



VersaVirtual Appliance User Manual

Catalog Number 9300-VVB-PRJ



Allen-Bradley

by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT

Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.



Identifies information that is useful and can help to make a process easier to do or easier to understand.

	Preface	
	About this Publication	5
	Abbreviations	5
	Features.....	6
	Overview.....	6
	Download Firmware, Add-on Profile, EDS, and Other Files.....	6
	Additional Resources	7
	Chapter 1	
Install the VersaVirtual Appliance	Install the VVA in a Rack	9
	Identify Ports and Components	10
	Connect Network Cables	11
	Connect Power Cables	12
	Install Front Bezel.....	12
	Chapter 2	
Integrate the Network	Connect the Appliance to the Network.....	15
	Use the Default VLAN	15
	Add Host Names to Local Host File.....	17
	Chapter 3	
Manage the System	Domain Name System Requirements.....	21
	Forward DNS Requests.....	21
	Configure the Management Computer	23
	Install VersaVirtual Licenses.....	27
	Change Default Passwords	34
	Baseboard Management Controller.....	34
	VMware vSphere	35
	VMware vCenter.....	37
	VMware vCenter Server Appliance	40
	Virtual Machines: NetSvcs	41
	Virtual Machines: Support-Probe	42
	Virtual Machines: Support-Proxy.....	43
	Configure Active Directory Authentication	45
	Update the Hardware Compatibility List	49
	Add a Virtual Machine.....	52
	Import an OVA Template	59
	Chapter 4	
System Shut down and Startup	Shut down vSAN Cluster.....	65
	Shut down NPU	66
	Restart NPU	67
	Restart vSAN Cluster	68

Appendix A	
Change the IP Address Schemes	
Shut Down the vSAN Cluster	69
Change the IPv4 Settings of the Witness Host	70
Reset IP Address of NPU	72
Update Access and Trunk Port with New VLAN Tag (Optional)	74
Reset iDRAC IP Addresses	74
Update NetSvcs IP	76
Update NetSvcs DNS Settings	78
Change VMware vCenter IP Address with the VMware vCenter Server Appliance	79
Apply new VLAN Tag to Port Groups (Optional)	82
Update IP Addresses on vSAN Hosts	85
Update High Availability	88
Reconnect Hosts	91
Restart vSAN Cluster	93
Appendix B	
Rename VersaVirtual Appliance Components	
Rename Procedures	
Preliminary Steps	96
Add New Name Information to DNS Server Hosted by NetSvcs	97
Factory default: ra.conf	98
Updated ra.conf	99
Rename NetSvcs	100
Rename VMware vCenter	101
Redeploy the vSAN Witness Virtual Machine	104
Unregister and Remove Existing Witness	104
Deploy the New vSAN Witness Virtual Machine	107
Register the New vSAN Witness	114
Rename Cluster Hosts	122
Rename Host 1	122
Rename Host 2	130
Rebalance Virtual Machines across the Cluster	131
Remove Obsolete Information from NetSvcs	131
Final ra.conf	132
Final steps	133
Index	135

About this Publication

This manual provides information on how to install, configure, and manage the Rockwell Automation Series B VersaVirtual™ Appliance (VVA), as follows.

Topic	Page
Install the VersaVirtual Appliance	9
Integrate the Network	15
Manage the System	21
Rename VersaVirtual Appliance Components	95
System Shut down and Startup	65

Abbreviations

This manual uses the following abbreviations.

Abbreviation	Meaning
AD	Active Directory
BMC	Baseboard Management Controller
BOSS	Boot Optimized Server Storage
DCUI	Direct Console User Interface
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HA	High Availability
HCL	Hardware Compatibility List
HD	Hard drive
HSRP	Hot standby Router Protocol
iDRAC	Integrated Dell Remote Access Controller
LDAP	Lightweight Directory Access Protocol
MAC	Machine Access Controller
NAT	Network Address Translation
NPU	Nano Processing Unit
NTP	Network Time Protocol
OVF	Open Virtualization Format
SSD	Solid-state drive
SSH	Secure Shell
SSO	Single Sign On
VA	Virtualization Appliance
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
vSAN	Virtual Storage Area Network
VVA	VersaVirtual Appliance

Features

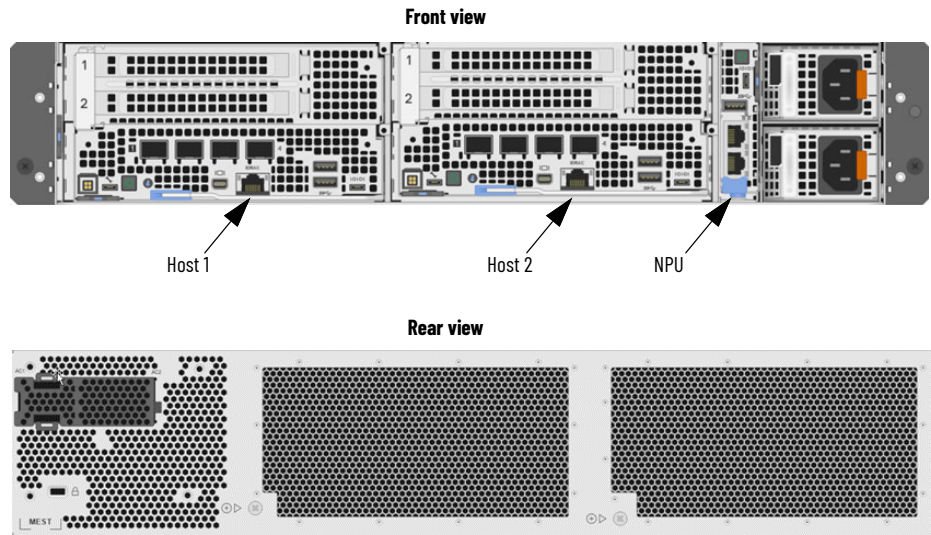
Overview

The Rockwell Automation VVA is a hyperconverged (integrated computer, networking, and storage) appliance intended for entry-level virtualization in a managed environment. The VVA ships in a fully configured state, and includes support services to help minimize on-site customer configuration.

The VVA CPU, memory, and storage are fully customizable. A VVA has the following baseline specifications.

Component	Baseline specification
Processor (CPU)	3rd Generation Intel Xeon D-2776NT 2.10 Ghz
Memory	128 GB
Storage controllers	Boot Optimized Storage Subsystem (BOSS), 2 x M.2 SSDs 480 GB
Network (Ethernet) connection ports	4 x 10GbE SFP (max 50 Gb)
Usable storage	1.9 TB
Operating system	VMware vSphere® Standard
Input power	100...240V AC, 50/60 Hz, dual
Operating temperature range	-5...55 °C (23...131 °F), with a cold start temperature of 0 °C (32 °F)
Mounting options	Rack

Figure 1 - VersaVirtual™ Series B Overview



Download Firmware, Add-on Profile, EDS, and Other Files

You can download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Additional Resources

The following documents contain information for related Rockwell Automation products.

You can view or download additional publications at rok.auto/literature.

Resource	Description
EtherNet/IP™ Network Devices User Manual, ENET-UM006	Describes how to configure and use EtherNet/IP devices to communicate on the EtherNet/IP network.
Ethernet Reference Manual, ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
System Security Design Guidelines Reference Manual, SECURE-RM001	Provides guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.
UL Standards Listing for Industrial Control Products, publication CMPNTS-SR002	Assists original equipment manufacturers (OEMs) with construction of panels, to help ensure that they conform to the requirements of Underwriters Laboratories.
American Standards, Configurations, and Ratings: Introduction to Motor Circuit Design, publication IC-AT001	Provides an overview of American motor circuit design, based on methods outlined in the NEC.
Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley™ industrial automation controls and assemblies.
Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies that incorporate solid-state components.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
ProposalWorks™ configuration software, rok.auto/systemtools	Helps configure complete, valid catalog numbers, and build complete quotes that are based on detailed product information.
Rockwell Automation Global SCCR tool, rok.auto/sccr	Provides coordinated high-fault branch circuit solutions for motor starters, soft starters, and component drives.
Product Certifications website, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

Notes:

Install the VersaVirtual Appliance

To install the VVA, perform the steps that are contained in the following sections:

- [Install the VVA in a Rack](#)
- [Identify Ports and Components](#)
- [Connect Network Cables](#)
- [Connect Power Cables](#)
- [Install Front Bezel](#)

Install the VVA in a Rack

The VVA must be mounted in a rack.

IMPORTANT

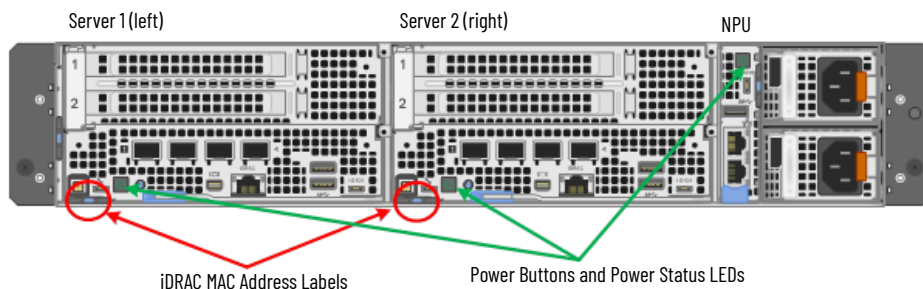
Before you install the VVA into your rack, perform the following steps.

1. Review and follow any safety guidelines that are included in the rack installation instructions.
 2. Unbox the VVA and remove the shipping brackets and front bezel.
 3. Install the cable management arms.
 4. Mount the VVA in your rack using the hardware that came with your VVA and rack.
-

Identify Ports and Components

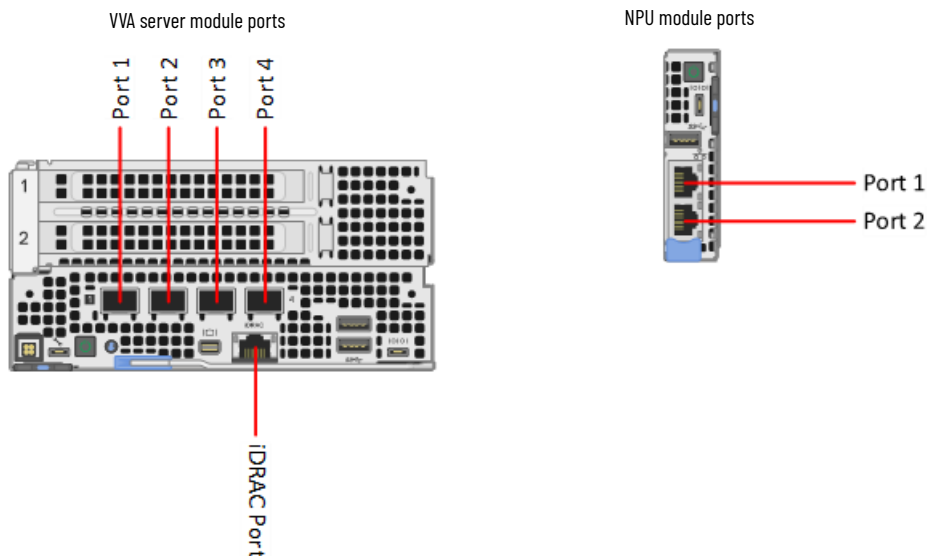
The VVA contains the following ports and components:

- Two server modules — left and right
- One NPU module, which is used as a dedicated host for the VMware vSAN™ witness host and other appliances
- Two power supplies



Each server module has five network ports, including one Integrated Dell Remote Access Controller (iDRAC) port. These server module ports must be connected to your network switch.

The NPU module has two network ports that must also be connected to your network switch.



Connect Network Cables

The VVA ships with the following items:

- Eight Ethernet patch cables
- Two copper direct attach cables (DAC)
- Four copper transceiver modules

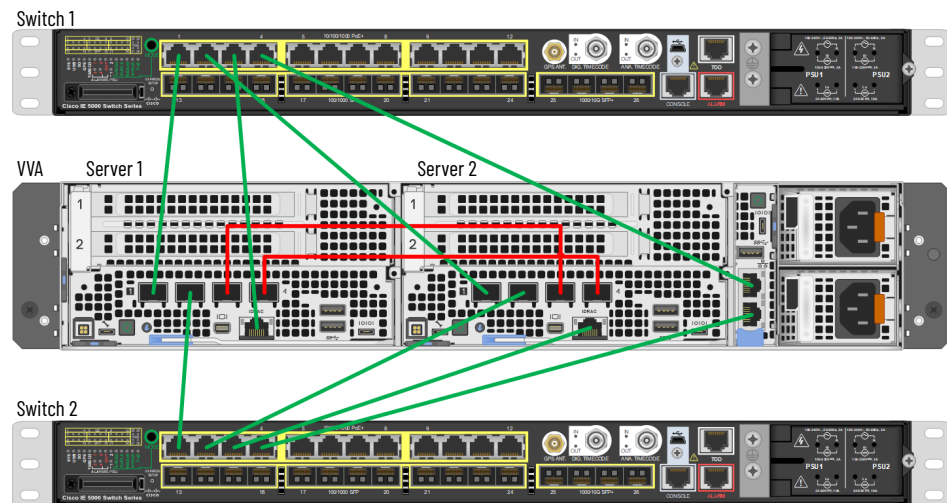


In order for the VVA to function properly, you must allocate eight GbE ports in your network switch: four access ports, and four trunk ports.



Rockwell Automation recommends that you configure your VVA to use two switches that are connected to the balance of plant network, or separate power sources. This configuration can help improve redundancy and avoid disruption due to maintenance or failure. For more information, see [Integrate the Network on page 15](#).

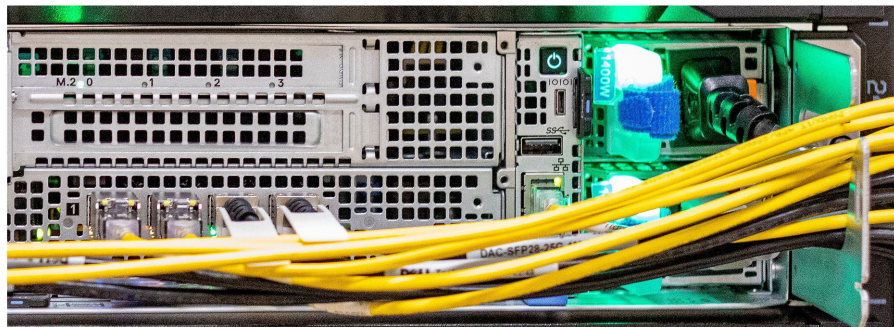
To connect your VVA to two switches, perform the following procedures.



1. Insert a transceiver module into **ports 1 and 2 on both servers**.
2. Connect an Ethernet cable from **port 1 of server 1**, to **port 1 of switch 1**.
3. Connect an Ethernet cable from **port 2 of server 1**, to **port 1 of switch 2**.
4. Connect an Ethernet cable from **iDRAC port of server 1**, to **port 3 of switch 1**.
5. Connect an Ethernet cable from **port 1 of server 2**, to **port 2 of switch 1**.
6. Connect an Ethernet cable from **port 2 of server 2**, to **port 2 of switch 2**.
7. Connect an Ethernet cable from **iDRAC port of server 2**, to **port 3 of switch 2**.
8. Connect an Ethernet cable from **NPU port 1**, to **port 4 of switch 1**.
9. Connect an Ethernet cable from **NPU port 2**, to **port 4 of switch 2**.
10. Connect one DAC cable from **port 3 of server 1**, to **port 3 of server 2**.
11. Connect one DAC cable from **port 4 of server 1**, to **port 4 of server 2**.
12. Install dust filtration bezel.

Connect Power Cables

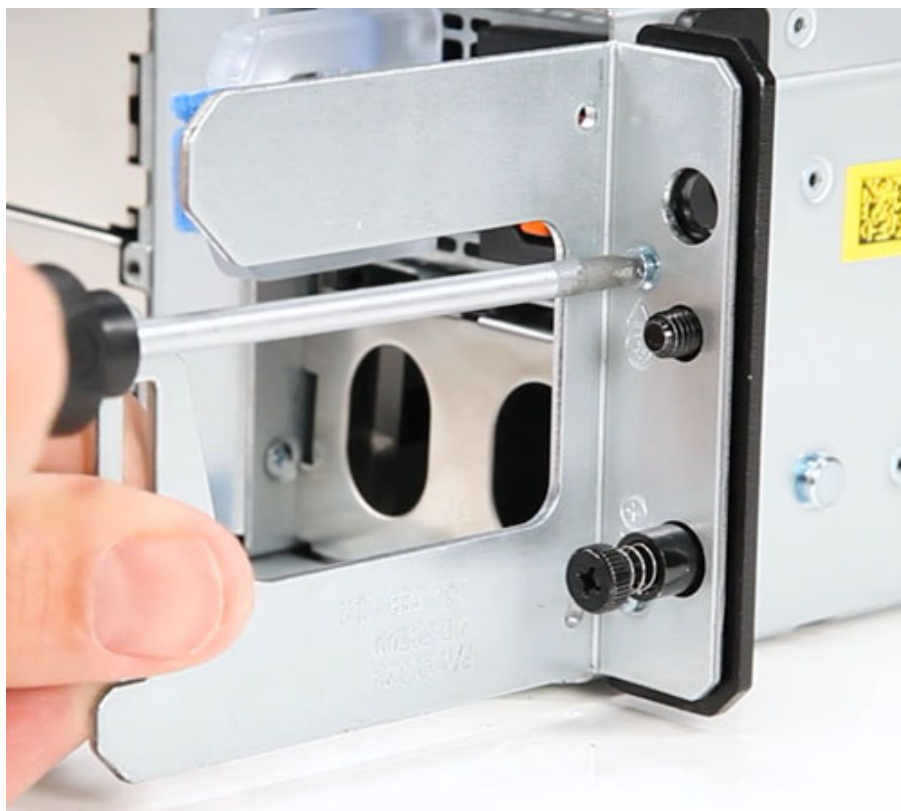
Connect the appliance to a power source with the supplied power cables. When connected, the power supply indicators illuminate.



Install Front Bezel

To install the front bezel, perform the following steps.

1. Align the right bracket to the right ear of the unit.
2. Tighten the two screws to secure the right bracket to the right ear.



3. Repeat this process for the left bracket.



4. Align the bezel with the brackets and press until the bezel clicks into place.



The front bezel is now installed.

Notes:

Integrate the Network

This section provides information on how to integrate the VVA into your network.

Connect the Appliance to the Network

Before you connect the appliance to your network, note the following:

- Rockwell Automation recommends that you configure your VVA to use two switches. The switches do not need to be stacked or configured as a redundant pair, but should be connected to the balance of plant network, or separate power sources. This configuration can help improve redundancy and avoid disruption due to maintenance or failure.
- Rockwell Automation recommends that you use the default virtual local area network (VLAN) and subnet address. For more information, see the [Use the Default VLAN](#) section.
- If you use the VVA default VLAN and subnet, the default management VLAN 3249 should be added to the layer 3 core switch or router, and all switches between the server access switches and core switch. The core switch should also be configured with an IP address of 192.168.249.1/24 on VLAN 3249.
- Rockwell Automation recommends that you add a list of default VVA IP addresses and corresponding host names to your host file. For more information, see the [Add Host Names to Local Host File](#) section on page 17.
- IP address schemes can be changed. For more information, see [Change the IP Address Schemes on page 69](#).
- In order to manage the VVA, you must configure the management ports on you switch as trunk ports. The iDRAC ports on your switch must also be configured as access ports. Check the documentation that came with your switch for more information.

Use the Default VLAN

The default VLAN for the VVA is 3249 and uses subnet 192.168.249.0/24. To add the default VVA VLAN to your network and assign your router an IP address of 192.168.249.1, perform the following steps.

IMPORTANT The following two steps are based on the use of a Cisco® Stratix® 5410 core switch and two Stratix 5410 access switches.

1. Sign in to your core router and add the following entries:

```
router#config term
router#config terminal
router(config)#vlan 3249
router(config-vlan)#name VersaVirtual
router(config-vlan)#interface vlan 3249
router(config-if)#ip address 192.168.249.1 255.255.255.0
router(config-if)#description VersaVirtual Management
router(config-if)#exit
router(config)#end
router#wr
```

2. Verify the configuration of your switches.
The configuration should resemble the following.

Switch 1

```
vlan 3249
  name VVA_Management
!
vlan 3250
  name VVA_vMotion
!
vlan 3251
  name VVA_vSAN
!
interface GigabitEthernet1/1
  description host 1 port 1
  switchport mode trunk
!
interface GigabitEthernet1/2
  description host 2 port 1
  switchport mode trunk
!
interface GigabitEthernet1/3
  description Host 1 iDRAC
  switchport access vlan 3249
  switchport mode access
!
interface GigabitEthernet1/4
  description NPU port 1
  switchport access vlan 3249
  switchport mode access
```

Switch 2

```
vlan 3249
  name VVA_Management
!
vlan 3250
  name VVA_vMotion
!
vlan 3251
  name VVA_vSAN
!
interface GigabitEthernet1/1
  description host 1 port 2
  switchport mode trunk
!
interface GigabitEthernet1/2
  description host 2 port 2
  switchport mode trunk
!
interface GigabitEthernet1/3
  description Host 2 iDRAC
  switchport access vlan 3249
  switchport mode access
!
interface GigabitEthernet1/4
  description NPU port 2
  switchport access vlan 3249
  switchport mode access
```

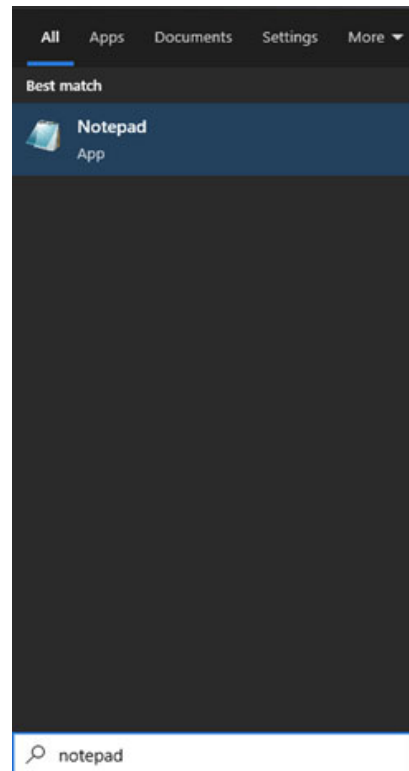
Add Host Names to Local Host File

To add a list of default VVA IP addresses and corresponding host names to your local host file, perform the following steps.



Note: the procedures in this section are based on a Windows 10 computer. Other versions of Windows might vary.

1. Open Windows® Notepad from the Windows Start menu or Search bar.

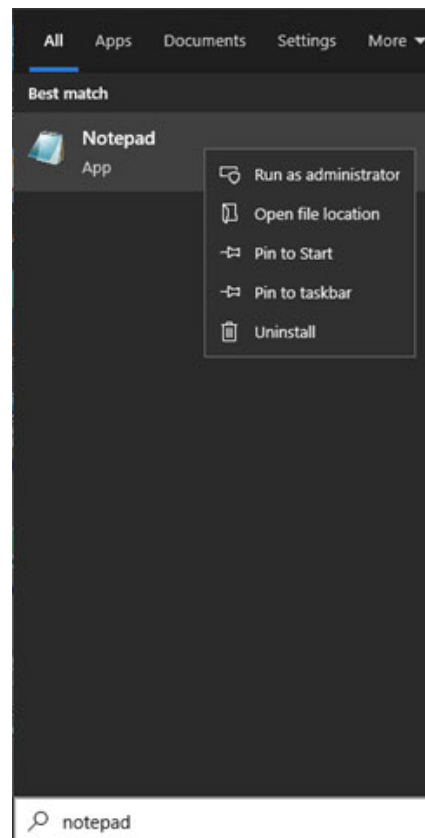


2. Copy and paste the following list of IP addresses and host names into a new note.

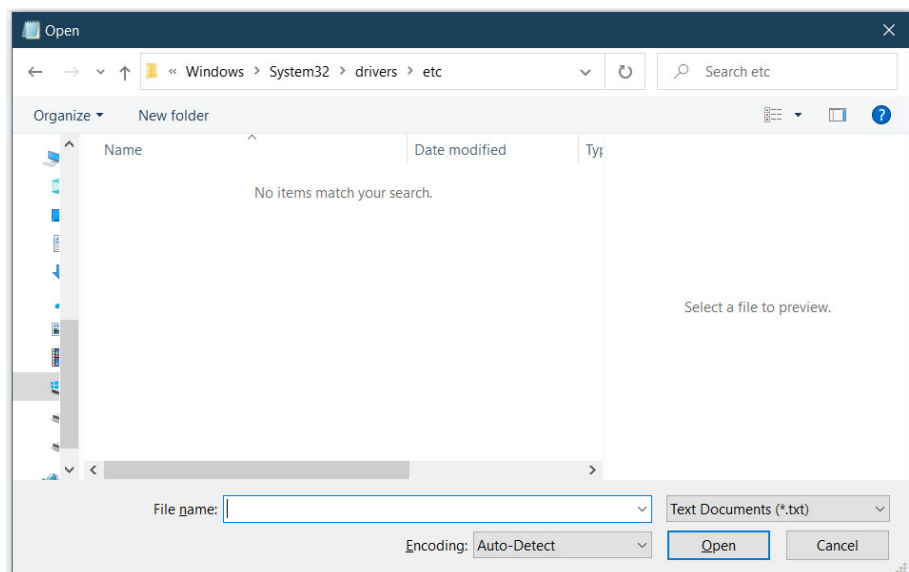
```
192.168.249.11 host1-bmc.ra.internal # Host 1 BMC
192.168.249.12 host2-bmc.ra.internal # Host 2 BMC
192.168.249.18 vCenter.ra.internal # vCenter server
192.168.249.14 host1.ra.internal # cluster host 1
192.168.249.15 host2.ra.internal # cluster host 2
192.168.249.13 npu.ra.internal # management host
192.168.249.16 witness.ra.internal # witness host
192.168.249.17 netsvcs.ra.internal # DNS server
192.168.249.19 support-probe.ra.internal # Support probe
192.168.249.20 support-proxy.ra.internal # Support proxy
```

3. Leave the note open.

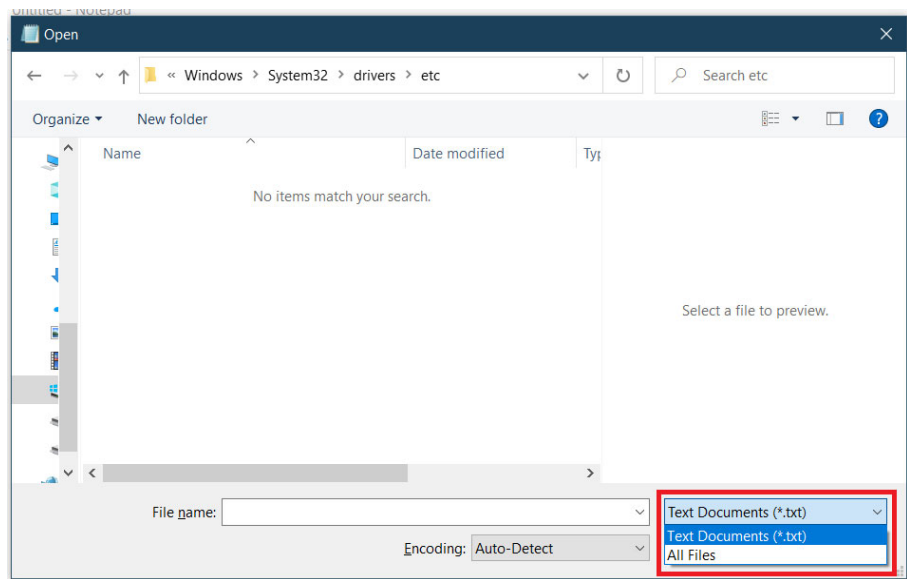
4. Run Windows Notepad as administrator:
 - a. Right-click Notepad from the Start menu, or Search bar
 - b. Select Run as Administrator.



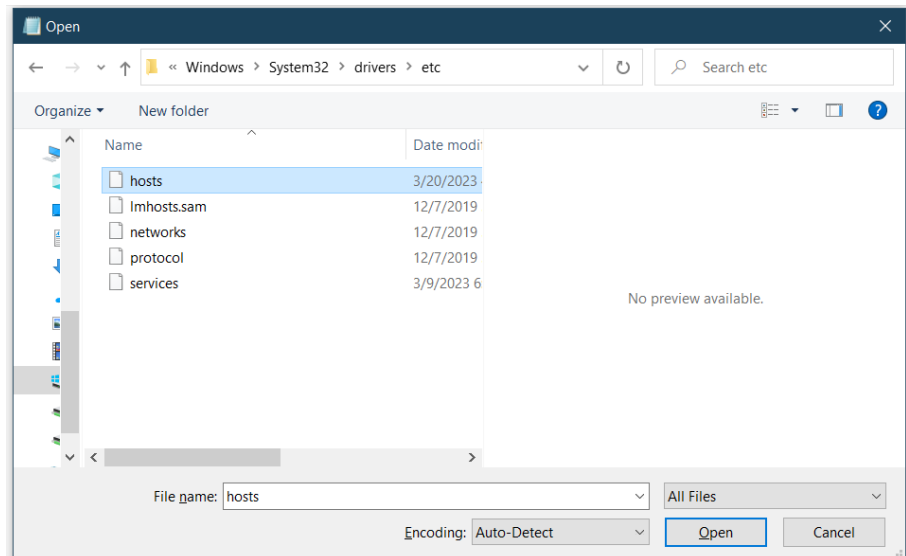
5. Select the File menu > Open.
6. Navigate to the following Windows directory:
Local Disk (C:)\Windows\System32\Drivers\etc



7. From the File Type dropdown menu, select All Files.



8. Select the hosts file and then Open.




9. In the hosts file, delete any entries for the Default VVA Network scheme.

See step 2. for the default values.

10. Return to your original Windows Notepad document that contains the list of new hosts and IP addresses.



11. Select all entries with CTRL+A.

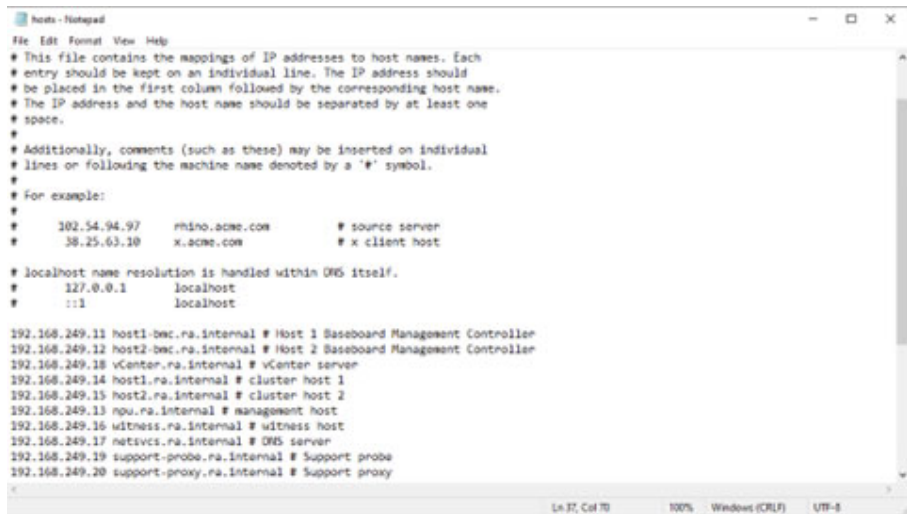


```

192.168.249.11 host1-bmc.ra.internal # Host 1 Baseboard Management Controller
192.168.249.12 host2-bmc.ra.internal # Host 2 Baseboard Management Controller
192.168.249.13 vCenter.ra.internal # vCenter server
192.168.249.14 host1.ra.internal # cluster host 1
192.168.249.15 host2.ra.internal # cluster host 2
192.168.249.16 npu.ra.internal # management host
192.168.249.17 witness.ra.internal # witness host
192.168.249.18 netsvc.ra.internal # DNS server
192.168.249.19 support-probe.ra.internal # Support probe
192.168.249.20 support-proxy.ra.internal # Support proxy

```

12. Copy the entries with CTRL+C.
13. Return to the hosts file.
14. Place your cursor below the last line of text.
15. Paste the new entries with CTRL+V.



```

# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       192.54.94.97 rhino.acme.com      # source server
#       38.25.63.10 x.acme.com         # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1 localhost
#       ::1 localhost
#
192.168.249.11 host1-bmc.ra.internal # Host 1 Baseboard Management Controller
192.168.249.12 host2-bmc.ra.internal # Host 2 Baseboard Management Controller
192.168.249.13 vCenter.ra.internal # vCenter server
192.168.249.14 host1.ra.internal # cluster host 1
192.168.249.15 host2.ra.internal # cluster host 2
192.168.249.16 npu.ra.internal # management host
192.168.249.17 witness.ra.internal # witness host
192.168.249.18 netsvc.ra.internal # DNS server
192.168.249.19 support-probe.ra.internal # Support probe
192.168.249.20 support-proxy.ra.internal # Support proxy

```

16. From the File menu, select Save and then close the file.

The default VVA IP addresses are now part of the local hosts file.

