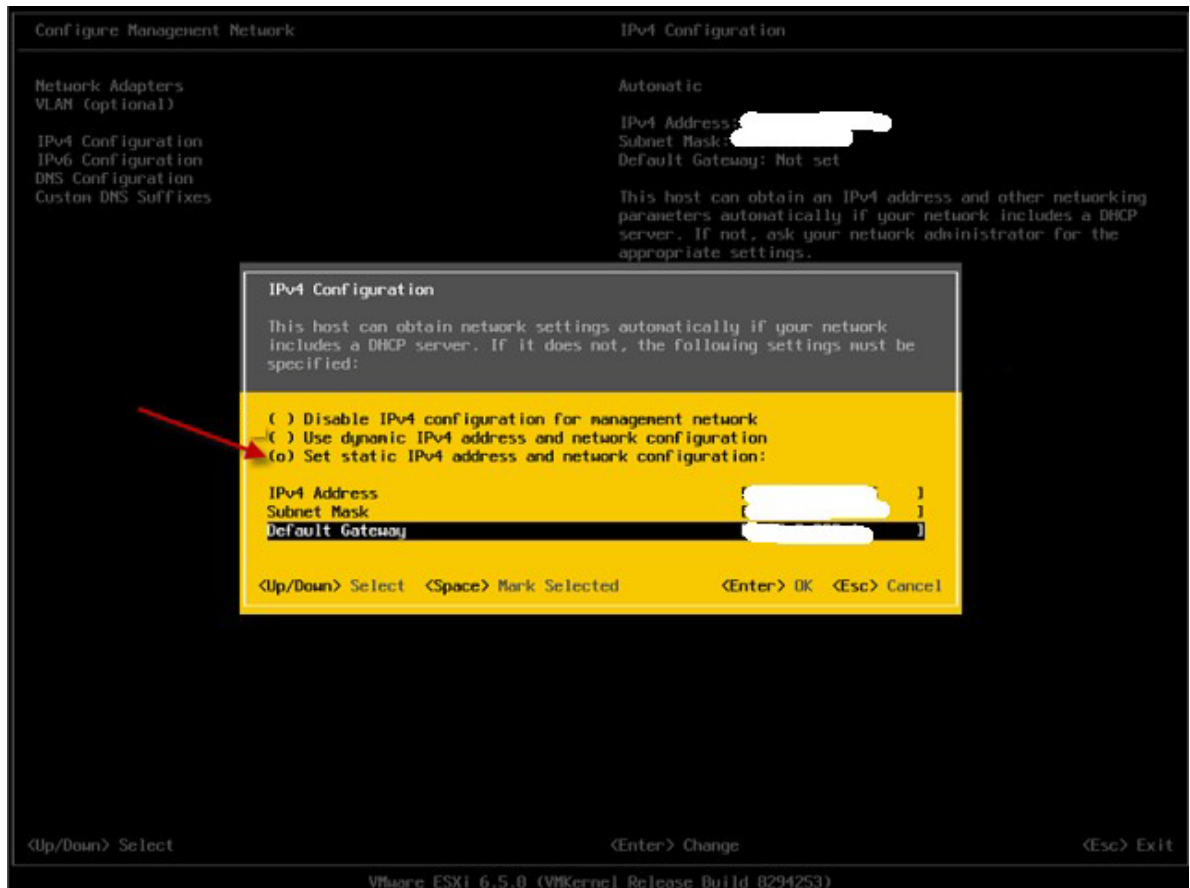
6. Select **Configure Management Network** and press **Enter**.



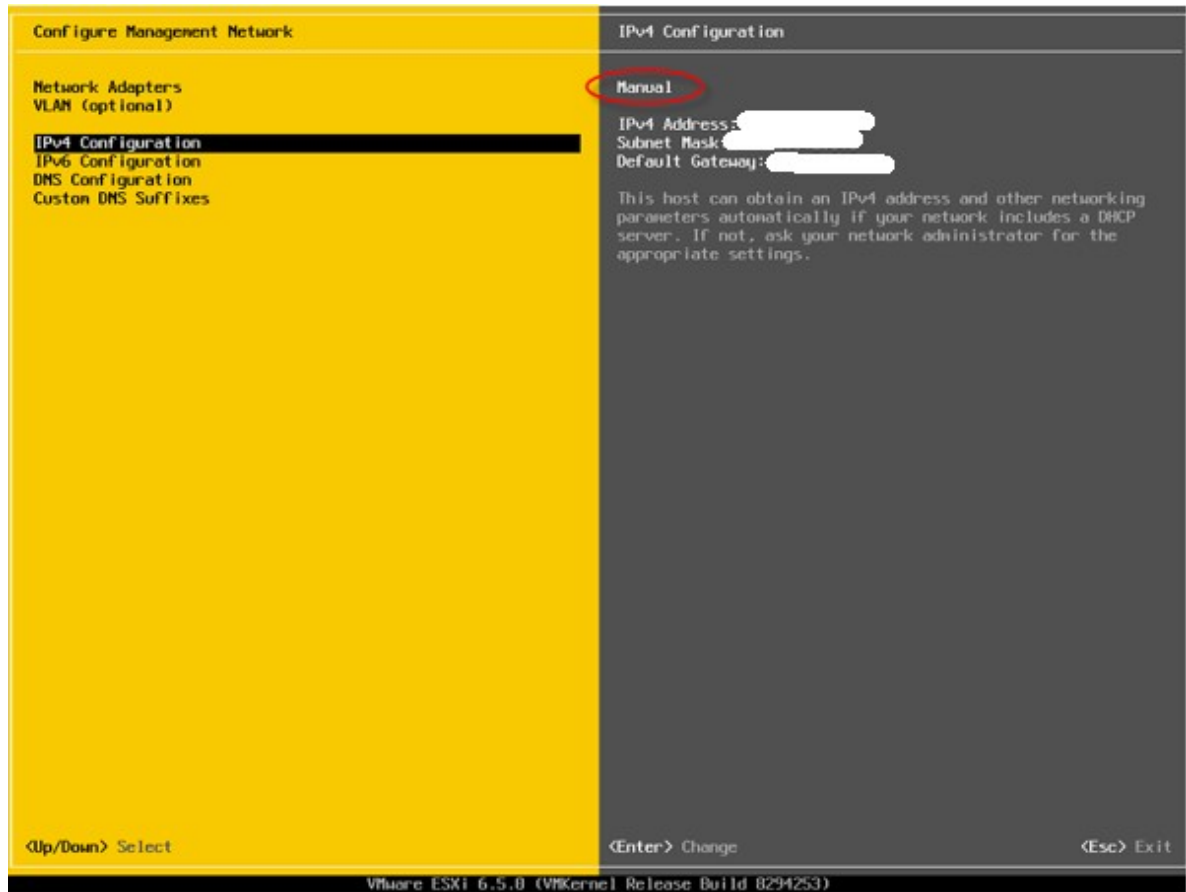
7. Select **IPv4 Configuration** and press **Enter**.



8. Tab to **Set static IPv4 address and network configuration** and press the spacebar to select this option. Tab down to enter related IP information. When complete, press **Enter**.



9. The **Manual** label should now be associated with the IP address fields, indicating static addressing is now required.



10. Select **DNS Configuration** and press **Enter**.

Configure Management Network

Network Adapters
VLAN (optional)
IPv4 Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes

DNS Configuration

Manual

Primary DNS Server:
Not set
Alternate DNS Server:
Not set

Hostname
localhost

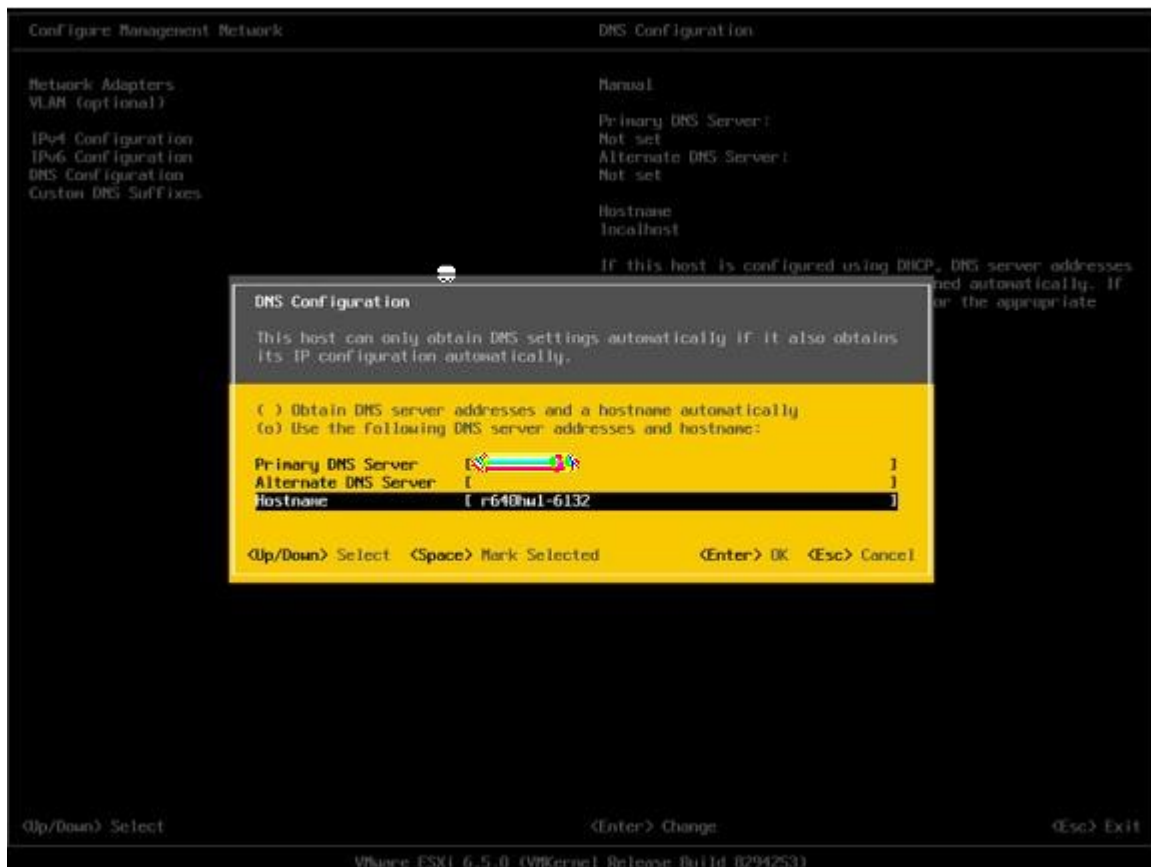
If this host is configured using DHCP, DNS server addresses and other DNS parameters can be obtained automatically. If not, ask your network administrator for the appropriate settings.

<Up/Down> Select <Enter> Change <Esc> Exit

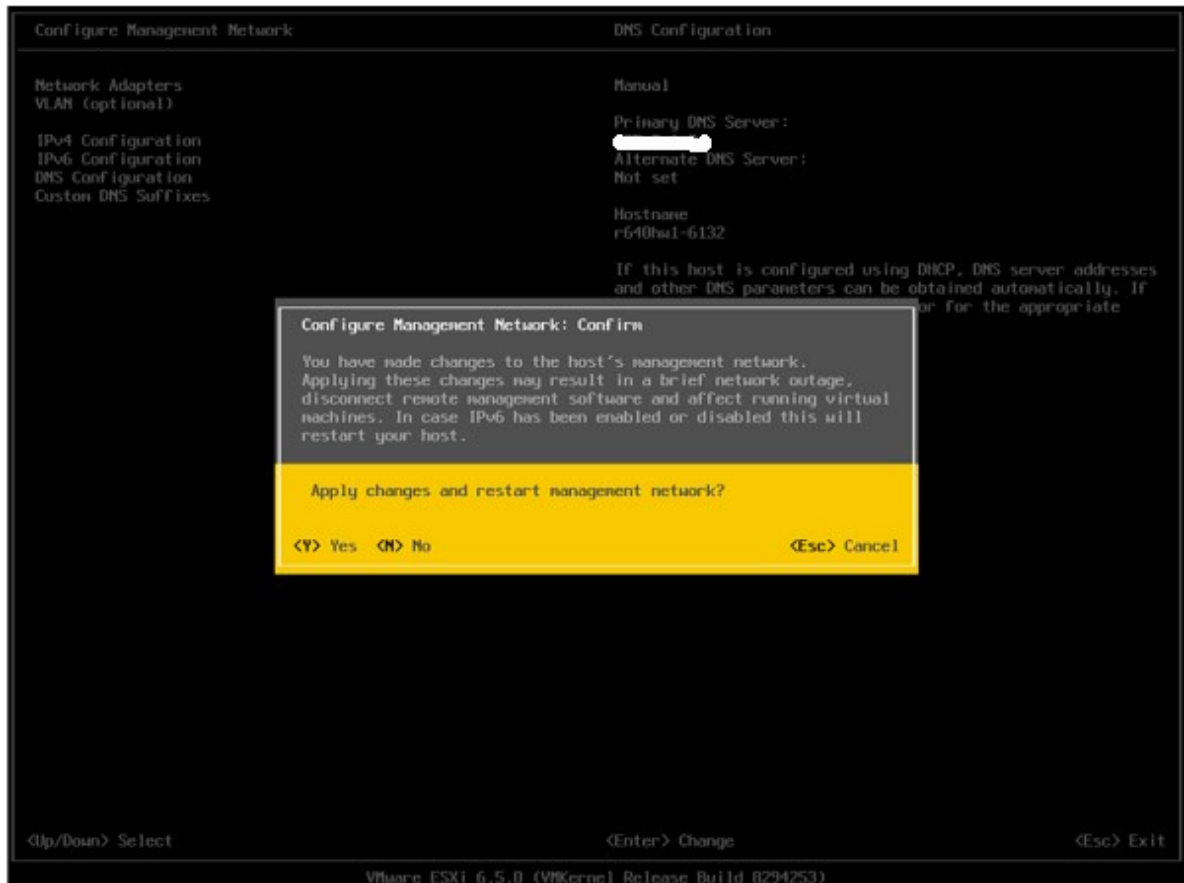
VMware ESXi 6.5.0 (VMKernel Release Build 8294253)

11. Obtain DNS server addresses and a hostname automatically will be selected as default. Tab to **Use the following DNS server addresses and hostname** and press the

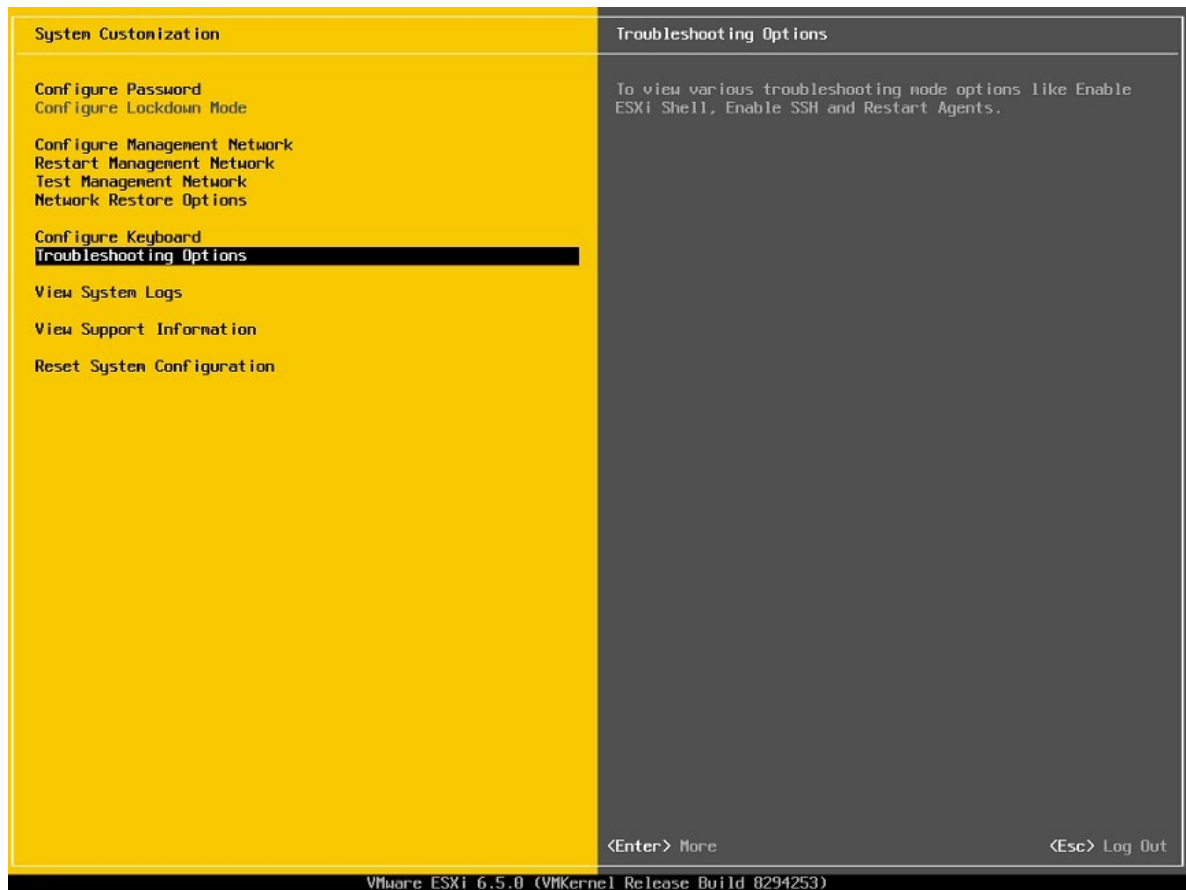
spacebar to select it. Tab down to enter the IP address(es) of the DNS server and the hostname of the server. When complete, press **Enter**.



12. After pressing **Enter** a second time from the main **Configure Network Management** screen, VMware prompts the administrator to save the configuration. Type **Y** (Yes) to save, and then press **Esc** to back out to the previous admin level.



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



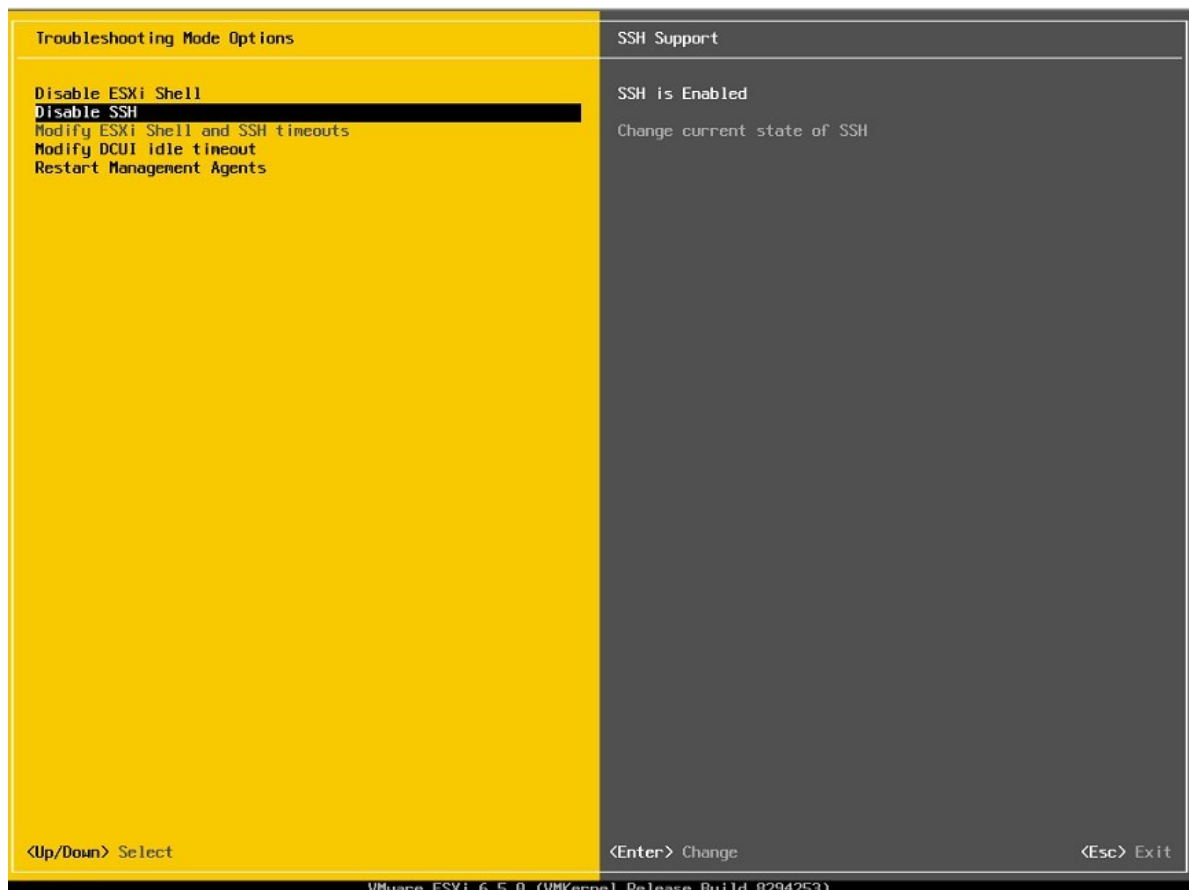
14. ESXi Shell is enabled by the Integrator. However, for a new install of ESXi, you must enable this setting. From the submenu, highlight **Disable ESXi Shell**. The function is

disabled by default; press **Enter** to change the state to **Enabled**, as seen on the right side of the screen.