Manage the System

Domain Name System Requirements

The Domain Name System (DNS) on your network can be configured to access to the VMware vSphere® Web Client from your VVA. DNS can also be configured to integrate the VVA into an Active Directory (AD) environment. See [Configure Active Directory Authentication on page 45](#) for more information.

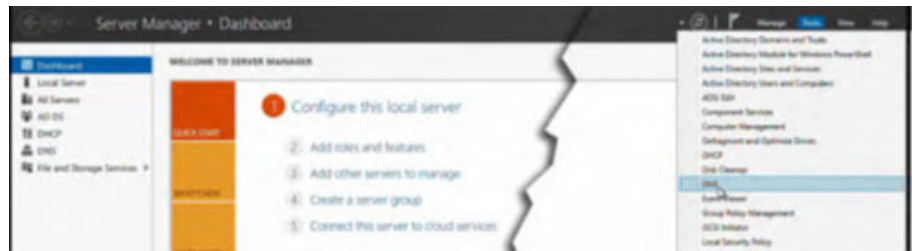
To access the VMware vSphere Web Client, you must complete one of the following procedures:

- Configure your AD to forward DNS requests from the ra.internal domain to the NetSvcs virtual machine (VM) default IP address — 192.168.249.17.
- Configure your management computer to use the NetSvcs VM default IP address as your DNS server — IP address 192.168.249.17.
- Add entries in your host file for the VVA in the management computer.

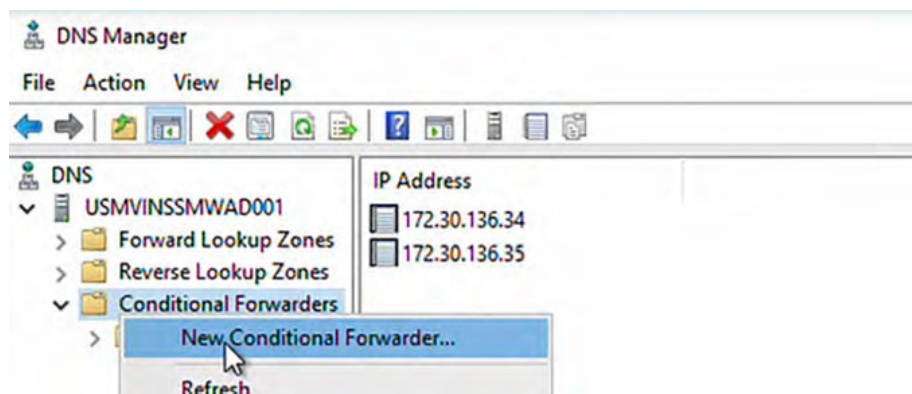
Forward DNS Requests

To add DNS conditional forwarders to the VVA, perform the following steps.

1. Open the Server Manager from the Windows® Start menu.
2. On the Server Manager dashboard, select Tools and then DNS.



3. In the Navigation pane on DNS Manager, right-click Conditional Forwarders and select New Conditional Forwarder.



The New Conditional Forwarder box displays.

4. In the DNS Domain field, add the following domain:
ra.internal

New Conditional Forwarder

DNS Domain:
ra.internal

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...>		
✗ 192.168.249.17	<Unable to resolve>	A timeout occurred duri...

☒ Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest

! This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers
Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

OK Cancel

5. Select the <Click here to add...> field and add an IP address.

New Conditional Forwarder

DNS Domain:
ra.internal

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...>		
✗ 192.168.249.17	<Unable to resolve>	A timeout occurred duri...

☒ Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest

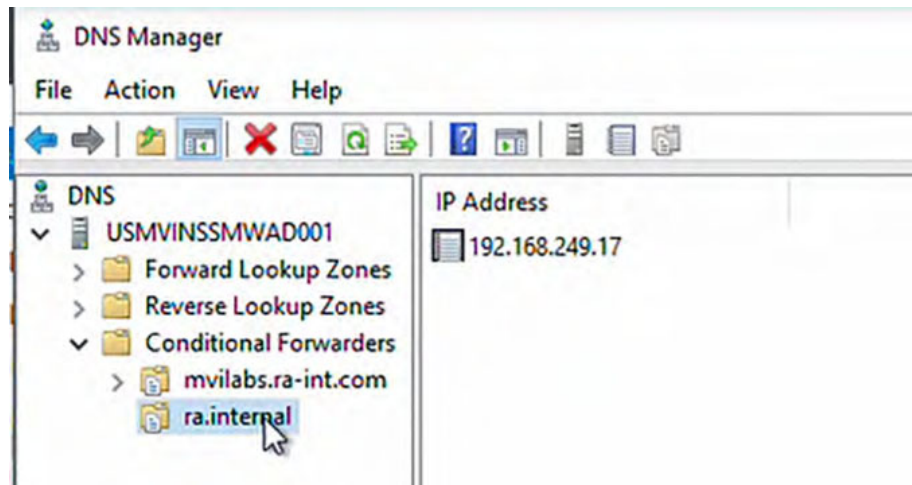
! This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers
Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

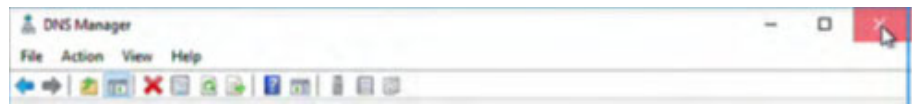
OK Cancel

6. To query and validate the IP address, check the "Store this conditional forwarder in Active Directory..." option.
The query timeout settings value can be adjusted as needed.
7. After the IP address is established and validated, select Ok.

8. Confirm ra.internal is listed under the DNS Conditional Forwarder list.



9. To return to the Server Manager dashboard, close the DNS Manager window.



The entry is now added as a DNS conditional forwarder.

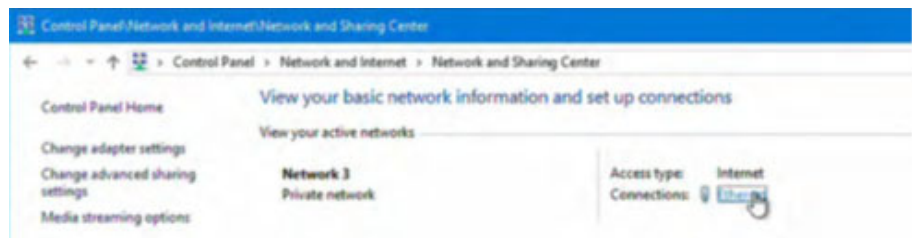
Configure the Management Computer

To add the DNS server address to a Windows[®] computer, perform the following steps.

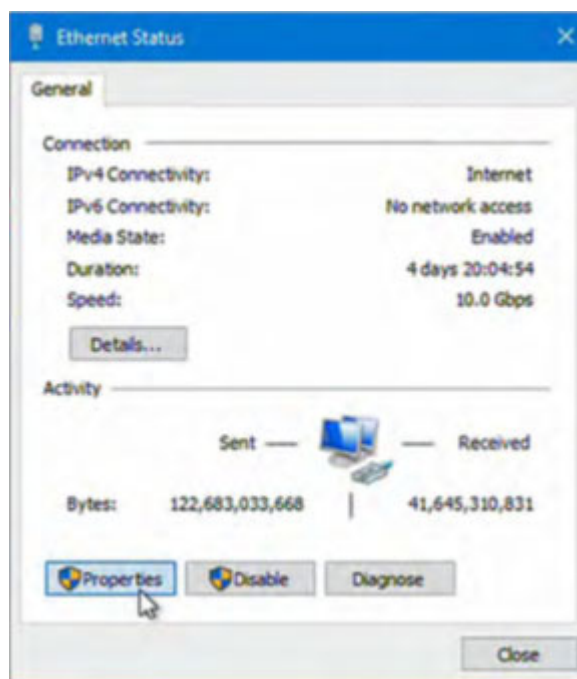


Note: the procedures in this section are based on a Windows 10 computer. Other versions of Windows might vary.

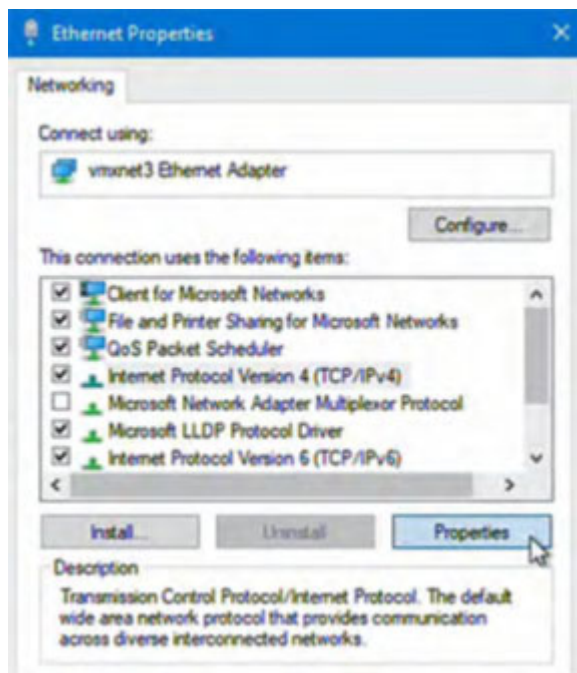
1. From the Start menu, open the Control Panel.
2. In the Control Panel, select Network and Internet.
3. On the Network and Sharing Center, select the Ethernet link.



- On the General tab of Ethernet Status, select Properties.



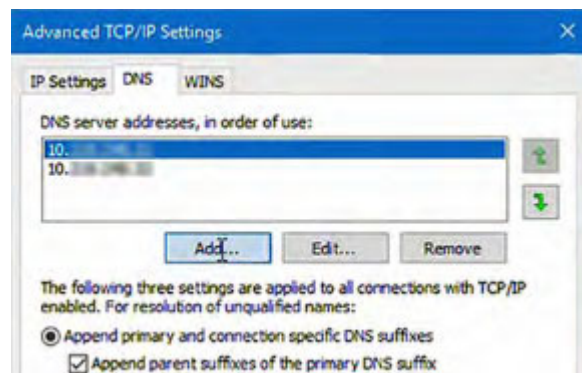
- On the Networking tab, select Properties.



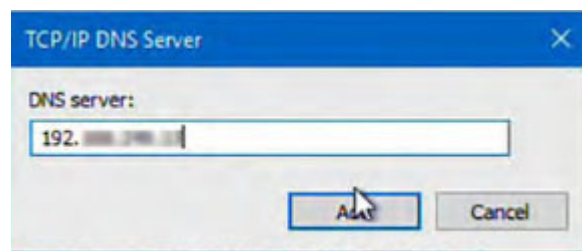
- On the General tab, select Advanced.



- On the DNS tab, select Add.



- Enter the IP address for your DNS server and select Add.



9. On the DNS tab, select the new DNS address, press the green up-arrow until the address is at the top of the order, and then select Ok.



10. On the General tab, verify that the IP address just added is the preferred DNS server address.
11. Once verified, select Ok.



12. On the Networking tab, select Close.
 13. On the General tab, Close.
 14. Close Networking and Sharing Center window.
- The DNS server address is now reachable via the Ethernet connection.

Install VersaVirtual Licenses

This section provides information on how to install VVA licenses within 90 days of purchase.

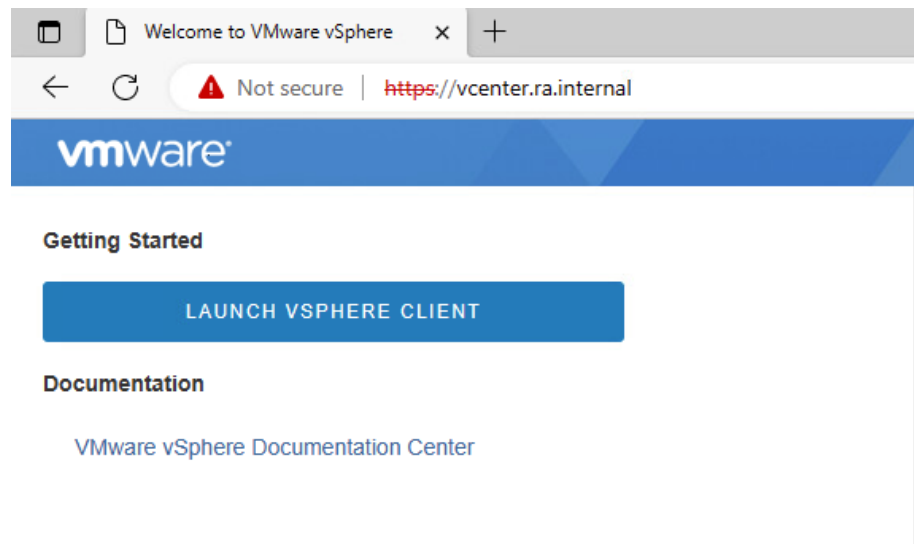
IMPORTANT The VVA ships with a 90-day evaluation license. To continue uninterrupted service, Rockwell Automation recommends that you install a license before the end of the 90-day evaluation period.

To install a license after the VVA 90-day evaluation has expired, visit the [Rockwell Automation Knowledgebase](#) and search for “VersaVirtual.”

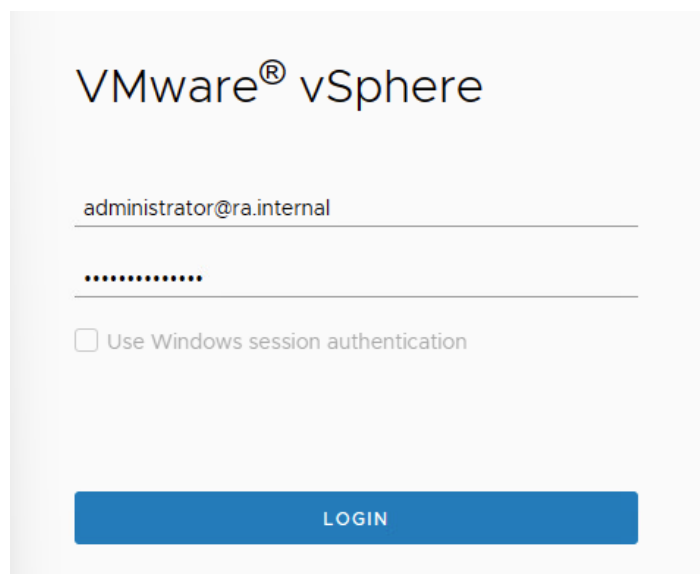
Other application licenses, such as those for Microsoft®, are not included with the VVA.

To install VVA licenses, perform the following steps.

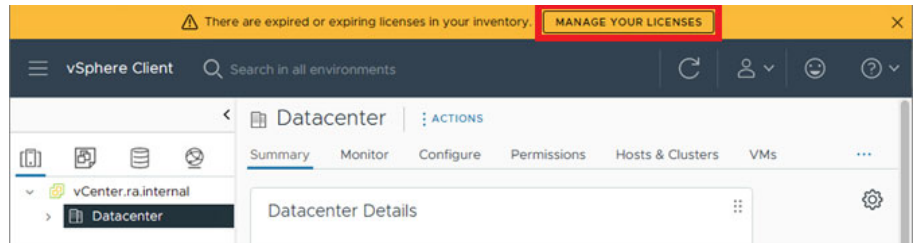
1. Access the following VMware® website:
<https://vcenter.ra.internal>.
2. Under Getting Started, select Launch vSphere Client.



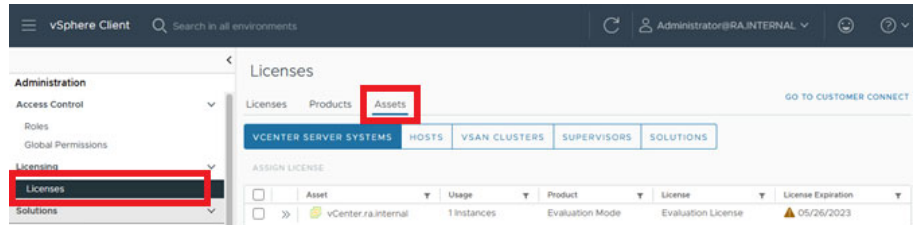
3. Logon with the following credentials.
Username: administrator@ra.internal
Password: <system-specific password>
4. Select Login.



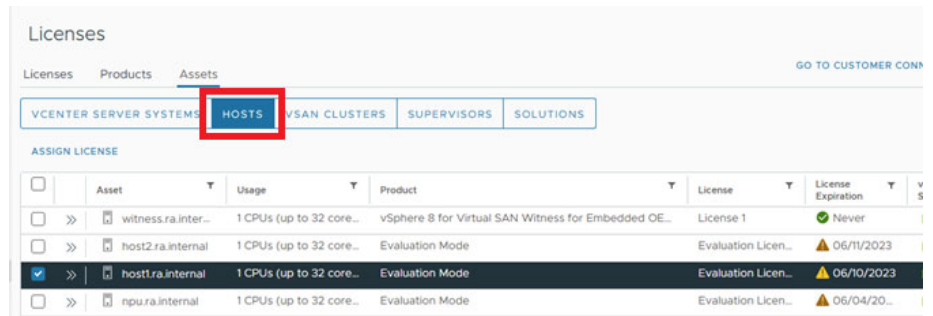
- At the top of the home page, select Manage Your Licenses.



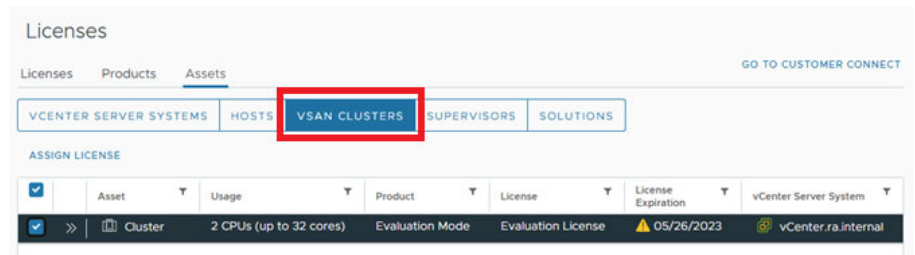
- In the left pane, select Licenses, then select the Assets tab, and then verify the vCenter.ra.internal asset is selected.



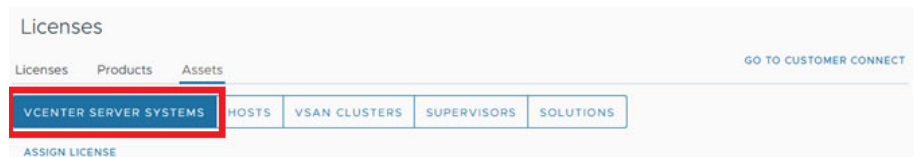
- From the top, select the Hosts tab and verify host1.ra.internal is selected.



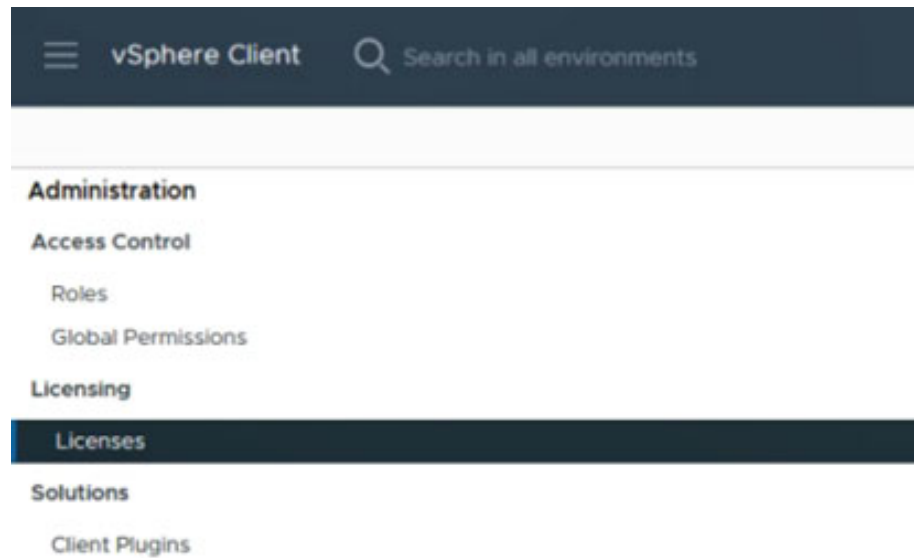
- From the top, select vSAN Clusters and verify that Cluster is selected.



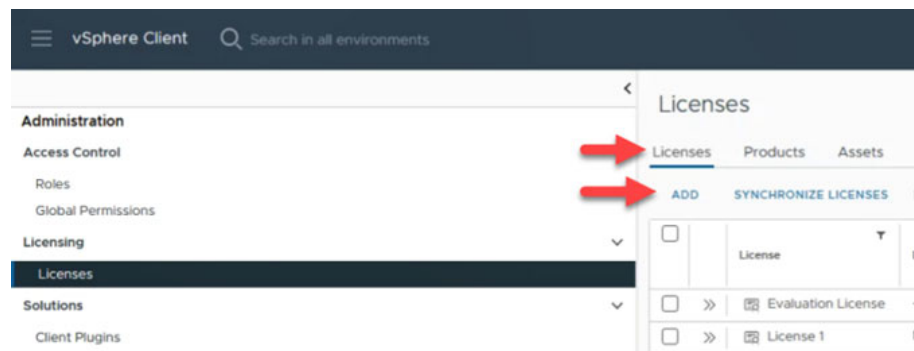
- From the top, select vCenter Server Systems.



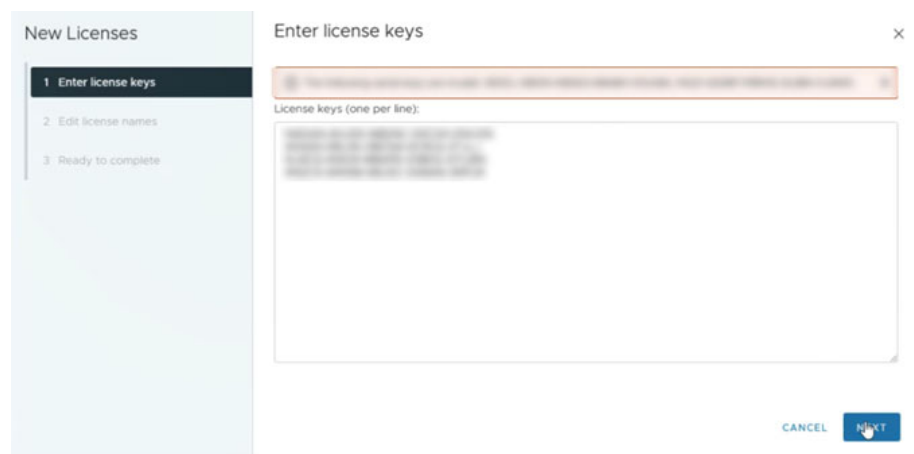
10. In the left pane, select Licensing > Licenses.



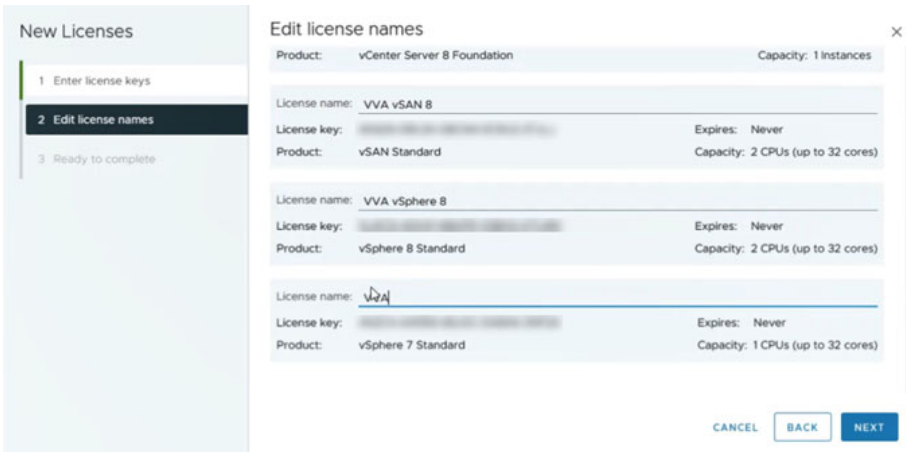
11. In the right pane, under Licenses, select Add.



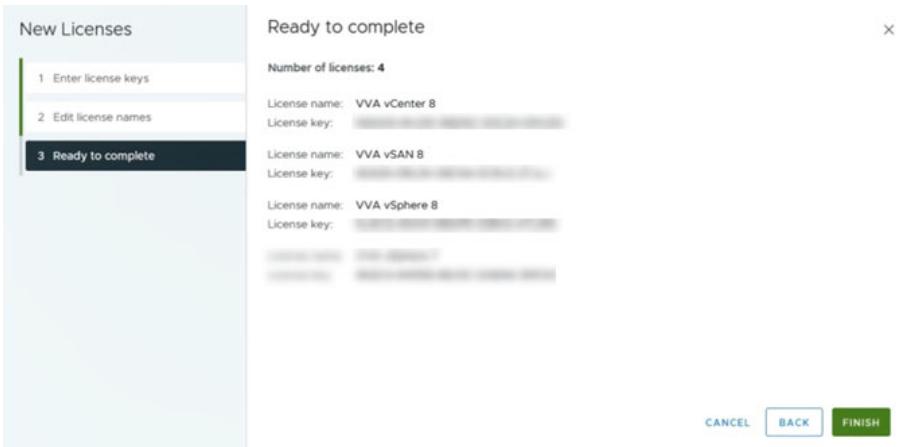
12. Enter the license keys that were supplied with your appliance purchase and select Next.



13. Rename each license key as needed and select Next.



14. Verify the license key names. If any changes are needed, select Back.

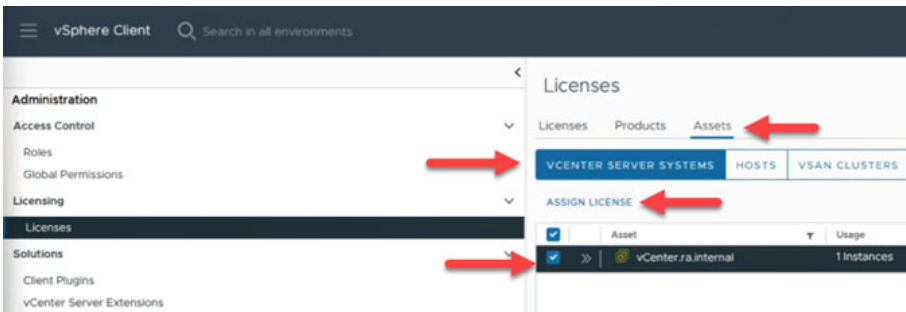


15. After verifying the license names, select FINISH.

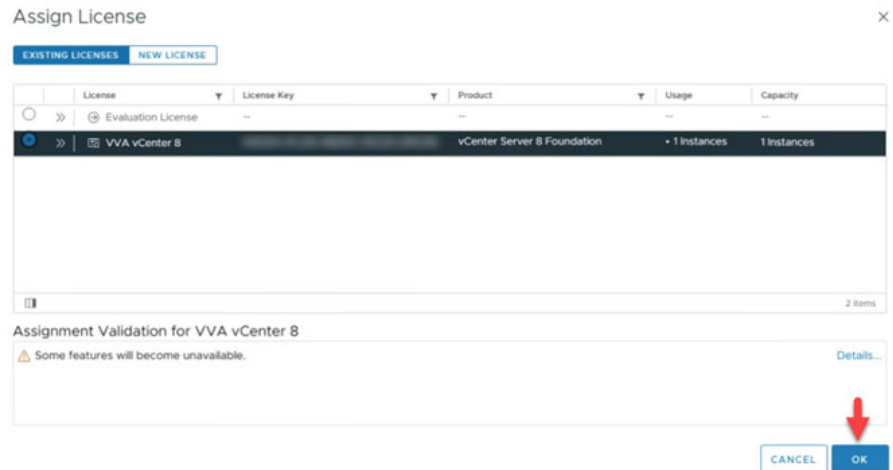
The main License page is displayed.

16. In the left pane, select Licenses, then the Assets tab at the top.

17. Verify that the vCenter.ra.internal asset is selected and then select the Assign License link.

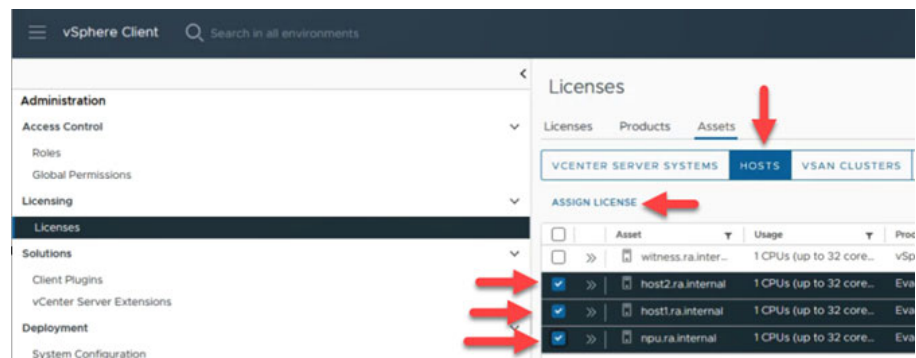


18. On the Assign License page, verify that the new vCenter Foundation license key is available and selected and then select Ok.



The main Assets page is displayed.

19. Select HOSTS and verify that the following three assets are checked:
- host1.ra.internal
 - host2.ra.internal
 - npv.ra.internal



20. Select the Assign License link.
21. An Assign License dialog box is displayed to confirm license configuration on multiple objects. Select Yes.

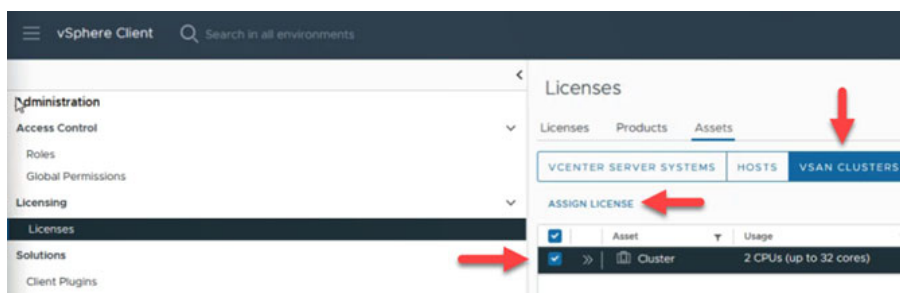


22. The Assign License page appears.
- Verify the new vSphere standard license key is available and selected and select Ok.

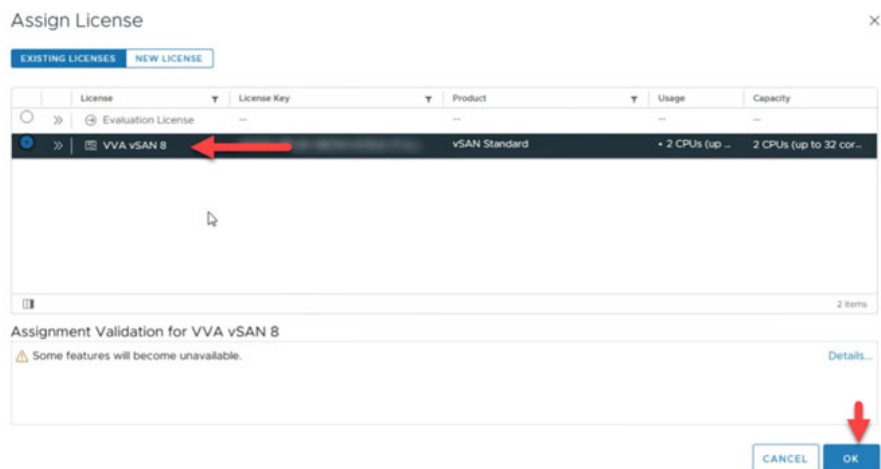


The Hosts page is displayed.

23. Select vSAN Clusters.
Verify that Cluster is selected and select the Assign License link.

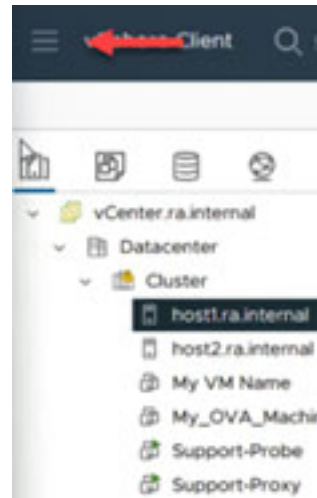


24. On the Assign License page, verify the new vSAN standard license key is available and selected and select **Ok**.

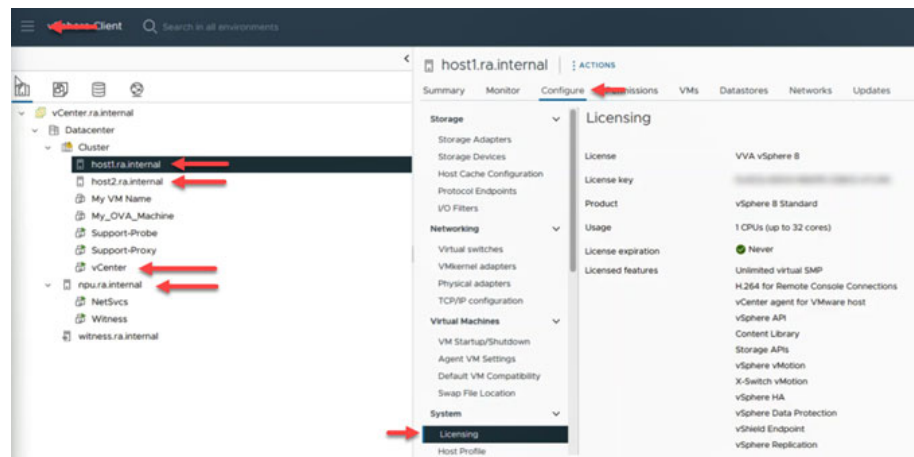


The Cluster page is displayed.

25. In the upper-left corner, select the menu navigation icon > Inventory.



26. Confirm that each asset that the license was applied to is now visible.



Repeat the prior steps to add any licenses not installed on the system.

Change Default Passwords

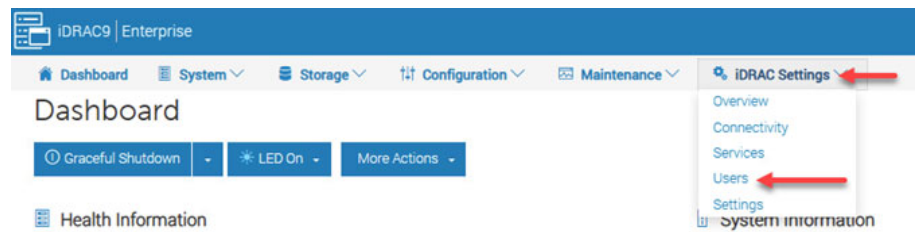
This section provides details on how to change the default passwords for each component.

Baseboard Management Controller

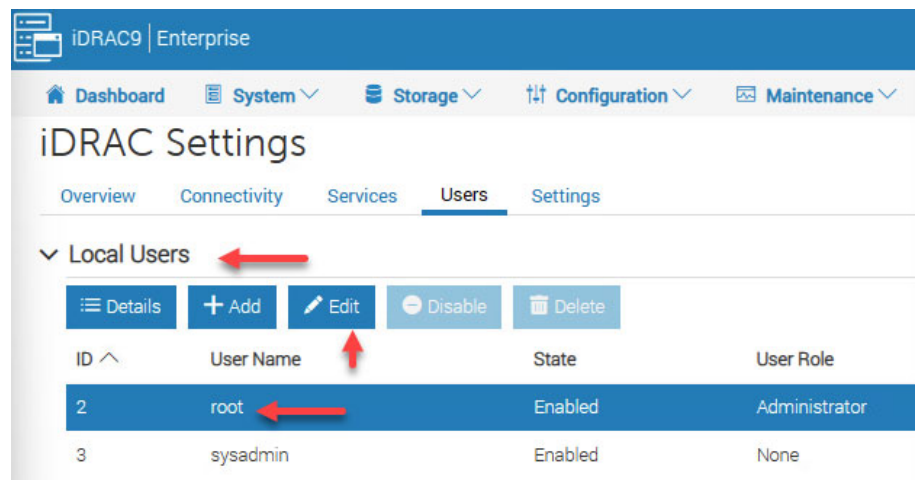
Each VVA has a Baseboard Management Controller (BMC) with two host management controllers. To change the system password on each BMC, perform the following steps.

1. Open a web browser and navigate to:
`https://192.168.249.11`
2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Log In.

4. On the Dashboard page, select iDRAC Settings > Users.



5. On the iDRAC Settings page, select Local Users, then root user, then Edit.



6. In the Edit User dialog box, enter the new password in the Password and Confirm Password fields.
7. When finished, select Save.

8. When the success dialog box is displayed, select Ok.
9. Sign out of the BMC website and the new credentials.
10. Repeat steps 1...9 for the other host management controller.



For step 1, use the URL address for the other host controller:
<https://192.168.249.12>

VMware vSphere

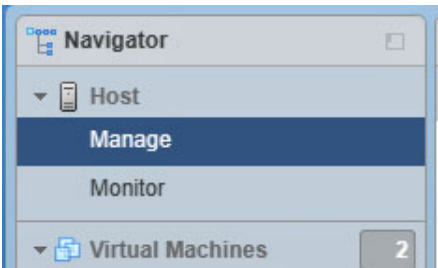
The VMware vSphere has one NPU, one Witness, and two cluster hosts. To change the password for each one, perform the following steps on each host.

1. Open a web browser and navigate to:
<https://192.168.249.13>
2. Sign in with the following credentials.
 Username: root
 Password: <system-specific password>

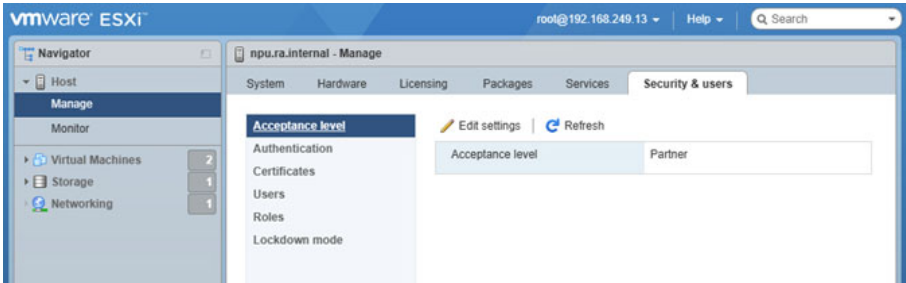
3. Select Login.



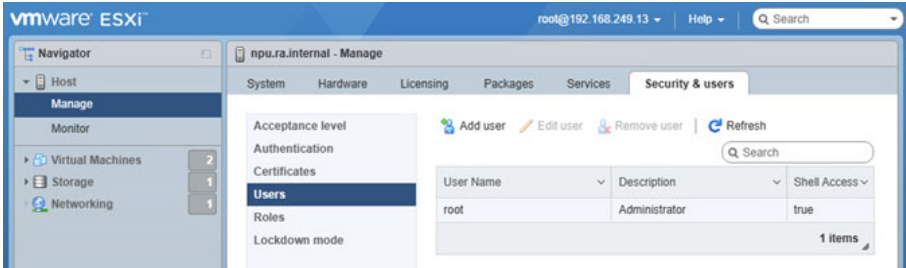
4. Under the navigation pane, select Manage.



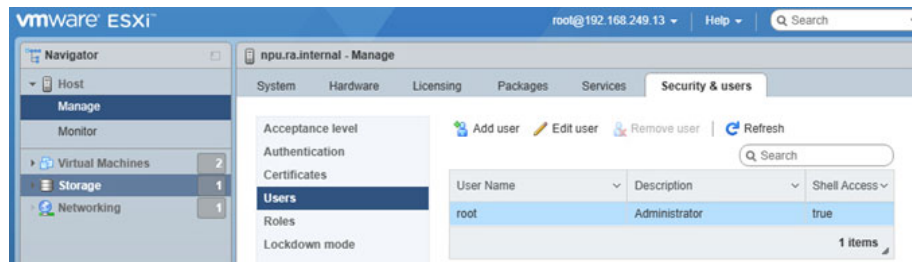
5. On the Manage page, select the Security and Users tab.



6. Under the Acceptance Level Navigation Pane, select Users.



7. Select root and then Edit User.



8. In the Edit User dialog box, enter the new password in the Password and Confirm Password fields.

Edit User

User name	root
Description	Administrator
Password
Confirm password
Enable Shell Access	<input checked="" type="checkbox"/>

Save Cancel

9. When finished, select Save.
10. Sign out of the VMware ESXi™ webpage and the new credentials.
11. Repeat steps 1...10 for each of the two cluster hosts and the Witness.



For step 1, use the following URL addresses for each ESX host:

host1: <https://192.168.249.14>

host2: <https://192.168.249.15>

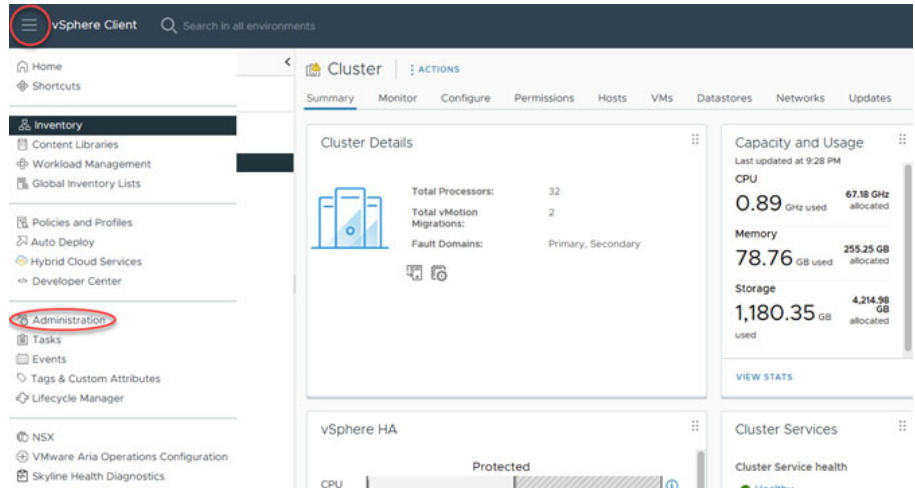
Witness: <https://192.168.249.16>

VMware vCenter

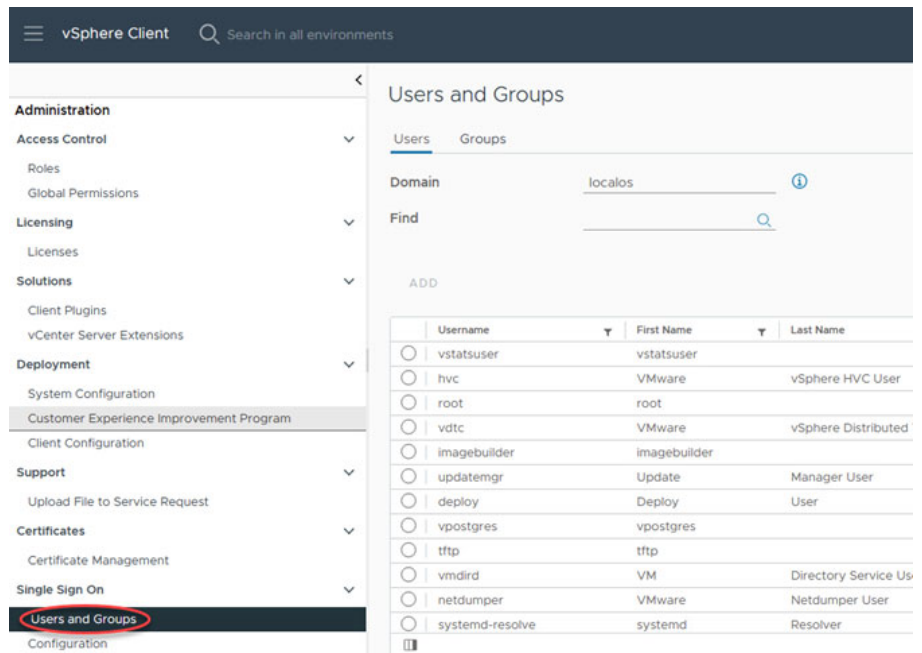
To change the password in VMware vCenter®, perform the following steps.

1. Open a web browser and navigate to:
<https://192.168.249.18>
2. Sign in with the following credentials.
Username: administrator@ra.internal
Password: <system-specific password>
3. Select Login.

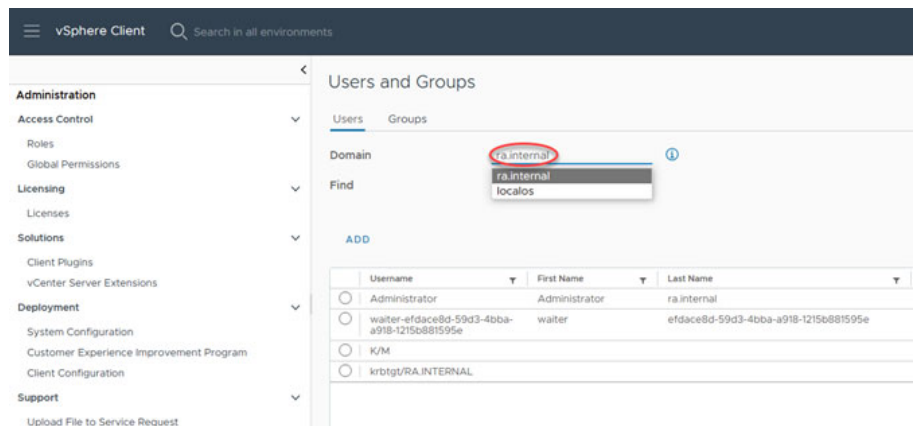
4. On the Home Page, select the menu navigation icon and then select Administration on the left side.



5. Under the Administration Navigation pane, select Single Sign On > Users and Groups.



6. From the Domain dropdown menu, verify ra.internal is selected.



7. Under the ra.internal domain users, select the Administrator radio button.

8. Select Edit.
9. In the Edit User dialog box, enter the new password in the Password and Confirm Password fields.
10. When finished, select Save.

Dialog box titled "Edit User" with a close button (X) in the top right corner.

Fields and values:

- Username: Administrator
- Password: [Masked] (Eye icon for visibility toggle)
- Confirm Password: [Masked] (Eye icon for visibility toggle)
- First Name: Administrator
- Last Name: ra.internal
- Email: [Empty]
- Description: [Empty text area]

Buttons: CANCEL, SAVE

11. Sign out of the vCenter webpage, and the new credentials.

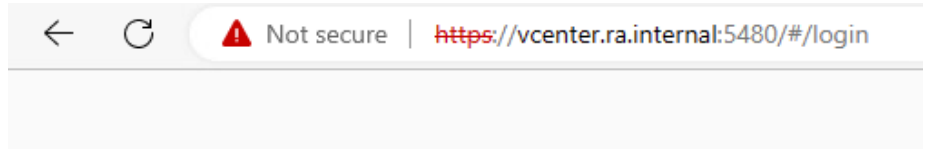
VMware vCenter Server Appliance

To change the password in VMware vCenter Server[®] Appliance[™], perform the following steps.

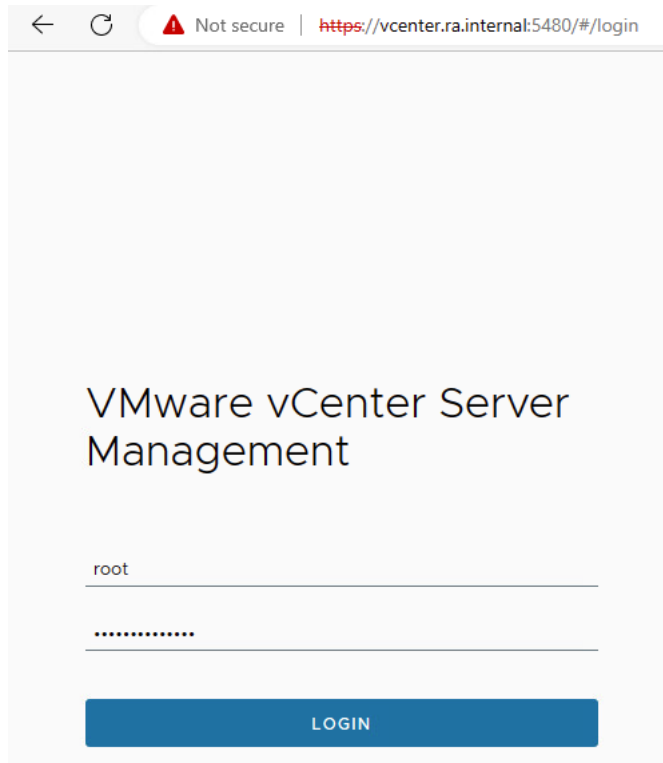
1. Open a web browser and navigate to <https://vcenter.ra.internal:5480/login>



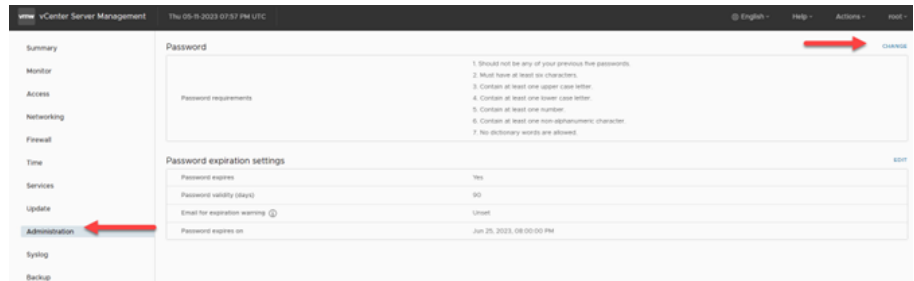
This configuration uses TCP port 5480.



2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Login.



4. In the left column, select Administration and then select Change in the top right.



5. Enter the Old Password and New Password and then select Save.

Change Password

Current password:
New password: ⓘ
Confirm password:

CANCEL
SAVE

6. Sign out of the vCenter Appliance and then the new credentials.

Virtual Machines: NetSvcs

To change the password in the NetSvcs VM, perform the following steps.

1. Open a web browser and navigate to:
`https://vcenter.ra.internal`
2. Sign in with the following credentials.
Username: `administrator@ra.internal`
Password: <system-specific password>
3. Select Login.
4. On the Hosts and Cluster view, expand `npv.ra. internal` and select NetSvcs.
5. On the Summary tab, select Launch Web Console.
6. On the Launch Console dialog box, select `seSign in` and `Ok`.
7. In the NetSvcs Web Console, sign in as root with the system-specific password.

```
NetSvcs login: root
Password:
```

```
Last login:
```

```
[root@NetSvcs ~]# _
```

8. Enter the following command:
`passwd`
9. Press ENTER.
10. Enter the new password and confirm the new password.

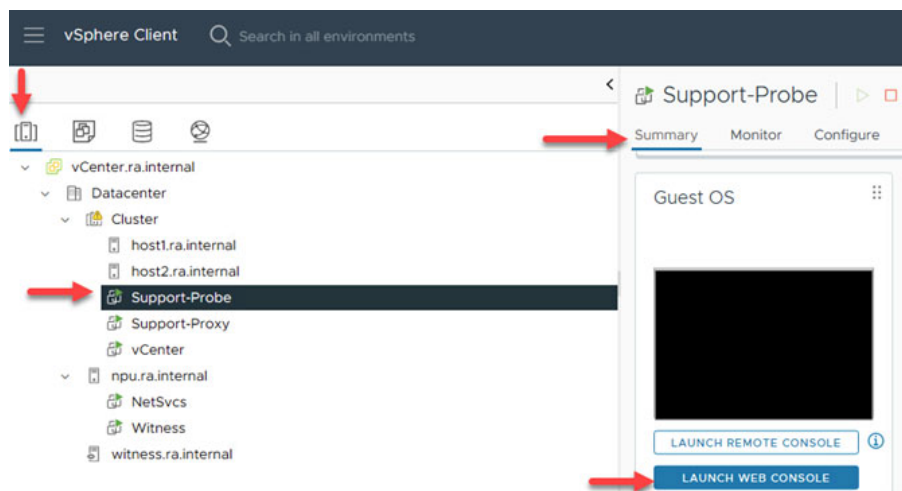
```
[root@netsvcs ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

11. Sign in as sysadmin and repeat steps 8 and 9.
12. To sign out, enter:
`logout`
13. Press ENTER.

Virtual Machines: Support-Probe

To change the password in the Support-Probe VM, perform the following steps.

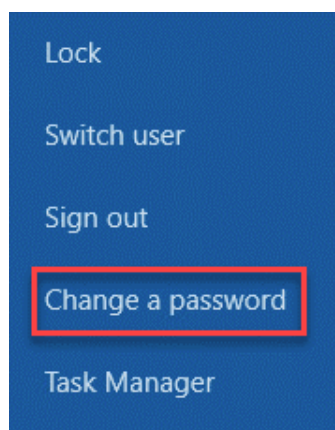
1. Open a web browser and navigate to:
<https://192.168.249>
2. Sign in with the following credentials.
Username: administrator@ra.internal
Password: <system-specific password>
3. Select Login.
4. Select the left Hosts and Clusters icon, expand vCenter.ra.internal, then expand Cluster, then select Support-Probe.
5. On the right Summary tab, select Launch Web Console.



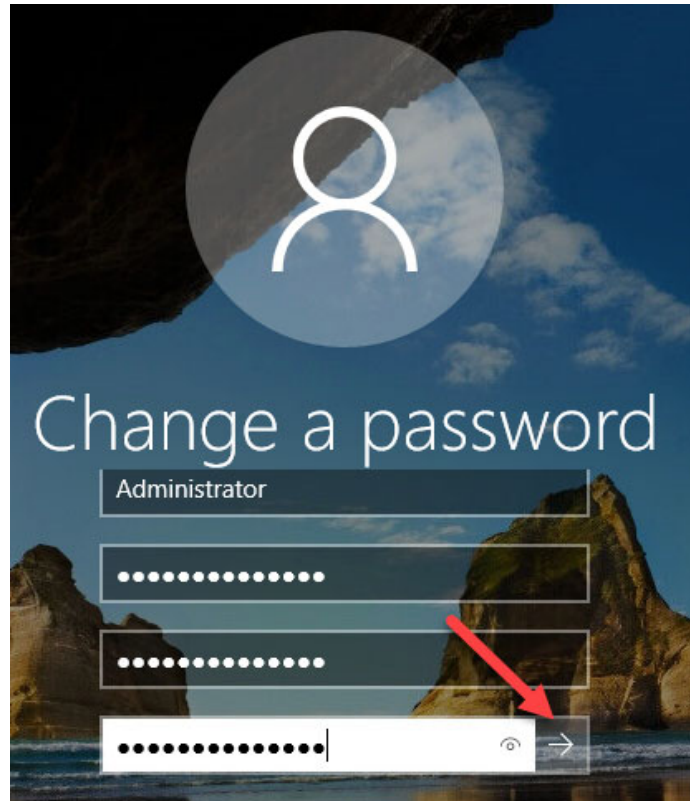
6. In the upper right corner of the console, select Send Ctrl+Alt+Delete.



7. Once logged in, press CTRL+ALT+DELETE on the keyboard and then select Change a Password.



8. Enter the current password, then enter the new password twice to confirm the change. When finished, select the arrow.



9. Sign out of Windows and sign on again to confirm the new credentials.

Virtual Machines: Support-Proxy

To change the password in the Support Proxy, perform the following steps.

1. Open a web browser and navigate to:
`https://vcenter.ra.internal`
2. Sign in with the following credentials.
Username: `administrator@ra.internal`
Password: `<system-specific Password>`
3. Select Log In.
4. On the Hosts and Cluster view, expand `vcenter.ra.internal` and select Support-Proxy.
5. On the Summary tab, select Launch Web Console.
6. On the Launch Console dialog box, select Ok.
7. In the Support-Proxy Web Console, sign in as root with the system-specific password.

```
Support-Proxy login: root
Password:
Last login: Tue Apr 18 11:28:30 on tty1

[root@Support-Proxy ~]# _
```

8. Enter the following command:
`passwd`
9. Press ENTER.

10. Enter the new password and confirm the new password.

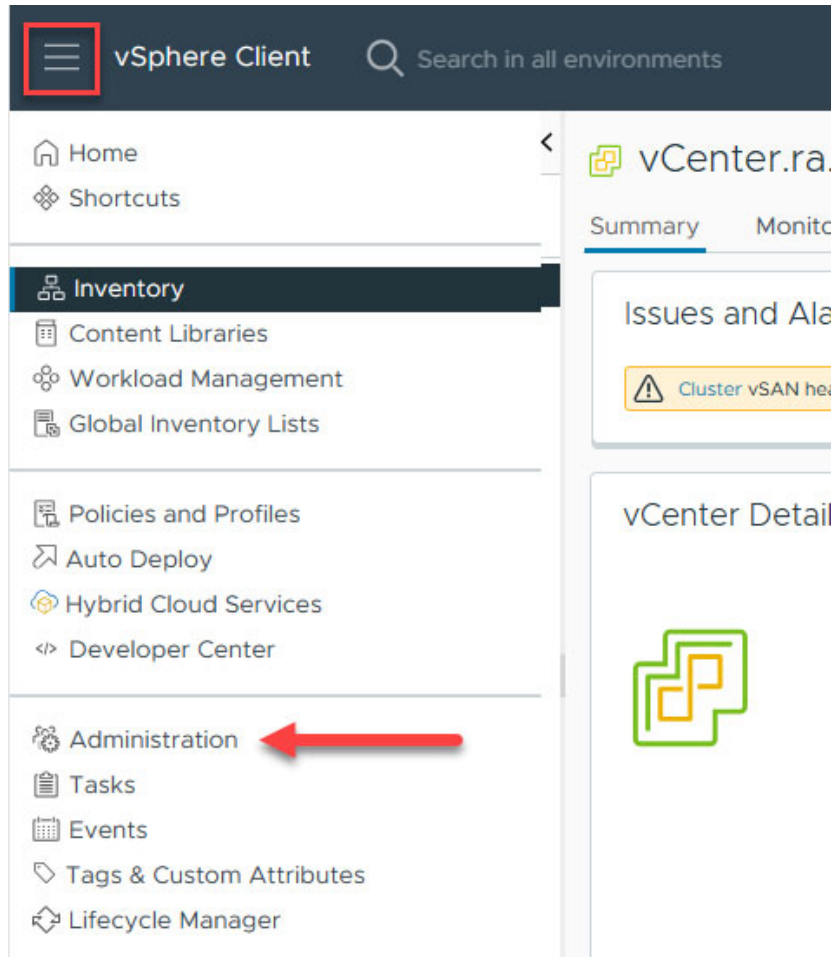
```
Changing password for user root.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

11. Sign in as sysadmin and repeat Step 5 and 6.
12. To sign out, enter:
 logout
13. Press ENTER.

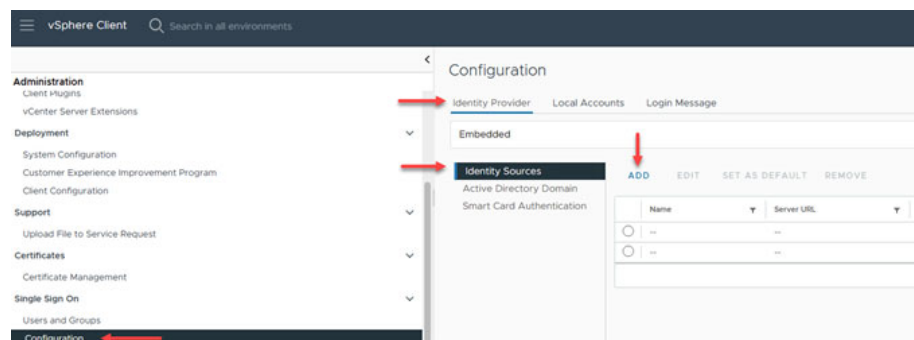
Configure Active Directory Authentication

You can use Active Directory user accounts to manage the VMware vCenter, by adding a Lightweight Directory Access Protocol (LDAP) identity source to your VVA. To implement this configuration, perform the following steps.

1. Open a web browser and navigate to:
`https://vcenter.ra.internal`
2. Sign in with the following credentials.
Username: `administrator@ra.internal`
Password: `<system-specific password>`
3. Select Login.
4. In the upper-left corner of the vSphere Web Client, select the menu navigation icon and then select Administration.



5. In the Administration navigation view, scroll down and select Configuration.
6. Select the Identity Provider tab, then select Identity Sources > Add.



7. In the Add Identity Source wizard, select the Active Directory over LDAP server.

Add Identity Source

Identity Source Type

Active Directory (Integrated Windows Authentication)

Active Directory (Integrated Windows Authentication)

Active Directory over LDAP

Open LDAP

Local operating system of SSO server

the node to an Active Directory domain.

⚠ Integrated Windows Authentication will be depreciated in vSphere 7.0. Support for IWA continues to be available in vSphere 7.0 and will be phased out in a future release. [Learn more](#)

Domain name *

example.com

• Use machine account

○ Use Service Principal Name (SPN)

CANCEL

ADD

8. In the Domain name field, add the following.

- For Name, enter the domain name (DN).
- For Base DN for users, enter the DN.

This string is formed by separating each part of the fully qualified domain name (FQDN) with 'DC='.

FQDN	DN
example.com	DC=example,DC=com
ra.rockwell.com	DC=ra,DC=rockwell,DC=com
csn.fabrikam.com	DC=CSN,DC=fabrikam,DC=COM

For example: If the FQDN is 'example.com', enter the DN of 'DC=example,DC=COM'.

- For the Base DN for groups, enter the preceding DN string.
- For Domain name, enter the FQDN.
- For Domain Alias, enter the NetBIOS alias of the domain.

By default, the NetBIOS alias is the first portion of the FQDN.

For example: If the FQDN is 'example.com', enter the NetBIOS alias of 'Example'.

FQDN	NetBIOS Alias
example.com	Example
ra.rockwell.com	RA
csn.fabrikam.com	CSN

- For Username, enter a domain user account that has administrative privileges in the domain.
- Enter the password for the administrative user.
- Select Add.

9. Select the newly created Identity Source, and then select Set as Default Domain.

10. A warning dialog box displays. Select Ok.

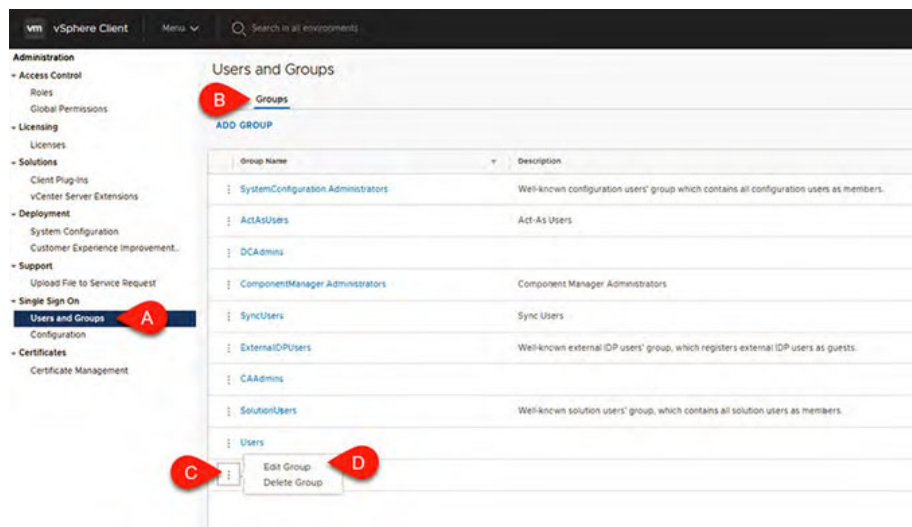


11. In the Administration navigation view, select Users and Groups (A).

12. On Users and Groups, select the Groups tab (B).

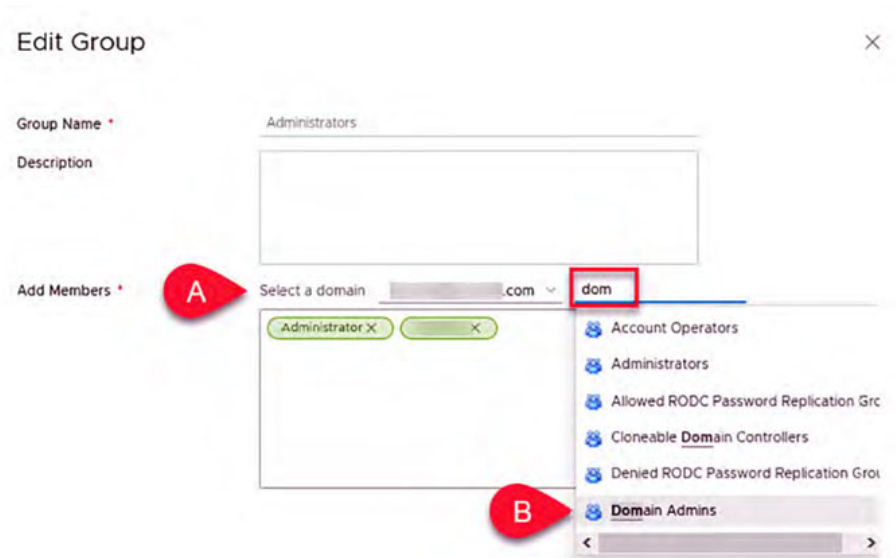
13. On Groups, select the vertical ellipsis icon next to the Administrators group (C).