*Shell will be enabled for all deployments unless otherwise requested by the customer

- SSH is enabled by the Integrator. However, for a new install of ESXi, you must enable this setting. Highlight **Disable SSH**. This function is disabled by default; press **Enter** to change the state to **Enabled**. Then press **Esc** to exit the admin process.



The server is now ready for OVA installation. You may now access the system using the *root* login and your customer defined password.

Configuring autostart on ESXi host using Embedded Host Client

About this task

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

Procedure

- Log into the ESXi Embedded Host Client using a web browser.
- In the Navigator pane on the left, click **Manage**.
- On the **System** tab, click **Autostart**.
- Click **Edit settings**.

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 120.
 - c. In the **Stop delay** field, type 120.
 - d. In the **Stop action** field, click **Shut down**.
 - e. In the **Wait for heartbeat** field, select **no**.
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.

Next steps

After the server has restarted, verify that all VMs are powered on and are correctly configured.

Configuring SNMP v2c on an ESXi 6.5 host

About this task

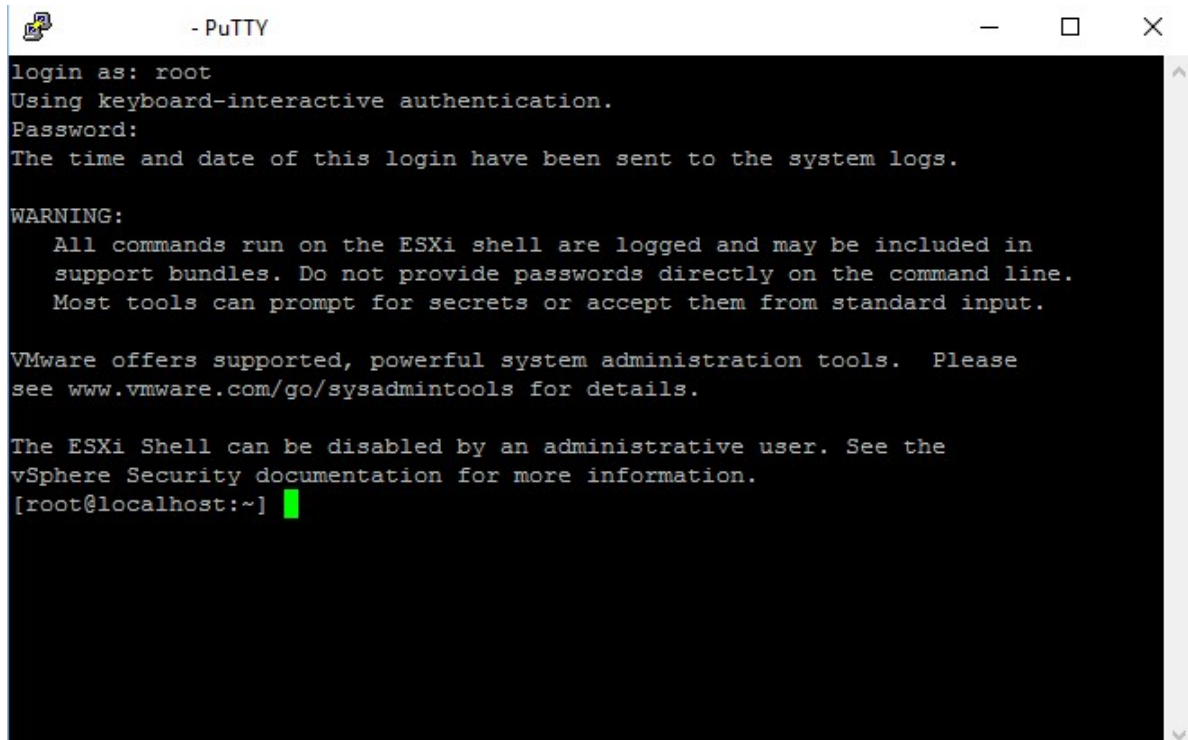
This section provides instructions on how to configure SNMP on the Avaya Solutions Platform 130 server. The Avaya Secure Access Link (SAL) Gateway, as an SNMP trap receiver, can support SNMP v1, v2c and v3. Some trap receivers may only support SNMP v2 and other may require SNMP v3. The ESXi host can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

 Note:

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 14 and 15 above under the “Steps for Configuring ESXi Network Settings” section to enable ESXi shell and SSH.

Procedure

1. From a Putty session, via SSH, access the ESXi host.



```

- PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

WARNING:
  All commands run on the ESXi shell are logged and may be included in
  support bundles. Do not provide passwords directly on the command line.
  Most tools can prompt for secrets or accept them from standard input.

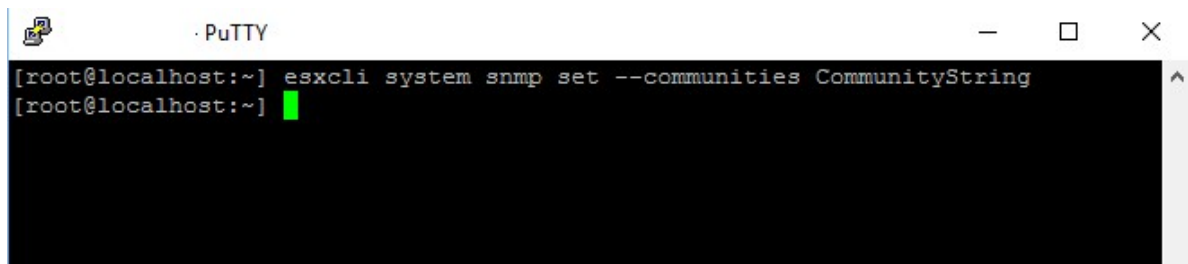
VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] █

```

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>
```



```

- PuTTY
[root@localhost:~] esxcli system snmp set --communities CommunityString
[root@localhost:~] █

```

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.

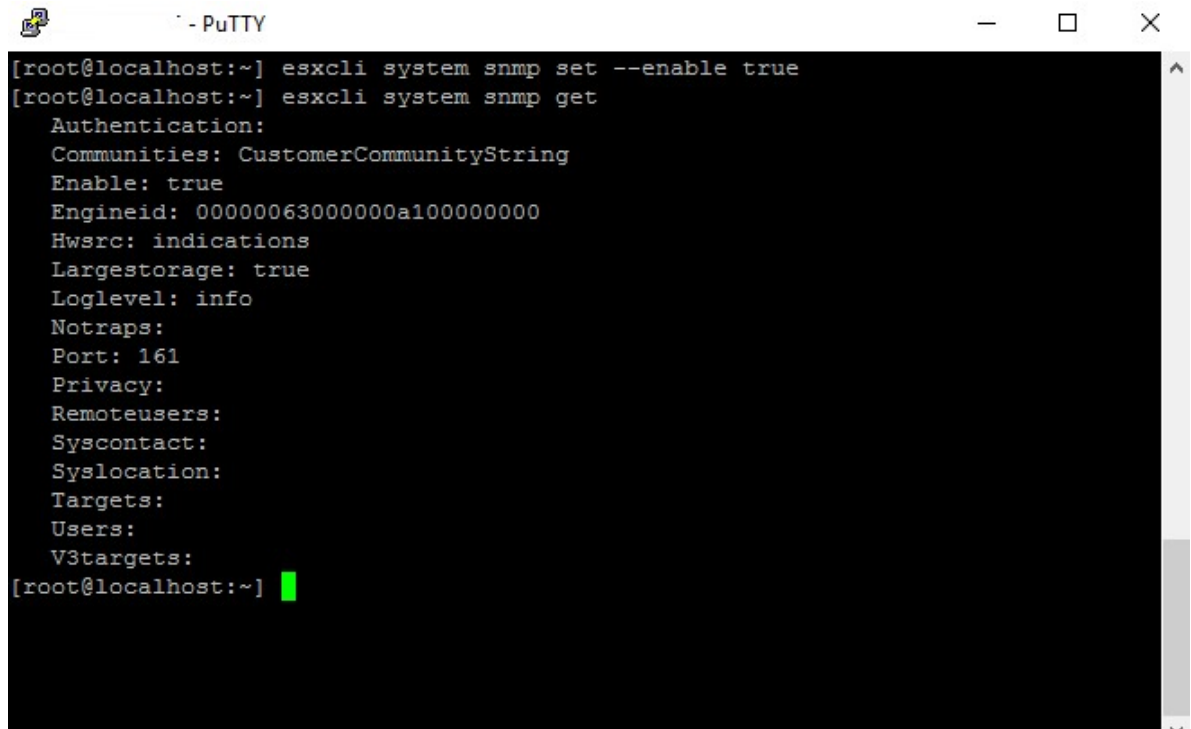
- Up to three trap destinations can be administered and must be separated by commas with no subsequent space.
- If sending traps to a System Manager server, the default port that the System Manager uses for trap reception is port 10162.

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
```



```

[root@localhost:~] esxcli system snmp set --enable true
[root@localhost:~] esxcli system snmp get
Authentication:
Communities: CustomerCommunityString
Enable: true
Engineid: 0000000630000000a100000000
Hwsrc: indications
Largestorage: true
Loglevel: info
Notraps:
Port: 161
Privacy:
Remoteusers:
Syscontact:
Syslocation:
Targets:
Users:
V3targets:
[root@localhost:~]

```

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 6.5 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:**

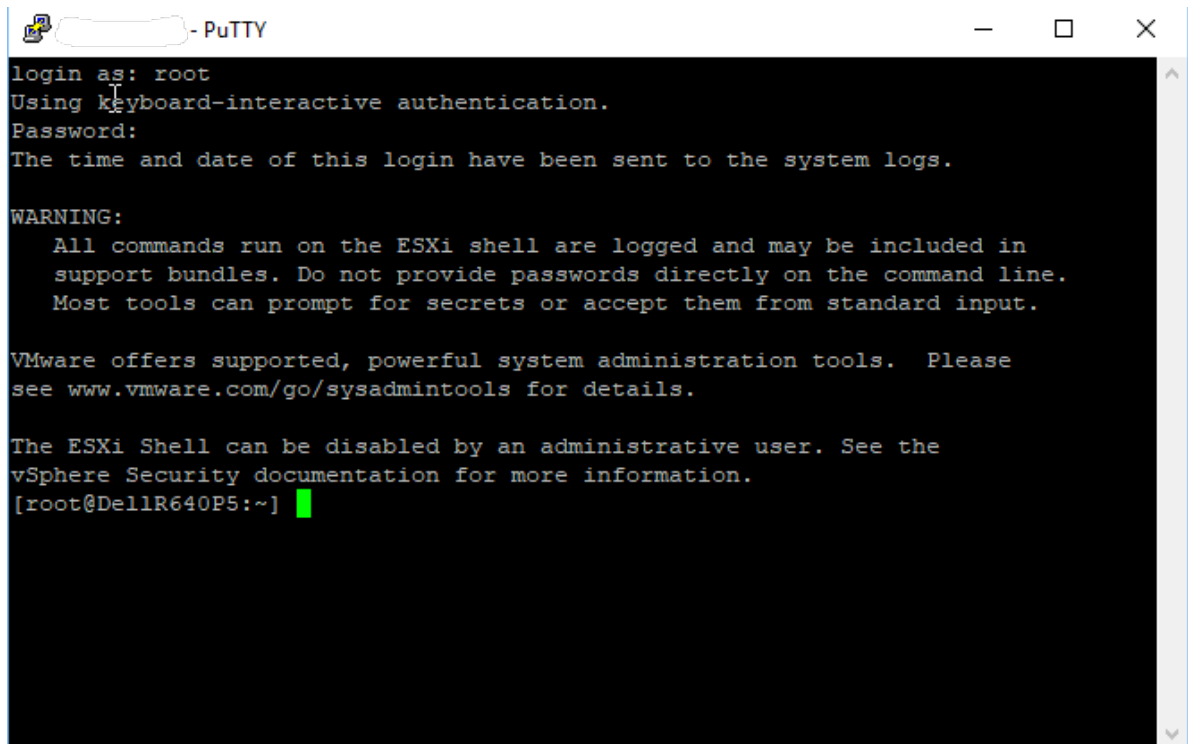
The SSH functionality must be enabled on ESXi. The Avaya installation guidelines direct administrators to enable SSH, so this should not be an issue. If, however, ESXi shell is not enabled, refer to steps 14 and 15 above under the “Steps for Configuring ESXi Network Settings” section to enable ESXi shell and SSH.

*** Note:**

The SAL GW does not support Engine ID info exchange; configuring that function has been omitted from this section. For details on creating/supporting Engine ID with other NMS devices, please refer to the following VMware KB article: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.monitoring.doc/GUID-4AF8AA5F-D652-4080-B984-B36A25456A4B.html>.

Procedure

1. From a Putty session, via SSH, access the ESXi host.



```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

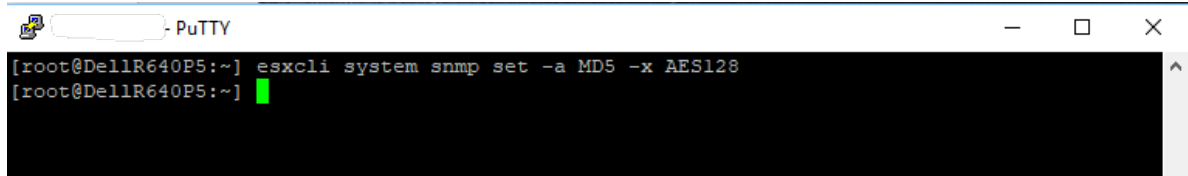
WARNING:
  All commands run on the ESXi shell are logged and may be included in
  support bundles. Do not provide passwords directly on the command line.
  Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@DellR640P5:~]
```

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

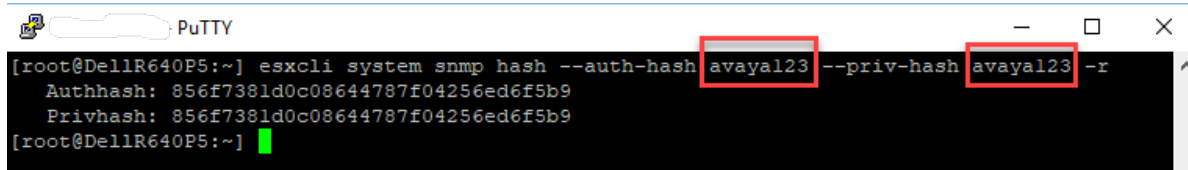
```
esxcli system snmp set -a MD5 -x AES128
```



```
[root@DellR640P5:~] esxcli system snmp set -a MD5 -x AES128
[root@DellR640P5:~]
```

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

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



```
[root@DellR640P5:~] esxcli system snmp hash --auth-hash avaya123 --priv-hash avaya123 -r
Authhash: 856f7381d0c08644787f04256ed6f5b9
Privhash: 856f7381d0c08644787f04256ed6f5b9
[root@DellR640P5:~]
```

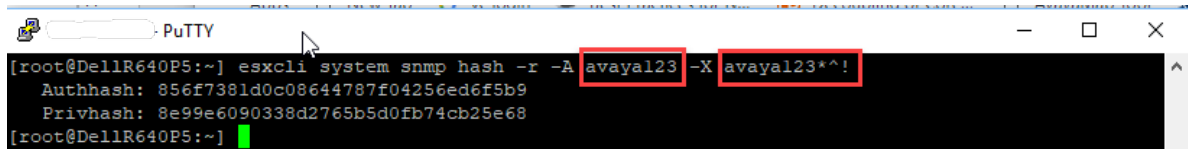
A shorthand method of typing this same command is available:

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

In the example above, the same “secret” was used for the authentication and privacy users: *avaya123*. 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 for each 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, *avayaauth* and *avayapriv*, produces a unique hash output for each element.



```
[root@DellR640P5:~] esxcli system snmp hash -r -A avaya123 -X avaya123*^!
Authhash: 856f7381d0c08644787f04256ed6f5b9
Privhash: 8e99e6090338d2765b5d0fb74cb25e68
[root@DellR640P5:~]
```

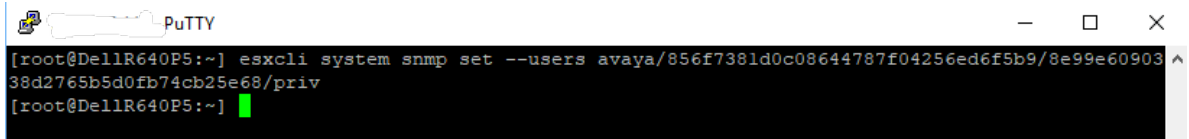
Passwords for ESXi 6.5 must be a minimum of 8 characters long.

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/security
```



```

[root@DellR640P5:~] esxcli system snmp set --users avaya/856f7381d0c08644787f04256ed6f5b9/8e99e6090338d2765b5d0fb74cb25e68/priv
[root@DellR640P5:~]

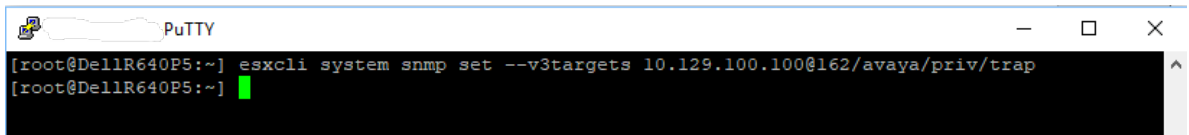
```

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/trap
```



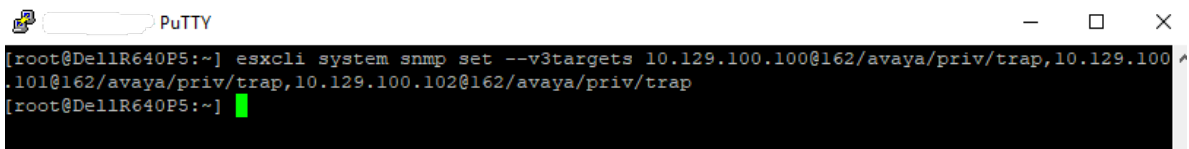
```

[root@DellR640P5:~] esxcli system snmp set --v3targets 10.129.100.100@162/avaya/priv/trap
[root@DellR640P5:~]

```

*** 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.



```

[root@DellR640P5:~] esxcli system snmp set --v3targets 10.129.100.100@162/avaya/priv/trap,10.129.100.101@162/avaya/priv/trap,10.129.100.102@162/avaya/priv/trap
[root@DellR640P5:~]

```

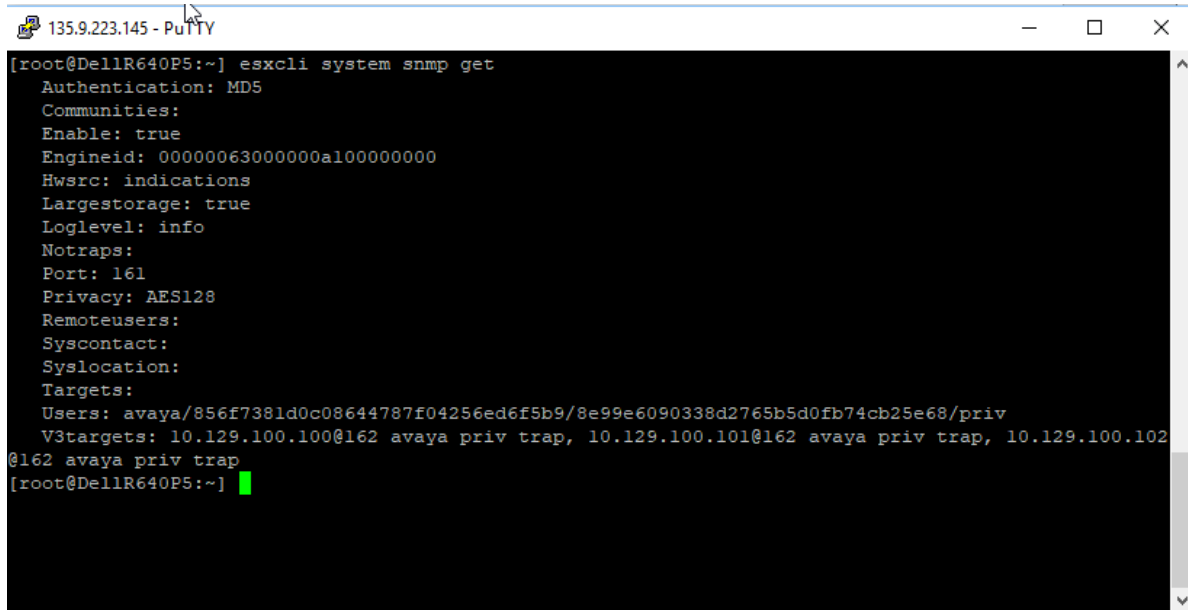
6. Enable SNMP service.

```
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
```



```

135.9.223.145 - PuTTY
[root@DellR640P5:~] esxcli system snmp get
Authentication: MD5
Communities:
Enable: true
Engineid: 000000630000000a100000000
Hwsrc: indications
Largestorage: true
Loglevel: info
Notraps:
Port: 161
Privacy: AES128
Remoteusers:
Syscontact:
Syslocation:
Targets:
Users: avaya/856f7381d0c08644787f04256ed6f5b9/8e99e6090338d2765b5d0fb74cb25e68/priv
V3targets: 10.129.100.100@162 avaya priv trap, 10.129.100.101@162 avaya priv trap, 10.129.100.102
@162 avaya priv trap
[root@DellR640P5:~]