14. From the Administrators group dropdown menu, select Edit Group (D).



15. In the Edit Group window:

- From the Select a Domain dropdown menu, select the newly added Windows Active Directory (A).
- In the search field, enter:
dom
- From the search finds (B), select the Domain Admins user group.



16. Select Ok.

17. Select the username in the top right of the window (A).

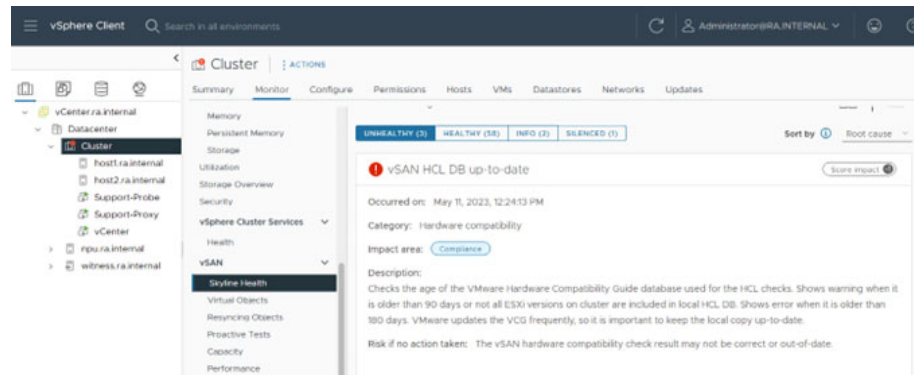
18. From the dropdown menu, select Logout (B).

19. In the vSphere web client sign in, verify you can sign in with AD credentials.

Update the Hardware Compatibility List

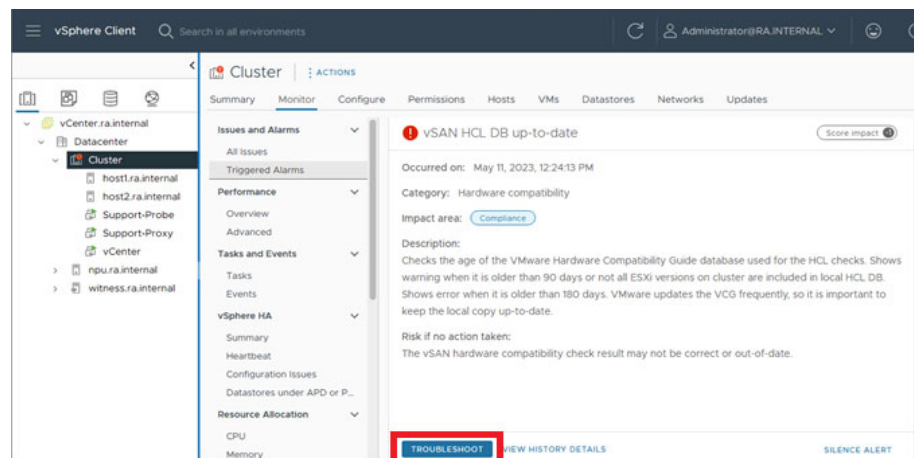
You must keep your hardware compatibility list (HCL) updated, as it is critical to the stability of the VMware vSAN environment.

If the VVA displays an error that the VVA cannot automatically access the most current version, the HCL must be updated.

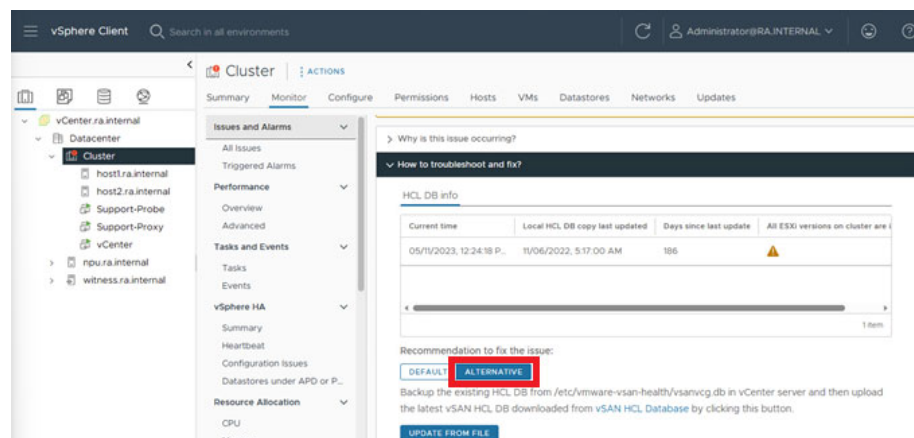


To update the HCL to the most current version, perform the following steps.

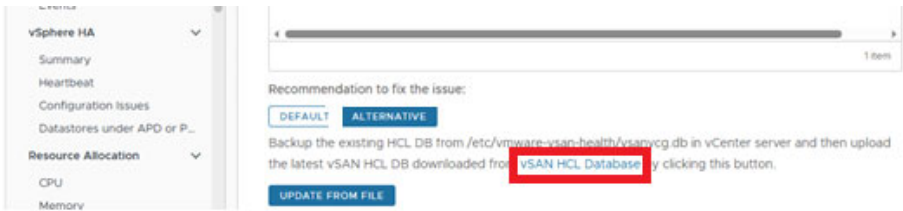
1. On the bottom of the vSAN HCL DB up-to-date alert page, select Troubleshoot.



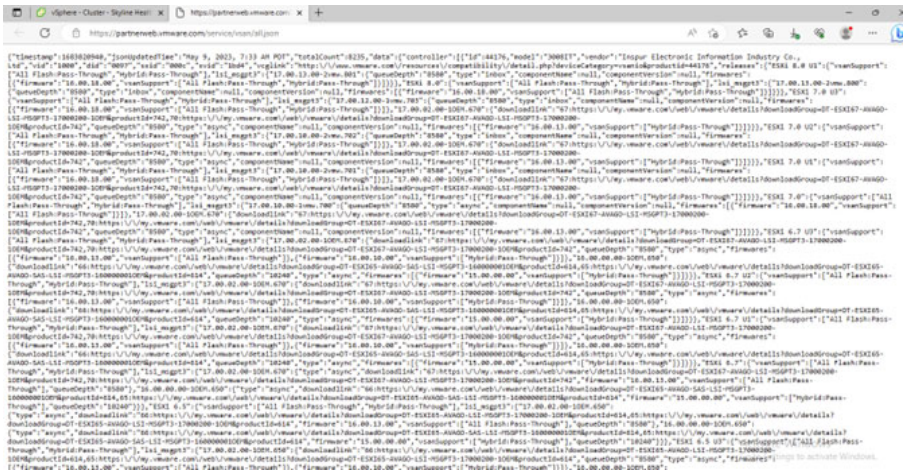
2. In the bottom Recommendation to fix the issue section, select Alternative.



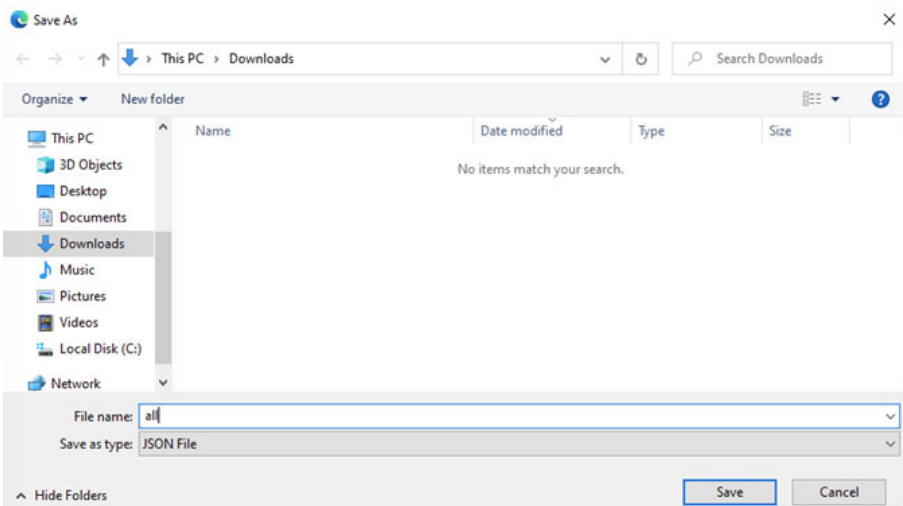
3. In the Recommendation description, select the vSAN HCL Database hyperlink.



4. The web browser displays a database file similar to the following.



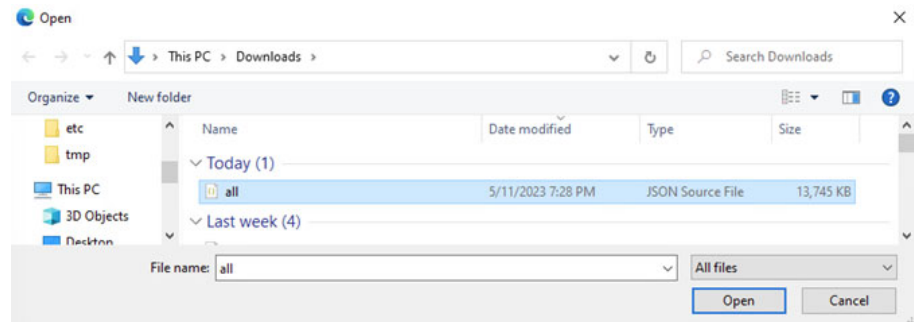
5. In the webpage, right-click and save the page as a JSON file. Functionality can vary depending on the web browser.



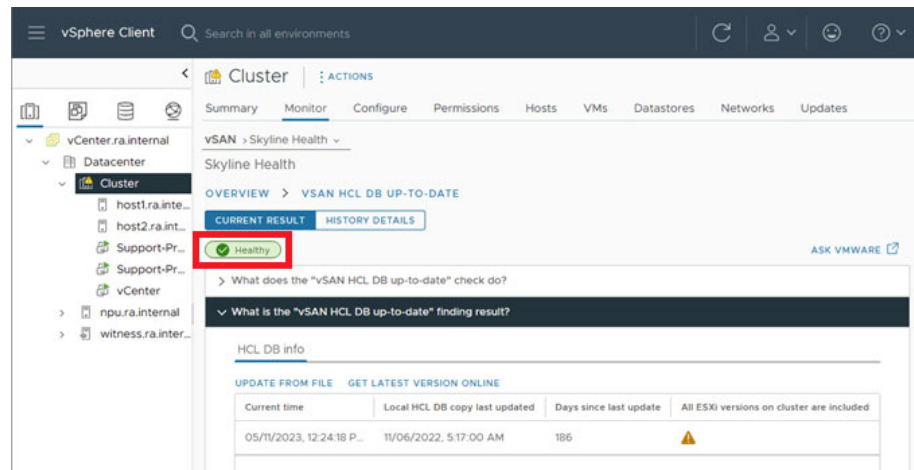
6. Return to the vCenter.

7. At the bottom of the page, select Update from File.

8. Select the file that is downloaded in step 5 and then select Open.



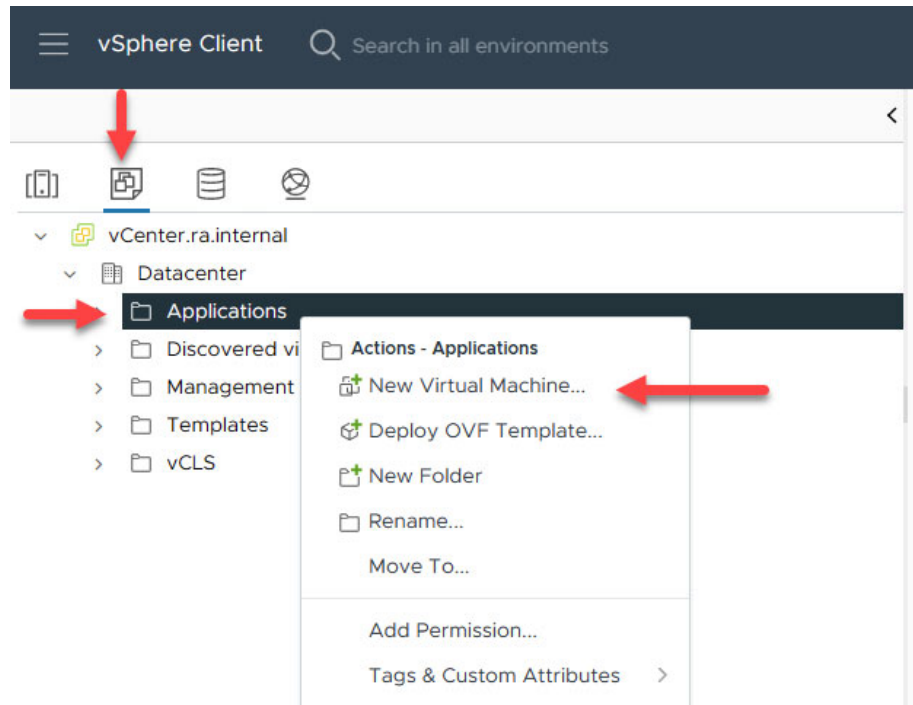
9. The HCL begins the update.
When the update is complete, a green *Healthy* logo is displayed.



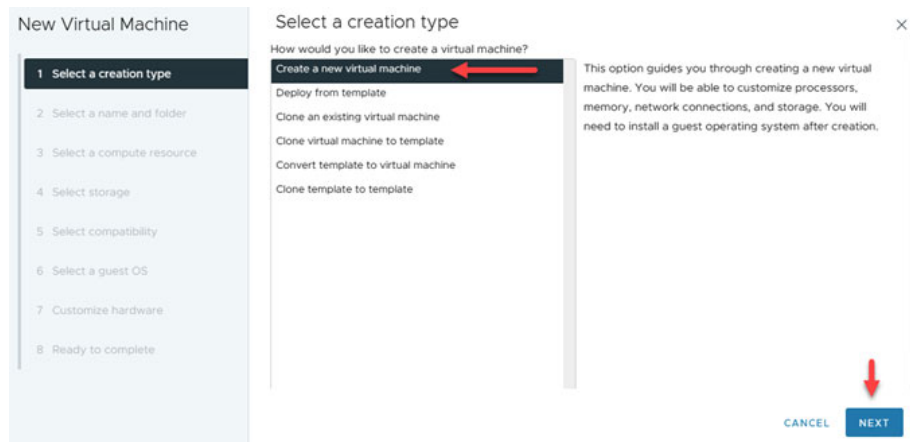
Add a Virtual Machine

To add a VM, perform the following steps.

1. Open a web browser and navigate to:
`https://vcenter.ra.internal`
2. Sign in with the following credentials.
Username: `administrator@ra.internal`
Password: <system-specific password>
3. Select Login.
4. In the left pane, navigate to the Applications folder.
Right-click on the Applications folder and then select New Virtual Machine.



5. Select Create a new VM and then select Next.



6. Name the VM, select the Application Folder, and then select Next.

New Virtual Machine

- Select a creation type
- Select a name and folder**
- Select a compute resource
- Select storage
- Select compatibility
- Select a guest OS
- Customize hardware
- Ready to complete

Select a name and folder
Specify a unique name and target location

Virtual machine name: My VM_Name

Select a location for the virtual machine.

- vCenter.ra.internal
 - Datacenter
 - Applications**
 - Discovered virtual machine
 - Management
 - Templates
 - vCLS

CANCEL BACK **NEXT**

7. Select host1.ra.internal as the compute resource.

In the Compatibility section, verify that the compatibility check is successful and then select Next.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource**
- Select storage
- Select compatibility
- Select a guest OS
- Customize hardware
- Ready to complete

Select a compute resource
Select the destination compute resource for this operation

- Datacenter
 - Cluster
 - host1.ra.internal**
 - host2.ra.internal
 - npu.ra.internal
 - witness.ra.internal

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK **NEXT**

8. Select vSanDatastore for the data storage location and then select Next.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource
- Select storage**
- Select compatibility
- Select a guest OS

Select storage
Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy: Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type
<input type="radio"/>	host1.BOSS	--	319 GB	9.37 GB	309.63 GB	VMFS 6
<input checked="" type="radio"/>	vsanDatastore	--	3.49 TB	12.01 TB	2.34 TB	vSAN

Items per page: 10 2 items

CANCEL BACK **NEXT**

9. From the Compatible with dropdown menu, select the VMware ESXi software that is most compatible with the intended application.

In this example, the most current version of 8.0 is selected.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource
- Select storage
- Select compatibility**
- Select a guest OS
- Customize hardware
- Ready to complete

Select compatibility

Select compatibility for this virtual machine depending on the hosts in your environment. The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: **ESXi 8.0 and later**

Virtual machines using hardware version 20 provide the best performance and latest features available in ESXi 8.0.

CANCEL BACK **NEXT**

10. Select the operating system and version that the VM will be installed on, and then select Next.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource
- Select storage
- Select compatibility
- Select a guest OS**
- Customize hardware
- Ready to complete

Select a guest OS

Choose the guest OS that will be installed on the virtual machine. Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: **Windows**

Guest OS Version: **Microsoft Windows Server 2019 (64-bit)**

☐ Enable Windows Virtualization Based Security

Compatibility: ESXi 8.0 and later (VM version 20)

CANCEL BACK **NEXT**

11. Configure the fields so the new VM is set up appropriately for the intended application.



The default setting for adapter type is E1000E.

Rockwell Automation recommends using the VMXNET 3 adapter, which can be selected from the Adapter Type dropdown menu.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource
- Select storage
- Select compatibility
- Select a guest OS
- Customize hardware**
- Ready to complete

Customize hardware

> CPU: 2

> Memory: 4 GB

> New Hard disk *: 90 GB

> New SCSI controller: LSI Logic SAS

> New Network: **Management VM Network**

Status: ☒ Connect At Power On

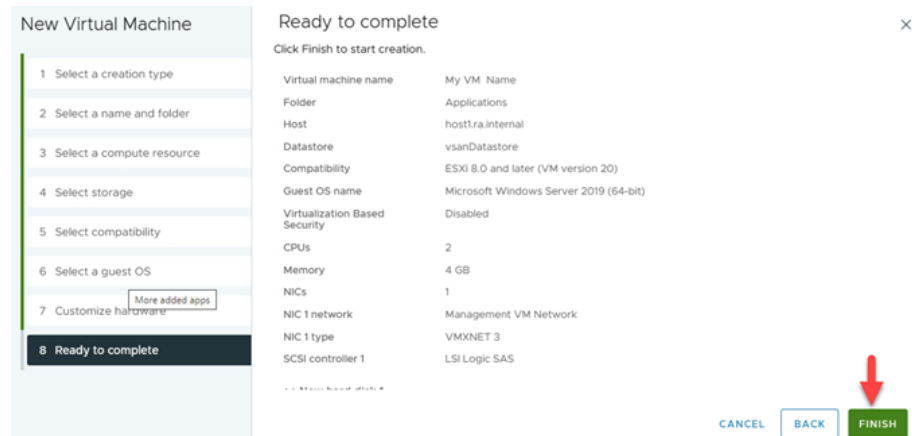
Adapter Type: **VMXNET 3**

MAC Address: Automatic

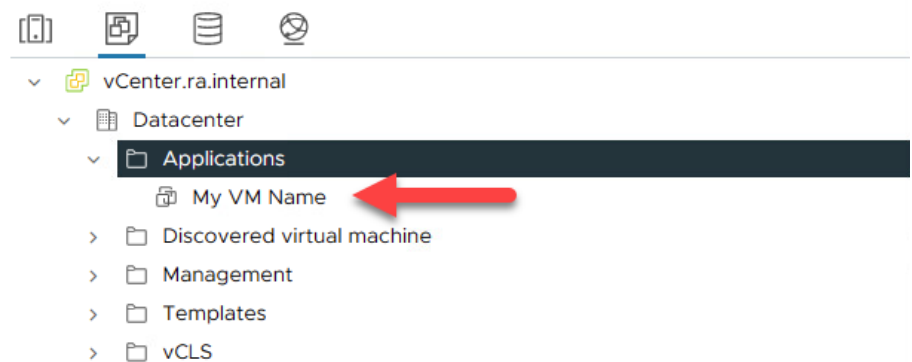
> New CD/DVD Drive: ☐ Connect At Power On

CANCEL BACK **NEXT**

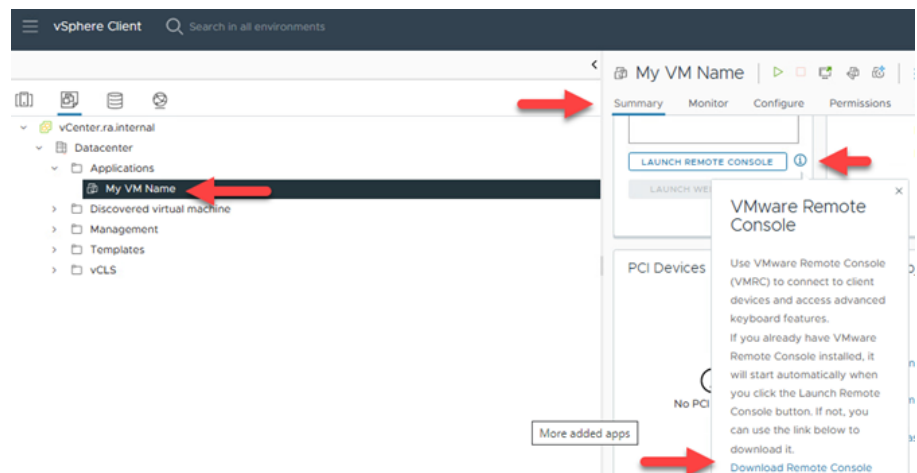
12. Review the configuration for the new VM.
If any changes are needed, select Back.
If the configuration is correct, select Finish.



13. The new VM is now visible under Actions Navigation pane > Applications.



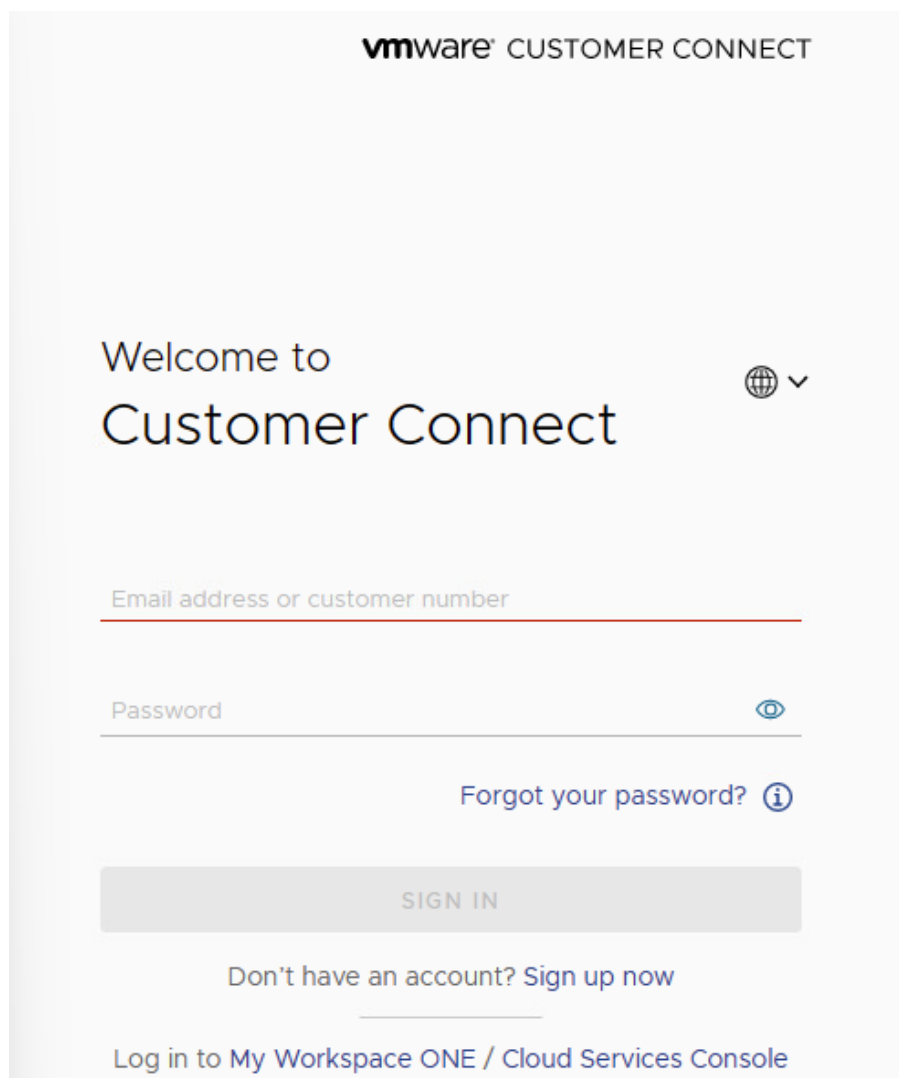
14. On the Summary tab of the new VM, select the Launch Remote icon, then select Download Remote Console.



15. From the download page, select the correct OS version for your application.

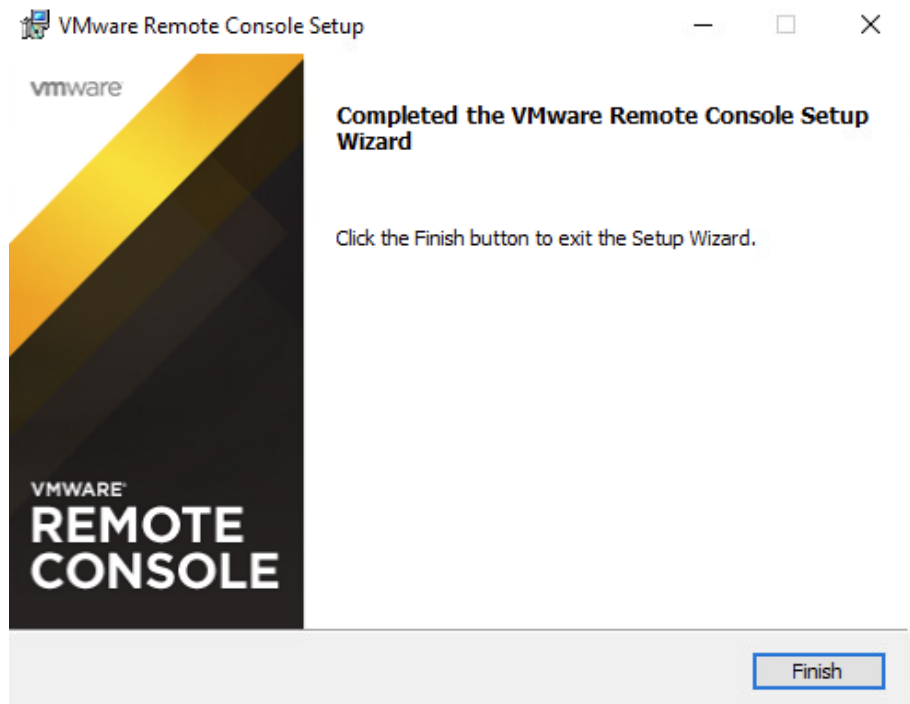


16. Sign in to VMware Customer Connect with your email address or customer number and password.

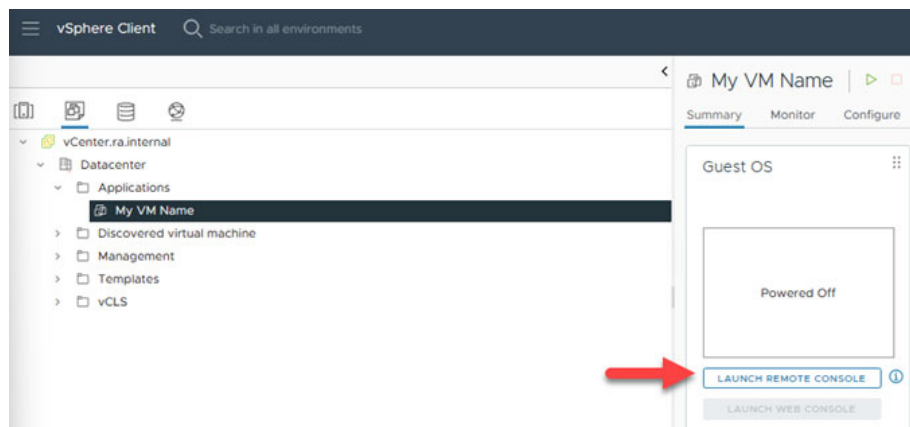


17. A zip file is downloaded.
18. Extract the zip file and launch the EXE (application) file.
19. The VMware Remote Console™ Install Wizard is displayed.
20. Accept the end user license agreement and install the software application.

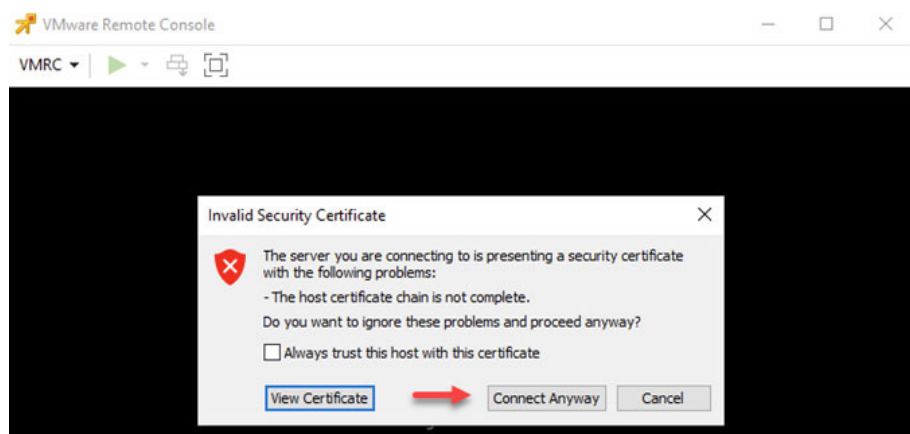
21. When the installation is complete, select Finish.



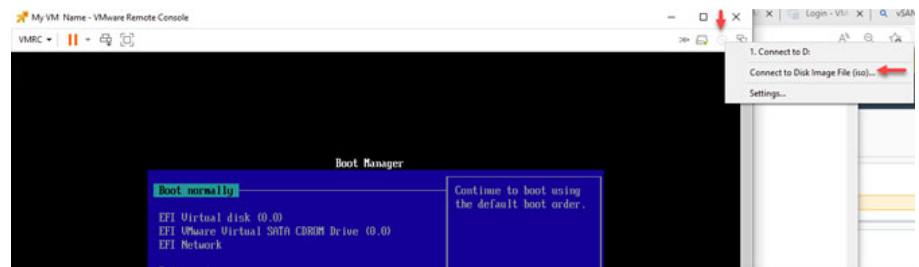
22. Return to vCenter and select Launch Remote Console.



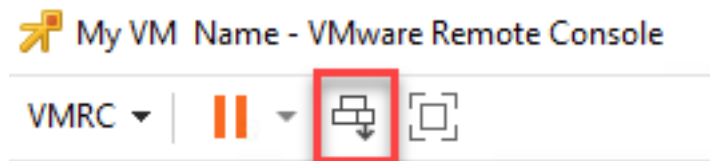
23. If any certificate warnings are displayed, select Connect Anyway.



24. On the Boot Manager Screen, in the quick access toolbar, right-click the disk image and select Connect to Disk image file (iso).



25. In Windows File Explorer, navigate to the disk image and select Open.
26. On the Boot Manager screen, in the quick access toolbar, select the Send Ctrl+Alt+Delete icon.



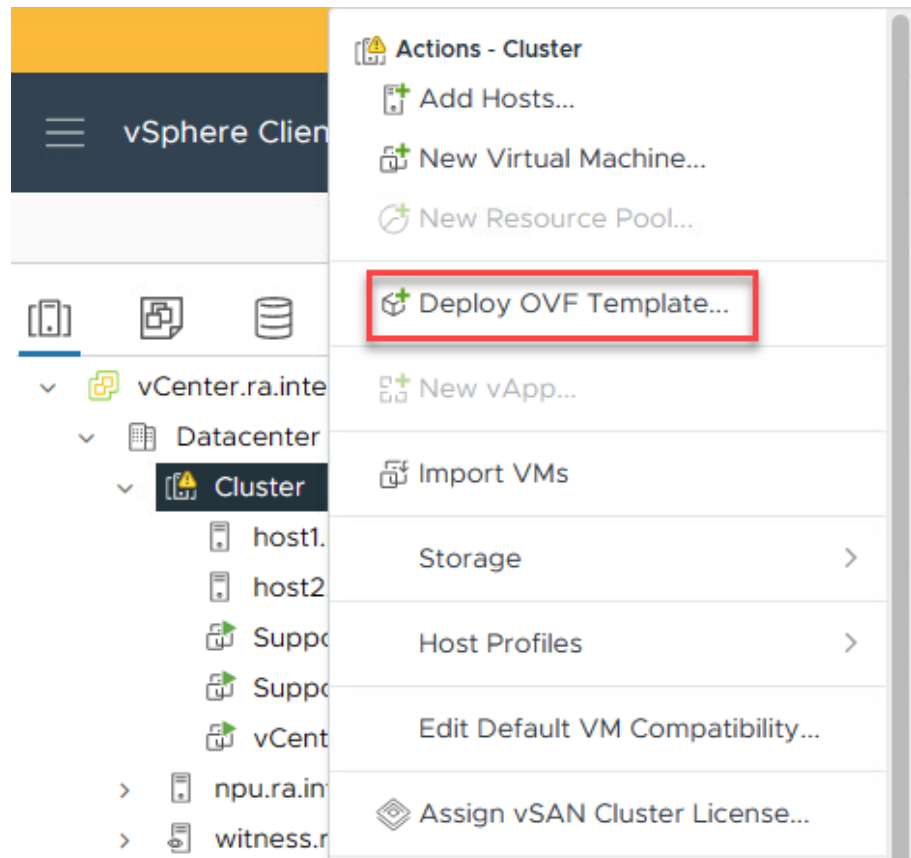
27. To finish the installation, follow the prompts.
Prompts might vary based on the operating system you are using.

The new VM is now added to your network.

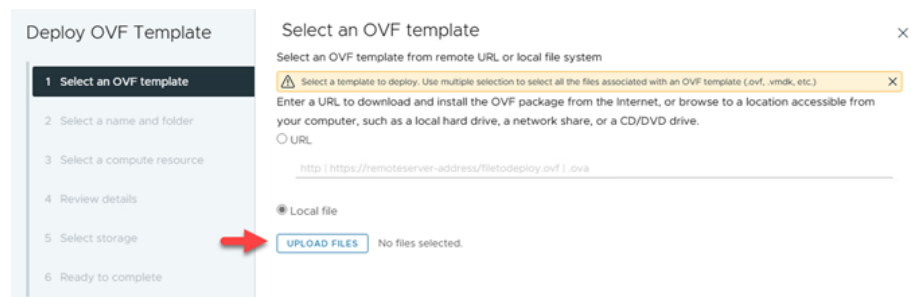
Import an OVA Template

To import an OVA template, perform the following steps.

1. Open a web browser and navigate to:
`https://vcenter.ra.internal`
2. Sign in with the following credentials.
Username: `administrator@ra.internal`
Password: <system-specific password>
3. Select Login.
4. On the Main Navigation pane, right-click on Clusters and select Deploy OVF Template...



5. Select the Local file radio button, and then select Upload Files.



6. In Windows File Explorer, navigate to the appropriate OVA file, select Open, and then select Next.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/flatiddeploy.ovf | .ova

Local file

UPLOAD FILES

Alma8-20230227r.ova

CANCEL

NEXT

7. Name the VM something specific to its intended use, select the location for the VM, and then select Next.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

My_OVA_Machine

Select a location for the virtual machine.

vCenter.ra.internal

Datacenter

Applications

Discovered virtual machine

Management

Templates

vCLS

CANCEL

BACK

NEXT

8. Select a compute resource, then select the VM.
Be sure the compatibility check succeeded and then select Next.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- ▼ Datacenter
 - > Cluster ←
 - > npu.ra.internal
 - > witness.ra.internal

Compatibility

✓ Compatibility checks succeeded. ←

CANCEL BACK **NEXT**

9. Review the details of the template and then select Next.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Select networks
- Ready to complete

Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Download size	2.4 GB
Size on disk	4.4 GB (thin provisioned) 60.0 GB (thick provisioned)
Advanced configuration	nvrnm = ovt/file/file2

CANCEL BACK **NEXT**

10. Select the storage for the OVA file. In the Compatibility section, verify that the compatibility check is successful and then select Next.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format As defined in the VM storage policy ▼

VM Storage Policy Datastore Default ▼

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Placement
<input type="radio"/>	host1.BOS5	---	319 GB	9.37 GB	309.63 GB	VMFS 6	Local
<input type="radio"/>	host2.BOS5	---	319 GB	1.95 GB	317.05 GB	VMFS 6	Local
<input checked="" type="radio"/>	vsanDatasto...	---	3.49 TB	12.19 TB	2.34 TB	vSAN	Local

Items per page 10 3 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

11. From the Destination Network dropdown menu, select the desired port group and then select Next.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

12. Verify the configuration.

If any changes are needed, select Back.

If the configuration looks correct, select Finish.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Select networks
- Ready to complete**

Ready to complete

Review your selections before finishing the wizard

Select a name and folder

NameMy_OVA_Machine
Template nameAlma8-20230227r
FolderApplications

Select a compute resource

ResourceCluster

Review details

Download size2.4 GB

Select storage

Size on disk60.0 GB
Storage mapping1
All disksDatastore: vsanDatastore; Format: As defined in the VM storage policy

Select networks



Network mapping1
VM NetworkVM Network
IP allocation settings
IP protocolIPv4
IP allocationStatic - Manual



CANCEL

BACK

FINISH

13. Verify OVF template deployment on the Cluster Recent Tasks panel.

Task Name	Target	Status
Deploy OVF template	Cluster	51% 
Import OVF package	Cluster	53% 

Task Name	Target	Status
Deploy OVF template	Cluster	Completed 
Import OVF package	Cluster	Completed 

Notes:

System Shut down and Startup

This section provides information on how to shut down and startup the VVA.

Shut down vSAN Cluster

To shut down the vSAN cluster, perform the following steps.

1. To to import the necessary module, open Windows® PowerShell and enter:

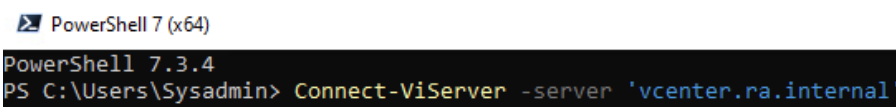
```
Install-Module vmware.powercli
```



2. Press ENTER.

3. To connect to the VMware vCenter enter:

```
Connect-ViServer -Server 'vcenter.ra.internal'
```



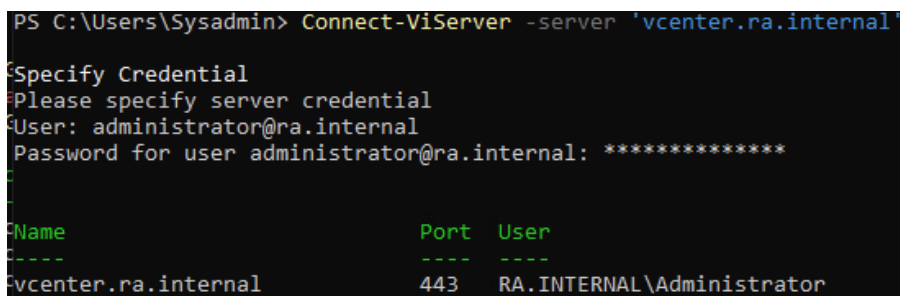
4. Press ENTER.

5. Sign in with the following credentials.

Username: administrator@ra.internal

Password: <system-specific password>

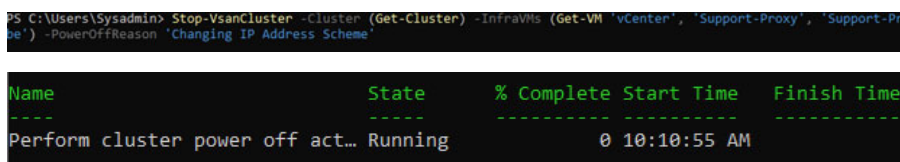
6. Press ENTER.



7. To stop the vSAN cluster, enter:

```
Stop-VsanCluster -Cluster (Get-Cluster) -InfraVMs (Get-VM 'vCenter', 'Support-Proxy', 'Support-Probe') -PowerOffReason 'Changing IP Address Scheme'
```

8. Press ENTER.



The power button and power status indicators on each server module turn off when the cluster shuts down.

9. To restart each server module, press the power button on each.

10. Monitor the VMware vCenter webpage until it becomes available:

<https://vcenter.ra.internal>

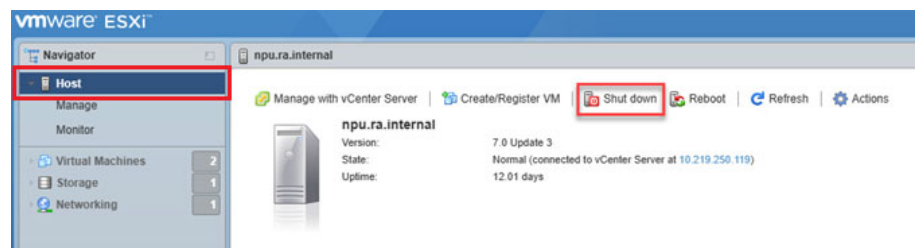
Shut down NPU

To shut down the NPU, perform the following steps.

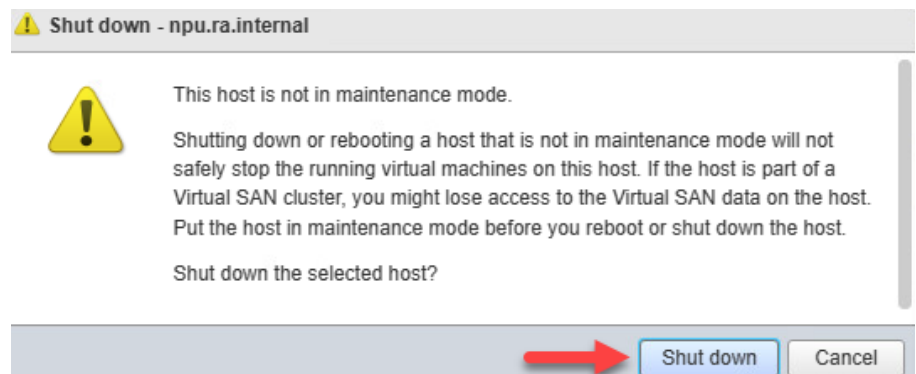
1. Open a web browser and navigate to:
`https://192.168.249.13`
2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Log in.



4. On the left side of the Navigator pane, select Host, and then select Shut Down on the center of the page.



5. On the Shut down warning dialog box, select Shut Down.

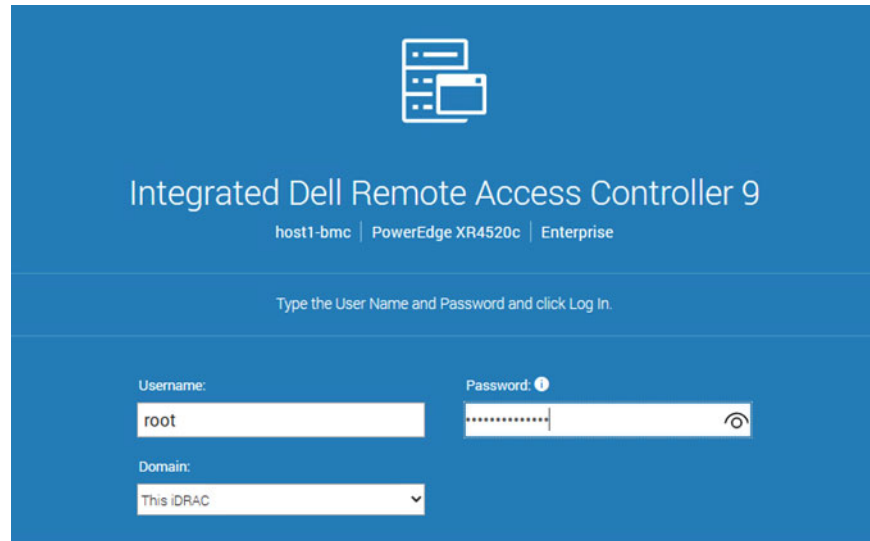


The system shuts down.

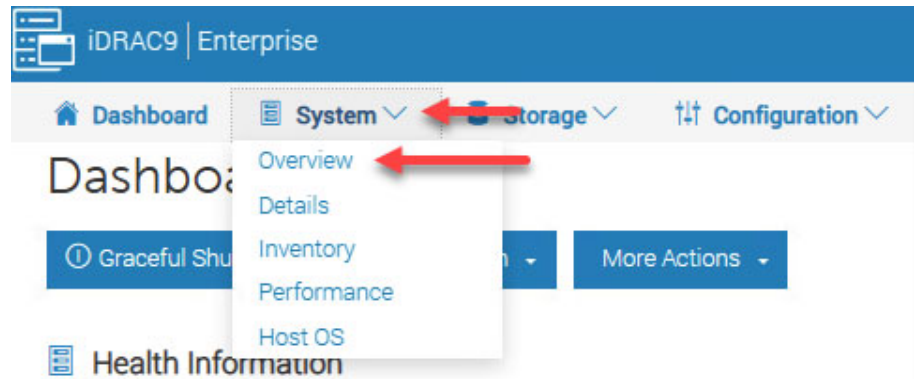
Restart NPU

To restart the NPU, perform the following steps.

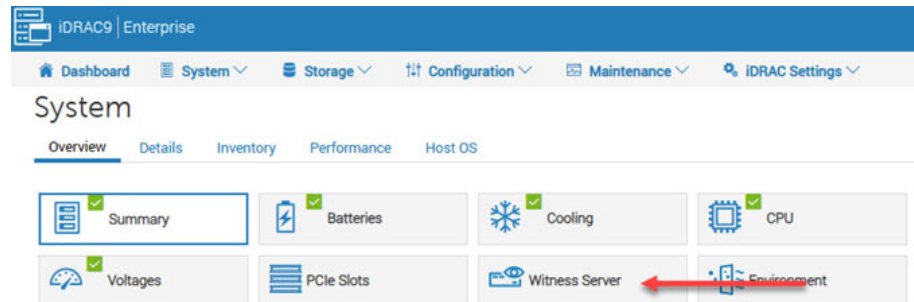
1. Open a web browser and navigate to:
<https://192.168.249.14>
2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Log In.



4. From the System dropdown menu, select Overview.



5. Select Witness Server.



6. In Power Control Settings, select the Action dropdown menu > Power On.
7. Select Apply.

Restart vSAN Cluster

To restart the vSAN cluster, perform the following steps.

1. Press the power button on both server modules.
2. Open a web browser and monitor the VMware vCenter webpage until it becomes available:
`https://vcenter.ra.internal`
3. Once available, sign in into the VMware vCenter.
4. In the Navigator Pane, right-click the Cluster.
5. Navigate to vSAN and select Restart Cluster.
6. Select Ok.

Change the IP Address Schemes

This chapter provides information on how to modify the VVA network scheme for the following items:

- IP address
- subnet mask
- default gateway
- VLAN configurations, where applicable.

To modify the VVA network scheme, perform the procedures that are contained in this chapter.

Shut Down the vSAN Cluster

To shut down the vSAN Cluster, perform the following steps.

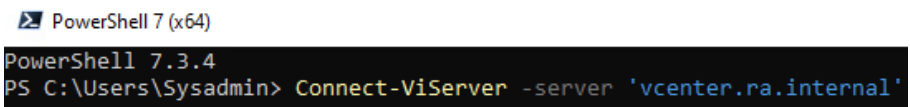
1. To import the necessary module, open Windows PowerShell from the Start menu and enter:

```
Install-Module vmware.powercli
Press ENTER.
```



2. To connect to the VMware vCenter, enter:

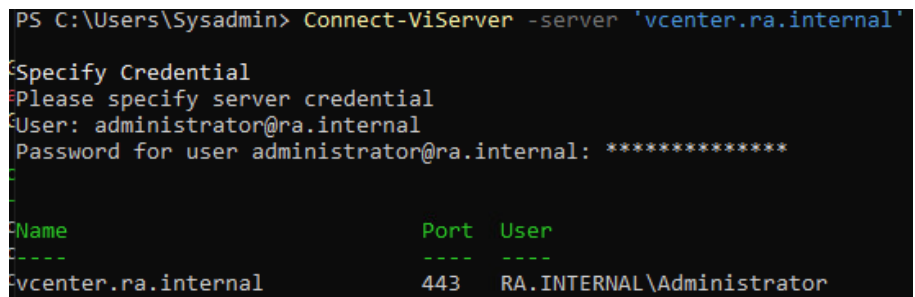
```
Connect-ViServer -Server 'vcenter.ra.internal'
Press ENTER.
```



3. Enter the following credentials.

```
Username: administrator@ra.internal
Password: <system-specific password>
```

4. Press ENTER.



- To stop the vSAN cluster, enter:

```
Stop-VsanCluster -Cluster (Get-Cluster) -InfraVMs (Get-VM 'vCenter', 'Support-Proxy', 'Support-Probe') -PowerOffReason 'Changing IP Address Scheme'
```

Press ENTER.

```
PS C:\Users\Sysadmin> Stop-VsanCluster -Cluster (Get-Cluster) -InfraVMs (Get-VM 'vCenter', 'Support-Proxy', 'Support-Probe') -PowerOffReason 'Changing IP Address Scheme'
```

Name	State	% Complete	Start Time	Finish Time
Perform cluster power off act...	Running		0 10:10:55 AM	

- When the cluster has stopped, the power button and power status indicators on each server module turn off.
- To restore power to each module, press the power button on each unit.
- Open a web browser and monitor the VMware vCenter webpage until the cluster becomes available:
<https://vcenter.ra.internal>



If you have not added ra.internal to your host file, you can monitor the VMware vCenter webpage with the following IP address:

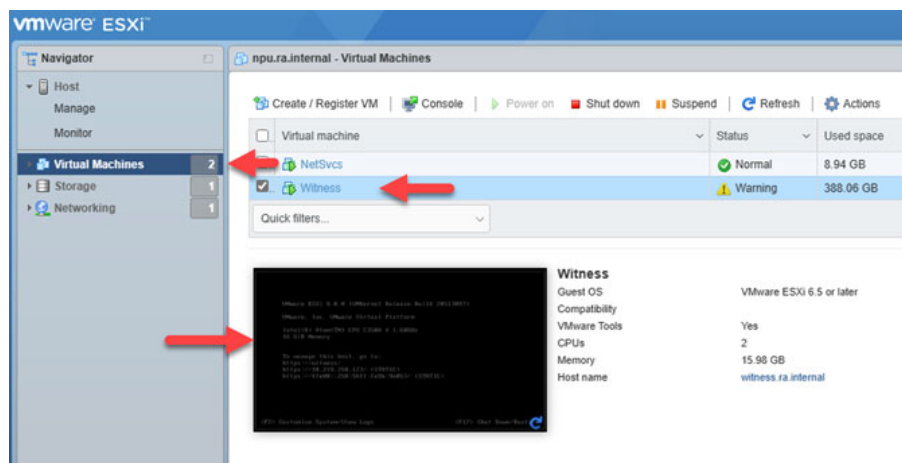
<https://192.168.249.18>

For information on updating your host file, see [Add Host Names to Local Host File on page 17](#).

Change the IPv4 Settings of the Witness Host

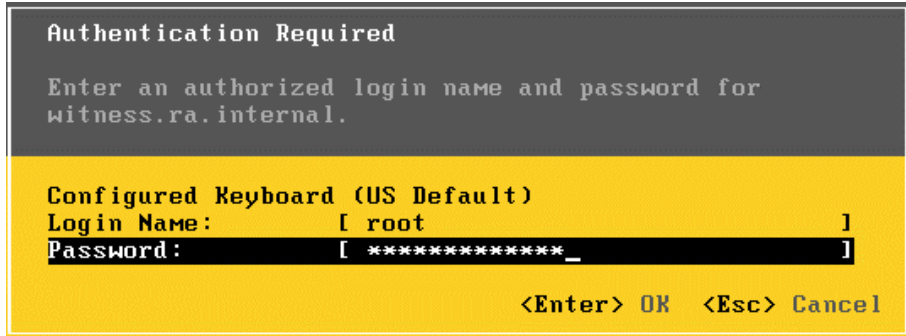
Because the Witness host is nested, the DCUI console can be accessed through the VMware ESXi web interface. To access the DCUI console, perform the following steps.

- Open a web browser and navigate to the IP address of the NPU host:
<https://192.168.249.13>
- In the left side navigation of the NPU host, navigate to Virtual Machines and select Witness.
- Select the command window thumbnail, which opens the Witness browser console



- When the console displays, press F2.
- Sign in with the following credentials.
Username: root
Password: <system-specific password>

6. Press ENTER.

A screenshot of a terminal window showing an authentication prompt. The title is "Authentication Required". The text says "Enter an authorized login name and password for witness.ra.internal.". Below this, it says "Configured Keyboard (US Default)". There are two input fields: "Login Name:" with the value "[root]" and "Password:" with the value "[*****_]". At the bottom right, it says "<Enter> OK <Esc> Cancel".

Authentication Required

Enter an authorized login name and password for
witness.ra.internal.

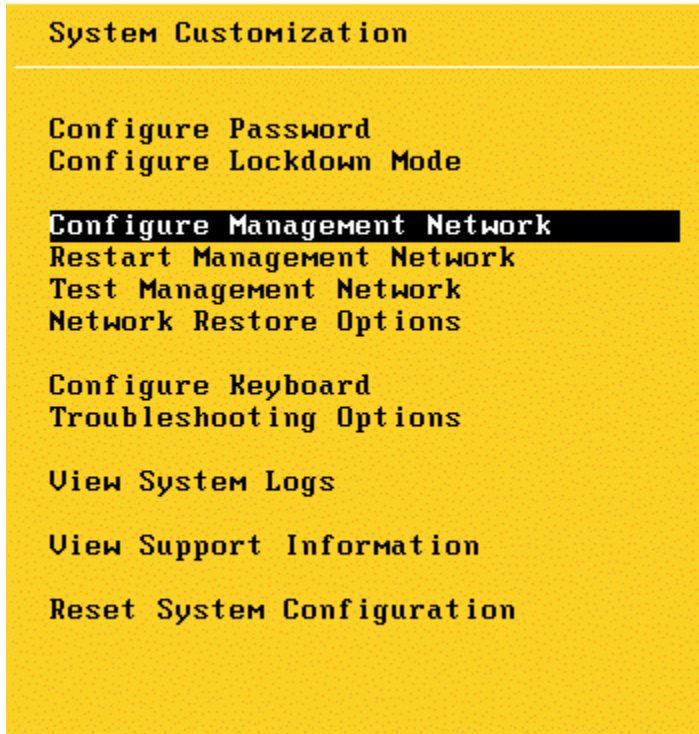
Configured Keyboard (US Default)

Login Name: [root]

Password: [*****_]

<Enter> OK <Esc> Cancel

7. In the VMware ESXi DCUI, use the arrow keys to navigate to Configure Management Network and press ENTER.

A screenshot of the VMware ESXi DCUI "System Customization" menu. The menu is displayed on a yellow background with black text. The options are: "Configure Password", "Configure Lockdown Mode", "Configure Management Network" (which is highlighted with a black bar), "Restart Management Network", "Test Management Network", "Network Restore Options", "Configure Keyboard", "Troubleshooting Options", "View System Logs", "View Support Information", and "Reset System Configuration".

System Customization

Configure Password

Configure Lockdown Mode

Configure Management Network

Restart Management Network

Test Management Network

Network Restore Options

Configure Keyboard

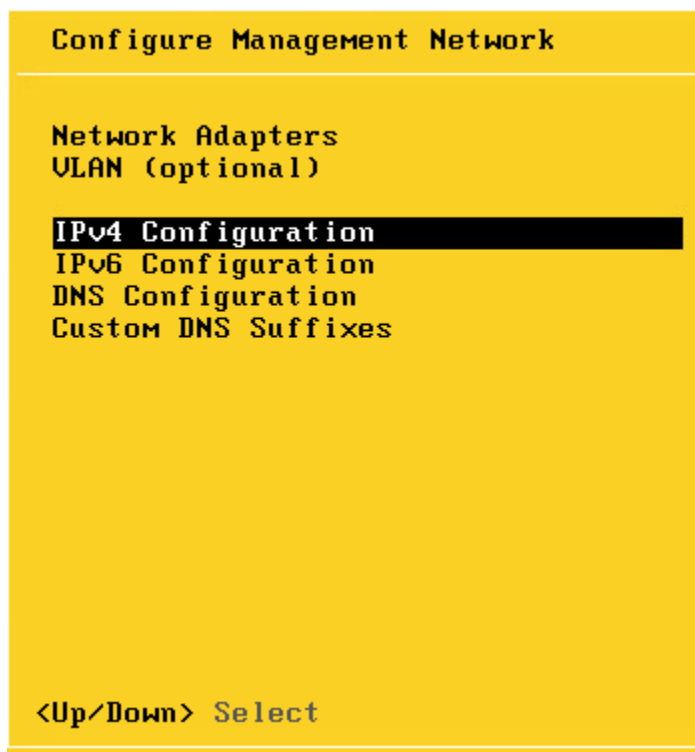
Troubleshooting Options

View System Logs

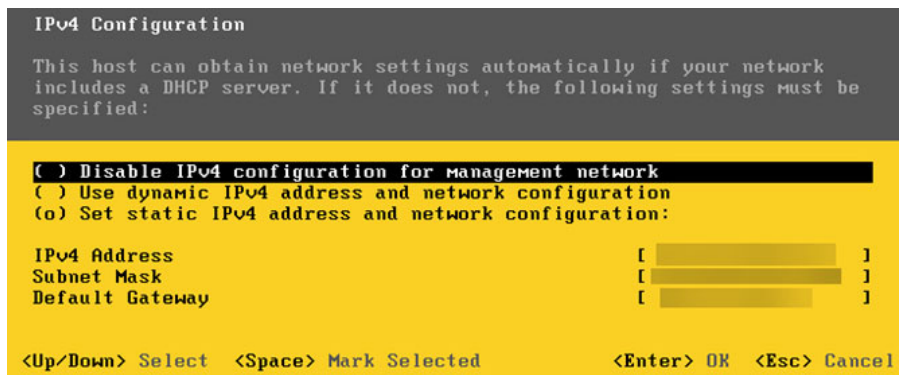
View Support Information

Reset System Configuration

8. Select IPv4 Configuration, and press ENTER.



9. Use the UP and DOWN arrow keys to navigate the IPv4 setting, and input the new configuration.



10. When configuration is complete, press ENTER.
11. To exit, press the ESC key, and Y to confirm the changes.

Reset IP Address of NPU

To change the IP address of the NPU, perform the following steps.

1. Open a web browser and navigate to the IP address of the NPU host:
`https://192.168.249.13`
2. Enter the following credentials.
Username: root
Password: <system-specific password>

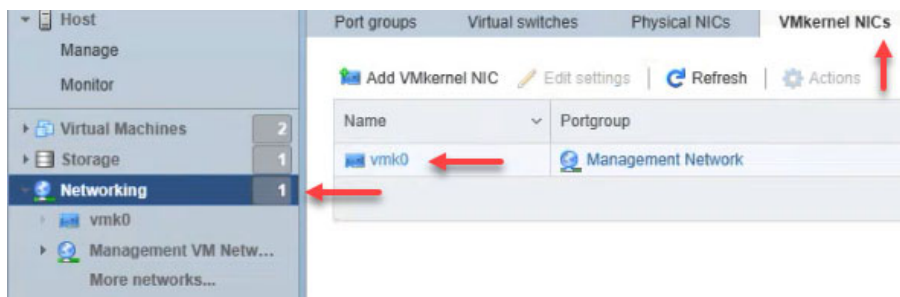
3. Select Log In.



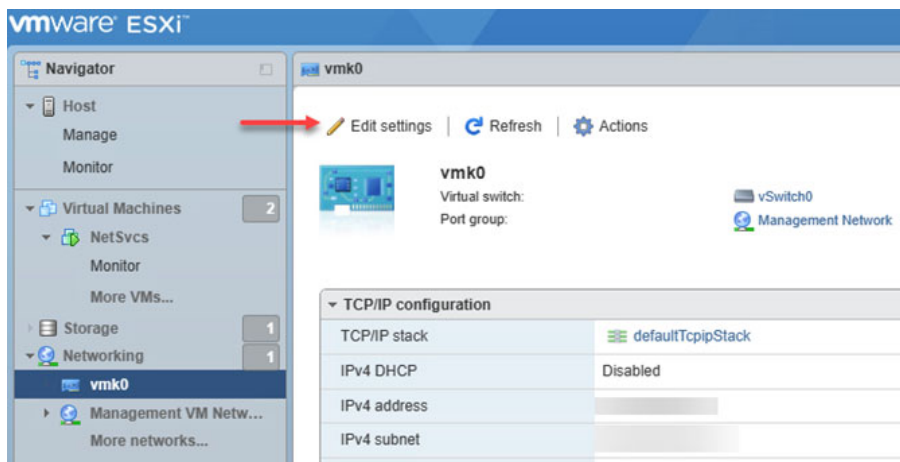
4. On the left side of the navigation pane, select Networking.

5. From the Networking submenu, select vmk0.

6. On the top right, select the VMkernel NICs tab.



7. Select Edit settings.



8. On the settings screen, edit the Address and Subnet Mask as needed.

9. When finished, select Save.

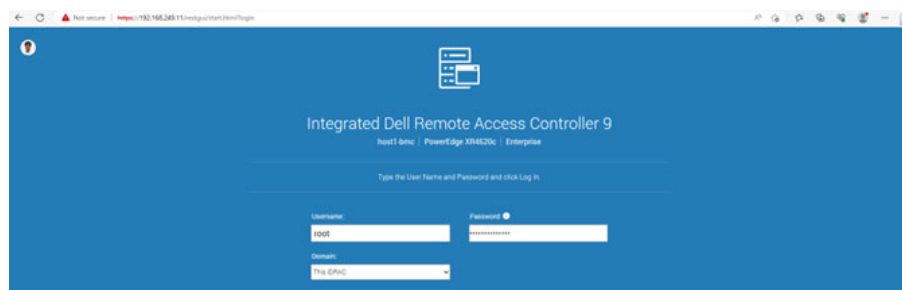
Update Access and Trunk Port with New VLAN Tag (Optional)

If the default VLAN of 3249 must be changed, the access ports on the switch must be tagged with the new VLAN ID and the trunk ports must also be configured to allow the new VLAN ID.

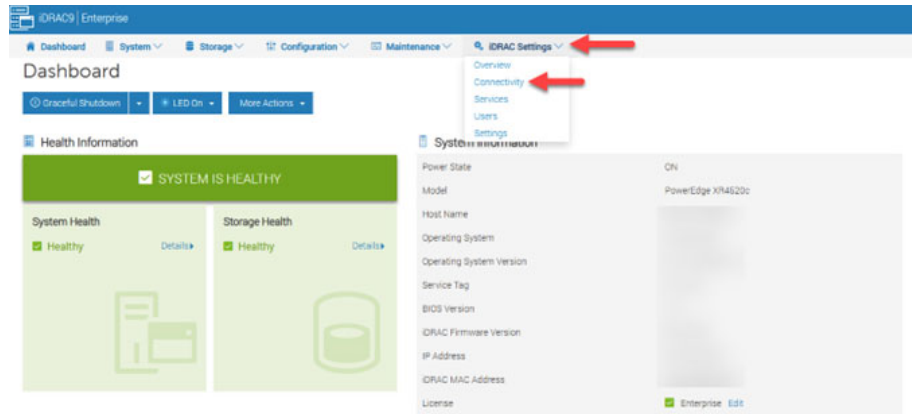
Reset iDRAC IP Addresses

To reset the iDRAC IP addresses, perform the following steps.