```

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
```

Services Port Configuration

Purpose

This section provides instructions for configuring the Avaya Converged Platform 130 Series services port using the `ACP130srvprt-cfg.sh` script. The services port will provide Avaya support and technicians with access to the server for maintenance and troubleshooting activities.

Configuring Avaya Converged Platform 130 Services Port

About this task

Use this procedure to configure Avaya Converged Platform 130 Services Port.

Important:

For any Avaya Converged Platform 130 server shipped before March 15, 2019, the services port was not configured at the factory. Avaya Converged Platform 130 server recovery or software remastering will require the `ACP130srvprt-cfg.sh` script to be copied to the ESXi shell and the script to be run. On a recovery, this script should be run prior to deploying any OVAs. Refer to the *Before you begin* section below before running the services port script, to

validate the configuration before proceeding. The `ACP130srvprt-cfg.sh` script can be obtained from <http://plds.avaya.com> using the PLDS download ID ACP0000002.

Before you begin

Validate that the Services port group has not been created and configured or that another application has not configured the vSwitch1 for their product implementation.

- Log in to the vSphere Web Client for the ESXi Host.
- Go to **Networking > Port Groups**.
- Validate that there is not a **Services** port group created or that another application has not already assigned to vSwitch1 for their product deployment.
 - If Services port and vSwitch1 has not been created, follow the procedure below to create it.
 - If the Services port is configured, then there is no need to run the script to configure the Services port. If the vSwitch1 has been created for another use besides a Services port, contact Avaya Support for configuration of the Services port if needed. Do not run the script and overwrite the existing vSwitch1 arrangement.

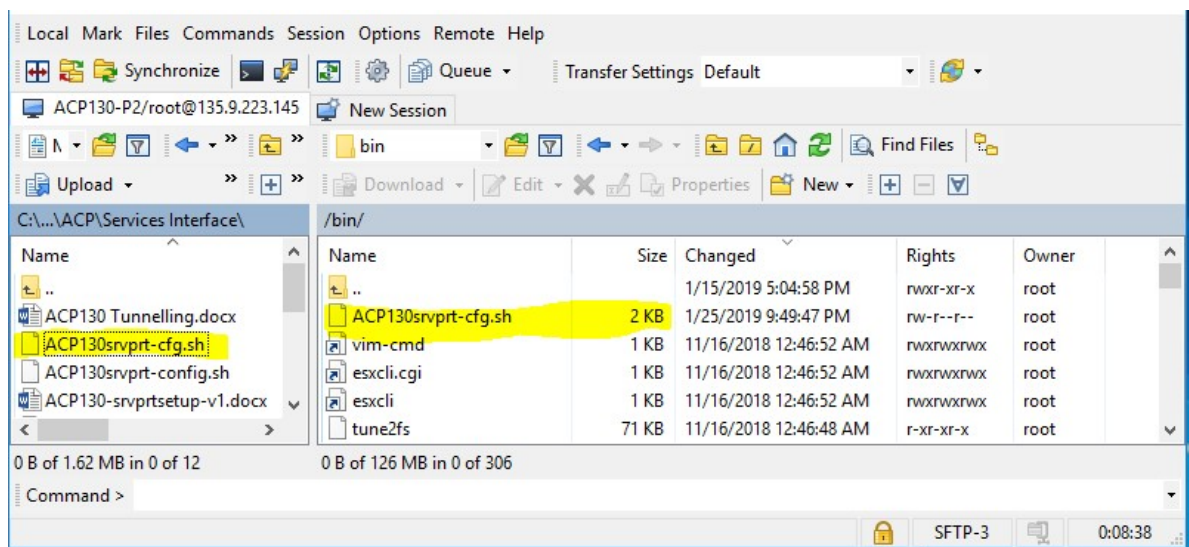
! Important:

Running the script will overwrite the current services port group or vSwitch1 if it is configured.

Procedure

1. Copy file `ACP130srvprt-cfg.sh` to the Avaya Converged Platform 130 ESXi 6.5 directory `/bin`.
2. Use WinSCP from a Windows machine or scp from a Linux machine for copying file to ESXi host.

Using WinSCP



Using Linux SCP

```
drunix1(dck) ->/home/dck/rje: scp ACP130srvprt-cfg.sh root@135.9.223.145:/bin
Password:
ACP130srvprt-cfg.sh
drunix1(dck) ->/home/dck/rje: 100% 1901 1.9KB/s 00:00
```

3. Refer to the screen shot below for the steps to configure Avaya Services Port:

- a. Log in to the ACP130 ESXi 6.5 host SSH console using root credentials, using PuTTY.

The default password is: ACP130_pw

- b. Run the following command:

```
cd /bin
```

- c. Ensure that the file, ACP130srvprt-cfg.sh is present and permissions for root are executable (make executable if required ["chmod 755" command in scrape below]).
- d. Run ./ACP130srvprt-cfg.sh, to configure vSwitch1.
- e. Verify **vSwitch0** and **vSwitch1** are now configured and the services port group is set to IP address **192.11.13.6/30 on vmk1**. Type `exit` to terminate the session.

The services port is now configured.

```
[root@localhost:~] cd /bin
[root@localhost:/bin] ls -l | grep ACP130
-rw-r--r-- 1 root root 1901 Jan 26 00:37 ACP130srvprt-cfg.sh
[root@localhost:/bin] chmod 755 ACP130srvprt-cfg.sh
[root@localhost:/bin] ls -l | grep ACP130
-rwxr-xr-x 1 root root 1901 Jan 26 00:37 ACP130srvprt-cfg.sh
[root@localhost:/bin] ./ACP130srvprt-cfg.sh
Setting up Services Technician Laptop port on ACP130 Server
Cleaning any old Services vSwitch Configuration. ignore any errors...
Cleanup complete.
Adding Services vSwitch
Configure Services Portgroup
Enable ssh and http client usage
Generating Certificates with current hostname [localhost]
Setup is complete
New vmkl for Services Port
Name IPv4 Address IPv4 Netmask IPv4 Broadcast Address Type Gateway DHCP DNS
----
vmkl 192.11.13.6 255.255.255.252 192.11.13.7 STATIC 0.0.0.0 false
Two Vswitches currently setup on server
vSwitch0
  Name: vSwitch0
  Class: etherswitch
  Num Ports: 1682
  Used Ports: 4
  Configured Ports: 128
  MTU: 1500
  CDP Status: listen
  Beacon Enabled: false
  Beacon Interval: 1
  Beacon Threshold: 3
  Beacon Required By:
  Uplinks: vmnic0
  Portgroups: VM Network, Management Network
vSwitch1
  Name: vSwitch1
  Class: etherswitch
  Num Ports: 1682
  Used Ports: 4
  Configured Ports: 128
  MTU: 1500
  CDP Status: listen
  Beacon Enabled: false
  Beacon Interval: 1
  Beacon Threshold: 3
  Beacon Required By:
  Uplinks: vmnic1
  Portgroups: Services
[root@localhost:/bin]
```

Validating vSwitch1 Configuration

About this task

Use this procedure to verify vSwitch1 configuration using the 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**.

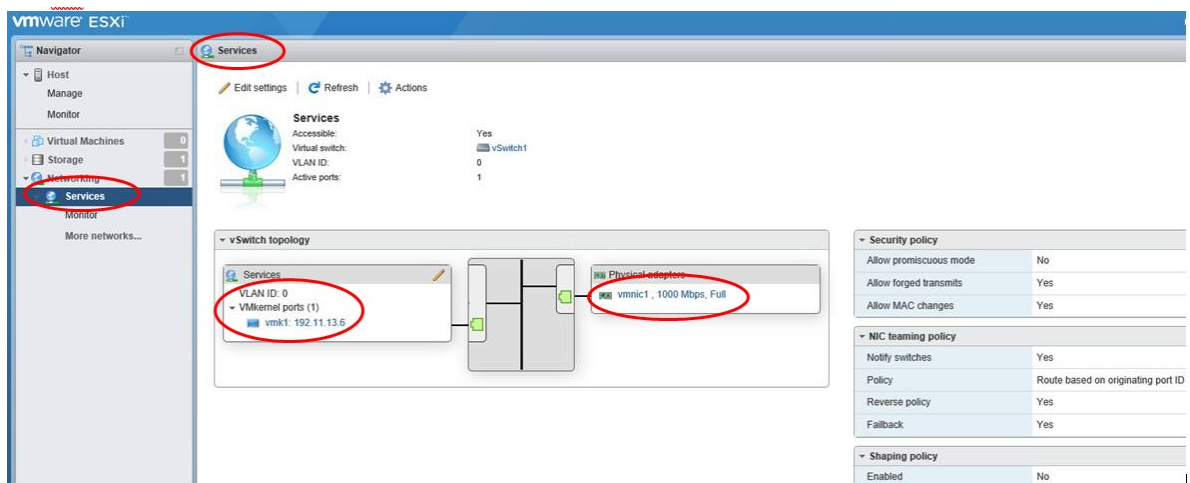
The Services standard port group should be created and assigned to **vSwitch1**.



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

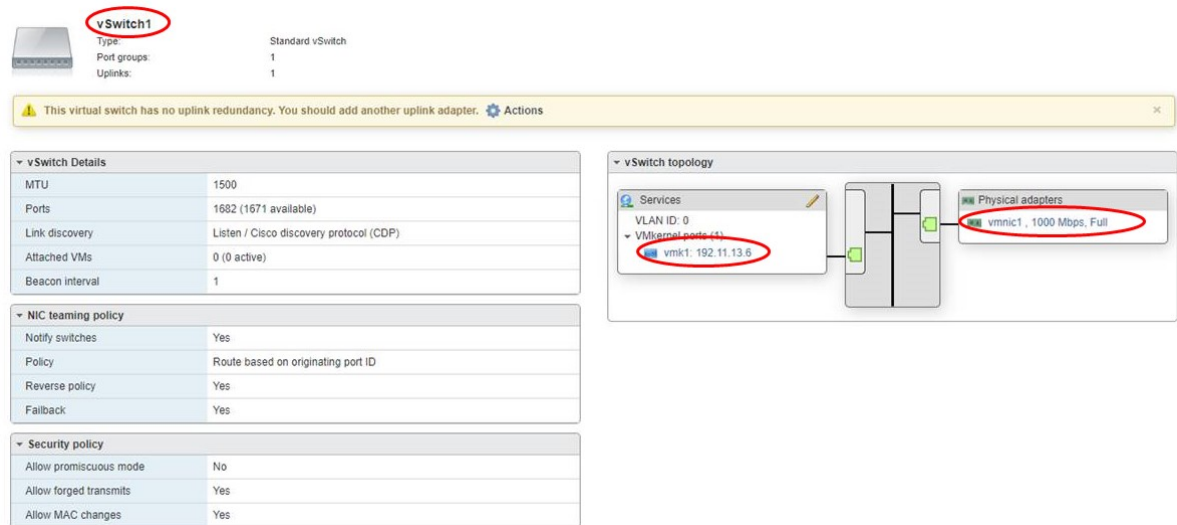


4. Go to **Networking > Virtual Services**.

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

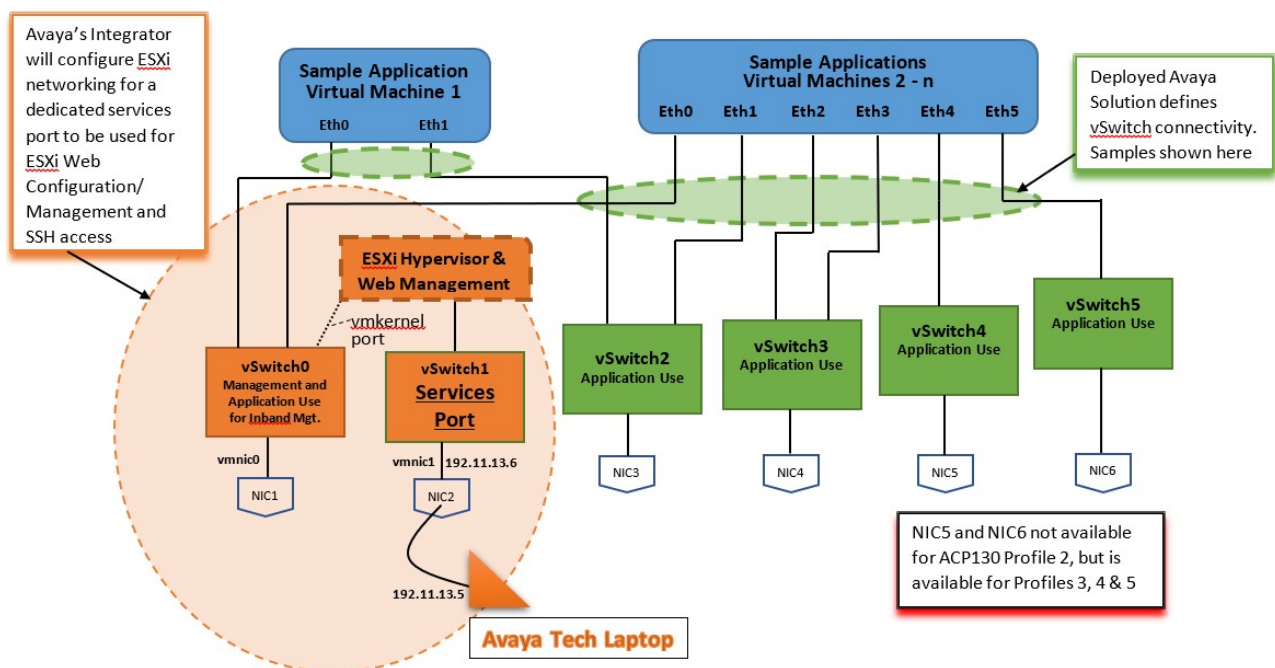
Configuration



Sample Service's vSwitch Configuration

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

Avaya ACP 130 Service's vSwitch Configuration



Management of the TLS protocol configuration for vSphere 6.5 U2 Environment

As of March 2019, TLS v1.0 and TLS v1.1 are disabled in Avaya Solutions Platform 130 servers shipping from the Avaya integrator. TLS v1.0 and TLS v1.1 on servers shipped prior to March 2019 might be enabled. This section provides instructions for disabling TLS v1.0 and TLS v1.1.

Using the vCenter application

Management of the TLS protocol configuration requires direct interaction with the **vCenter** application. The standard Avaya Solutions Platform 130 offer does not include vCenter. Since the ACP 130 server will most likely not have vCenter deployed, you can temporary use the free version of the application.

Download a free 60-day trial of vCenter from the VMware website: <https://my.vmware.com/web/vmware/details?productId=614&downloadGroup=VC650>

TLS protocol management

This section covers the process for disabling TLS v1.0 and TLS v1.1 and enabling TLS v1.2 only within the vCenter Server Appliance and ESXi host. By default, TLS v1.0, v1.1 and v1.2 are enabled, TLS v1.2 cannot be disabled. Use **TLS Reconfigurator Utility Tool** to enable and disable TLS protocols. You can download the tool from the VMware website.

Note:

If you have your ACP 130 server shipped and provided prior to the end of March 2019, you must disable TLS v1.0 and v1.1 and enable only TLS v1.2 by following the procedures in this section.

For more information on TLS, see the VMware Knowledge Base article: <https://kb.vmware.com/s/article/2147469>

Related links

[Installing the TLS Reconfigurator Utility Tool](#) on page 59

[Viewing Enabled TLS Version](#) on page 60

[Configuring TLS v1.2 only for vCenter Server Appliance and Platform Services Controller Appliance](#) on page 61

[Configuring TLS v1.2 only for an individual ESXi host](#) on page 62

[Validating TLS v1.0 and v1.1 disablement on an ESXi Host](#) on page 63

Installing the TLS Reconfigurator Utility Tool

About this task

For vCenter Server Appliance 6.5 U2, the version of the TLS Reconfigurator Utility Tool to install will be the following:

VMware-vSphereTlsReconfigurator-6.5.0-7766806.x86_64.rpm

Procedure

1. Go to My.VMware.com to download the .rpm file listed above for vCenter Server Appliance 6.5 U2.
2. Using WinSCP upload the .rpm file to a location on the vCenter Server Appliance.
3. Open an SSH session into the vCenter Server Appliance using the root credentials.
4. Locate the directory where the .rpm file was uploaded.
5. Run the following command to install the TLS Reconfigurator Utility Tool:

```
rpm -Uvh VMware-vSphereTlsReconfigurator-6.5.0-7766806.x86_64.rpm
```



```
[ ~ ]# rpm -Uvh VMware-vSphereTlsReconfigurator-6.5.0-7766806.x86_64.rpm
Preparing...                               ##### [100%]
Updating / installing...
 1:VMware-vSphereTlsReconfigurator-6##### [100%]
[ ~ ]#
```

Related links

[Management of the TLS protocol configuration for vSphere 6.5 U2 Environment](#) on page 59

Viewing Enabled TLS Version

About this task

Use the following procedure to identify the TLS versions enabled on your vCenter Server Appliance environment before making the TLS changes.

Procedure

1. Connect to the vCenter Server Appliance using SSH and administrative credentials.
2. Run the following command to navigate to the VcTlsReconfigurator directory.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3. Run the following command to view enabled TLS versions. The output of this command should be similar to the following example:

```
./reconfigureVc scan
```

```
===== Scanning vCenter Server TLS endpoints =====
```

Service Name	TLS Endpoint Port	TLS Version(s)
vmware-std	7444	TLSv1.0 TLSv1.1 TLSv1.2
vami-lighttp	5480	TLSv1.1 TLSv1.2
vmcam		NOT RUNNING
vmware-rhttpproxy	443	TLSv1.0 TLSv1.1 TLSv1.2
rsyslog	1514	TLSv1.0 TLSv1.1 TLSv1.2
vmddird	636	TLSv1.0 TLSv1.1 TLSv1.2
vmddird	11712	TLSv1.0 TLSv1.1 TLSv1.2
vmware-vpxd	8089	TLSv1.0 TLSv1.1 TLSv1.2
vmware-rbd-watchdog		NOT RUNNING
vmware-updatemgr	8084	TLSv1.0 TLSv1.1 TLSv1.2
vmware-updatemgr	9087	TLSv1.0 TLSv1.1 TLSv1.2
vsphere-client	9443	TLSv1.0 TLSv1.1 TLSv1.2
vsphere-ui	5443	TLSv1.2

Related links

[Management of the TLS protocol configuration for vSphere 6.5 U2 Environment](#) on page 59

Configuring TLS v1.2 only for vCenter Server Appliance and Platform Services Controller Appliance

About this task

Use the following procedure to disable TLS v1.0 and TLS v1.1 and enable v1.2 only for the vCenter Server Appliance and Platform Services Controller Appliance.

Before you begin

- Create a snapshot of the vCenter Server Appliance virtual machine before performing this procedure.
- The vCenter Server Appliance must be rebooted when all tasks in the procedure have been completed. Ensure this procedure is performed in a maintenance window where the temporary unavailability of the VCSA instance will not impact service.

Procedure

1. Open an SSH session into the vCenter Server Appliance.
2. Enable Bash shell by typing shell in the command line.
3. Run the following command to change to the following directory:

```
cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator
```

4. To disable TLSv1.0 and TLS v1.1 and enable only TLSv1.2, execute the following command:

```
./reconfigureVc update -p TLSv1.2
```

* Note:

It will provide a message stating that the vCenter Server is going to be restarted. Type **Y** to continue.

```

vCenter Transport Layer Security reconfigurator, version=6.5.0, build=7766906
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TLSReconfigurator/VcTlsReconfigurator.log".
vCenter Server is going to be restarted. Do you want to continue (Y/N)? Y
===== Backing up vCenter Server TLS configuration =====
Using backup directory: /tmp/20181030T215043
Backing up: vmware-std
Backing up: vami-lighttp
Backing up: vmcam
Backing up: vmware-rhttpproxy
Backing up: rsyslog
Backing up: vmdird
Backing up: vmware-vpxd
Backing up: vmware-rbd-watchdog
Backing up: vmware-updatemgr
Backing up: vsphere-client
Backing up: vsphere-ui
===== Scanning vCenter Server TLS endpoints =====
+-----+-----+-----+-----+
| Service Name | TLS Endpoint Port | TLS Version(s) |
+-----+-----+-----+-----+
| vmware-std | 7444 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vami-lighttp | 5480 | TLSv1.1 TLSv1.2 |
| vmcam | | NOT RUNNING |
| vmware-rhttpproxy | 443 | TLSv1.0 TLSv1.1 TLSv1.2 |
| rsyslog | 1514 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vmdird | 636 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vmdird | 11712 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vmware-vpxd | 8089 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vmware-rbd-watchdog | | NOT RUNNING |
| vmware-updatemgr | 8084 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vmware-updatemgr | 9087 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vsphere-client | 9443 | TLSv1.0 TLSv1.1 TLSv1.2 |
| vsphere-ui | 5443 | TLSv1.2 |
+-----+-----+-----+-----+

```

5. When the TLS change completes it will provide a list like the one below showing the enabled TLS version for each service.