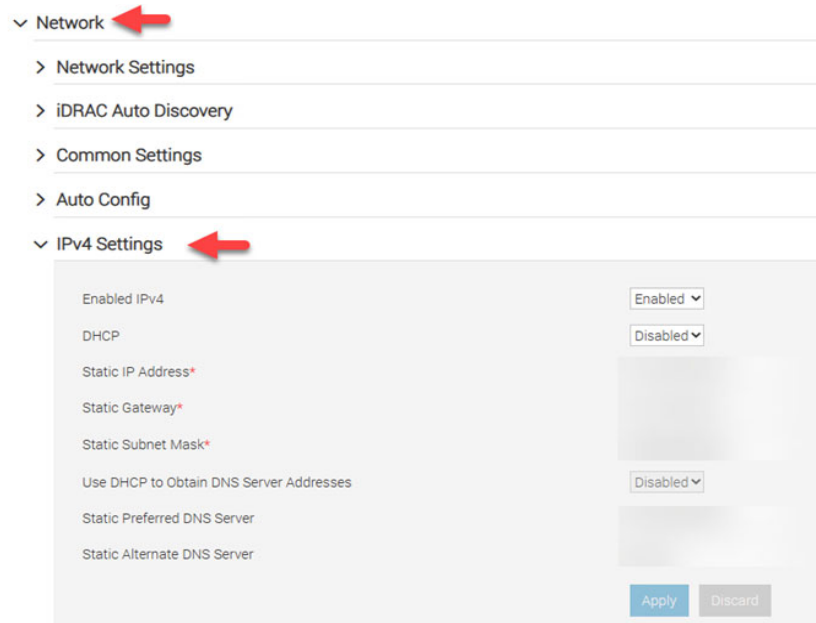
1. Open a web browser and navigate to:
<https://192.168.249.11>
2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Log In.



4. From the dropdown menu, select iDRAC Settings, then Connectivity.



5. From the dropdown menu, select Network, then select IPv4 Settings.



6. Configure each text field as needed, then select Apply.
7. On the Success window, select Ok.

 **Success**

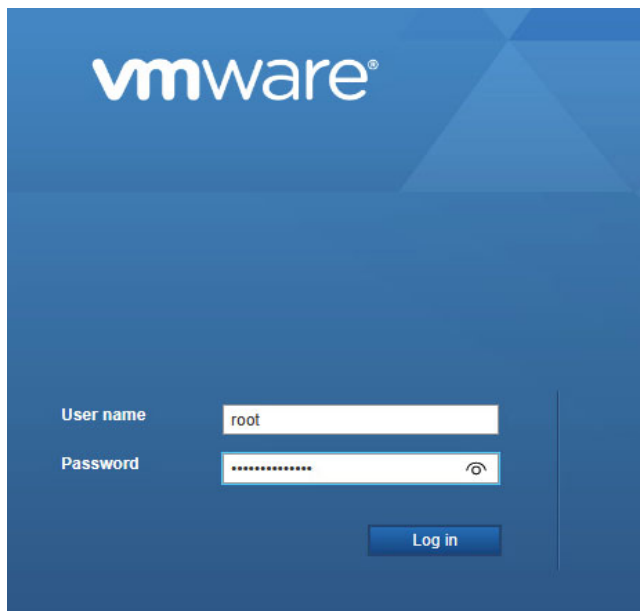
Ok

8. To reset the iDRAC IP of another host, repeat the prior steps 1...7.

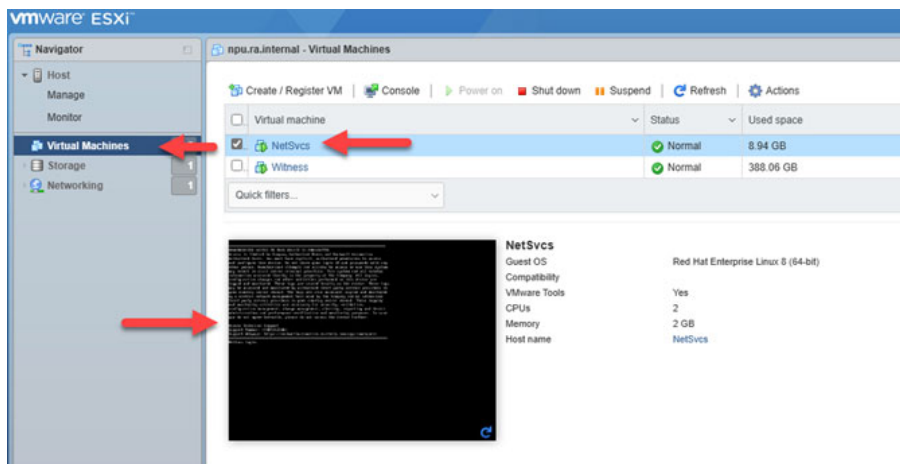
Update NetSvcs IP

To modify the IP address of the NetSvcs VM, perform the following steps.

1. Open a web browser and navigate to the new IP address of the NPU host.
2. Sign in with the following credentials.
Username: root
Password: <system-specific password>
3. Select Log In.



4. From the Inventory Navigator on the left, select Virtual Machines.
5. Select NetSvcs, then select the command thumbnail window, which opens the NetSvcs DCUI.



6. Sign in to the NetSvcs VM with the following credentials.
Username: sysadmin
Password: <system-specific password>

7. Press ENTER.

```
NetSvcs login: sysadmin
Password:
Last login: Thu Apr 13 11:03:15 on tty1
[sysadmin@NetSvcs ~]$ _
```

8. Bring down the Ethernet interface with the following command:

```
nmcli connection down ens192
```

```
[sysadmin@NetSvcs ~]$ nmcli connection down ens192
Connection 'ens192' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[sysadmin@NetSvcs ~]$ _
```

9. Modify the interface with the correct IP Address, CIDR/subnet mask, and gateway with the following command:

```
nmcli connection modify ens192 ipv4.addresses
xx.xx.xx.xx/25 ipv4.gateway xx.xx.xx.xx
```

```
[sysadmin@NetSvcs ~]$ nmcli connection modify ens192 ipv4.addresses [redacted] ipv4.gateway [redacted]
[sysadmin@NetSvcs ~]$ _
```

10. Activate the ens192 interface with the following command:

```
nmcli connection up ens192
```

```
[sysadmin@NetSvcs ~]$ nmcli connection up ens192
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
```

11. Verify that the IP address changed with the following command:

```
ip a
```

```
[sysadmin@NetSvcs ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 08:0c:29:a9:d9:d3 brd ff:ff:ff:ff:ff:ff
    inet [redacted]/25 brd [redacted] scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
```

12. Test the connection to the newly assigned gateway with ping:

```
ping <new gateway IP address>
```

```
[sysadmin@NetSvcs ~]$ ping [redacted]
PING [redacted] 56(84) bytes of data.
64 bytes from [redacted]: icmp_seq=1 ttl=254 time=1.20 ms
64 bytes from [redacted]: icmp_seq=2 ttl=254 time=1.24 ms
64 bytes from [redacted]: icmp_seq=3 ttl=254 time=1.21 ms
64 bytes from [redacted]: icmp_seq=4 ttl=254 time=1.15 ms
64 bytes from [redacted]: icmp_seq=5 ttl=254 time=1.24 ms
64 bytes from [redacted]: icmp_seq=6 ttl=254 time=2.09 ms
64 bytes from [redacted]: icmp_seq=7 ttl=254 time=1.16 ms
64 bytes from [redacted]: icmp_seq=8 ttl=254 time=1.15 ms
64 bytes from [redacted]: icmp_seq=9 ttl=254 time=1.16 ms
64 bytes from [redacted]: icmp_seq=10 ttl=254 time=1.08 ms
64 bytes from [redacted]: icmp_seq=11 ttl=254 time=1.09 ms
^C
--- [redacted] ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10016ms
rtt min/avg/max/mdev = 1.079/1.251/2.091/0.271 ms
[sysadmin@NetSvcs ~]$
```


Update NetSvcs DNS Settings

To update the NetSvcs DNS settings, perform the following steps.

1. If you are not already signed into the NetSvcs VM, login as detailed in steps 1...5 of [Update NetSvcs IP on page 76](#).
2. Once logged in, edit the DNS configuration file with the following command:

```
sudo vim /etc/unbound/local.d/ra.conf
```
3. Press ENTER.

```
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
access-control: allow
unblock-lan-zones: yes
local-zone: "ra.internal." transparent
  local-data: "npu.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] 13 npu.ra.internal"
  local-data: "host1.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] host1.ra.internal"
  local-data: "host2.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] host2.ra.internal"
  local-data: "witness.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] witness.ra.internal"
  local-data: "NetSvcs.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] NetSvcs.ra.internal"
  local-data: "vCenter.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] vCenter.ra.internal"
  local-data: "Support-Probe.ra.internal. IN A [REDACTED]"
  local-data-ptr: "[REDACTED] Support-Probe.ra.internal"
forward-zone:
  name: "."
  forward-addr: [REDACTED]
```

4. Enter insertion mode by typing "i."
5. Use the arrow keys to navigate and make any needed changes.
6. To exit insertion mode, press ESC.
7. To save and exit the file, enter:

wq
and press ENTER.

8. Enter the following command:
- ```
sudo systemctl restart unbound
```
- and press ENTER.

```
[sysadmin@NetSvcs ~]$ sudo systemctl restart unbound
[sysadmin@NetSvcs ~]$
```

- To confirm the unbound configuration status, enter:  

```
systemctl status unbound
```

  
and press ENTER.

10. Look for:  
Active (running)  
and  
status=0/SUCCESS

```

(sysadmin@ctosce: ~) $ systemctl status unbound
● unbound.service - Unbound recursive Domain Name Server
 Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled; vendor preset: disabled)
 Active: active (running) since Fri 2023-05-12 13:23:05 EDT; 14min ago
 Process: 1274398 ExecStartPre=/bin/bash -c if [! "$DISABLE_UNBOUND_ANCHOR" == "yes"]; then /usr/sbin/unbound-anchor -a /var
 Process: 1274396 ExecStartPre=/usr/sbin/unbound-checkconf (code=exited, status=0/SUCCESS)
 Main PID: 1274583 (unbound)
 Tasks: 4 (limit: 11341)
 Memory: 19.8M
 CGroup: /system.slice/unbound.service
 └─1274583 /usr/sbin/unbound -d

lines 1-18/18 (END)

```



If this command returns any errors, check for any misspellings or errors in the configuration.

If neither are found, return to step 1 and repeat the procedure.

11. To exit the unbound configuration status command, enter:

q

12. To sign out, enter:

logout

and press ENTER.

## Change VMware vCenter IP Address with the VMware vCenter Server Appliance

To change the IP address of VMware vCenter, perform the following steps.

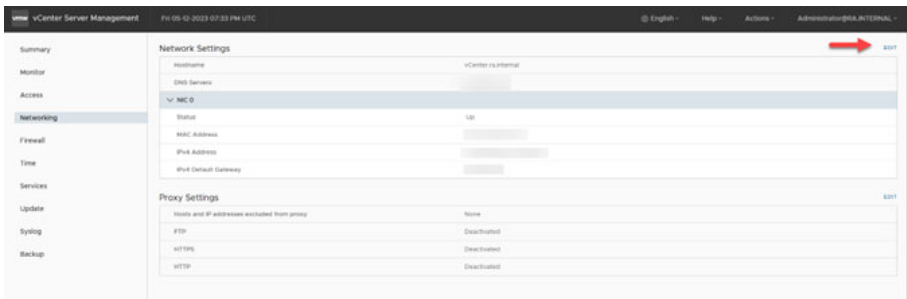
1. Open a web browser and navigate to the VMware vCenter Server Appliance:  
<https://192.168.249.18:5480>
2. Sign in with the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>
3. Select Login.
4. On the left side of the Appliance Manager, select Networking.

vmware vCenter Server Management | Fri 05-12-2023 07:30 PM UTC

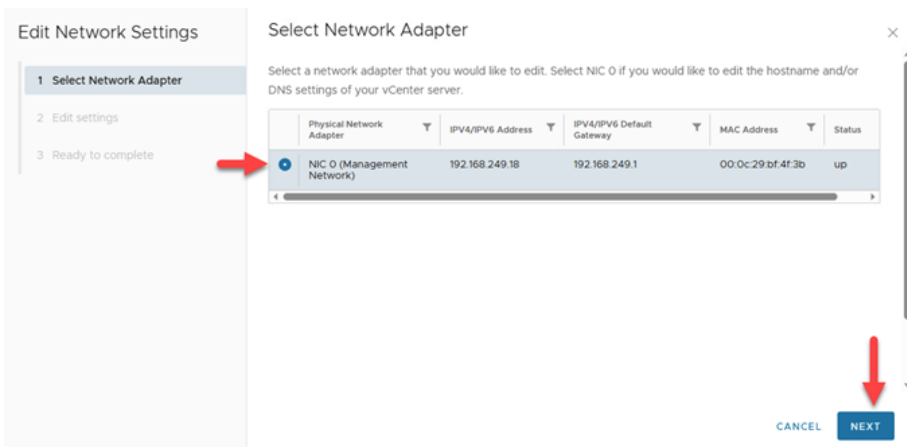
| System Information |                       |
|--------------------|-----------------------|
| Hostname:          | vCenter.ra.internal   |
| Product:           | VMware vCenter Server |
| Version:           | 8.0.1.00000           |
| Build number:      | 21560480              |
| Uptime:            | 4 hours 51 minutes    |

| Health Status  |                                               |
|----------------|-----------------------------------------------|
| Overall Health | Good (Last checked May 12, 2023, 03:30:36 PM) |
| CPU            | Good                                          |
| Memory         | Good                                          |
| Database       | Good                                          |
| Storage        | Good                                          |
| Swap           | Good                                          |

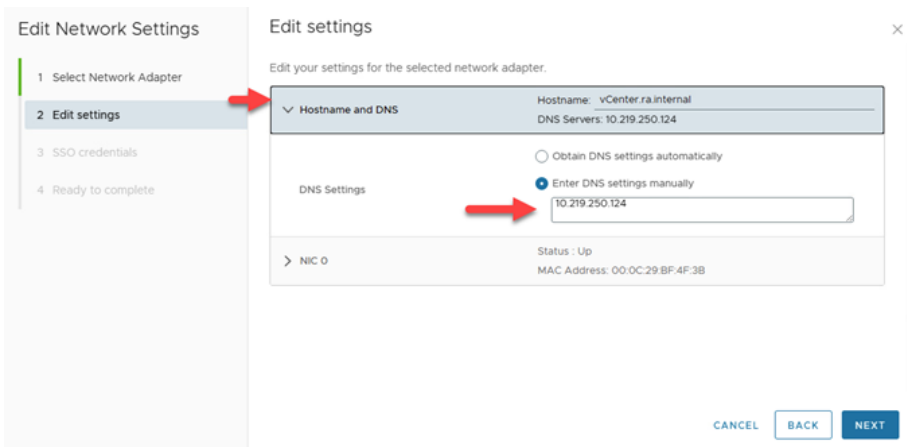
5. On the top left, select Edit.



6. Select NIC 0 (Management Network) and then on the bottom right, select Next.



7. Select the Hostname and DNS dropdown menu.



8. Edit the DNS server settings text field as needed.

## 9. Select the NIC 0 dropdown menu.

## 10. Edit the IPv4 text fields as needed.

When finished, select Next.

## 11. In the SSO credentials settings, enter the following credentials.

Username: administrator@ra.internal

Password: <system-specific password>

## 12. Select Next.

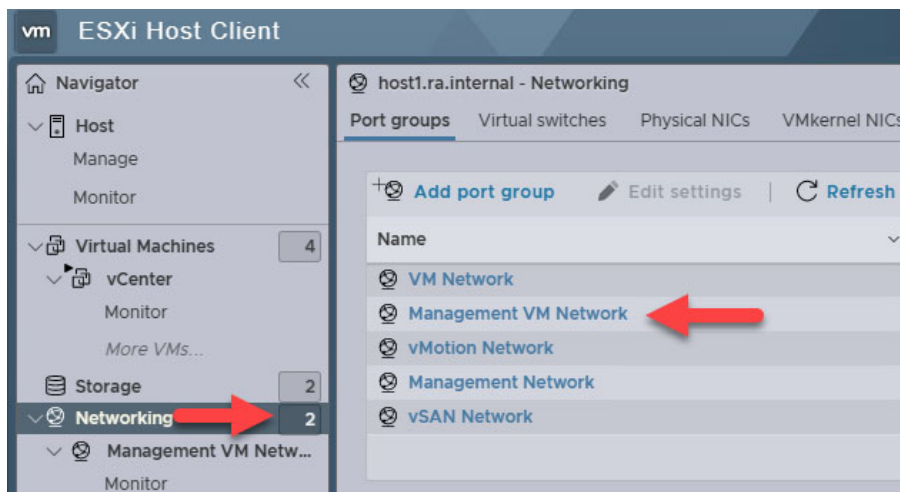
## 13. To save the updated IP address settings, select the Acknowledgment box and then select Finish.

The VMware vCenter saves the updated settings.

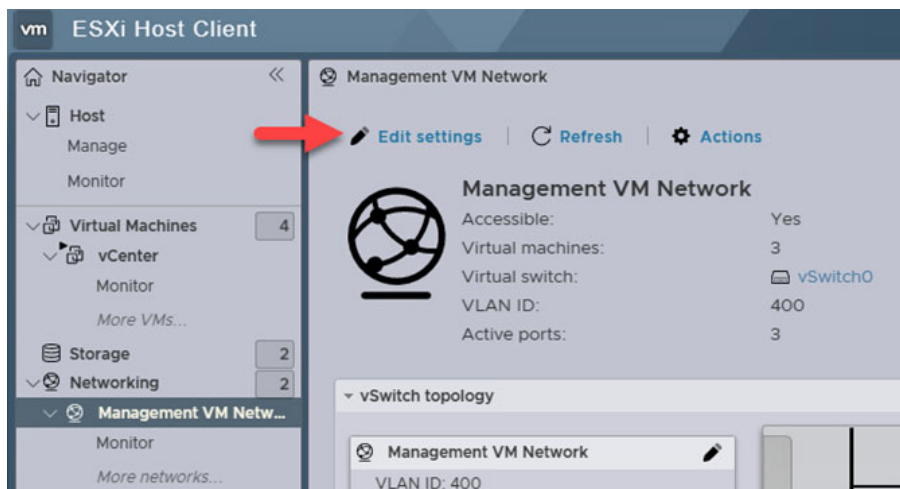
## Apply new VLAN Tag to Port Groups (Optional)

If the default VLAN of 3249 must be changed, each VMware ESXi host must be updated with the VLAN ID of each host. To do so, perform the following steps.

1. Open a web browser and navigate to:  
<https://192.168.249.14>
2. Sign in with the following credentials.  
Username: root  
Password: <system-specific password>
3. Select Login.
4. On the left side, select Networking and then select Management VM Network.



5. Select Edit settings.



6. Populate the VLAN ID with the appropriate VLAN ID and then select Save.

Edit port group - Management VM Network

Name: Management VM Network

VLAN ID:

Virtual switch: vSwitch0

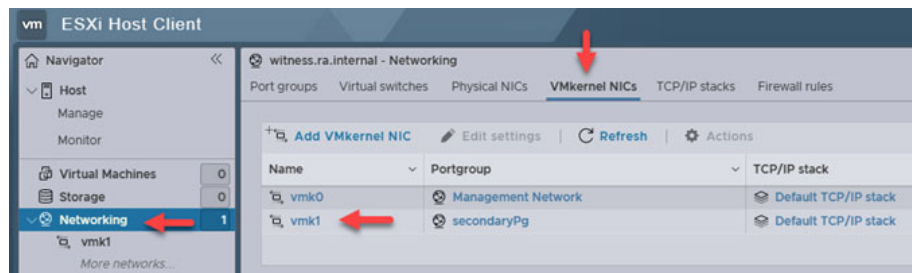
> Security: Click to expand

> NIC teaming: Click to expand

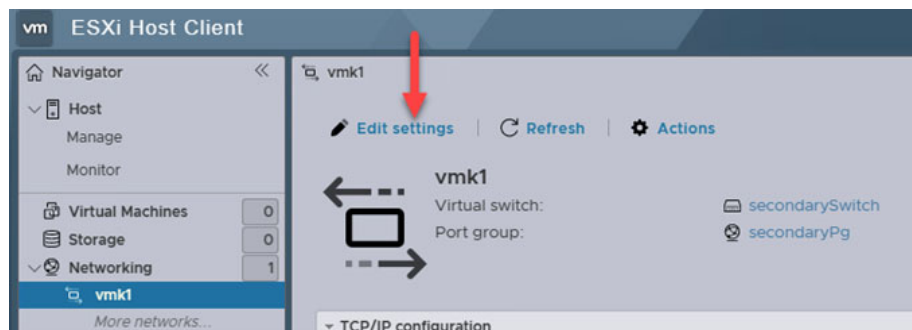
> Traffic shaping: Click to expand

CANCEL SAVE

7. Repeat Steps 1...4 for additional hosts.
8. Open a new web browser tab or window and sign in to the Witness host:  
<https://witness.ra.internal>
9. Sign in with the following credentials.  
Username: root  
Password: <system-specific password>
10. From the Navigator, select Networking.
11. Select the VMkernel NICs tab.
12. Select vmk1.



13. Select Edit settings.



14. Input the appropriate address and subnet mask.

Edit settings - vmk1

|                 |                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port group      | secondaryPg                                                                                                                                                                                                                                  |
| MTU             | 1500                                                                                                                                                                                                                                         |
| IP version      | IPv4 and IPv6                                                                                                                                                                                                                                |
| IPv4 settings   |                                                                                                                                                                                                                                              |
| Configuration   | <input type="radio"/> DHCP <input checked="" type="radio"/> Static                                                                                                                                                                           |
| Address         |                                                                                                                                                                                                                                              |
| Subnet mask     |                                                                                                                                                                                                                                              |
| IPv6 settings   |                                                                                                                                                                                                                                              |
| Click to expand |                                                                                                                                                                                                                                              |
| TCP/IP stack    | Default TCP/IP stack                                                                                                                                                                                                                         |
| Services        | <input type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging<br><input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication |

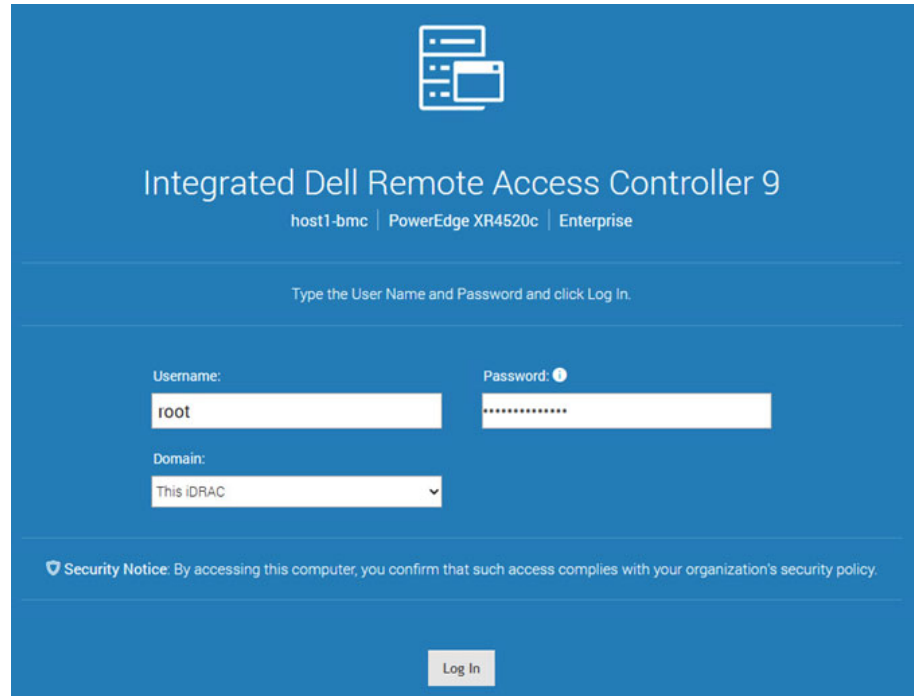
CANCEL SAVE

15. When finished, select Save.

## Update IP Addresses on vSAN Hosts

To update the IP addresses on the vSAN hosts, perform the following steps.

1. Open a web browser and navigate to the iDRAC on the host1:  
https://192.168.249.14
2. Sign in with the following credentials.  
Username: root  
Password: <system-specific password>
3. Select Log In.



Integrated Dell Remote Access Controller 9  
host1-bmc | PowerEdge XR4520c | Enterprise

Type the User Name and Password and click Log In.

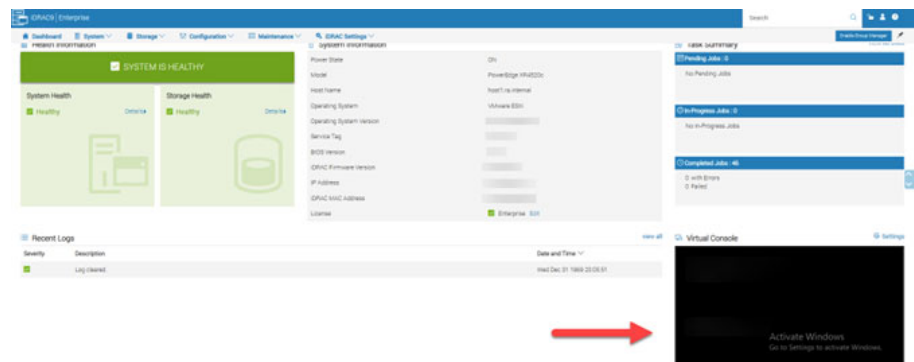
Username:  Password:

Domain:

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

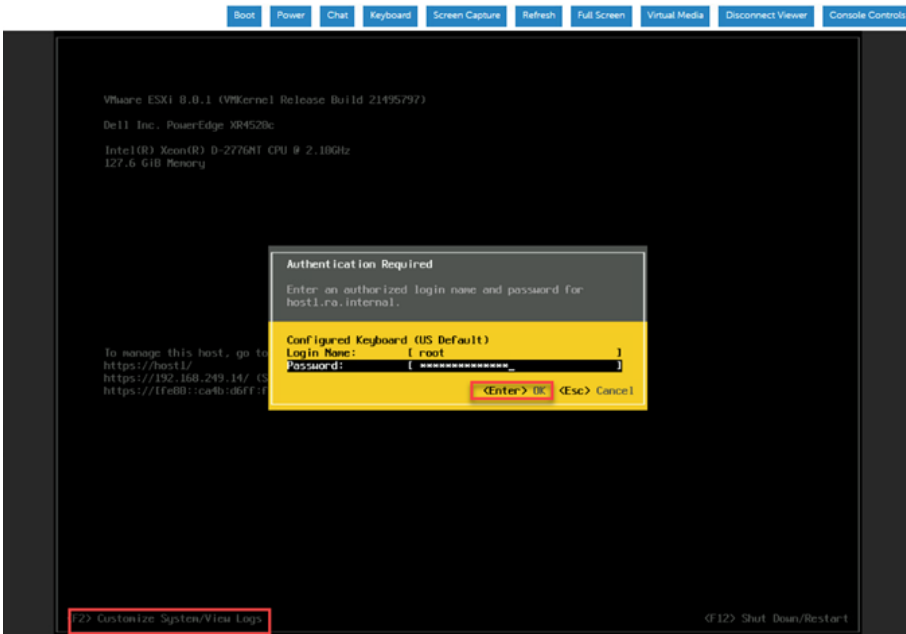
Log In

4. Select the Virtual Console thumbnail.





5. Click inside the console and press the F2 key, which displays an authentication dialog box.



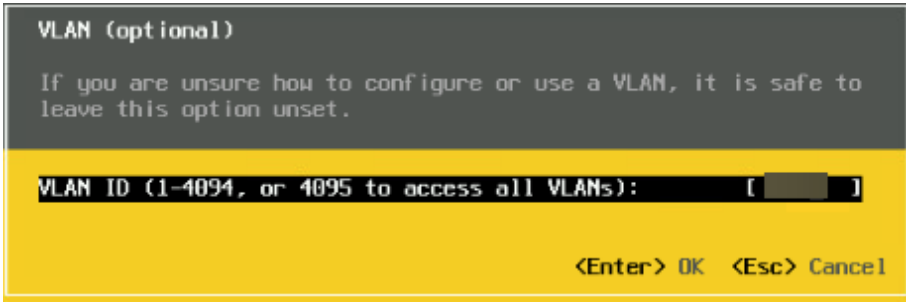
6. Sign in with the root and system-specific password, and then press ENTER.
7. In the VMware ESXi Direct Console User Interface (DCUI), navigate to Configure Management Network and press ENTER.



8. Select VLAN (Optional) and press ENTER.



9. Replace VLAN ID 3249 with the desired VLAN ID and press ENTER.



10. Select IPv4 Configuration and press ENTER.

| Configure Management Network                                                                                                       | IPv4 Configuration                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Adapters<br>VLAN (optional)<br><b>IPv4 Configuration</b><br>IPv6 Configuration<br>DNS Configuration<br>Custom DNS Suffixes | <b>Manual</b><br>IPv4 Address: [ ]<br>Subnet Mask: [ ]<br>Default Gateway: [ ]<br>This host can obtain an IPv4 address and other networking parameters automatically if your network includes a DHCP server. If not, ask your network administrator for the appropriate settings. |

11. Change the IPv4 settings to the desired configuration.

12. When finished, press ENTER.

| IPv4 Configuration                                                                                                                                                                                                                         |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| This host can obtain network settings automatically if your network includes a DHCP server. If it does not, the following settings must be specified:                                                                                      |     |
| <input type="radio"/> Disable IPv4 configuration for management network<br><input type="radio"/> Use dynamic IPv4 address and network configuration<br><input checked="" type="radio"/> Set static IPv4 address and network configuration: |     |
| IPv4 Address                                                                                                                                                                                                                               | [ ] |
| Subnet Mask                                                                                                                                                                                                                                | [ ] |
| Default Gateway                                                                                                                                                                                                                            | [ ] |
| <Up/Down> Select   <Space> Mark Selected <b>&lt;Enter&gt; OK</b> <Esc> Cancel                                                                                                                                                              |     |

13. Use the down arrow key to navigate to the DNS Configuration field and press ENTER.

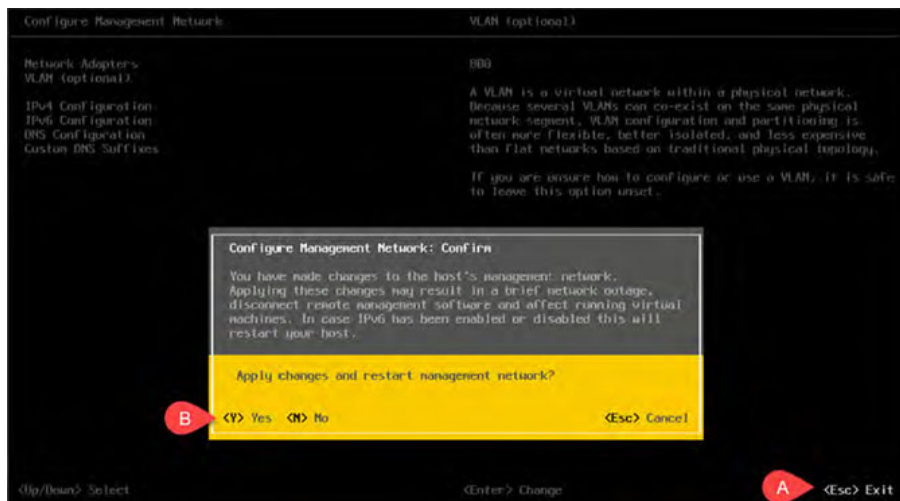
| Configure Management Network                                                                                                       | DNS Configuration                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Adapters<br>VLAN (optional)<br>IPv4 Configuration<br>IPv6 Configuration<br><b>DNS Configuration</b><br>Custom DNS Suffixes | <b>Manual</b><br>Primary DNS Server:<br>Alternate DNS Server:<br>Not set<br>Hostname<br>host1<br>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. |

14. Enter the new IP address of the NetSvcs (DNS).

15. When finished, press ENTER.

| DNS Configuration                                                                                                                                                       |                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.                                                             |                    |
| <input checked="" type="radio"/> Obtain DNS server addresses and a hostname automatically<br><input type="radio"/> Use the following DNS server addresses and hostname: |                    |
| Primary DNS Server                                                                                                                                                      | [ 10.219.250.124 ] |
| Alternate DNS Server                                                                                                                                                    | [ ]                |
| Hostname                                                                                                                                                                | [ host1 ]          |
| <Up/Down> Select   <Space> Mark Selected <b>&lt;Enter&gt; OK</b> <Esc> Cancel                                                                                           |                    |

16. To exit, press ESC and then press Y to confirm the changes.

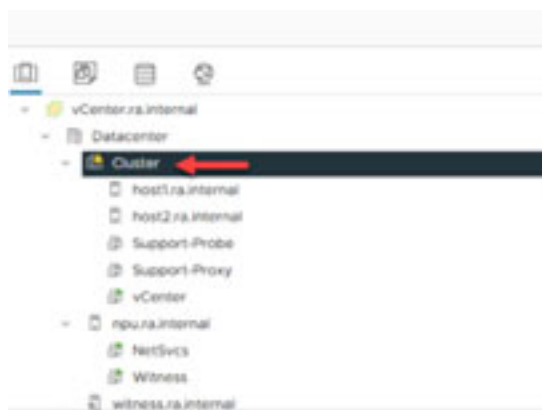


17. Repeat the preceding steps 1...16 for host2.

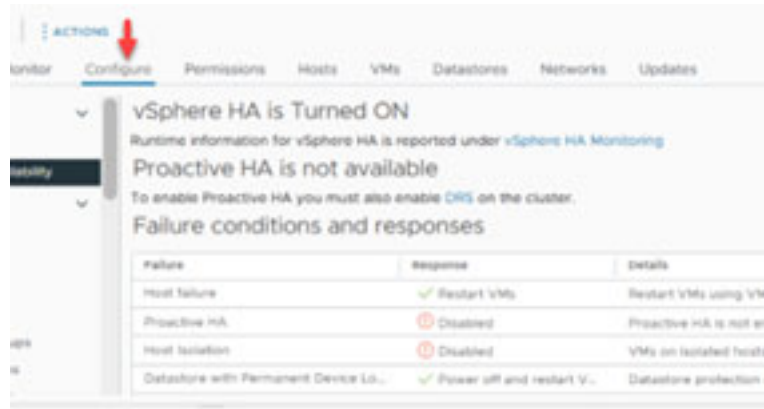
## Update High Availability

To update the high availability configuration, perform the following steps.

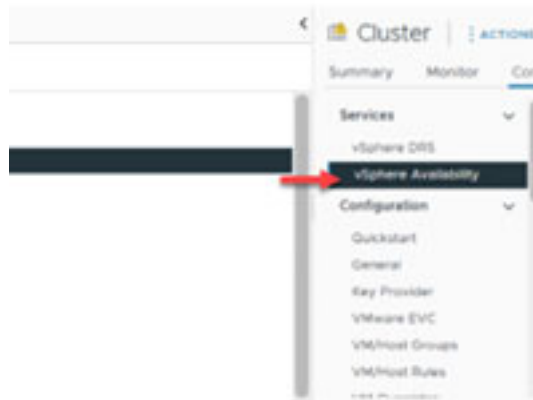
1. Open a web browser and navigate to the VMware vCenter:  
<https://192.168.249.14>
2. Sign in with the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>
3. Select Login.
4. From the left pane, select Cluster.



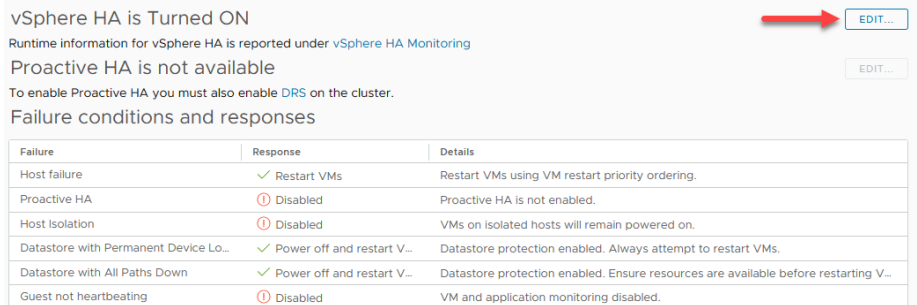
5. From the top, select the Configure tab.



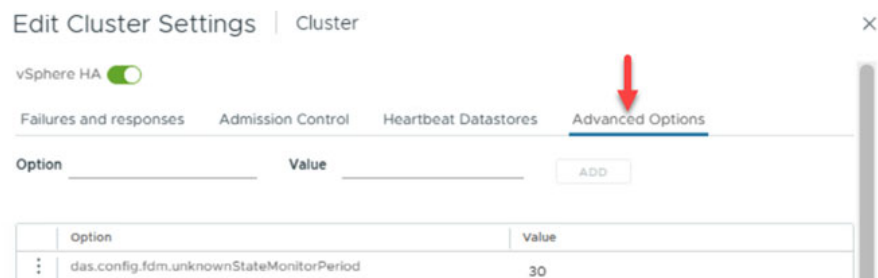
6. From the left Services dropdown menu, select vSphere Availability.



7. From the top right, select Edit.



8. From the top right, select the Advance Options tab.



9. Update the das.isolationaddress0 text field with the new IP address.

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

Option

Value

ADD

| Option                                   | Value |
|------------------------------------------|-------|
| das.config.fdm.unknownStateMonitorPeriod | 30    |
| das.isolationaddress0                    |       |
| das.reregisterrestartdisabledvms         | True  |
| das.usedefaultisolationaddress           | False |

4 items

10. When finished, select Ok.

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

Option

Value

ADD

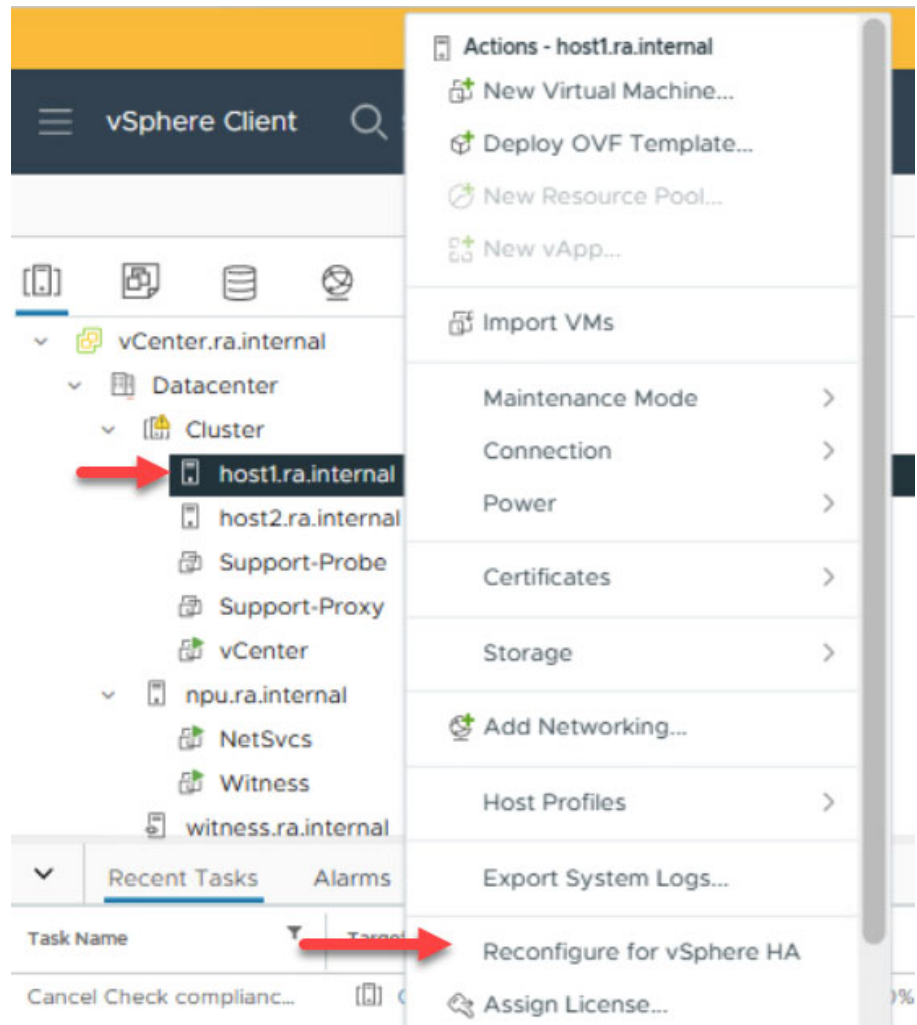
| Option                                   | Value |
|------------------------------------------|-------|
| das.config.fdm.unknownStateMonitorPeriod | 30    |
| das.isolationaddress0                    |       |
| das.reregisterrestartdisabledvms         | True  |
| das.usedefaultisolationaddress           | False |

4 items

CANCEL

OK

11. Right-click on host1 and select Reconfigure for vSphere HA.



The warning clears after a moment.

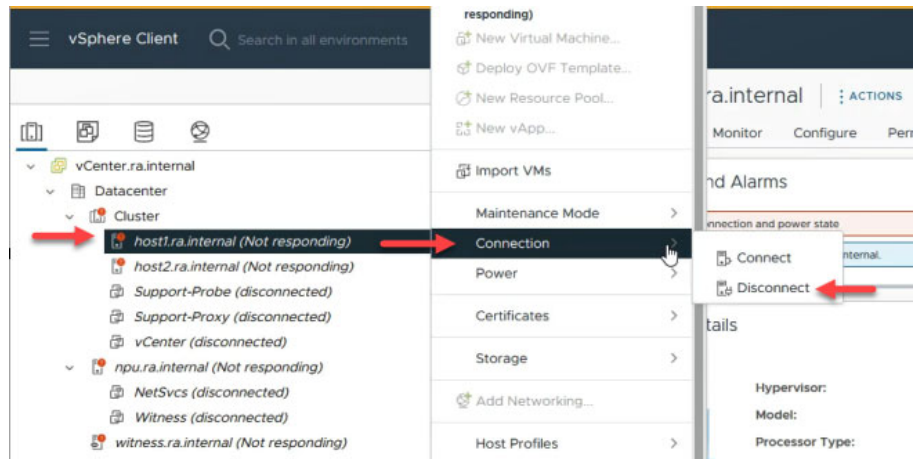
12. Repeat steps 4...10 for host2.

## Reconnect Hosts

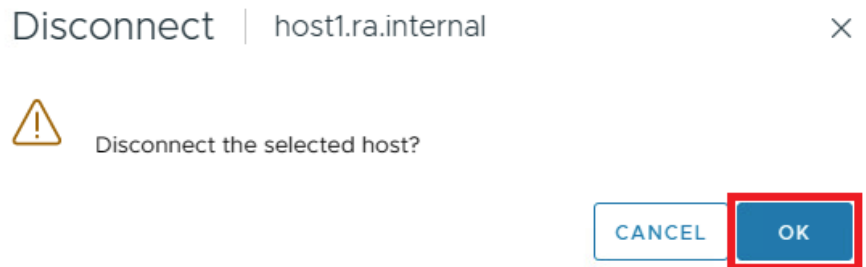
If the VMware vCenter displays an error that it cannot synchronize the host, the four hosts (host1, host2, NPU, and Witness) must be disconnected and reconnected. To do so, perform the following steps.

1. Open a web browser and navigate to the VMware vCenter:  
<https://192.168.249.14>
2. Sign in with the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>
3. Select Login.

4. Right-click host1, select Connection > Disconnect.

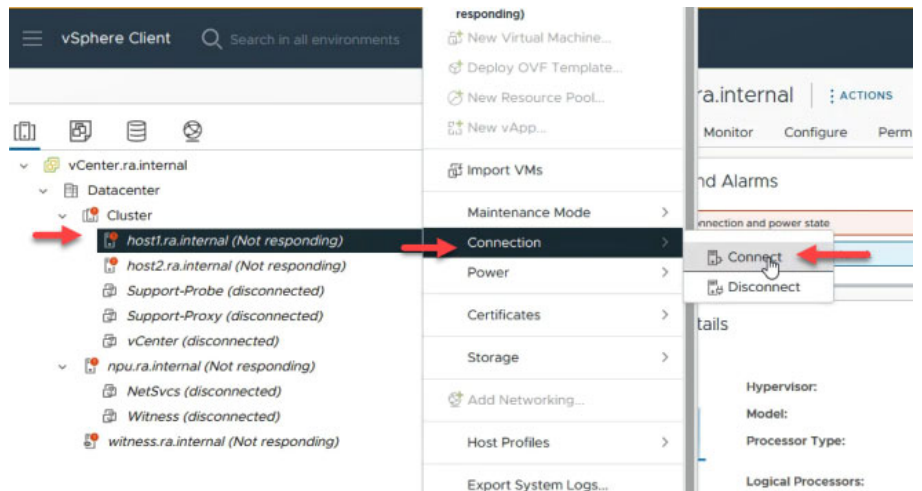


5. To disconnect host1, select Ok.

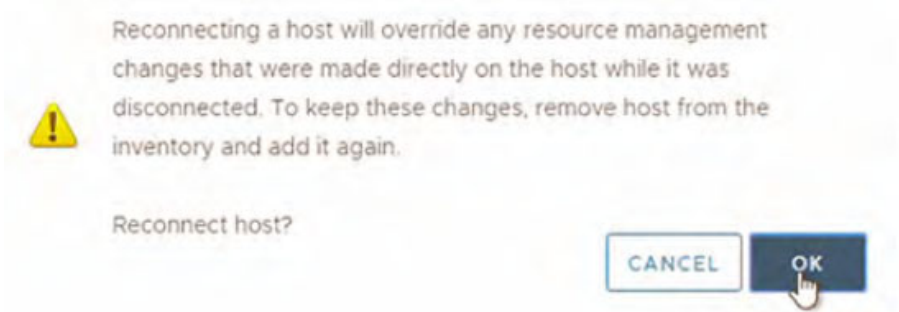


6. Repeat steps 3 and 4 for the host2, NPU, and Witness.

7. After all four hosts are disconnected, right-click on host1 and select Connection > Connect.



8. To reconnect the host, select Ok.

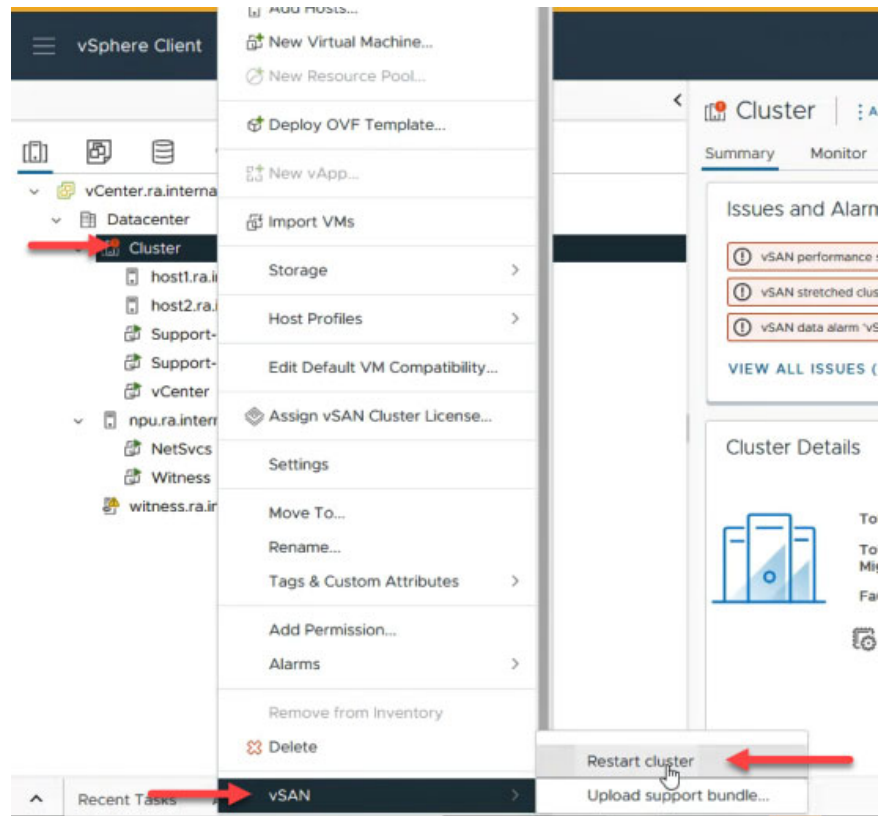


9. Repeat steps 7 and 8 for the remaining hosts.

## Restart vSAN Cluster

To restart the vSAN cluster, perform the following steps.

1. In the VMware vCenter, right-click the Cluster and select vSAN > Restart cluster.



2. Select Restart.



The vSAN cluster restarts.



**Notes:**

## Rename VersaVirtual Appliance Components

This chapter provides information on how to rename the VVA components. The procedures that are outlined in this chapter require approximately 1...2 hours to complete.

When multiple VVA units are installed on the same network, it is helpful to rename one of the units so both can be managed from one workstation. Renaming one of the units also reduces the need to edit the host file or reconfigure the DNS records.

---

**IMPORTANT** The procedures documented in this section can be performed without system downtime. However, when you implement the steps in this section, system redundancy is degraded, which can result in downtime, should a hardware or software component fail during procedure execution.

Rockwell Automation recommends that you implement the procedures in this section during a time when an unexpected failure will not cause the loss of production or other hazards.

---

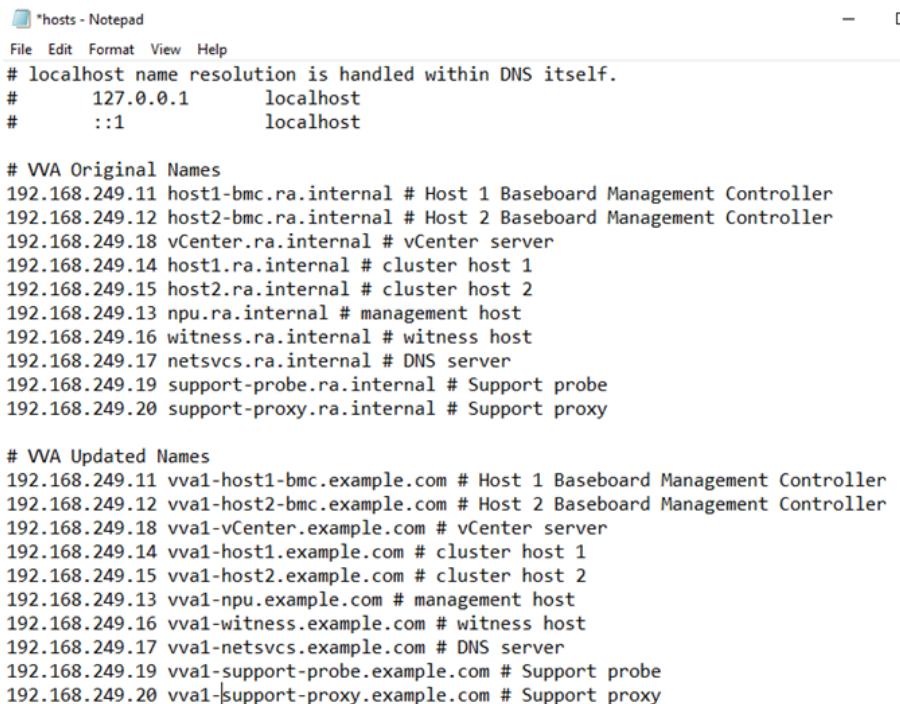
Before you perform the procedures in this section, consider the following:

- Host and domain names can be changed.
- Since vSphere is configured to use FQDNs, the process remains consistent regardless of the change being requested.
- The procedures in this section are based on components that are configured with default names and IP addresses, such as *vcenter.ra.internal* and *host1.ra.internal*.
- When a new host name is required, these procedures use "vva1-" at the start of the host name being changed – for example, *vva1-\*.example.com*.
- The domain "ra.internal" is replaced with "example.com."
- During implementation, the example values used in this section are meant to be replaced with the desired host and domain names.

## Preliminary Steps

Before you begin the rename process, perform the following preliminary steps.

1. Confirm you have a current backup of any VM stored on the vSAN cluster. While this process should be safe to perform without data loss or disruption, one of the procedures temporarily removes nodes from the vSAN cluster. If a component fails during this time, data loss could result.
2. Verify that the hosts and VMware vCenter are running VMware vSphere 6.7u3 or later.
3. Update the local hosts file or DNS server for the computer that is used to perform these steps. Doing so helps ensure that the new and default host names resolve properly. Following is an example of a host file that reflects the default and updated host names.



```

*hosts - Notepad
File Edit Format View Help
localhost name resolution is handled within DNS itself.
127.0.0.1 localhost
::1 localhost

VVA Original Names
192.168.249.11 host1-bmc.ra.internal # Host 1 Baseboard Management Controller
192.168.249.12 host2-bmc.ra.internal # Host 2 Baseboard Management Controller
192.168.249.18 vCenter.ra.internal # vCenter server
192.168.249.14 host1.ra.internal # cluster host 1
192.168.249.15 host2.ra.internal # cluster host 2
192.168.249.13 npu.ra.internal # management host
192.168.249.16 witness.ra.internal # witness host
192.168.249.17 netsvcs.ra.internal # DNS server
192.168.249.19 support-probe.ra.internal # Support probe
192.168.249.20 support-proxy.ra.internal # Support proxy

VVA Updated Names
192.168.249.11 vva1-host1-bmc.example.com # Host 1 Baseboard Management Controller
192.168.249.12 vva1-host2-bmc.example.com # Host 2 Baseboard Management Controller
192.168.249.18 vva1-vCenter.example.com # vCenter server
192.168.249.14 vva1-host1.example.com # cluster host 1
192.168.249.15 vva1-host2.example.com # cluster host 2
192.168.249.13 vva1-npu.example.com # management host
192.168.249.16 vva1-witness.example.com # witness host
192.168.249.17 vva1-netsvcs.example.com # DNS server
192.168.249.19 vva1-support-probe.example.com # Support probe
192.168.249.20 vva1-support-proxy.example.com # Support proxy

```

# Rename Procedures

## Add New Name Information to DNS Server Hosted by NetSvcs

Host name information must first be added to the DNS server hosted by NetSvcs. When you add host name information to this server, the VMware vCenter can resolve new and existing host names for the VMware vCenter and other system components. Adding host name information can also be helpful if you rename your VVA components.

To add new host name information to the DNS server hosted by NetSvcs, perform the following steps.

1. Connect to a terminal session on the NetSvcs VM, either through the VM remote console or through SSH.

Rockwell Automation recommends that you use SSH with an editor such as Microsoft® Visual Studio® Code so you can edit the DNS server configuration files offline and paste changes from the editor into the configuration file.

2. Once connected, edit the ra.conf file with the following command:

```
sudo nano /etc/unbound/local.d/ra.conf
```

```
[sysadmin@NetSvcs ~]$ sudo nano /etc/unbound/local.d/ra.conf _
```

3. In the editor, add new records for forward and reverse entries.
  - a. If only the host name is changing, add the new records to the existing "local-zone" section.
  - b. If you change the domain name, create a "local-zone" section as show in the sample updated configuration in the Updated ra.conf at the end of this section.

Confirm that the updated configuration contains records for both original and new names. Original records are removed as the last step in the configuration process.

4. Press CTRL+O and enter to save the file.
5. To exit the editor, press CTRL+X.
6. With the file updated, enter:

```
sudo systemctl restart unbound
```

The process might take several minutes to complete. Completion status is not typically displayed.

7. To verify status after running the command in step 6, enter:
 

```
systemctl status unbound
```
8. Look for active (running) status.

```

[sysadmin@NetSvcs ~]$ systemctl status unbound
● unbound.service - Unbound recursive Domain Name Server
 Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled; vendor preset: disabled)
 Active: active (running) since The 2023-06-22 18:42:48 EDT; 1min 37s ago
 Process: 2688824 ExecStartPre=/usr/sbin/unbound-checkconf -c /etc/nsswitch.conf (code=exited, status=0/SUCCESS)
 Main PID: 2688185 (unbound)
 Tasks: 4 (limit: 11341)
 Memory: 19.0M
 Group: /system.slice/unbound.service
 CGroup: /system.slice/unbound.service
 └─ 2688185 /usr/sbin/unbound -d

[sysadmin@NetSvcs ~]$ sudo hostnamectl set-hostname

```

Leave the shell session open.

## Factory default: ra.conf

Following is an example of the default *ra.conf* file.

---

```
access-control: 192.168.249.17/24 allow
access-control: 192.168.249.49/25 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.190/16 allow
access-control: 130.151.185.147/22 allow
access-control: 169.254.110.230/16 allow
access-control: 127.0.0.1/8 allow
unblock-lan-zones: yes
local-zone: "ra.internal." transparent
 local-data: "npu.ra.internal. IN A 192.168.249.13"
 local-data-ptr: "192.168.249.13 npu.ra.internal"
 local-data: "host1.ra.internal. IN A 192.168.249.14"
 local-data-ptr: "192.168.24v9.14 host1.ra.internal"
 local-data: "host2.ra.internal. IN A 192.168.249.15"
 local-data-ptr: "192.168.249.15 host2.ra.internal"
 local-data: "witness.ra.internal. IN A 192.168.249.16"
 local-data-ptr: "192.168.249.16 witness.ra.internal"
 local-data: "NetSvcs.ra.internal. IN A 192.168.249.17"
 local-data-ptr: "192.168.249.17 NetSvcs.ra.internal"
 local-data: "vCenter.ra.internal. IN A 192.168.249.18"
 local-data-ptr: "192.168.249.18 vCenter.ra.internal"
 local-data: "Support-Probe.ra.internal. IN A 192.168.249.19"
 local-data-ptr: "192.168.249.19 Support-Probe.ra.internal"
forward-zone:
 name: "."
forward-addr: 192.168.249.1s
```

---

## Updated ra.conf

Following is an example of an *ra.conf* file, after it has been updated.

---

```

access-control: 192.168.249.17/24 allow
access-control: 192.168.249.49/25 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.190/16 allow
access-control: 130.151.185.147/22 allow
access-control: 169.254.110.230/16 allow
access-control: 127.0.0.1/8 allow
unblock-lan-zones: yes
local-zone: "ra.internal." transparent
 local-data: "npu.ra.internal. IN A 192.168.249.13"
 local-data-ptr: "192.168.249.13 npu.ra.internal"
 local-data: "host1.ra.internal. IN A 192.168.249.14"
 local-data-ptr: "192.168.249.14 host1.ra.internal"
 local-data: "host2.ra.internal. IN A 192.168.249.15"
 local-data-ptr: "192.168.249.15 host2.ra.internal"
 local-data: "witness.ra.internal. IN A 192.168.249.16"
 local-data-ptr: "192.168.249.16 witness.ra.internal"
 local-data: "NetSvcs.ra.internal. IN A 192.168.249.17"
 local-data-ptr: "192.168.249.17 NetSvcs.ra.internal"
 local-data: "vCenter.ra.internal. IN A 192.168.249.18"
 local-data-ptr: "192.168.249.18 vCenter.ra.internal"
 local-data: "Support-Probe.ra.internal. IN A 192.168.249.19"
 local-data-ptr: "192.168.249.19 Support-Probe.ra.internal"
local-zone: "example.com." transparent
 local-data: "vval-npu.example.com. IN A 192.168.249.13"
 local-data-ptr: "192.168.249.13 vval-npu.example.com"
 local-data: "vval-host1.example.com. IN A 192.168.249.14"
 local-data-ptr: "192.168.249.14 vval-host1.example.com"
 local-data: "vval-host2.example.com. IN A 192.168.249.15"
 local-data-ptr: "192.168.249.15 vval-host2.example.com"
 local-data: "vval-witness.example.com. IN A 192.168.249.16"
 local-data-ptr: "192.168.249.16 vval-witness.example.com"
 local-data: "vval-NetSvcs.example.com. IN A 192.168.249.17"
 local-data-ptr: "192.168.249.17 vval-NetSvcs.example.com"
 local-data: "vval-vCenter.example.com. IN A 192.168.249.18"
 local-data-ptr: "192.168.249.18 vval-vCenter.example.com"
 local-data: "vval-Support-Probe.example.com. IN A
192.168.249.19"
 local-data-ptr: "192.168.249.19 vval-Support-
Probe.example.com"
forward-zone:
 name: "."
forward-addr: 192.168.249.1

```

---

## Rename NetSvcs

To rename the NetSvcs VM, perform the following procedures.

1. From the same shell session that was used to update the DNS server settings (in the [Add New Name Information to DNS Server Hosted by NetSvcs](#) section), enter:

```
sudo hostnamectl set-hostname <new fqdn>
```

Replace "<new fqdn>" with the new host name and domain name for NetSvcs. For example:

```
sudo hostnamectl set-hostname vval-
netsvcs.example.com
```

```
[sysadmin@netsvcs ~]$ sudo hostnamectl set-hostname vval-netsvcs.example.com
```

No information is returned after you run this command.

2. To verify that the host name and domain name have changed, enter:

```
hostnamectl
```

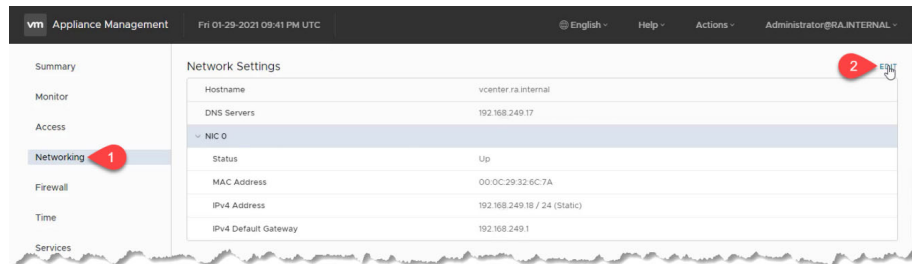
Review the output and confirm the new host name and domain name in the static host name field.

```
[sysadmin@netsvcs ~]$ hostnamectl
Static hostname: vval-netsvcs.example.com
Icon name: computer-vm
Chassis: vm
Machine ID: cae06e6fc52e4ff9b0e63e3e36cf0f2d
Boot ID: 0bc3f9ea77de41578fb2a51e934b9a97
Virtualization: vmware
Operating System: CentOS Linux 7 (Core)
CPE OS Name: cpe:/o:centos:centos:7
Kernel: Linux 3.10.0-957.12.1.el7.x86_64
Architecture: x86-64
[sysadmin@netsvcs ~]$
```

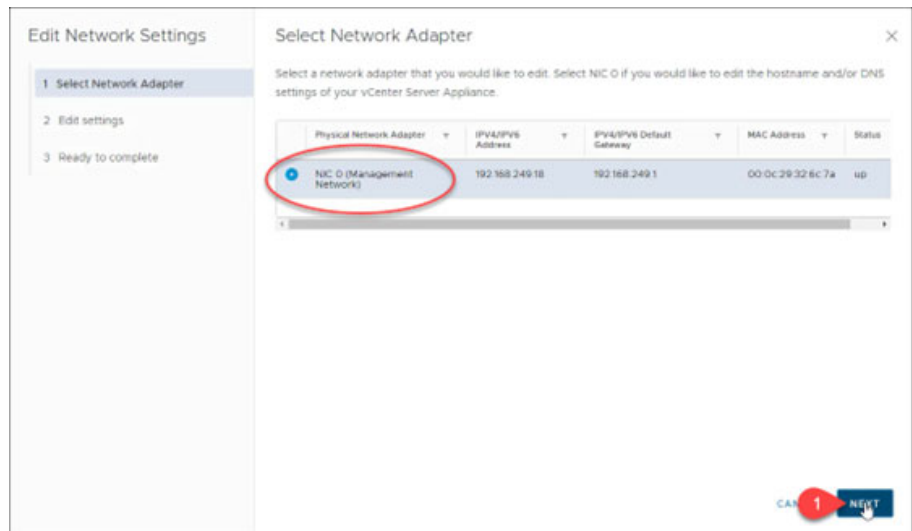
## Rename VMware vCenter

To rename the VMware vCenter, perform the following procedures.

1. Open a web browser and navigate to the VMware vCenter Server Appliance management interface:  
https://vcenter.ra.internal:5480
2. Sign in with the following credentials.  
Username: root (or) administrator@ra.internal  
Password: <system-specific password>
3. Select Next.
4. To open the network settings wizard, select Networking from the left navigation. Then, from the upper right, select Edit.