```

===== Scanning vCenter Server TLS endpoints =====
+-----+-----+-----+-----+
| Service Name | TLS Endpoint Port | TLS Version(s) |
+-----+-----+-----+-----+
| vmware-std | 7444 | TLSv1.2 |
| vami-lighttp | 5480 | TLSv1.2 |
| vmcam | | NOT RUNNING |
| vmware-rhttpproxy | 443 | TLSv1.2 |
| rsyslog | 1514 | TLSv1.2 |
| vmdird | 636 | TLSv1.2 |
| vmdird | 11712 | TLSv1.2 |
| vmware-vpxd | 8089 | TLSv1.2 |
| vmware-rbd-watchdog | | NOT RUNNING |
| vmware-updatemgr | 8084 | TLSv1.2 |
| vmware-updatemgr | 9087 | TLSv1.2 |
| vsphere-client | 9443 | TLSv1.2 |
| vsphere-ui | 5443 | TLSv1.2 |
+-----+-----+-----+-----+

```

Related links

[Management of the TLS protocol configuration for vSphere 6.5 U2 Environment](#) on page 59

Configuring TLS v1.2 only for an individual ESXi host

About this task

Use the following procedure to disable TLS v1.0 and TLS v1.1 and enable TLS v1.2 only for an individual ESXi host

Before you begin

- The ESXi host must be rebooted for the change to take effect. Ensure this procedure is performed in a maintenance window where the temporary unavailability of the host will not impact service.
- When running the script on an individual ESXi host it will prompt for a password. This is the vCenter Server Appliance **root** or **administrator@vsphere.local** password.

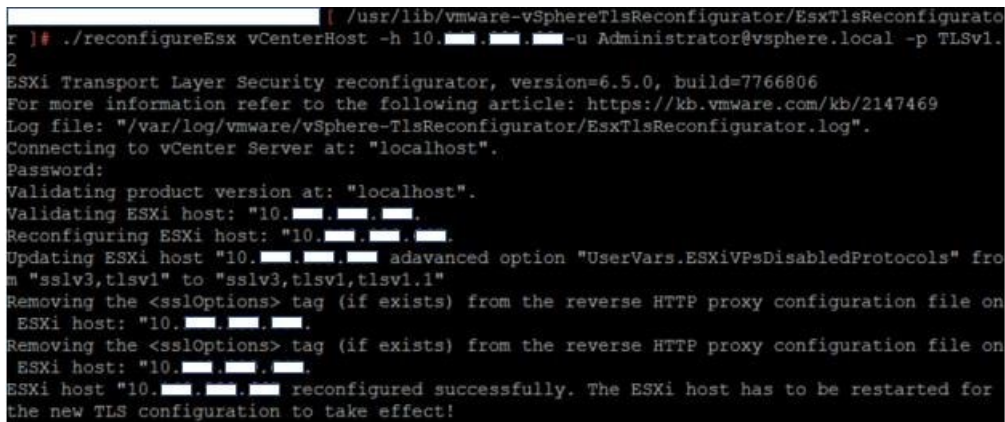
- Reverting TLS changes in an ESXi host is **not** supported.

Procedure

1. Open an SSH session into the vCenter Server Appliance.
2. Enable Bash shell by typing shell in the command line
3. Type the following command to change to the following directory:
4. To disable TLSv1.0 and TLS v1.1 and enable TLSv1.2 only on an individual ESXi host, execute the following command:

```
cd /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator
```

```
./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u <Administrative_User> -p TLSv1.2
```



```
[ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator
r ]# ./reconfigureEsx vCenterHost -h 10.10.10.10 -u Administrator@vsphere.local -p TLSv1.2
ESXi Transport Layer Security reconfigurator, version=6.5.0, build=7766806
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/EsxTlsReconfigurator.log".
Connecting to vCenter Server at: "localhost".
Password:
Validating product version at: "localhost".
Validating ESXi host: "10.10.10.10".
Reconfiguring ESXi host: "10.10.10.10".
Updating ESXi host "10.10.10.10" advanced option "UserVars.ESXiVPsDisabledProtocols" from
"sslsv3,tlsv1" to "sslsv3,tlsv1,tlsv1.1"
Removing the <sslOptions> tag (if exists) from the reverse HTTP proxy configuration file on
ESXi host: "10.10.10.10".
Removing the <sslOptions> tag (if exists) from the reverse HTTP proxy configuration file on
ESXi host: "10.10.10.10".
ESXi host "10.10.10.10" reconfigured successfully. The ESXi host has to be restarted for
the new TLS configuration to take effect!
```

Once completed, the host will be flagged for a reboot.

Related links

[Management of the TLS protocol configuration for vSphere 6.5 U2 Environment](#) on page 59

Validating TLS v1.0 and v1.1 disablement on an ESXi Host

About this task

Use the following procedure to validate if TLS v1.0 and v1.1 have been disabled on an ESXi host

Procedure

1. To validate TLS v1.0, disablement do the following:
 - a. Open an SSH session into the ESXi host.
 - b. Enable Bash shell by typing shell in the command line.
 - c. Type the following command to validate if TLS v1.0 has been disabled:

```
openssl s_client -connect localhost:443 -tls1
```

Command results should display that there is no certificate and no Master-Key assigned. See example below

```

---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1547763087
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)

```

If there is a peer certificate and a Master-Key listed, TLS v1.0 is still enabled.

2. To validate TLS v1.1 disablement, do the following:
 - a. Open an SSH session into the ESXi host.
 - b. Enable Bash shell by typing `shell` in the command line.
 - c. Type the following command to validate if TLS v1.1 has been disabled:

```
openssl s_client -connect localhost:443 -tls1_1
```

Command results should display that there is no certificate and no Master-Key assigned. See example below:

```

---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.1
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1547764137
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---

```

If there is a peer certificate and a Master-Key listed, TLS v1.1 is still enabled

Related links

[Management of the TLS protocol configuration for vSphere 6.5 U2 Environment](#) on page 59

Performing server recovery or software remastering

About this task

In the event of server failure, you should take necessary steps to recover the server data. You may also need to replace or remaster the system software on Avaya Solutions Platform 130 Appliance.

Before you begin

Ensure that you have the following:

- Console VGA monitor
- USB Keyboard
- Appropriate ESXi software downloaded from PLDS. See *PSN027079u- Avaya Converged Platform 130 Dell® R640 Customized Image of VMware ESXi 6.5 U2*.
- Latest Avaya certified BIOS/FW update for ACP 130. See *PSN027078u- Avaya Converged Platform 130 Dell® R640 Avaya Certified BIOS/FW Update*.

If you are replacing the server, first attempt to import the drives from the failed server. For more information, see [Replacing the host server](#) on page 71 and *Dell® R640 FRU Replacement Process*.

Procedure

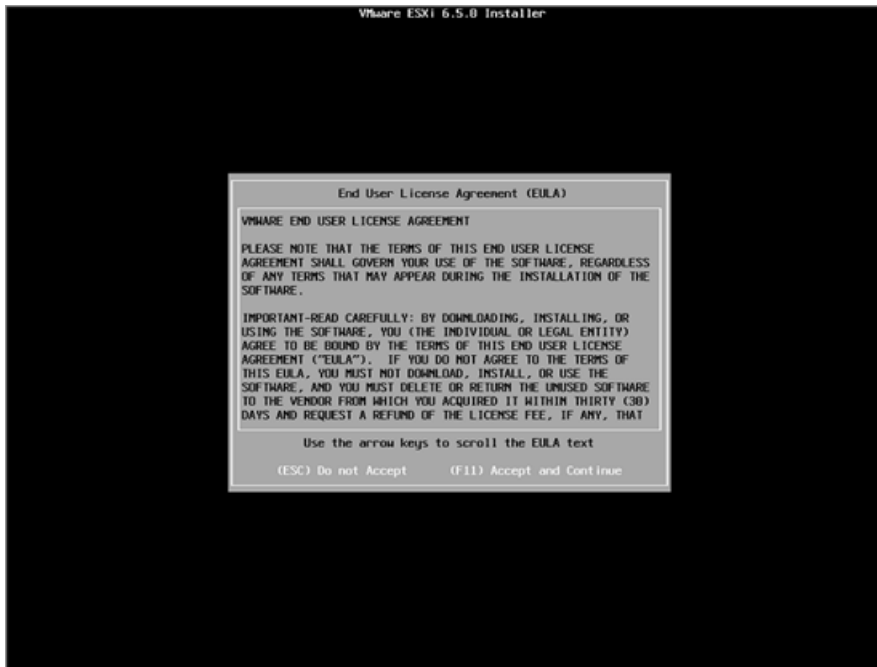
1. Download the ESXi installation ISO file from PLDS.
2. Burn the ESXi installation ISO file on a DVD.
3. Place the ESXi installation DVD in the DVD tray and boot the server.

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

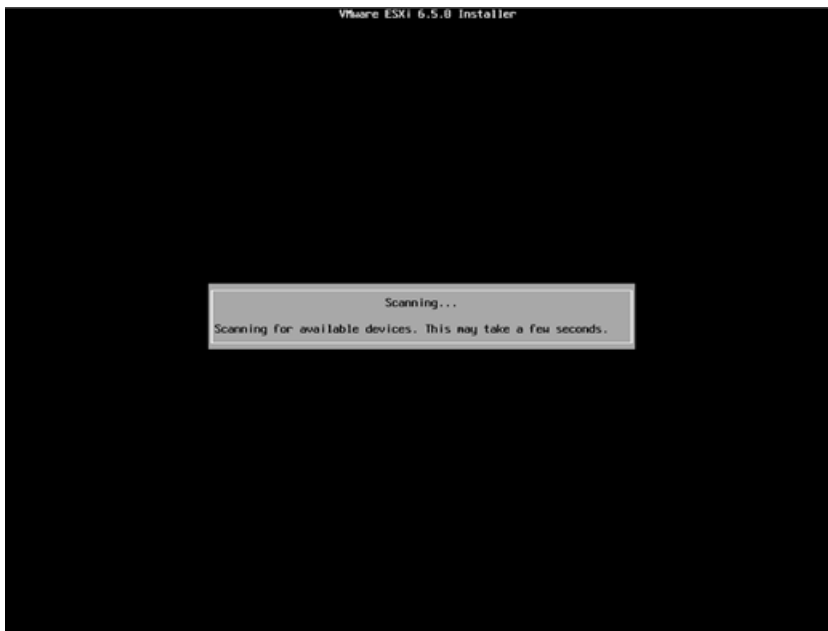
4. On the Welcome screen, press `Enter` to continue.



5. On the EULA screen, press **F11** to accept the EULA and continue the installation.



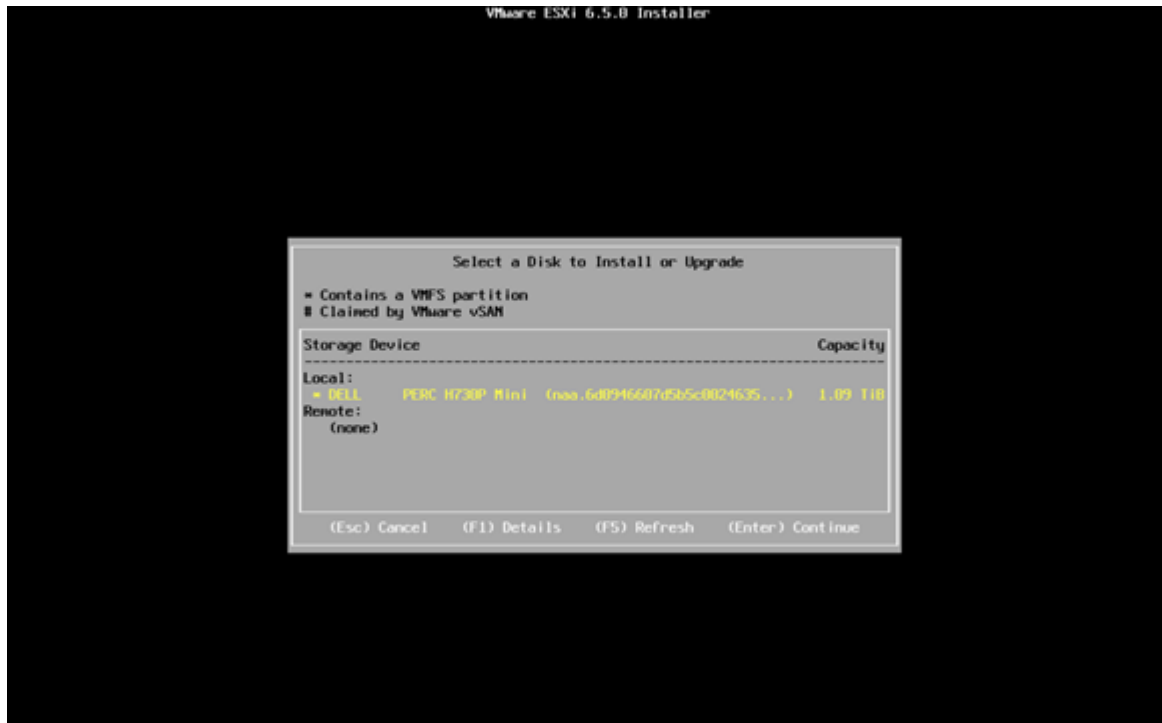
The installation program scans the server to identify all available drives to accept the software.



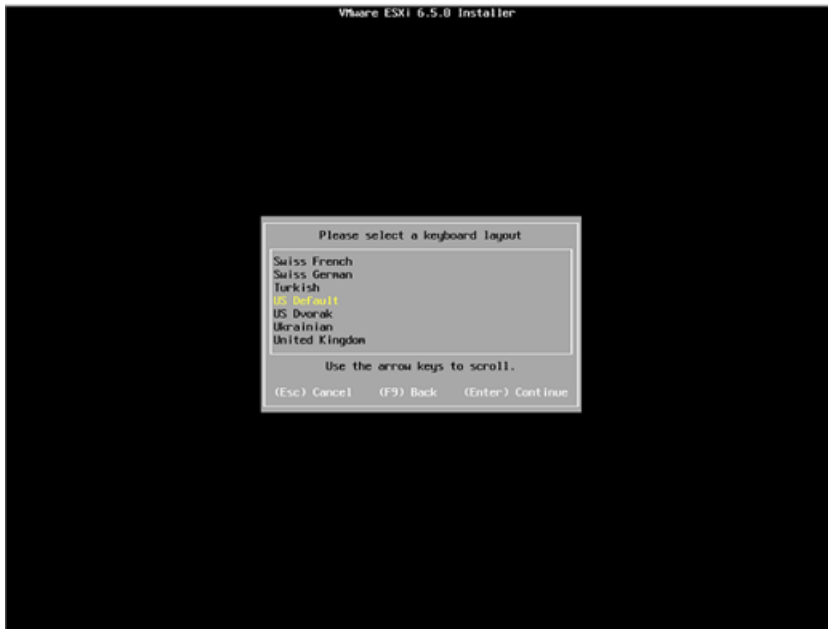
6. On the Select a Disk to Install or Upgrade screen, ensure that the PERC H730P Mini drive is highlighted and press **Enter** to continue.

*** Note:**

If the PERC H730P Mini is not displayed as a disk for installation, then configure the RAID Controller first. For more information, see [Dell R640 RAID Configuration](#) on page 73. Once the RAID configuration is complete, you can start the installation process again.



7. On the Please select a keyboard layout screen, use the arrow keys to select the language to be used on the ACP 130 solution, and press `Enter` to continue.



8. On the Enter a root password screen, type `ACP130_pw` in the **Root password** and **Confirm password** fields.
9. Press `Enter` to continue.



10. On the Confirm install screen, press F11 to confirm the installation of the software.



11. After the installation is complete, remove the DVD from the tray.



12. Press Enter to reboot and load the ESXi software.

The server will shutdown and reboot.

13. Proceed with the next steps.

Next steps

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

- Configure ESXi network settings. For more information, see [Configuring ESXi Network Settings](#) on page 33.
- Add the license key and install the license. For more information, see [Adding the license key for server recovery or software remastering](#) on page 72.
The license key is located on the server lid. If this is a server replacement, move the lid from the original server to the newly installed server.
- Enable the Services Port. For more information, see [Services Port Configuration](#) on page 53.

Replacing the host server

About this task

In the event of server failure, you may need to replace the host server on Avaya Solutions Platform 130 Appliance.

Before you begin

Ensure that you have the following:

- Console VGA monitor
- USB Keyboard
- Correct ESXi software downloaded from PLDS. See *PSN027079u- Avaya Converged Platform 130 Dell® R640 Customized Image of VMware ESXi 6.5 U2*
- Latest Avaya certified BIOS/FW update for ACP 130. See *PSN027078u- Avaya Converged Platform 130 Dell® R640 Avaya Certified BIOS/FW Update*

Procedure

1. Import the drives from the failed server. For more information, see *Dell® R640 FRU Replacement Process*.
2. Do one of the following:
 - If importing the drives is successful, reboot the server. Replacement server now has all previous configurations of ESXi.
If applicable, configure the iDRAC for remote access and alarming.
 - If importing the drives is not successful, configure the RAID array. For more information, see *Dell® R640 FRU Replacement Process*.
Update the BIOS/Firmware of the platform. For more information, see *PSN027078u- Avaya Converged Platform 130 Dell® R640 Avaya Certified BIOS/FW Update*.
3. Enable and configure iDRAC on the replacement server. For more information, see *Avaya Converged Platform 130 Series iDRAC9 Best Practices*.

Next steps

Continue with the procedure to perform server recovery.

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:

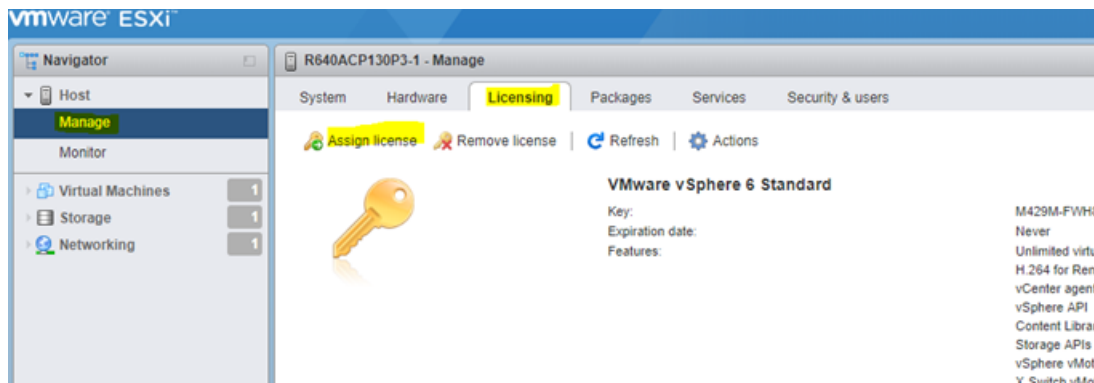
- Take the VMware license key from the original server lid.
- Move the original server lid to the new ACP 130 server if you are replacing the server.

Procedure

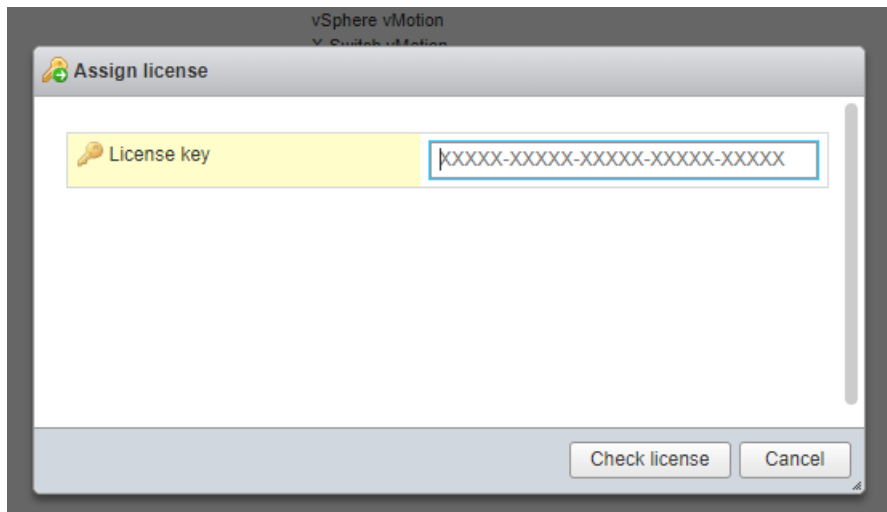
1. Log in to the ESX/ESXi host at the URL `https://[IP Address of host]/ui`.

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

2. In the Navigator pane on the left, click **Manage**.
3. On the **Licensing** tab, click **Assign license**.



4. In the Assign license window, enter the license key in the **License key** field.



5. Click **Check license**.
6. After the license checking is complete, click **Assign license**.

Dell USB R640 RAID Configuration

Introduction

The Dell R640 RAID controller (H730P Mini) 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) for Avaya Solutions Platform (ACP) 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 prepare the Dell R640 RAID controller (H730P Mini) for Avaya ACP 1XX RAID Array configuration. For that, you must delete all the existing configurations from the controller.

! 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.

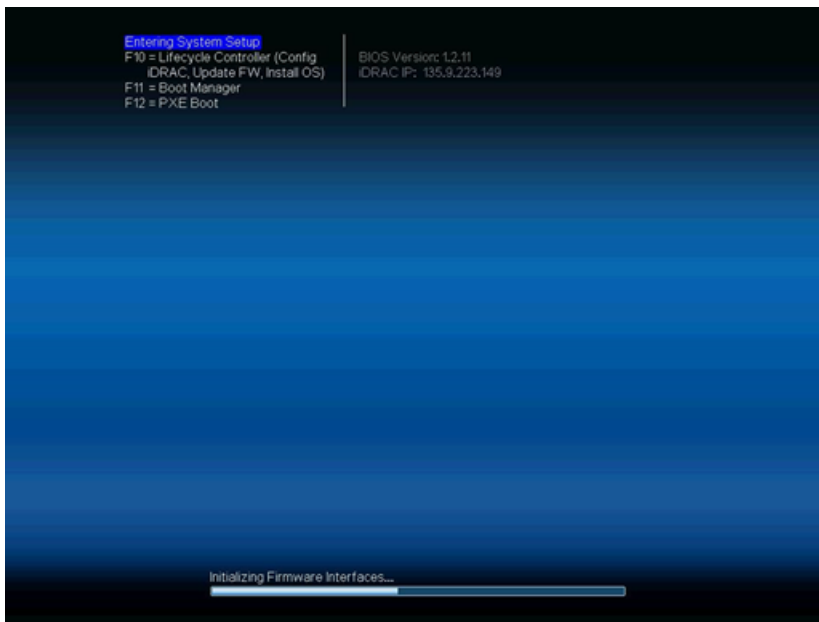
Before you begin

- Connect your VGA monitor, USB keyboard, and USB mouse to the server.
- Power up the server.

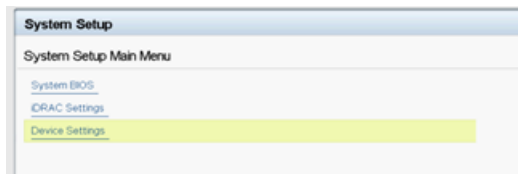
Procedure

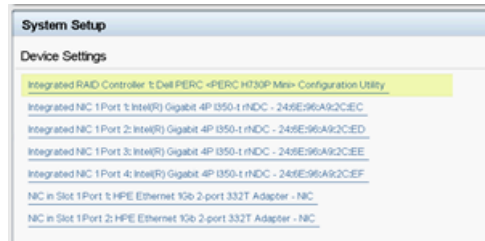
1. When the hardware boot screen appears, select **<F2>System Setup**.

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



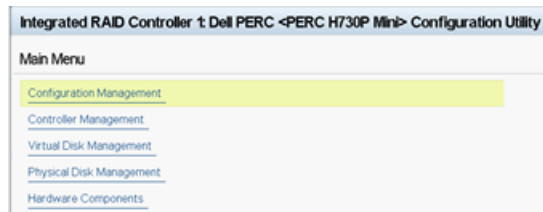
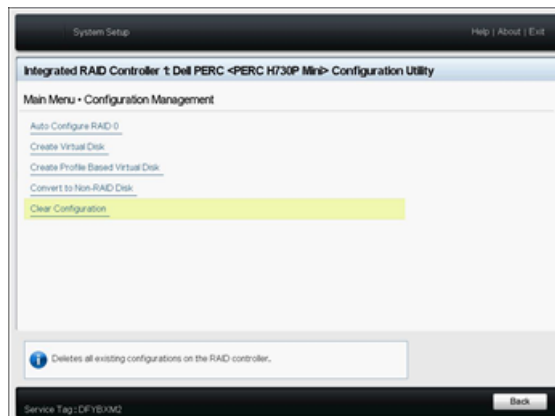
2. Clear all existing arrays by doing the following:
 - a. Click **Device Settings > Integrated RAID Controller 1: Dell <PERC H730P Mini> Configuration Utility**.



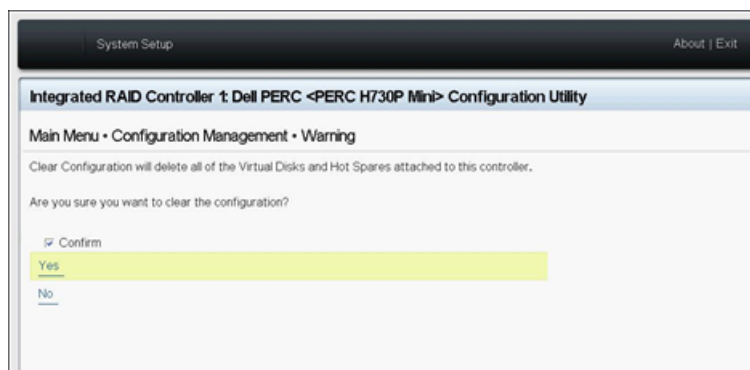


- b. On the Main Menu, click **Configuration Management > Clear Configuration**.

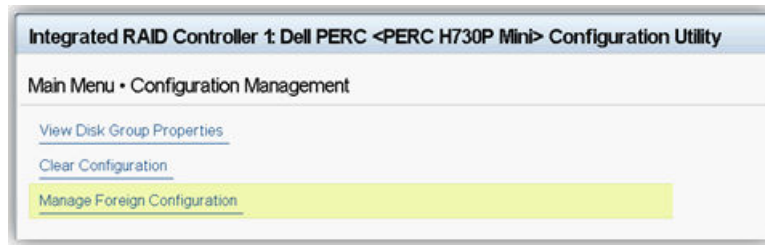
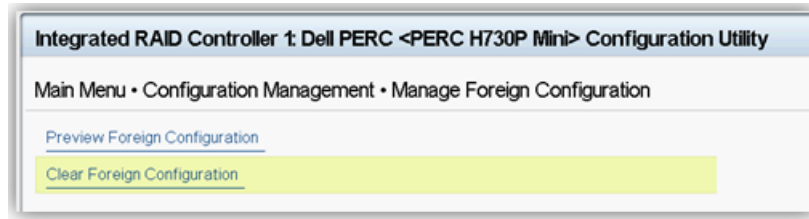
This command deletes all existing configurations from the RAID controller.



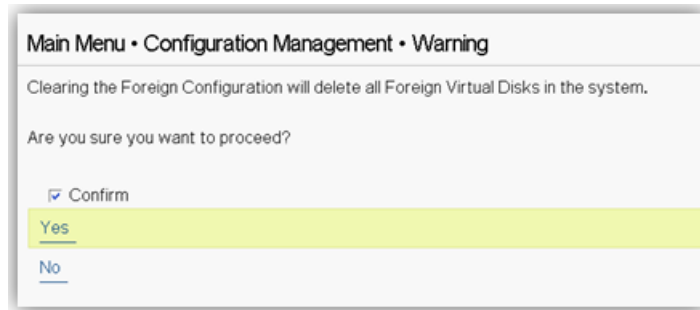
- c. Check the **Confirm** box, select **Yes**, and click **OK**.



- 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 76 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.

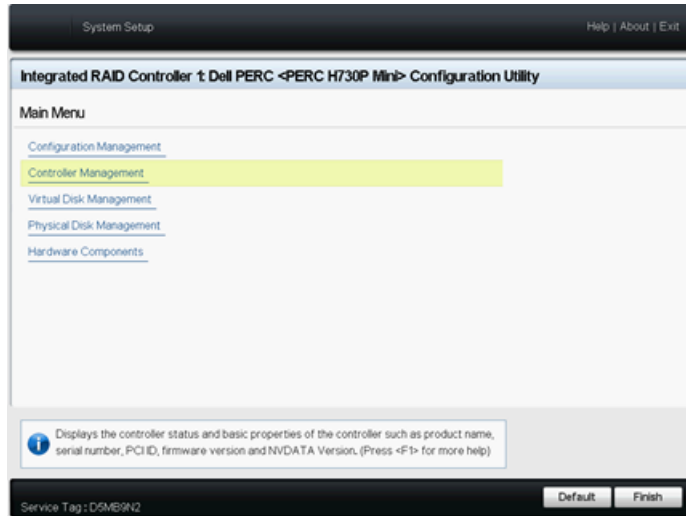
Before you begin

Delete all existing configurations on the RAID controller.

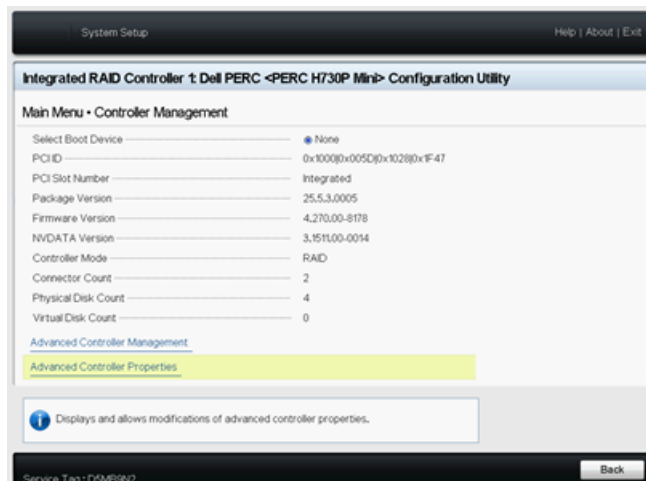
Procedure

1. On the **Main Menu** of **Integrated RAID Controller 1: Dell <PERC H730P Mini> Configuration Utility**, click **Controller Management**.

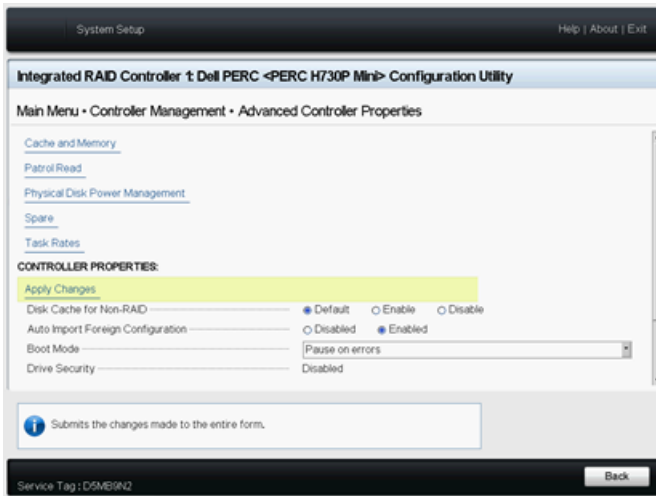
This section displays and allows modifications of the advance controller properties.



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



3. Under Controller Properties, set **Auto Import Foreign Configuration** to **Enabled**.



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

Next steps

Proceed to [Creating a virtual disk](#) on page 78 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

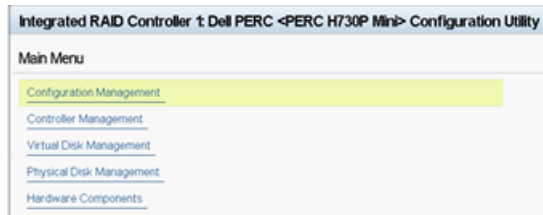
Use this procedure to create a virtual disk by selecting the RAID level, physical disks, and virtual disk parameters.

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**.

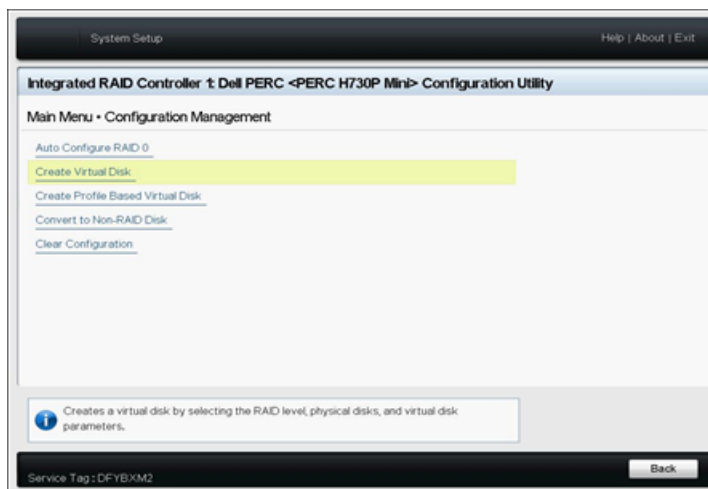
Procedure

1. On the **Main Menu** of **Integrated RAID Controller 1: Dell <PERC H730P Mini> Configuration Utility**, 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.



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. In **Virtual Disk Name**, do not change the default value, that is, VD0, unless you are specified another Virtual Disk Name.
 - 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 81.

8. Click **Create Virtual Disk**.

System Setup Help | About | Exit

Integrated RAID Controller 1: Dell PERC <PERC H730P Mini> Configuration Utility

Main Menu • Configuration Management • Create Virtual Disk

Create Virtual Disk

Select RAID Level: RAID6

☐ Secure Virtual Disk

Select Physical Disks From: ☒ Unconfigured Capacity ☐ Free Capacity

Select Physical Disks

CONFIGURE VIRTUAL DISK PARAMETERS:

Virtual Disk Name: VD0

Virtual Disk Size: 1090

Virtual Disk Size Unit: ☐ MB ☐ GB ☒ TB

Strip Element Size: 256 KB

Read Policy: ☐ No Read Ahead ☒ Read Ahead

Write Policy: ☒ Write Back ☐ Write Through ☐ Force Write Back

Submits the changes made to the entire form and creates a virtual disk with the specified parameters.

Service Tag : D5MB9H2 Back

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 82 for the steps to check the basic properties of a specific virtual disk.

Virtual disk size

The configuration of the RAID controller is possible only with the specification of the data storage space available. 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	ACP 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	
6	6x600 GB = 3.6 TB	2.4	2.18	5
6	7x600 GB = 4.2 TB	3.0	2.73	
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.

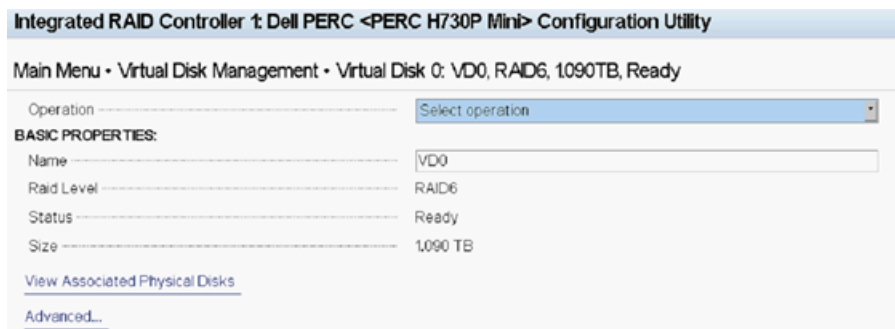
Procedure

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

The system shows the virtual disks available.



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



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.

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 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 Health
- Storage Health
- Updates
- Audit
- Configuration

Configuring SNMP v2c alerts using iDRAC9

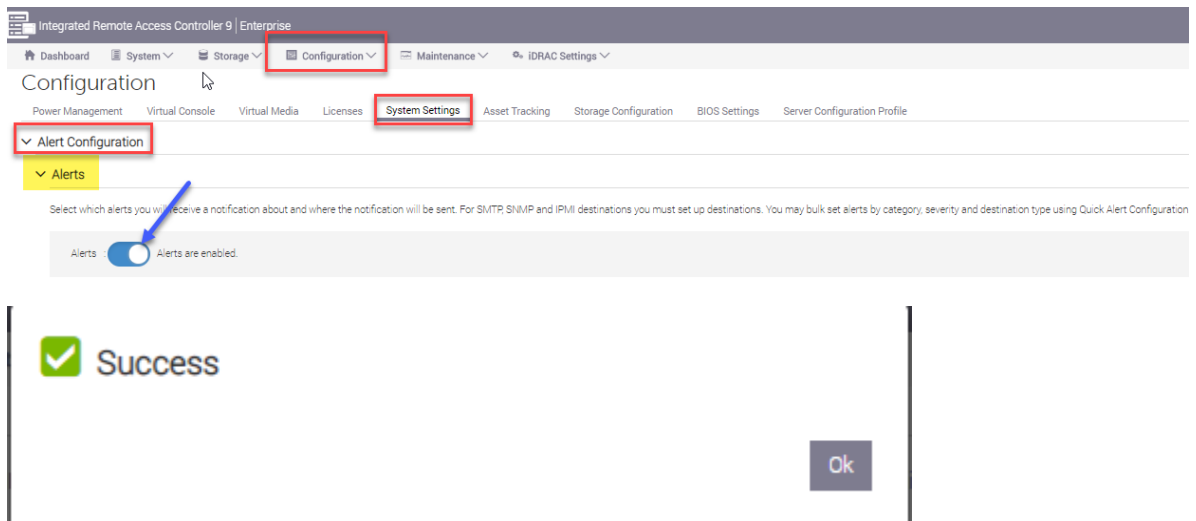
Before you begin

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

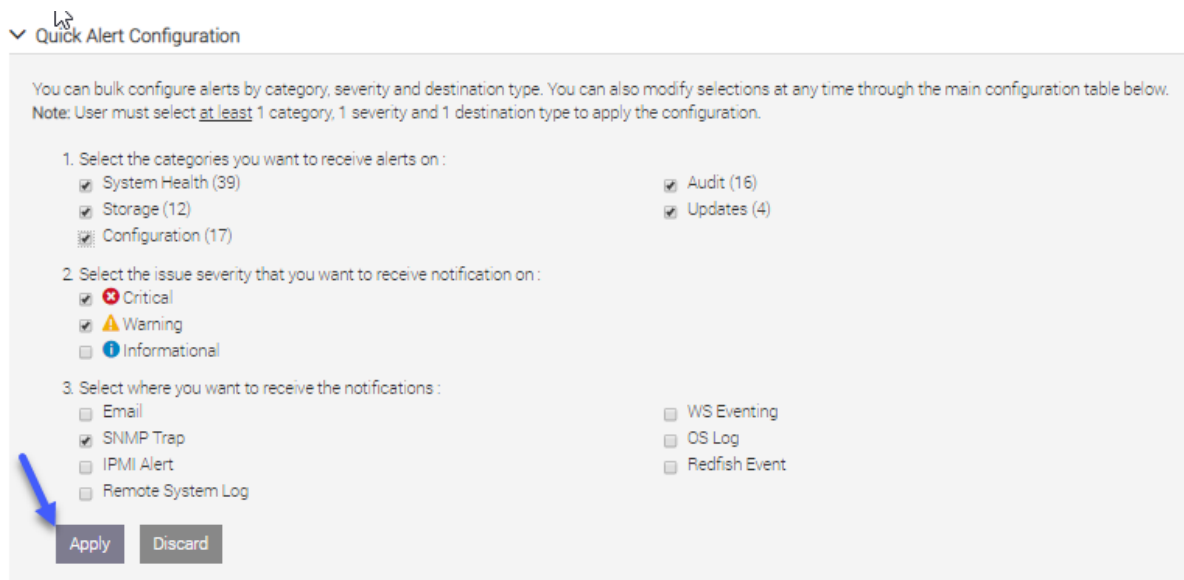
Procedure

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.

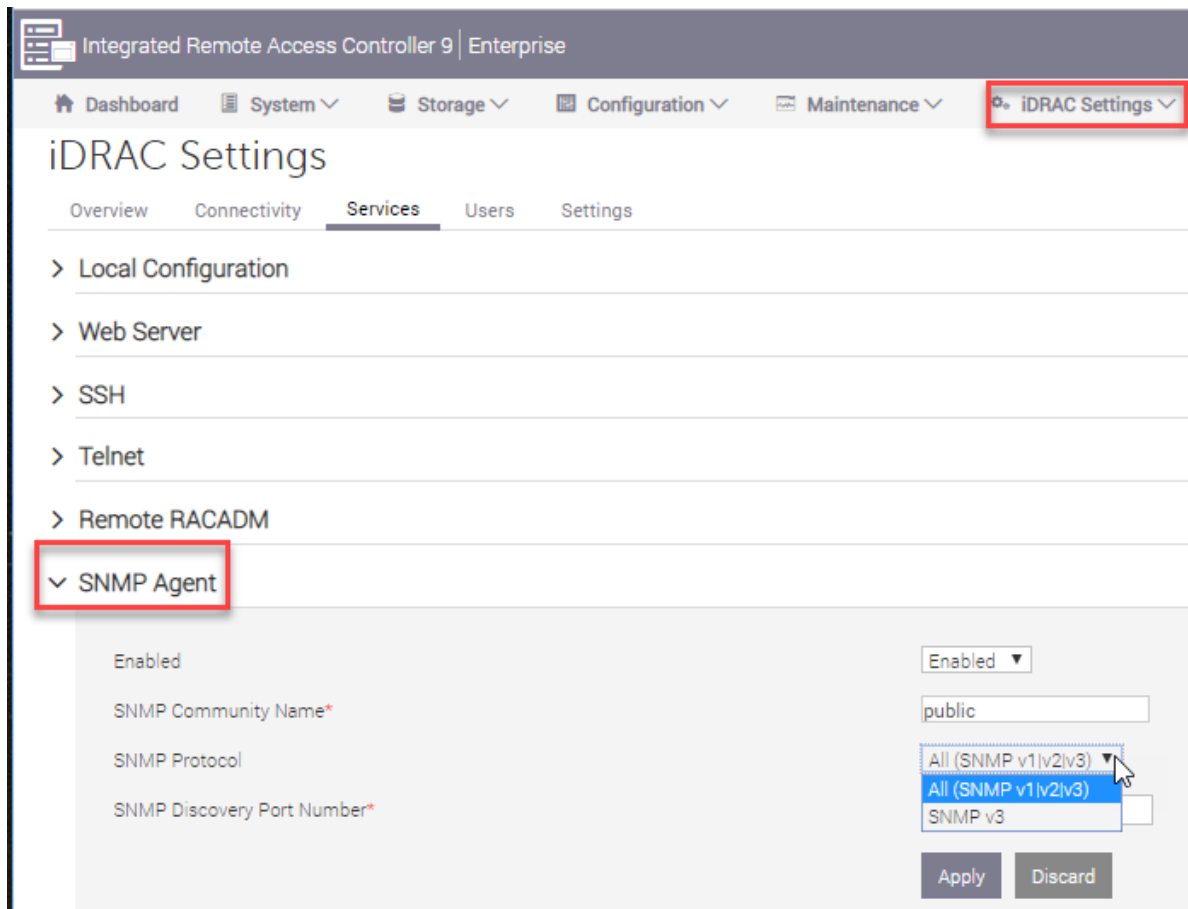
- A Success message will display. Click **OK**.



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.

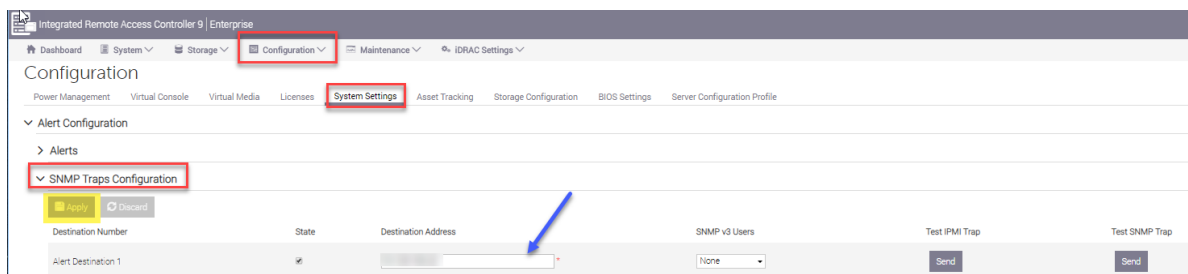


3. Redirect to **iDRAC Settings > Services > SNMP Agent**.
 - From the Enable drop-down menu, select **Enable**.
 - Enter the **SNMP Community Name**. The name "Public" is an indication of "read only" access permitted by SNMP agents.
 - From the **SNMP Protocol** drop-down menu, select **All** to enable SNMP v2c.
 - Click **Apply** to submit changes.



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.



5. 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 **SNMPv2**.

The screenshot shows the iDRAC9 Enterprise Configuration page. The 'Configuration' tab is selected, and the 'System Settings' sub-tab is active. Under 'Alert Configuration', the 'SNMP Traps Configuration' section is expanded. It features a table with 8 rows for 'Alert Destination' (1-8). Each row has columns for 'State' (checkbox), 'Destination Address' (text input), 'SNMP v3 Users' (dropdown), 'Test IPMI Trap' (Send button), and 'Test SNMP Trap' (Send button). Below the table, the 'SNMP Settings' section is highlighted, showing 'Community String' (avaya123), 'SNMP Alert Port Number' (162), and 'SNMP Trap Format' (SNMPv2). The 'SNMPv2' option is selected in the dropdown menu.

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.

* Note:

The command to remove the SNMP config (reset the configuration to factory default) is:

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

Configuring SNMP v2c traps for Dell R640 using iDRAC9

About this task

You can configure SNMP v2c 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 *Avaya iDRAC9 Best Practices* document for configuring the iDRAC.

Procedure

1. Navigate to **Configuration > System settings > SNMP Traps Configuration**.

The values shown in the following screenshot are only examples. The values may vary based on your requirements.

SNMP Traps Configuration

Apply Discard

Destination Number	State	Destination Address	SNMP v3 Users	Test IPMI Trap	Test SNMP Trap
Alert Destination 1	☒	195.9.0.0/24	jdoe	Send	Send

2. Select the **State** check box.
3. In the **Destination Address** field, enter the destination IP address of the SNMP receiver.
4. * **Note:**

Execute this step only if SNMP v3 traps are set.

(Optional) In the **SNMP v3 Users** field, click the drop-down arrow and click the user account that is enabled for SNMP v3.

To associate a user account with SNMP v3 traps, see Editing a user account to enable it for SNMP v3 traps.

5. In the **Community String** field, enter the SNMP community string value.
6. In the **SNMP Trap Format** field, click the required value.

The values shown in the following screenshot are only examples. The values may vary based on your requirements.

SNMP Settings

Community String* public

SNMP Alert Port Number* 162

SNMP Trap Format SNMP v3

Apply Discard

7. Click **Apply**.

Next steps

After the SNMP traps are configured, you can send a test SNMP trap to confirm the configuration by clicking the **Send** option in the **Test SNMP Trap** column.

- * **Note:**

The command to remove the SNMP config (reset the configuration to factory default) is:

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

Configuring SNMP v3 traps for Dell R640 using iDRAC9

About this task

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

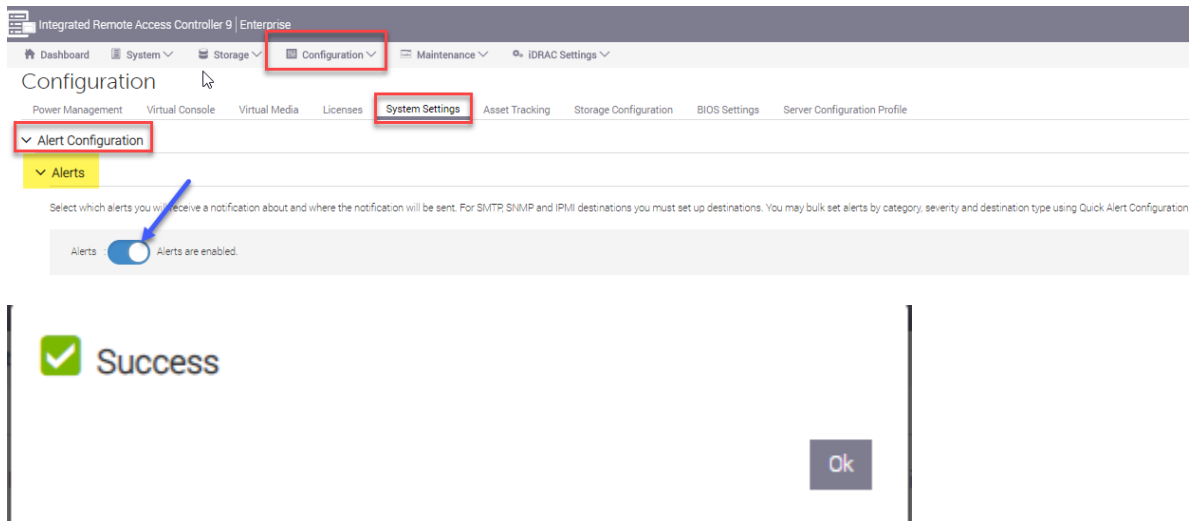
Before you begin

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

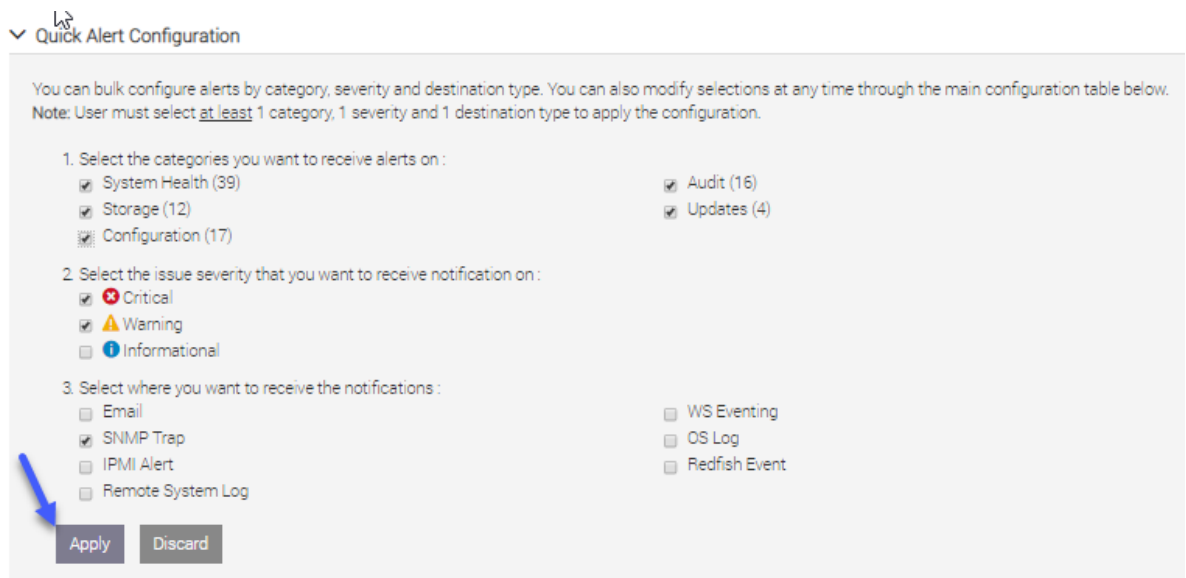
Procedure

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 Enable drop-down menu, select **Enable**.
- Enter the **SNMP Community Name**. The name “Public” is an indication of “read only” access permitted by SNMP agents.
- From the **SNMP Protocol** drop-down menu, select **SNMP v3**.
- Click **Apply** to submit changes.

Integrated Remote Access Controller 9 | Enterprise

Dashboard System Storage Configuration Maintenance **iDRAC Settings**

iDRAC Settings

Overview Connectivity **Services** Users Settings

> Local Configuration

> Web Server

> SSH

> Telnet

> Remote RACADM

▼ **SNMP Agent**

Enabled Enabled ▼

SNMP Community Name*

SNMP Protocol SNMP v3 ▼

SNMP Discovery Port Number*

Apply **Discard**

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

Integrated Remote Access Controller 9 | Enterprise

Dashboard System Storage Configuration Maintenance **iDRAC Settings**

iDRAC Settings

Overview Connectivity Services **Users** Settings

▼ Local Users

+Add **Edit** **Disable** **Delete**

ID	User Name	State	User Role	IPMI LAN Privilege	IPMI Serial Privilege	Serial Over LAN	SNMP v3
2	root	Enabled	Administrator	Administrator	Administrator	Enabled	Disabled
3							
4	admin	Enabled	Operator	No Access	No Access	Disabled	Enabled

*** 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.

Add New User ?

User Account Settings

ID 5 ▼

User Name* avaya

Password* *****

Confirm Password* *****

User Privileges

User Role None ▼

☐ Login to iDRAC	☐ Configure iDRAC	☐ Configure Users
☐ Clear Logs	☐ Control and Configure System	☐ Access Virtual Console
☐ Access Virtual Media	☐ Test Alerts	☐ Execute Debug Commands

Close
Save

6. Administer the bottom half of the form: **Advanced Settings > SNMP v3 Settings**.

- 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.
 - If the same **User Name** and **password** is to be used for both, select **MD5** and **AES** respectively.
 - If only 1 of the protocols will be associated with the new **User Name**, select one of the noted protocol types from the appropriate drop-down menu and select **None** for the protocol that will be assigned its own User Name. Repeat the process for the second User Name-Protocol assignment.
- Click **Save** to apply the administration and then click **Close**.

Add New User ?

Advanced Settings

IPMI User Privileges

LAN Privilege Level None ▼

Serial Port Privilege Level None ▼

Serial Over LAN Disabled ▼

SNMP v3 Settings

SNMP v3 Enabled ▼

Authentication Type MD5 ▼

Privacy Type AES ▼

DES

AES

None

Close Save

7. Return to **Configuration > System Settings > SNMP Traps Configuration**.

- Enter the IP address of the SAL GW in the **Destination Address** field. If there is more than 1 SAL, 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.

Integrated Remote Access Controller 9 | Enterprise

Dashboard System Storage **Configuration** Maintenance iDRAC Settings

Configuration

Power Management Virtual Console Virtual Media Licenses **System Settings** Asset Tracking Storage Configuration BIOS Settings Server Configuration Profile

Alert Configuration

Alerts

SNMP Traps Configuration

Apply Discard

Destination Number	State	Destination Address	SNMP v3 Users	Test IPMI Trap	Test SNMP Trap
Alert Destination 1	☒	<input type="text"/>	None	Send	Send

The screenshot shows the iDRAC9 Enterprise web interface. The navigation menu includes Dashboard, System, Storage, Configuration (highlighted), Maintenance, and iDRAC Settings. Under Configuration, the System Settings sub-menu is selected. The main content area shows the 'Alert Configuration' section, specifically 'SNMP Traps Configuration'. It features a table with columns for Destination Number, State, Destination Address, SNMP v3 Users, Test IPMI Trap, and Test SNMP Trap. Below the table is the 'SNMP Settings' section with fields for Community String, SNMP Alert Port Number, and SNMP Trap Format.

Destination Number	State	Destination Address	SNMP v3 Users	Test IPMI Trap	Test SNMP Trap
Alert Destination 1	☒		None	Send	Send
Alert Destination 2	☒		None	Send	Send
Alert Destination 3	☒		None	Send	Send
Alert Destination 4	☒		None	Send	Send
Alert Destination 5	☐		None	Send	Send
Alert Destination 6	☐		None	Send	Send
Alert Destination 7	☐		None	Send	Send
Alert Destination 8	☐		None	Send	Send

SNMP Settings

Community String:

SNMP Alert Port Number:

SNMP Trap Format:

Buttons: Apply, Discard

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**.

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.

* **Note:**

The command to remove the SNMP config (reset the configuration to factory default) is:

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

Configuring a user account for SNMP v3 traps

About this task

To configure an SNMP v3 traps, you must associate a user account with the traps. The password of this user account is used to encrypt the SNMP v3 traps. The same password must be used by the SNMP v3 trap receiver to decrypt trap information.

Before you begin

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

Procedure

1. Navigate to **iDRAC Settings > Users**.

iDRAC Settings

Overview Connectivity Services **Users** Settings

Local Users

Details Add Edit Disable Delete

ID	User Name	State	User Role	IPMI LAN Privilege	IPMI Serial Privilege	Serial Over LAN	SNMP v3
2	root	Enabled	Administrator	Administrator	Administrator	Enabled	Enabled
3	don	Enabled	Administrator	Administrator	Administrator	Enabled	Enabled
4	jdoe	Enabled	None	No Access	No Access	Disabled	Enabled

2. In the Local Users section, select the user that you want to edit for SNMP v3 traps.
3. Click **Edit**.
4. On the User Configuration tab, scroll down to the Advanced settings section.

Edit User

User Configuration SSH Key Configurations Smart Card Configuration

Advanced Settings

IPMI User Privileges

LAN Privilege Level

Serial Port Privilege Level

Serial Over LAN

SNMP v3 Settings

SNMP v3

Authentication Type

Privacy Type

Close Save

5. In the **SNMP v3** field click **Enabled**.
6. In the **Authentication type** field, click the required authentication type.
7. In the **Privacy type** field, click the required privacy type.
8. Click **Save**.

Chapter 6: Configuration Guidelines

Preface

Intended Audience

This chapter is intended for Avaya professional services, partners, and customers that have been tasked to install and configure an ACP 130 Release 1.0.

Purpose

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

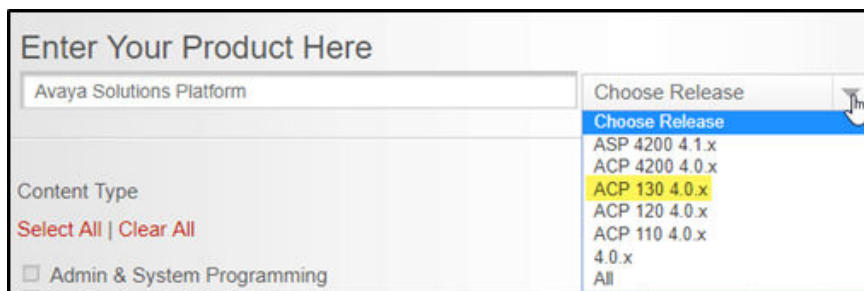
Scope

This chapter only includes the procedures and steps to implement suggested ACP 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 ACP 130 offer. It is advised that users refer to the <http://support.avaya.com/> website for the latest version of all ACP 130 documentation.



* Note:

Use of the Command Line interface to configure the server is not recommended unless specified.

Configuring Core Network Administration

Default Configuration

All ACP 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 Services. 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 use a different subnet mask than vSwitch0 or vSwitch1 for NIC Teaming. Avaya recommends that vSwitch2-5 be assigned to those other 4 NIC ports.

*** Note:**

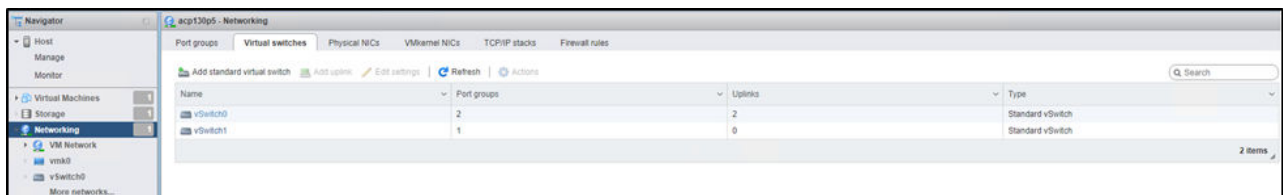
If you are using NIC Teaming, you will lose a physical NIC port for each vSwitch you will be teaming with.

Administer the foundational network configuration.

vSwitch Administration

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

- vSwitch 0
 - Assigned to all VM and ESXi management packet traffic
 - Associated to VMkernel NIC 0 for ESXi IP support
- vSwitch 1
 - Exclusively assigned to the direct-connect services port
 - No VM traffic should be assigned to this vSwitch
 - Associated to VMkernel NIC 1 for IP interaction between direct-connect PC and the server



*** Note:**

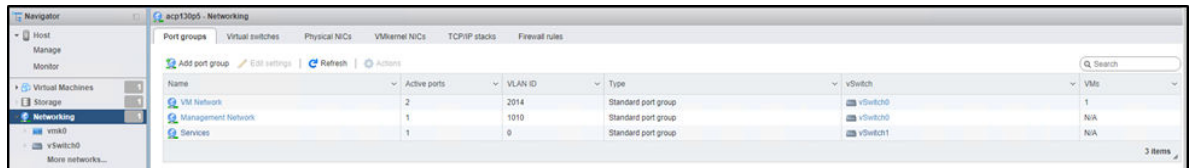
If Out of Band Management (OOBM) is desired in the configuration, an additional vSwitch (vSwitch2-5) should be created to carry the non-management traffic. It is recommended that the VMnetwork port group associated with this new vSwitch is named "Public". It is also recommended that VMkernel port groups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

Configure the Port Groups

Procedure

1. From the **Navigator** menu to the left, select the **Networking** option. Then select the **Port Groups** tab.

The port groups noted below will come standard and already configured inside the ESXi host. Any additional port groups desired by the customer may be added here, by selecting the **Add port group** option.



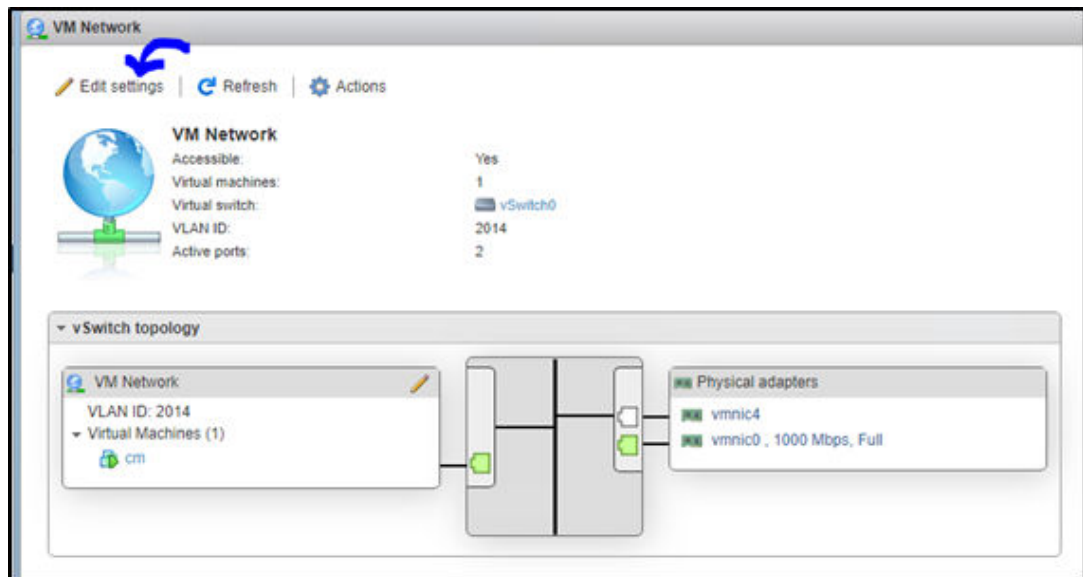
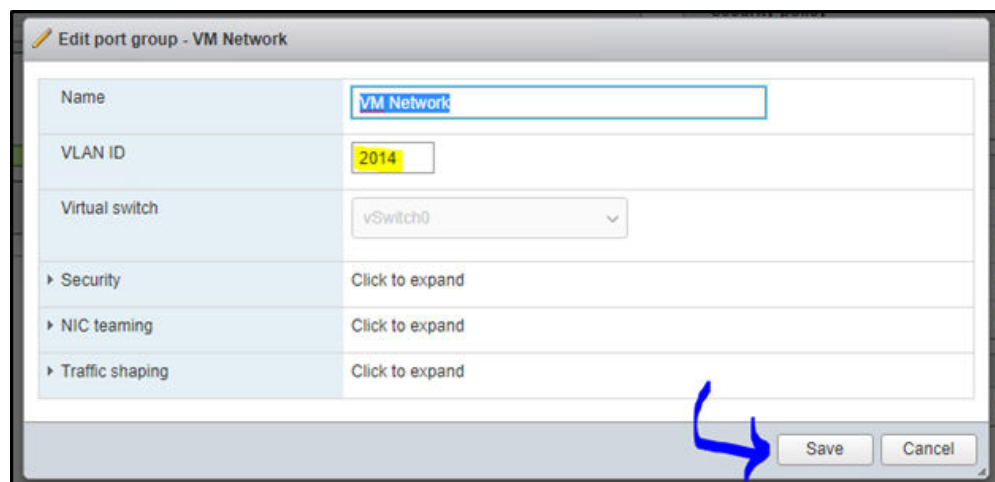
Add port group - New port group

Name	New port group
VLAN ID	0
Virtual switch	vSwitch0
Security	
Promiscuous mode	☐ Accept ☐ Reject ☒ Inherit from vSwitch
MAC address changes	☐ Accept ☐ Reject ☒ Inherit from vSwitch
Forged transmits	☐ Accept ☐ Reject ☒ Inherit from vSwitch

Buttons: Add, Cancel

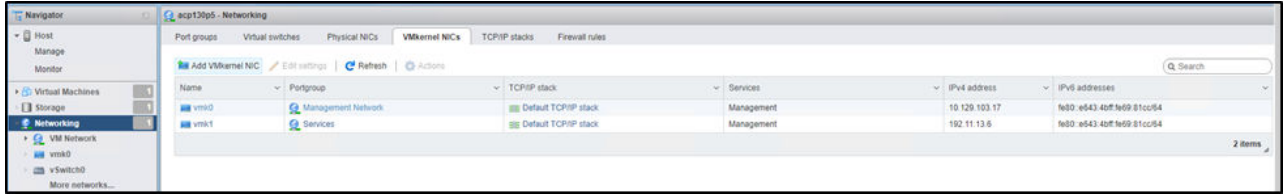
2. The VLAN tags noted in the example will not necessarily be administered. Work with your network team to decide how/if the different port group (networks) will be tagged. When a

value has been identified, click the port group that requires editing, and from the subsequent window, select **Edit Settings**, add the appropriate VLAN ID, and click **Save**.



VMkernel NIC Administration

VMkernel NICs also have been configured in the delivered ACP 130 server. Below are the two administered values that come as part of the standard configuration. A VMkernel NIC will only be required for NICs that need an IP address assigned to them for specific management/support purposes. In this case, VMkernel NICs are assigned for the services and ESXi management to allow remote access into the server via specific IP addresses.



* Note:

It is recommended that additional VMkernel NICs are not added or deleted from the Avaya-provided configuration.

Application Deployment on the ACP 130

Refer to your VE deployment guides for the procedure to install your application software on a stand-alone ACP 130 server.

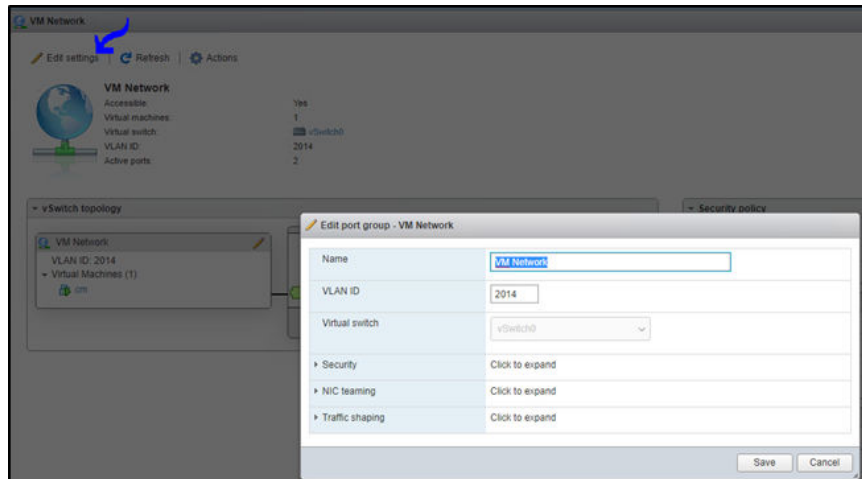
Before deploying any virtual machines, refer to the policies in *Policies for technical support of the Avaya Solutions Platform (ASP) 130*.

ACP 130 VLAN Tagging

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. Likewise, other NICs may also be shared by virtual machines supported across disparate networks.

The use of VLAN tagging will help support the network port-trunking infrastructure.

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 ACP 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.



*** Note:**

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

ACP 130 NIC Teaming

NIC Teaming is recommended to provide a redundant path for the management and VM traffic. For some of VMware's best practices and guidelines, refer to the following documents:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/landing-pages/virtual-support-day-best-practices-virtual-networking-june-2012.pdf>

<https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html>

Configure ESXi Management Interfaces in the Server for NIC Teaming

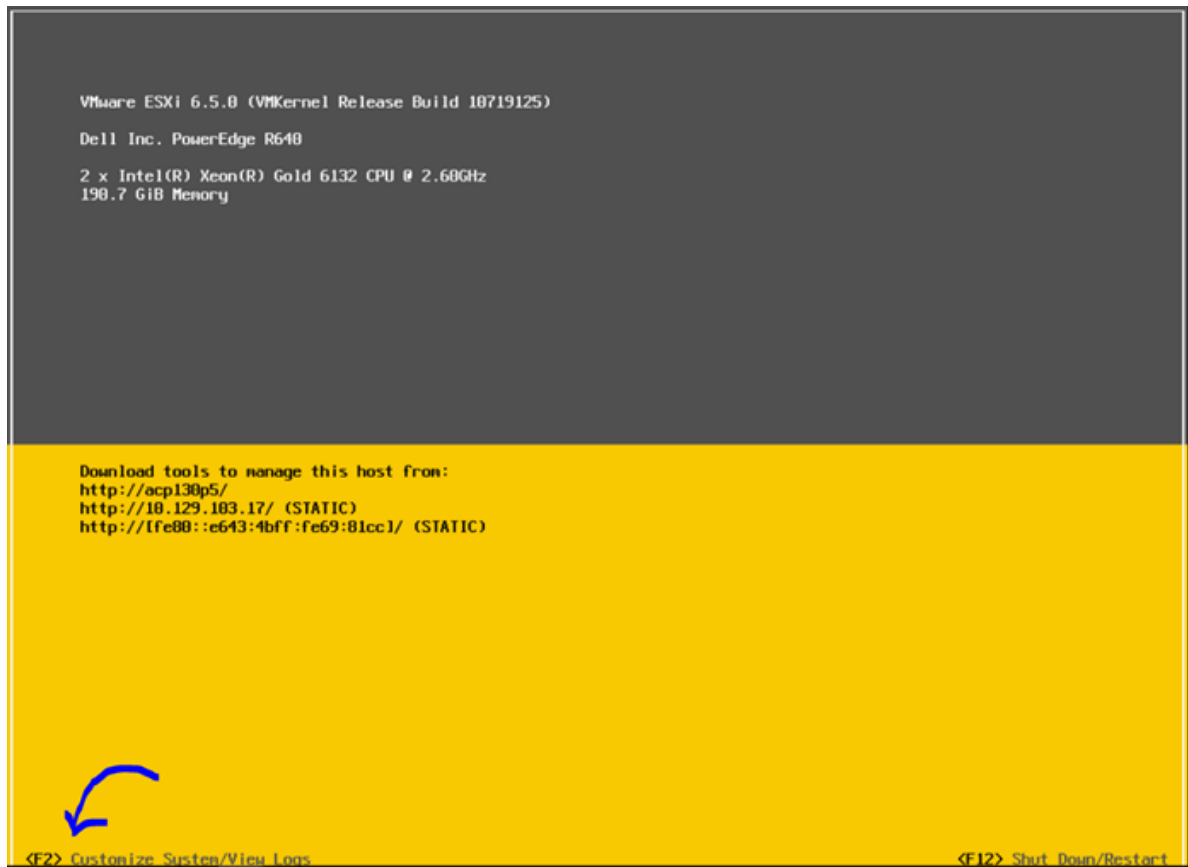
About this task

ESXi management information can also be applied to a NIC Teaming configuration. The following guidelines will help to configure the proper NICs on the server for that functionality.

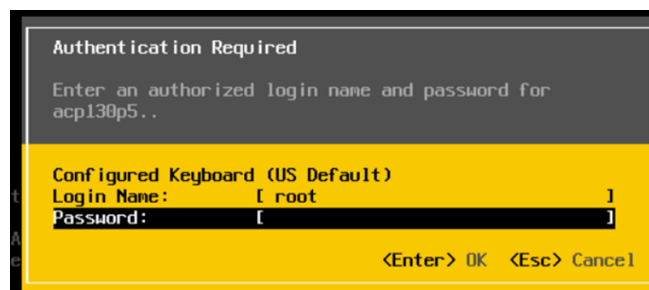
Procedure

1. Connect a keyboard, mouse, and monitor to the server and access the console locally.
A subsequent window will open.

2. Click inside the darkened screen that appears and press **Return**. The image shown below will be presented:

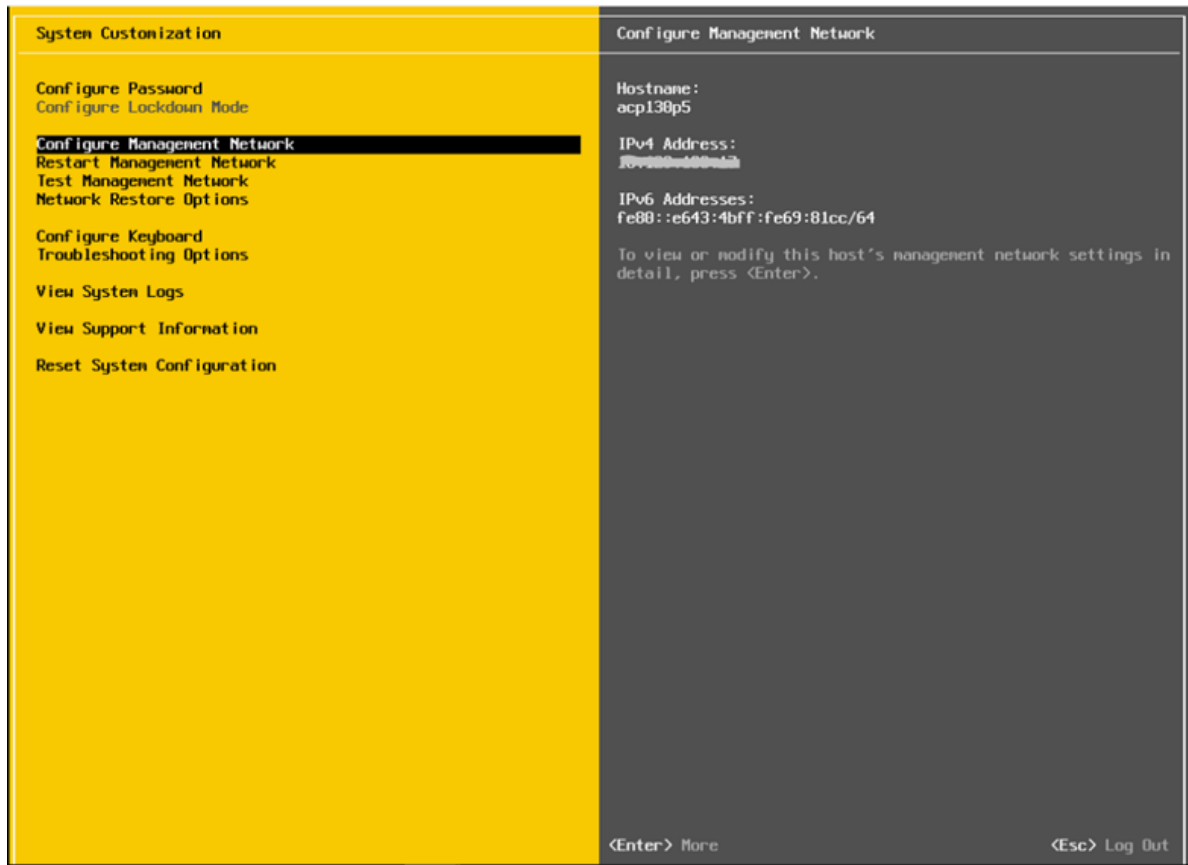


3. Once you see the console image, select **F2** to enter the System Customization menu.
4. When prompted to login to the ESXi console, use the `root` credential and password and press **Enter**.

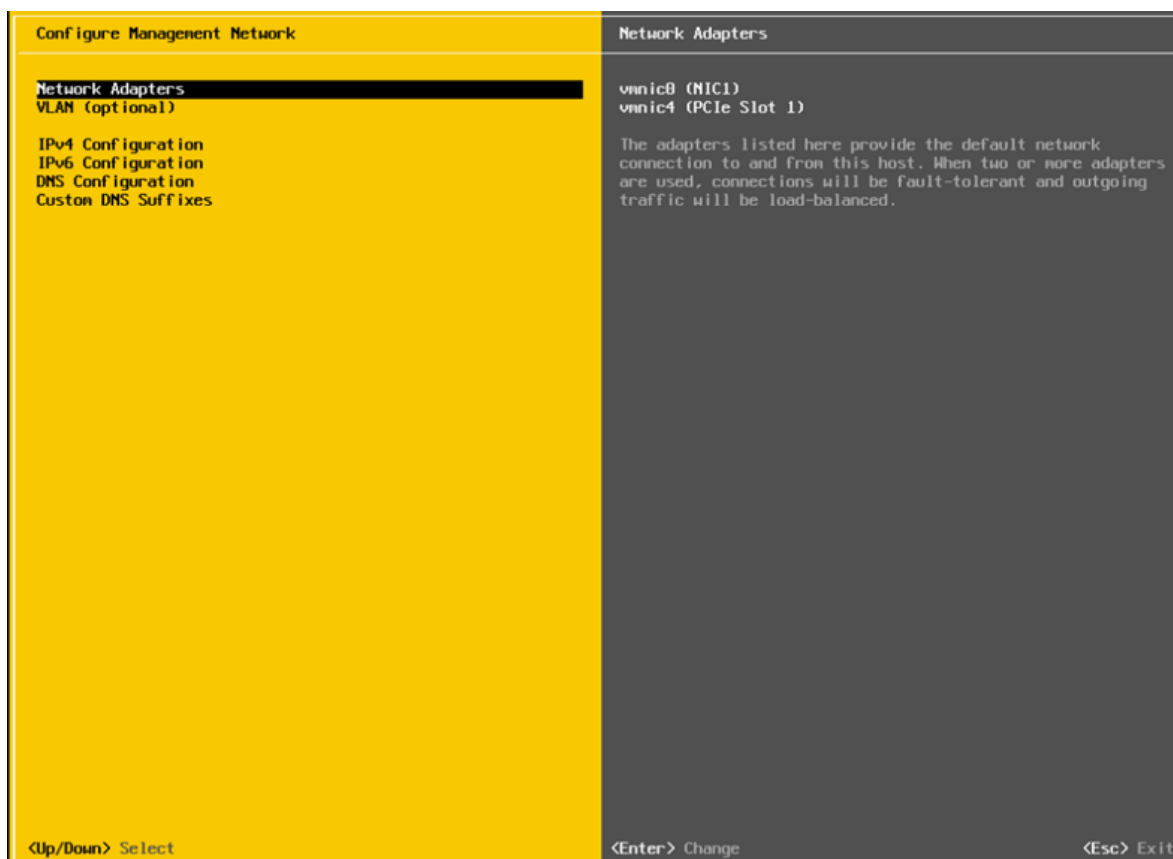


When/if credential and password are accepted, you will be returned to the previously noted console page. Press **F2** again.

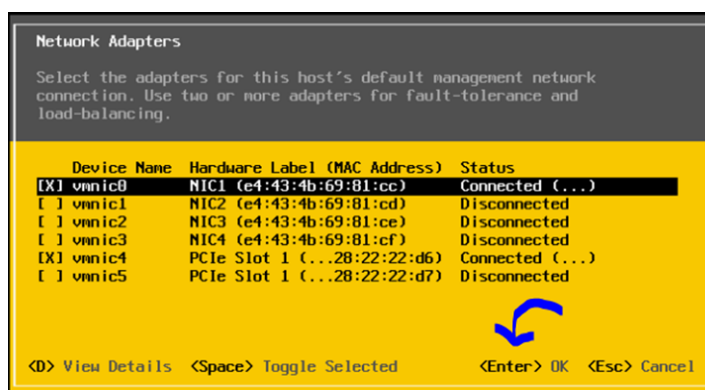
5. From the System Customization menu, select **Configure Management Network** and press **Enter**.



6. From the Configure Management Network menu, select **Network Adapters** and press **Enter**.

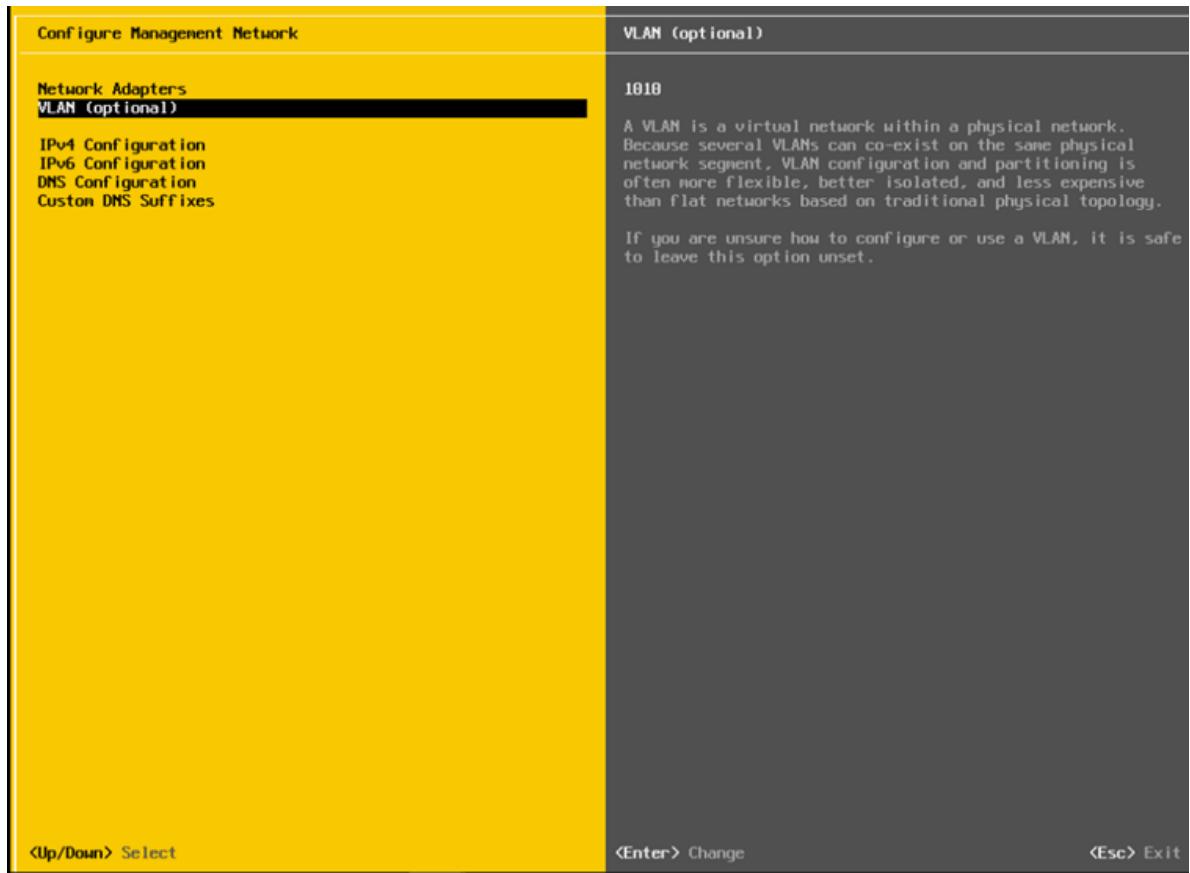


7. In the Network Adapters window, tab to the fields associated with the selection of specific NICs that will be used for ESXi management traffic and press the space bar to select the chosen ethernet interfaces.



In this example, **vmnic0** and **vmnic4** have been selected as the 2 NICs that will be teamed to support ESXi management traffic. Once the desired ports are selected, press **Enter**.

8. To assign a VLAN tag the ESXi management traffic, press **Esc** key in the previous menu to return to the Configure Management Network menu. Select **VLAN** and press **Enter**.



9. Enter the desired VLAN identifier in the VLAN administration field and press **Enter**.



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, at least for these earlier releases of ACP 130, the vSwitch will be the primary reference point for NIC Teaming behaviors and expectations. As shown in the following screen captures, the Port Group administration will “defer” to the administration in the vSwitch forms.

*** Note:**

In these early releases of ACP 130, there will be no advanced network switch configurations supported by Avaya Services.

Customers who have deployed advanced network packet distribution algorithms in the devices supporting the ACP 130 configuration, should be aware such configurations have not been approved and therefore are not documented.

NIC Teaming is a VMware feature, not an Avaya feature. Customers wishing to configure NIC Teaming on the ACP 130 are advised to refer to VMware documentation to identify administrative procedures for the desired NIC Teaming configuration. Once a specific load balancing and/or VLAN identifier is specified, the corresponding IP network must also be administered according to the desired NIC Teaming behavior. It is advised that customers/users refer to VMware documentation and/or Knowledge Based (KB) articles to insure the proper NIC teaming administration has been followed.

Some helpful VMware sites for troubleshooting NIC Teaming issues:

<https://blogs.vmware.com/kb/2013/02/troubleshooting-network-teaming-problems-in-esxesxi.html>

<https://blogs.vmware.com/kb/2013/03/troubleshooting-network-teaming-problems-with-ip-hash.html>

vSwitch NIC Teaming Administration

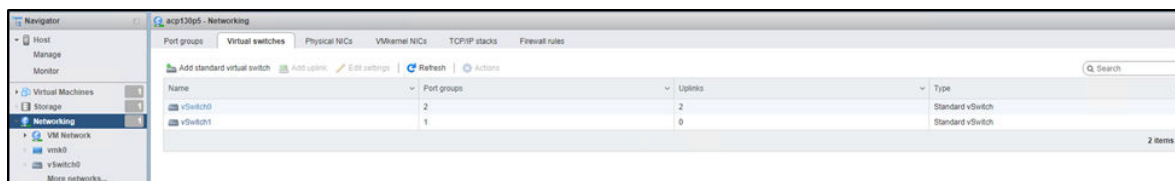
About this task

vSwitch1 is a dedicated services vSwitch, it will never be associated with NIC Teaming. Please leave this vSwitch administration and 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.

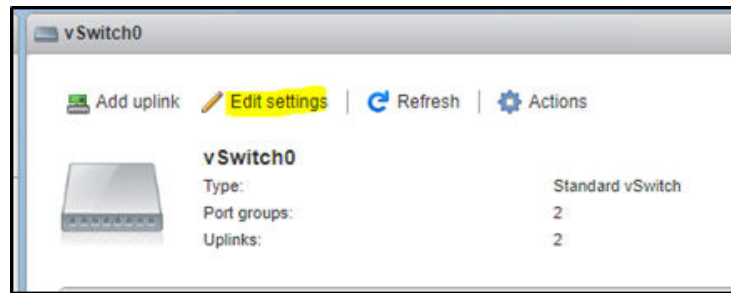
vSwitch0, supporting ESXi management and VM packet flows will be configured for NIC Teaming. In this example, vmnic0 is paired with vmnic4 to provide additional redundancy by distributing the backup functionality across 2 different NIC cards. For additional NIC Teaming administration, consider teaming vmnic2 with vmnic5.

Procedure

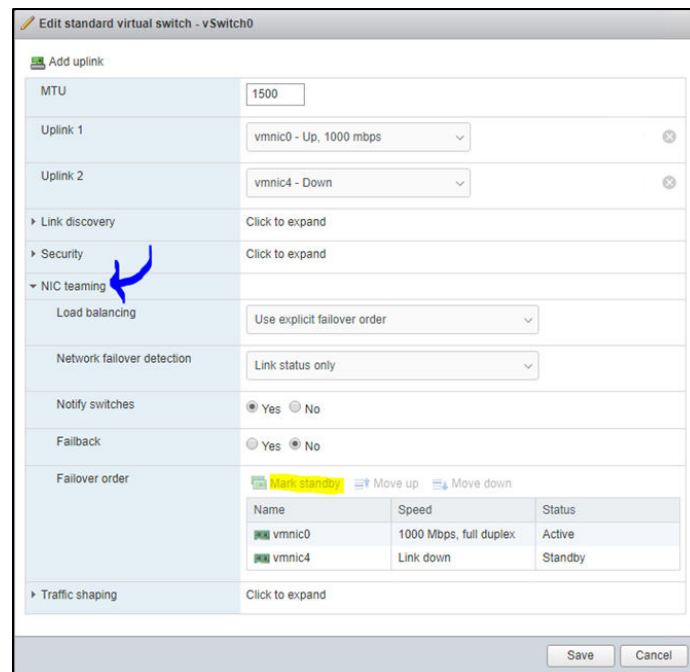
1. From the Networking menu option, select the **Virtual switches** tab and click **vSwitch0**:



- From the vSwitch0 submenu, select **Edit settings**:



- From the Edit setting options, click the **NIC teaming** drop-down arrow:



- Administer the options noted in this example.

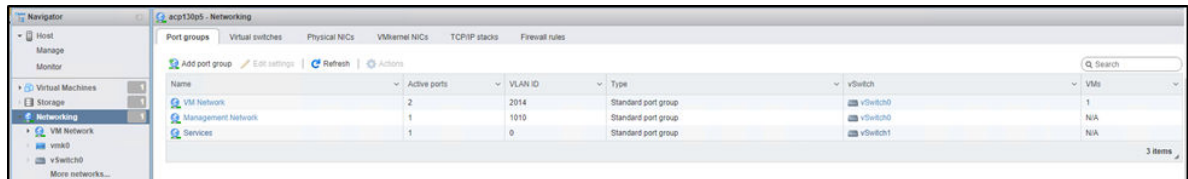
Deviations from the recommended settings could have negative impacts to the performance and stability of Avaya applications on the ACP 130 server and are not guaranteed.

- Load balancing will be set to **Use explicit failover order**.
- Network failover detection will be set to **Link status only**, supporting Layer 1 failure only at this time.
- 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).
- 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.

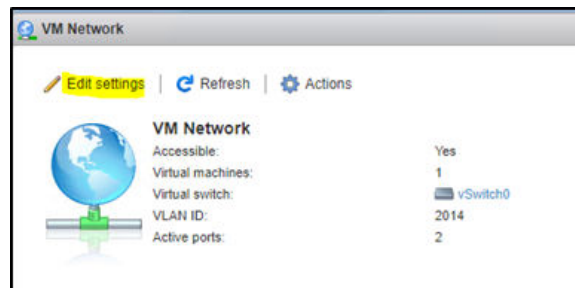
- e. Failover order is set by clicking the secondary vmnic element and then clicking the **Mark standby** option.
5. Click the **Save** button when finished.

Port Group NIC Teaming Administration Procedure

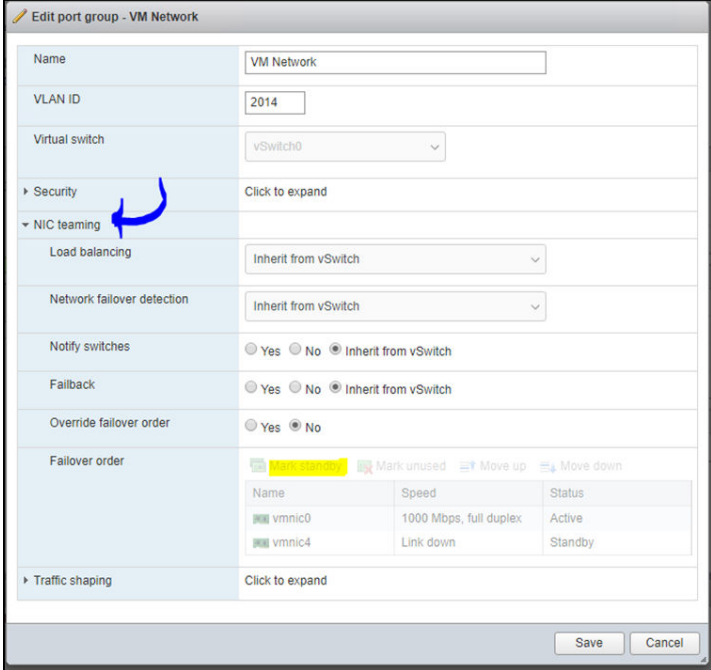
1. From the Networking menu item, select the **Port Groups** tab, and click **VM Network**:



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



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



Edit port group - VM Network

Name: VM Network

VLAN ID: 2014

Virtual switch: vSwitch0

Security: Click to expand

NIC teaming

Load balancing: Inherit from vSwitch

Network failover detection: Inherit from vSwitch

Notify switches: ☐ Yes ☐ No ☒ Inherit from vSwitch

Failback: ☐ Yes ☐ No ☒ Inherit from vSwitch

Override failover order: ☐ Yes ☒ No

Failover order:

Name	Speed	Status
vmnic0	1000 Mbps, full duplex	Active
vmnic4	Link down	Standby

Traffic shaping: Click to expand

Save Cancel

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 ACP 130 server and are not guaranteed.

- Load balancing is set to **Inherit from vSwitch**. This will keep the expected behaviors between both vSwitch and Port Groups aligned.
 - Network failover detection is set to **Inherit from vSwitch**.
 - Notify switches is set to **Inherit from vSwitch**.
 - Failback is set to **Inherit from vSwitch**.
 - Override failover order is set to **No** to continue the port group adherence to administration of the vSwitch assigned to this port group.
- Return to the **Networking > Port groups** tab and select **Management Network**.
 - Repeat the same administrative process as previously documented for the VM Network port group. Both port groups must have their NIC Teaming administration configured.

ACP 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 ACP 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 any of the procedures 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.

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/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://<IP address of ESXi host>/downloads/52c08d7e-3f2a-6156-ec7c-8f9cb8f77911/configBundle-cpd6-esxi1.sv.avaya.com.tgz
```

This URL is where the backup bundle can be downloaded.

4. SCP the backup files to a remote server.

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:

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.

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 in Maintenance Mode.
4. Use SCP 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/<filename that was copied>` to restore the configuration.

Log and File Collection to Aid in Troubleshooting

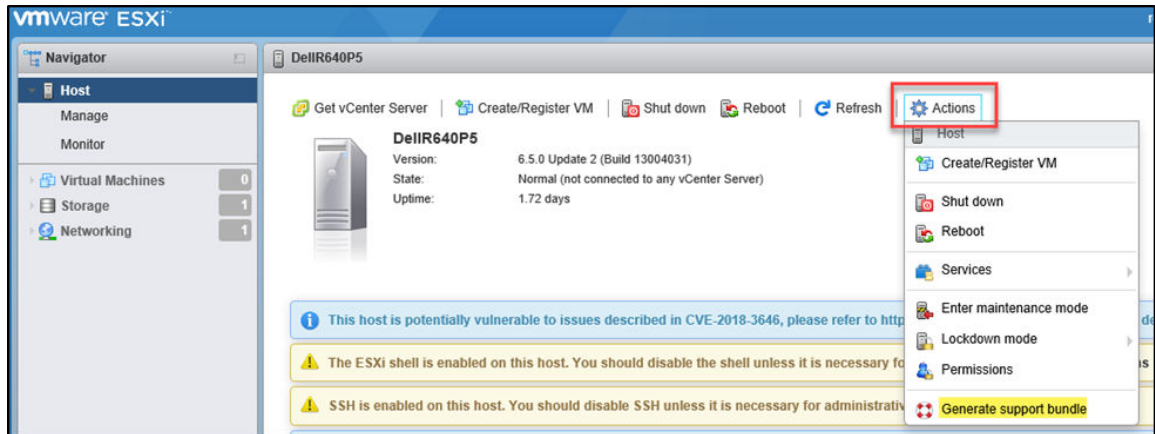
Collecting the VMware Support Bundle

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**.

- From the Actions drop-down menu, select **Generate support bundle**:



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

The log file construction will commence.

```
[root@DellR640P5:~] vm-support
vm-support v3.2: 19:25:58, action threads 4
19:25:58: Gathering output from /usr/lib/vmware/vm-support/bin/encryption-prolog
19:25:58: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa trace-info
19:25:58: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa get-metrics
19:25:58: Gathering output from /usr/lib/vmware/likewise/bin/lw-lsa get-status
19:25:58: Gathering output from vmware -vl
19:25:58: Gathering output from /usr/sbin/localcli system coredump partition get
19:25:58: Gathering output from /usr/sbin/esxcfg-info -a |
19:25:58: Gathering output from /usr/sbin/localcli system coredump partition lis
19:25:58: Gathering output from /sbin/vsi_traverse -s \
19:25:59: Gathering output from /usr/sbin/localcli --plugin-dir /usr/lib/vmware/
19:25:59: Gathering output from /usr/sbin/esxcfg-info -a \
19:26:03: Gathering output from /bin/localcli hardware ipmi sel get -p -i -n all
19:26:03: Gathering output from /sbin/vsi_traverse -s -
19:26:03: Gathering output from /bin/localcli hardware ipmi sel list -p -i -n al
19:26:03: Gathering output from /sbin/vsi_traverse -s
19:26:04: Gathering output from /bin/localcli hardware ipmi sdr get -p -i -n all
19:26:04: Gathering output from /sbin/vsi_traverse -s /
19:26:05: Gathering output from /sbin/vsi_traverse -s -
```

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

```

21:32:41: Gathering output from /sbin/localcli --plugin-dir /usr/lib/vmware/esxc
21:32:41: Gathering output from /sbin/localcli --formatter=json storage core dev
21:32:41: Gathering output from /bin/cat /var/log/vvold.log
21:32:41: Gathering output from /sbin/localcli --formatter=json storage nfs list
21:32:41: Gathering output from /usr/lib/vmware/vm-support/bin/encryption-epilog
21:32:41: Done.

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/datastore1/esx-DellR640P5-2020-
01-13--21.30-119367.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@DellR640P5:/vmfs/volumes/5e16855e-0d05a318-d18b-e4434b3e9050] ls -l
total 68632
drwxr-xr-x  1 root    root          1680 Jan 13 21:41 esx-DellR640P5-2020-01-10--19.25-84698
drwxr-xr-x  1 root    root          2100 Jan 10 23:54 esx-DellR640P5-2020-01-10--23.48-89028
-rw-r--r--  1 root    root        35381156 Jan 10 23:50 esx-DellR640P5-2020-01-10--23.48-89028.tgz
-rw-r--r--  1 root    root        34117224 Jan 13 21:32 esx-DellR640P5-2020-01-13--21.30-119367.tgz
d-w-r-xr-T  1 root    root           420 Jan  9 01:54 vmkdump
[root@DellR640P5:/vmfs/volumes/5e16855e-0d05a318-d18b-e4434b3e9050]

```

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

Chapter 7: Regulatory information

Regulatory information

For a complete listing of the DELL PowerEdge R640 regulatory information, refer to the following links:

- DELL Regulatory and Environmental Datasheet — <http://downloads.dell.com/rdoc/dell%20emc%20poweredge%20r640,e39s,e39s001,dell%20regulatory%20and%20environmental%20datasheet.pdf>
- EUROPEAN UNION - CE Declaration of Conformity — <http://downloads.dell.com/rdoc/dell%20emc%20poweredge%20r640,e39s,e39s001,european%20union%20-%20ce%20declaration%20of%20conformity.pdf>

Chapter 8: Resources

Documentation

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

Title	Description	Audience
Avaya Solutions Platform 100 series		
<i>Avaya Solutions Platform Overview and Specification</i>	Describes the key features of Avaya Solutions Platform	IT Management, sales and deployment engineers, solution architects, and support personnel
<i>Installing the Avaya Solutions Platform 130 Series</i>	Describes how to install Avaya Solutions Platform 130 Series.	Sales and deployment engineers, solution architects, and support personnel
<i>Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series</i>	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series.	Sales and deployment engineers, solution architects, and support personnel
<i>Avaya Solutions Platform 130 Series iDRAC9 Best Practices</i>	Describes the best practices of using Integrated Dell Remote Access Controller (iDRAC).	System administrators
<i>PSN027078u- Avaya Solutions Platform 130 Dell® R640 Avaya Certified BIOS/FW Update</i>	This is a Product Support Notice about Dell® R640 Avaya Certified BIOS/FW Update, Version 2.0.	
<i>PSN027079u- Avaya Solutions Platform 130 Dell® R640 Customized Image of VMware ESXi 6.5 U2</i>	This is a Product Support Notice about the availability of Dell® R640 Customized Image of VMware ESXi U2, A07, Build#10719125.	

Related links

[Finding documents on the Avaya Support website](#) on page 114

[Avaya Documentation Center navigation](#) on page 114

Finding documents on the Avaya Support website

Procedure

1. Navigate to <http://support.avaya.com/>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

[Documentation](#) on page 113

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
 - Click **Filters** to select a product and then type key words in **Search**.
 - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** () to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ().

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

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

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

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

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

 Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Related links

[Documentation](#) on page 113

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 Note:

Videos are not available for all products.

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

A

application deployment	98
array configuration	73
attaching cables	29
autostart virtual machines	
using embedded host client	46
Avaya Converged Platform 130 Series Services Port	
configuration	53
Avaya Solutions Platform appliance profiles	13

B

Back view of Dell™ PowerEdge™ R640 Server	
R640 Server	12
basic properties	82

C

collection	
delete	114
edit name	114
generating PDF	114
sharing content	114
configuration	
default	95
configure	
SNMP v2c alerts	83
SNMP v2c traps	86
Configure	
autostart on ESXi	46
configuring	
Avaya Converged Platform 130 Services port	53
controller properties	76
ESXi Network Settings	33
SNMP v2c on ESXi 6.5 host	47
SNMP v3 on ESXi 6.5 host	50
SNMP v3 traps	87
the advance controller properties	76
connecting power	30
content	
publishing PDF output	114
searching	114
sharing	114
sort by last updated	114
watching for updates	114
creation of a virtual disk	78

D

data storage space	81
deleting configurations	73

Dell PowerEdge R640 Server dimensions	14
documentation	113
documentation center	114
finding content	114
navigation	114
documentation portal	114
finding content	114
navigation	114
document changes	7

E

electrostatic discharge	23
environmental requirements	15
ESXi configuration	33

F

finding content on documentation center	114
Front view of the server	
R640 server	11

H

HealthCheck tool registration	18
-------------------------------------	----

I

installation checklist	23
installing	
LS Reconfigurator Utility Tool	59
installing the server	25

K

key features	9
--------------------	---

M

My Docs	114
---------------	-----

N

NIC Teaming	99
administering in ESXi vSphere client	103
ESXi Management Interfaces configuration	99
Port Group administration	106
vSwitch administration	104

O

overview	
Avaya Solutions Platform	9
Dell server	10

P

package contents	24
physical disks	78
Port Groups	
configuring	96
power requirements	17
preparing for configuration	73
purpose	7

R

RAID controller	73
RAID level	78
registering new device	19
registration	
overview	18
status	21
regulatory information	112
replacing host server	65 , 71

S

Sample Service's vSwitch Configuration	58
searching for content	114
server recovery	65
adding license key	72
sharing content	114
SNMP alerts	
overview	83
SNMP v2c alerts	
configure	83
SNMP v2c traps	
configure using iDRAC	86
SNMP v3 configuration	50
SNMP v3 traps	
edit user account	92
SNMP v3 traps configuration	87
software remastering	65
adding license key	72
sort documents by last updated	114
support	116
supported software	10

T

Technical Onboarding process	22
TLS protocol configuration	59

V

validating	
vSwitch1 Configuration	56
videos	115
viewing	
Enabled TLS Version	60
virtual disk	82
virtual disk parameters	78
virtual disk size	81
VLAN tagging	98
VMkernel NIC	
administration	97
VMware ESXi	
backing up the configuration	108
restoring the configuration	108
VMware support bundle	
collecting	109
vSphere 6.5 U2 Environment	59
vSwitch	
administration	95

W

watch list	114
------------------	---------------------