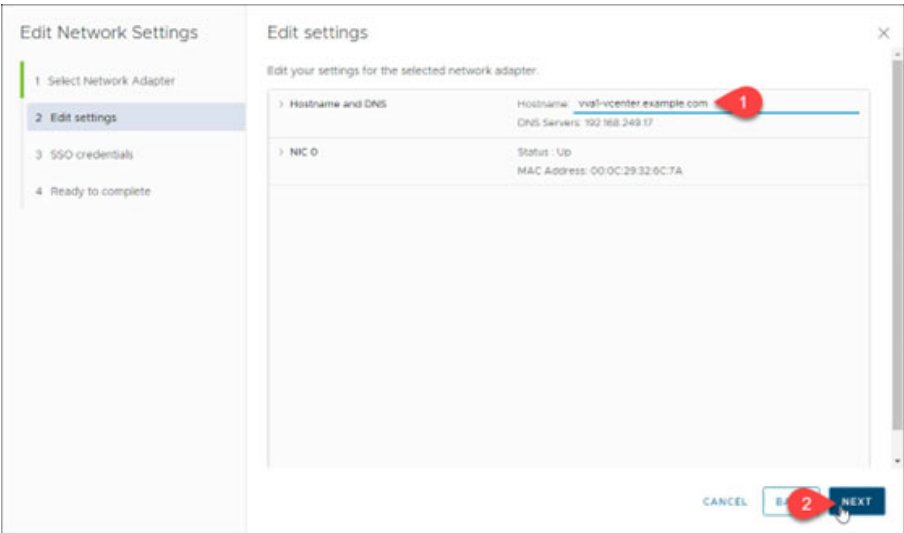


5. The standard VMware vCenter deployment displays one network adapter. Select next.





6. Update the host name field to the desired FQDN and then select Next.

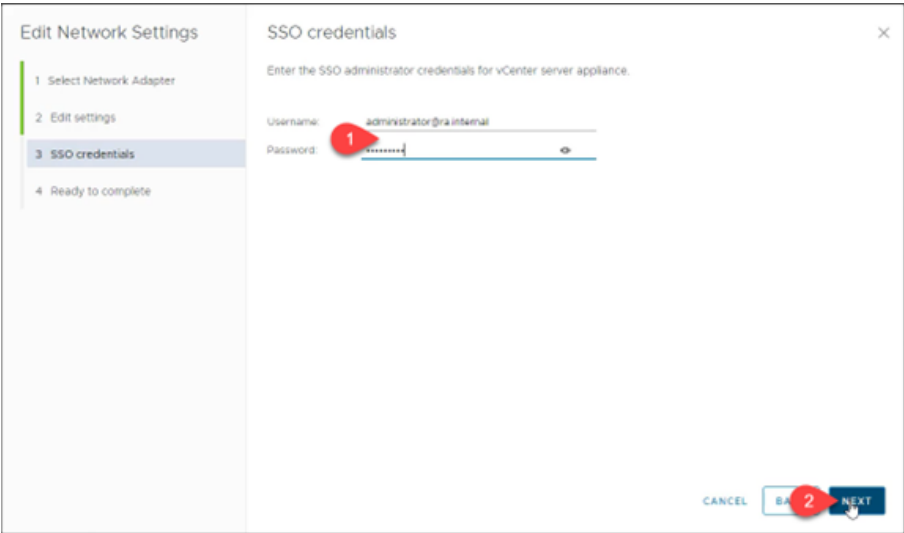


7. Enter the default SSO credentials for the unit:

Username: administrator@ra.internal

Password: <system-specific password>

8. Select Next.



9. Select the "I acknowledge that I have made a backup..." option and then select Finish.



**WARNING:** Do not refresh this page.

**WARNING:** After several minutes, the browser redirects you to the new FQDN.

**WARNING:** The VMware vCenter SSO is not functional at this point, so to sign in, use the root user name and password.



If you change the FQDN of VMware vCenter, the domain name that is used by the VMware vCenter SSO will not change. The default administrator account also remains unchanged:

administrator@ra.internal

10. The task progress window displays again.  
Continue to wait.
11. When the process is complete, select Close on the network update progress window.
12. The Summary page now reflects the new name of the VMware vCenter appliance.

## Redeploy the vSAN Witness Virtual Machine

It is typically more efficient to redeploy the vSAN witness VM with a new instance of the witness, rather than rename the existing instance. To redeploy the vSAN witness, perform the steps in this section.

### IMPORTANT

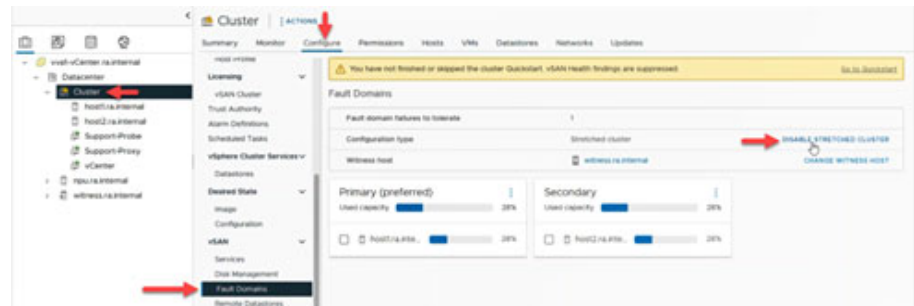
This process degrades the redundant state of the vSAN cluster. To reduce the risk of data loss due to a component failure during this procedure, backup and shut down any VMs that are running on the unit.

Any VMs that are running during this procedure continue to run. However, when you perform the steps in this procedure, the unit operates without redundancy, and will stop operating if a cluster host or disk fails during the procedure.

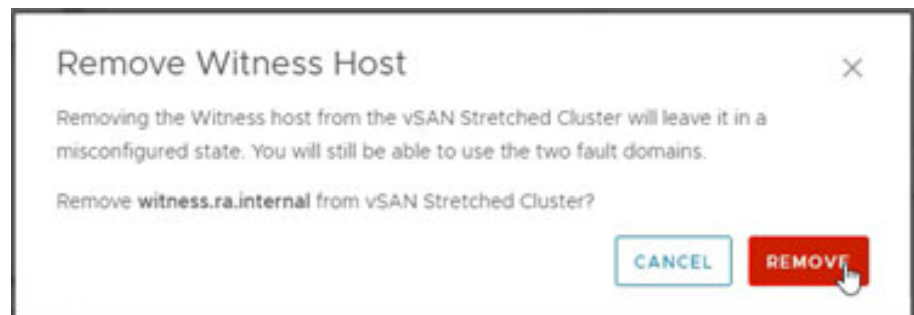
## Unregister and Remove Existing Witness

To unregister and remove the existing witness, perform the following procedures.

1. Sign in to the VMware vCenter Client
2. Open a web browser and navigate to the VMware vCenter Client:
3. <https://vcenter.ra.internal>
4. Sign in with the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>
5. Select Login.
6. Once logged in, select Cluster and then navigate to the Configure tab.
7. From the configuration list, select Fault Domains.
8. Select Disable Stretched Cluster.



9. A warning is displayed to indicate that the vSAN witness is about to be removed from the cluster, which could lead to a cluster misconfiguration. Select Remove.

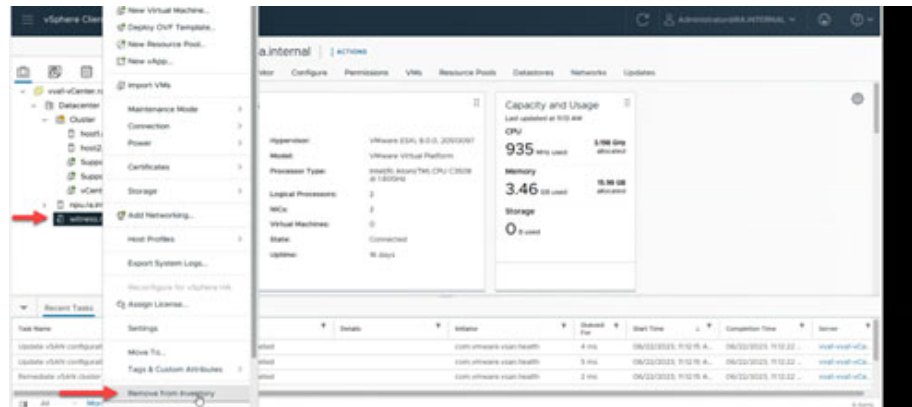


The cluster is degraded while the witness is replaced.

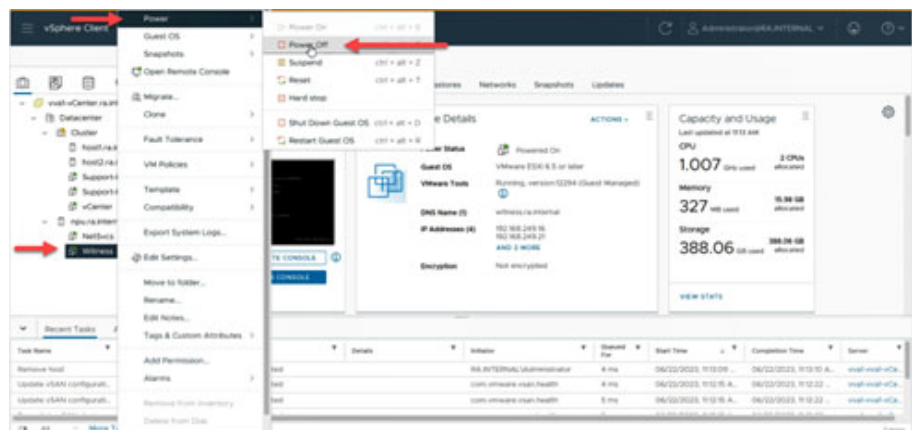
10. Wait for the Remove witness host and all Update vSAN configuration tasks to complete.

| Task Name                  | Target              | Status    |
|----------------------------|---------------------|-----------|
| Update vSAN configurati... | host2.ra.internal   | Completed |
| Update vSAN configurati... | host1.ra.internal   | Completed |
| Remediate vSAN cluster     | Cluster             | Completed |
| Update vSAN configurati... | witness.ra.internal | Completed |
| Update vSAN configurati... | witness.ra.internal | Completed |
| Remove witness host        | Cluster             | Completed |

11. Right-click the Witness host and select Remove from Inventory.

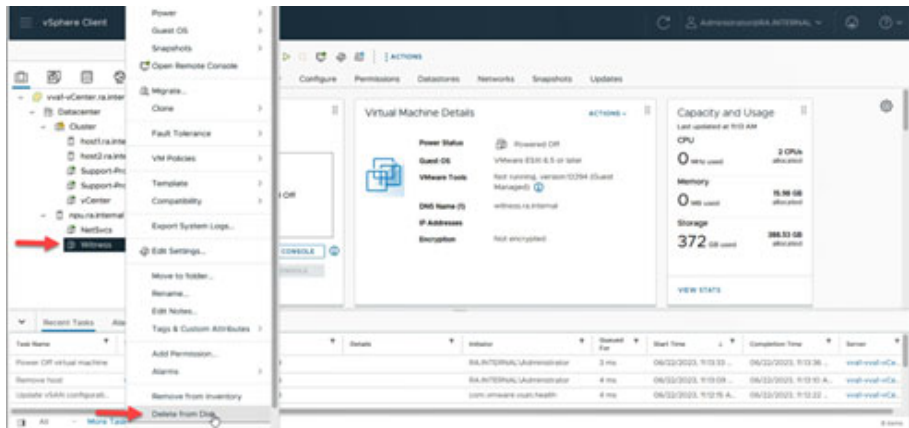


12. Right-click on the Witness VM and select Power > Power Off.



It is not necessary to shut down the guest OS since the VM is going to be removed and replaced.

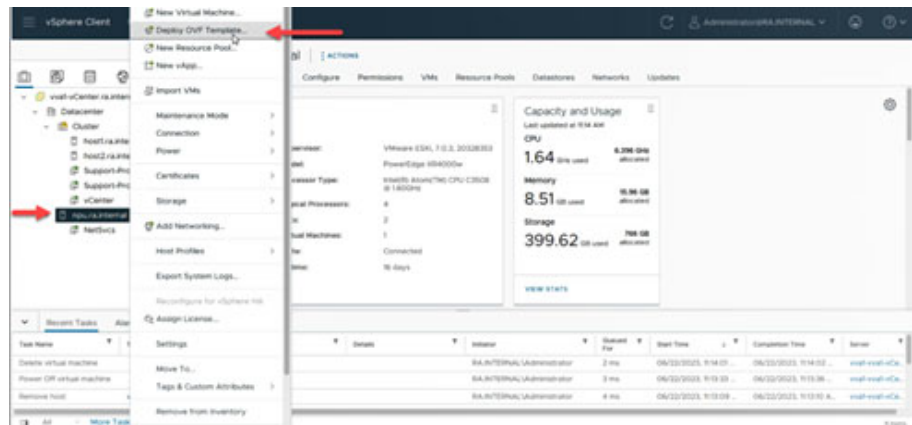
13. Right-click on the Witness VM and select Delete from Disk.



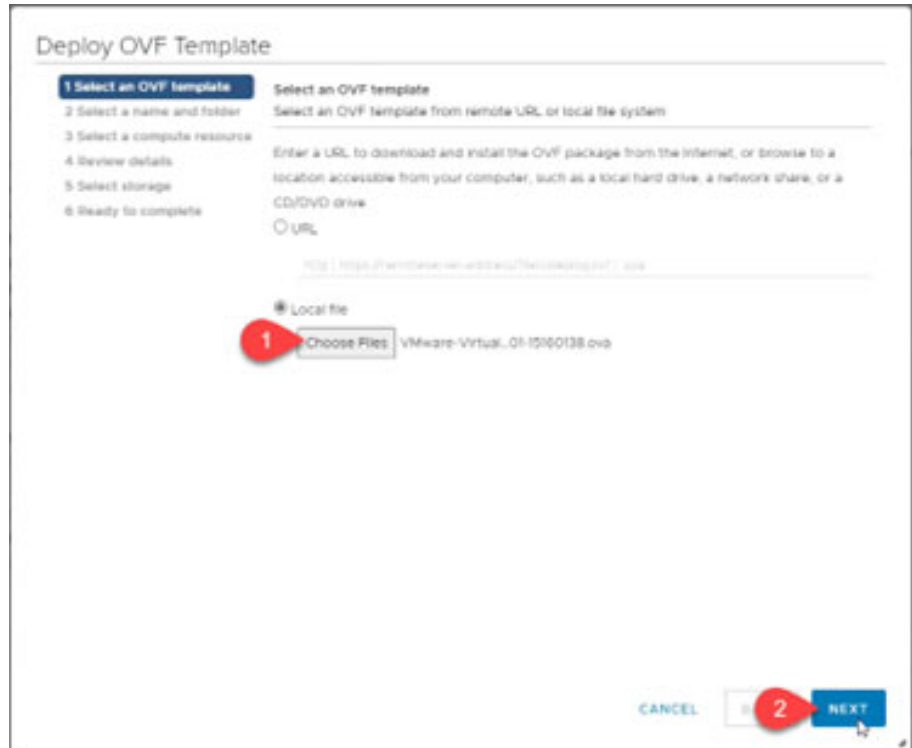
## Deploy the New vSAN Witness Virtual Machine

To deploy the new vSAN witness VM, perform the following steps.

1. Right-click on the NPU host and select Deploy OVF Template.



2. In the Deploy OVF Template wizard, select Local File > Choose Files. Browse to the location of *VMware-VirtualSAN-Witness-201912001-15160138.ovf*, or a newer version of that file provided by Rockwell Automation technical support. Then select Next.



## 3. Enter a name for the Witness VM.

Deploy OVF Template

✓ 1 Select an OVF template  
2 Select a name and folder  
3 Select a compute resource  
4 Review details  
5 Select storage  
6 Ready to complete

Select a name and folder  
Specify a unique name and target location

Virtual machine: **1** Witness

Select a location for the virtual machine

- ✓ vreal-vcenter.example.com
  - ✓ Datacenter
    - Applications
    - Discovered virtual machine
    - Management**
    - Templates

CANCEL **2** NEXT



The name does not have to match the host name or FQDN of the witness appliance.

Rockwell Automation recommends adding “witness” to the name to help identify it in the future.

4. Select Next.
5. Verify that the NPU host is selected and that no compatibility issues are displayed, and then select Next.

Deploy OVF Template

✓ 1 Select an OVF template  
✓ 2 Select a name and folder  
3 Select a compute resource  
4 Review details  
5 Select storage  
6 Ready to complete

Select a compute resource  
Select the destination compute resource for this operation

- ✓ Datacenter
  - Cluster1
  - 1** management.na.internal

Compatibility

**2** ✓ Compatibility checks succeeded

CANCEL **3** NEXT

## 6. Review the template details.

If you specify additional configuration information for the VM, additional steps might be added to the wizard.

## 7. After you confirm the template details, select Next.

**Deploy OVF Template**

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

**Review details**  
Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

|                        |                                                          |
|------------------------|----------------------------------------------------------|
| Publisher              | VMware, Inc. (Trusted certificate)                       |
| Product                | VMware vSAN Witness Appliance                            |
| Version                | 8.0U1                                                    |
| Vendor                 | VMware, Inc.                                             |
| Description            | VMware vSAN Witness Appliance                            |
| Download size          | 326.7 MB                                                 |
| Size on disk           | Unknown (thin provisioned)<br>2.5 TB (thick provisioned) |
| Advanced configuration | svs.maxWidth = 720                                       |

CANCEL **NEXT**

## 8. Review and accept the end-user license agreement and then select Next.

**Deploy OVF Template**

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements**
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

**License agreements**  
The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

**VMWARE END USER LICENSE AGREEMENT**

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID.

**1** ☒ I accept all license agreements.

CANCEL **2** **NEXT**



9. Confirm that the Medium configuration size is selected and click Next.

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration**
- Select storage
- Select networks
- Customize template
- Ready to complete

**Configuration**

☒ Medium (up to 500 VMs/21 Clusters)  
☐ Large (more than 500 VMs/24 Clusters)  
☐ Extra Large (Up to 64 Clusters)

Deployments of up to 500 VMs / 21 Clusters. Component Maximums: (1 Cluster: 25K Witness Components, 21 Clusters: 9K/Cluster). Please see the Deploying a vSAN Witness Appliance section of the vSAN Planning and Deployment guide for further details.

CANCEL **NEXT**

10. Select NPU.Datastore as the target datastore, confirm that the virtual disk format is set to Thick Provision Lazy Zeroed, and then select Next.

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage**
- Select networks
- Customize template
- Ready to complete

**Select storage**

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: NPU.Datastore

☐ Disable Storage DRS for this virtual machine

| Name          | Storage Compatibility | Capacity | Provisioned | Free      | Type   | Cluster |
|---------------|-----------------------|----------|-------------|-----------|--------|---------|
| NPU.Datastore | —                     | 766 GB   | 84.68 GB    | 754.52 GB | VMFS 6 |         |

Items per page: 10 | 1 item

**Compatibility**

✓ Compatibility checks succeeded.

CANCEL **NEXT**

11. On Select Networks, set Management Network to Management Network and Secondary Network to Management Network. Then select Next.

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks**
- Customize template
- Ready to complete

**Select networks**

Select a destination network for each source network.

| Source Network     | Destination Network   |
|--------------------|-----------------------|
| Management Network | Management VM Network |
| Secondary Network  | Management VM Network |

2 items

**IP Allocation Settings**

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL **NEXT**

12. On Customize Template enter the appliance password or desired password for the vSAN Witness, set Network for vSAN Traffic to Secondary. Then scroll down to complete the rest of the form.

**Deploy OVF Template**

1 Select an OVF template  
2 Select a name and folder  
3 Select a compute resource  
4 Review details  
5 License agreements  
6 Configuration  
7 Select storage  
8 Select networks  
9 **Customize template**  
10 Ready to complete

**Customize template**  
Customize the deployment properties of this software solution.

All properties have valid values

**System Configuration** 1 settings

Root password Set password for root account. A valid password must be at least 7 characters long and must contain a mix of upper and lower case letters, digits, and other characters.

Password  **1**  
Confirm Password

**vSAN Traffic** 1 settings

Network for vSAN Traffic Which network will be used for vSAN Traffic?  
**2** Secondary

**Management Network** 7 settings

IP Address IP Address of vmk0 (DHCP if left blank)

Netmask Netmask of vmk0 (DHCP if left blank)

**3**

CANCEL BACK NEXT

13. Configure the Management Network as follows:

- IP address: 192.168.249.16
- Netmask: 255.255.255.0
- Gateway: 192.168.249.1

**Deploy OVF Template**

1 Select an OVF template  
2 Select a name and folder  
3 Select a compute resource  
4 Review details  
5 License agreements  
6 Configuration  
7 Select storage  
8 Select networks  
9 **Customize template**  
10 Ready to complete

**Customize template**

Password   
Confirm Password

**vSAN Traffic** 1 settings

Network for vSAN Traffic Which network will be used for vSAN Traffic?  
Secondary

**Management Network** 7 settings

IP Address IP Address of vmk0 (DHCP if left blank)  
192.168.249.16

Netmask Netmask of vmk0 (DHCP if left blank)  
255.255.255.0

Gateway Gateway of vmk0 (DHCP if left blank)  
192.168.249.1

DNS Domain DNS Domain (DHCP if left blank)

CANCEL BACK NEXT



If the IP addresses in your unit have already been reconfigured per the procedures in this user manual, adjust the values in this section to match the new addresses used for the appliance.

IP addresses referenced in the following steps and screenshots are based on factory defaults.

## 14. Scroll down and continue the configuration, as follows.

- DNS Domain: ra.internal or the desired new domain name  
example: example.com
- Witness Host name: witness or the desired new host name  
example: vva1-witness
- DNS Server: 192.168.249.17

If the unit has been reconfigured per this user manual, use the new address that is assigned to NetSvcs

- NTP Servers: 192.168.249.1

If the unit has been reconfigured per this user manual, use the new addresses that are assigned to network module 1 and 2

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks
- Customize template**
- Ready to complete

**Customize template**

Management Network 7 settings

|                  |                                                             |
|------------------|-------------------------------------------------------------|
| IP Address       | IP Address of vmk0 (DHCP if left blank)<br>192.168.249.16   |
| Netmask          | Netmask of vmk0 (DHCP if left blank)<br>255.255.255.0       |
| Gateway          | Gateway of vmk0 (DHCP if left blank)<br>192.168.249.1       |
| DNS Domain       | DNS Domain (DHCP if left blank)<br>example.com              |
| Witness Hostname | Witness Hostname (DHCP if left blank)<br>vva1-witness       |
| DNS Servers      | Use comma separators (DHCP if left blank)<br>192.168.249.17 |
| NTP Servers      | Use comma separators or leave blank<br>192.168.249.1        |

CANCEL BACK **NEXT**

## 15. Scroll down and set the Secondary Network address to 192.168.250.70, with a subnet mask of 255.255.255.192.

Leave the gateway blank and select Next

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks
- Customize template**
- Ready to complete

**Customize template**

DNS Domain DNS Domain (DHCP if left blank)  
example.com

Witness Hostname Witness Hostname (DHCP if left blank)  
vva1-witness

DNS Servers Use comma separators (DHCP if left blank)  
192.168.249.17

NTP Servers Use comma separators or leave blank  
192.168.249.1

**Secondary Network 3 settings**

|            |                                                           |
|------------|-----------------------------------------------------------|
| IP Address | IP Address of vmk1 (DHCP if left blank)<br>192.168.249.21 |
| Netmask    | Netmask of vmk1 (DHCP if left blank)<br>255.255.255.192   |
| Gateway    | Gateway of vmk1 (Not set if left blank)                   |

CANCEL BACK **NEXT**

## 16. Review the configuration and then select Finish.

**Deploy OVF Template**

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks
- Customize template
- Ready to complete**

**Ready to complete**

Storage mapping 1  
All disks Datastore: NPU.datastore; Format: Thick provision lazy zeroed

Network mapping 2  
Management Network Management VM Network  
Secondary Network Management VM Network

IP allocation settings  
IP protocol IPv4  
IP allocation Static - Manual

Customize template  
Properties  
Network for vSAN Traffic = Secondary  
IP Address = 192.168.249.16  
Netmask = 255.255.255.0  
Gateway = 192.168.249.1  
DNS Domain = example.com  
Witness Hostname = vvaal-witness  
DNS Servers = 192.168.249.17  
NTP Servers = 192.168.249.1  
IP Address = 192.168.249.21  
Netmask = 255.255.255.192  
Gateway =

CANCEL FINISH

## 17. Wait for the Deploy OVF Template and Import OVF package tasks to complete.

| Recent Tasks        |                 |           | Alarms |
|---------------------|-----------------|-----------|--------|
| Task Name           | Target          | Status    |        |
| Deploy OVF template | npu.ra.internal | Completed |        |
| Import OVF package  | npu.ra.internal | Completed |        |

| Recent Tasks        |                 |           | Alarms |
|---------------------|-----------------|-----------|--------|
| Task Name           | Target          | Status    |        |
| Deploy OVF template | npu.ra.internal | Completed |        |
| Import OVF package  | npu.ra.internal | Completed |        |

## 18. Right-click on the new Witness VM and select Power &gt; Power On

**vSphere Client**

Power On

Power Status: Powered Off

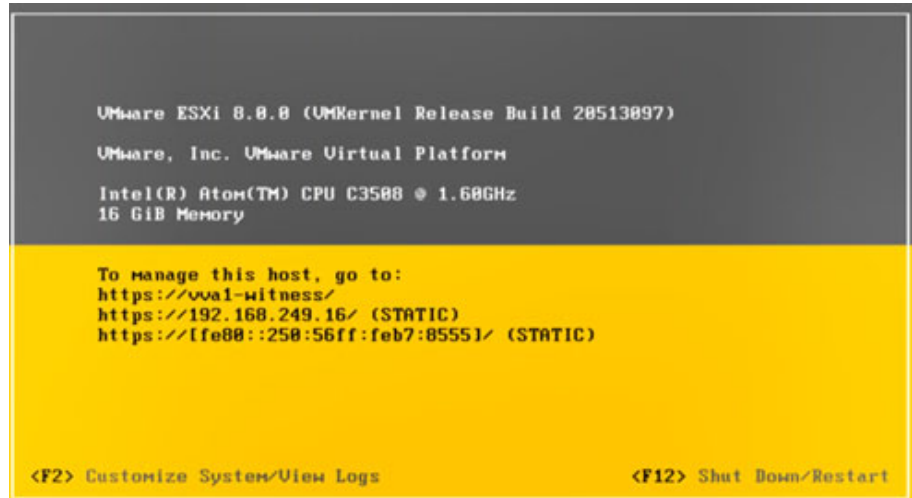
Capacity and Usage

CPU: 0% used, 2 CPUs allocated

Memory: 15.76 GB used, 16.00 GB allocated

Storage: 372 GB used, 500.00 GB allocated

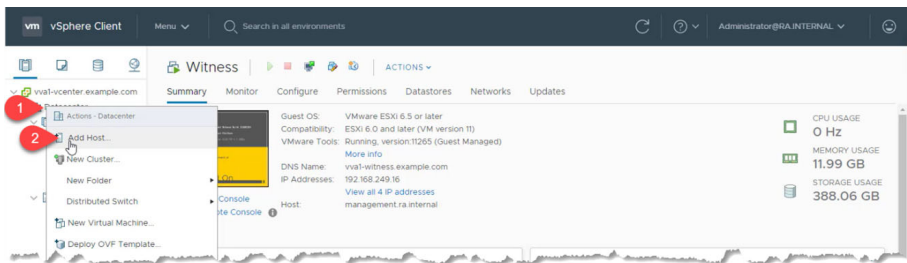
19. Wait for the VM to finish start up. To monitor the startup sequence, select the VM, which displays a small console status icon to the right of the selection.



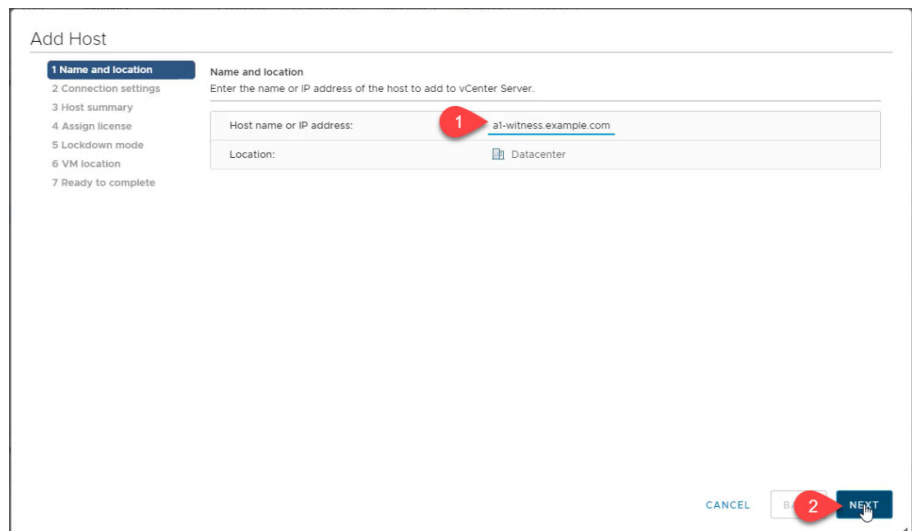
## Register the New vSAN Witness

To register the new vSAN witness, perform the following steps.

1. Right-click Datacenter and select Add Host...



2. Enter the new FQDN of the Witness and select Next



3. Enter the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>

## 4. Select Next.

Add Host

1 Name and location  
2 Connection settings  
3 Host summary  
4 Assign license  
5 Lockdown mode  
6 VM location  
7 Ready to complete

Connection settings  
Enter the host connection details

User name: root  
Password: .....

CANCEL BACK NEXT

## 5. To accept the certificate thumbprint, select Yes.

Add Host

1 Name and location  
2 Connection settings  
3 Host summary  
4 Assign license  
5 Lockdown mode  
6 VM location  
7 Ready to complete

Connection settings  
Enter the host connection details

Security Alert

The certificate store of vCenter Server cannot verify the certificate.

The SHA1 thumbprint of the certificate is:  
D4:6F:29:B3:DB:2F:38:05:C6:0B:E5:0D:DB:0C:F3:BE:9D:EA:27:B2

Click Yes to replace the host's certificate with a new certificate signed by the VMware Certificate Server and proceed with the workflow.

Click No to cancel connecting to the host.

YES

CANCEL BACK NEXT

## 6. Verify that the information on the Host summary screen is correct and click Next

Add Host

1 Name and location  
2 Connection settings  
3 Host summary  
4 Assign license  
5 Lockdown mode  
6 VM location  
7 Ready to complete

Host summary  
Review the summary for the host

|                  |                                  |
|------------------|----------------------------------|
| Name             | vva1-witness.example.com         |
| Vendor           | VMware, Inc.                     |
| Model            | VMware Virtual Platform          |
| Version          | VMware ESXi 6.7.0 build-15160138 |
| Virtual Machines |                                  |

CANCEL BACK NEXT

## 7. Accept the default license assignment and click Next

Add Host

1 Name and location  
2 Connection settings  
3 Host summary  
4 Assign license  
5 Lockdown mode  
6 VM location  
7 Ready to complete

Assign license  
Assign an existing or a new license to this host

| License                                    | License Key                   | Product                  | Usage  | Capacity |
|--------------------------------------------|-------------------------------|--------------------------|--------|----------|
| <input checked="" type="radio"/> License 1 | NH2HM-XXXXX-XXXXX-XXXXX-28DNP | VMware vSphere 6 for ... | 2 CPUs | 2 CPUs   |
| <input type="radio"/> vSphere              | 1N62L-2WK1J-WB487-QJ0U6-1RMNM | VMware vSphere 6 Sta...  | 3 CPUs | 3 CPUs   |
| <input type="radio"/> Evaluation License   | --                            | --                       | --     | --       |

Assignment Validation for License 1

☒ The license assignment is valid.

CANCEL BACK **2** NEXT

### IMPORTANT

DO NOT CHANGE THE LICENSE.

The vSAN Witness virtual appliance is provided with a pre-installed license from VMware.

If the license is changed, the witness must be removed and recreated.

## 8. Accept the Lockdown mode default configuration and select Next.

Add Host

1 Name and location  
2 Connection settings  
3 Host summary  
4 Assign license  
5 Lockdown mode  
6 VM location  
7 Ready to complete

Lockdown mode  
Specify whether to enable lockdown mode on the host

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.

If you are unsure what to do, leave lockdown mode disabled. You can configure lockdown mode later by editing Security Profile in host settings.

☒ Disabled

☐ Normal  
The host is accessible only through the local console or vCenter Server.

☐ Strict  
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

CANCEL BACK **2** NEXT

## 9. Select a VM location and then select Next.

Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- ✓ 4 Assign license
- ✓ 5 Lockdown mode
- 6 VM location**
- 7 Ready to complete

VM location

- ▼ Datacenter
  - Applications
  - Discovered virtual machine
  - Management**
  - Templates

CANCEL BACK **2** NEXT

## 10. Verify the configuration information and select Finish

Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- ✓ 4 Assign license
- ✓ 5 Lockdown mode
- ✓ 6 VM location
- 7 Ready to complete**

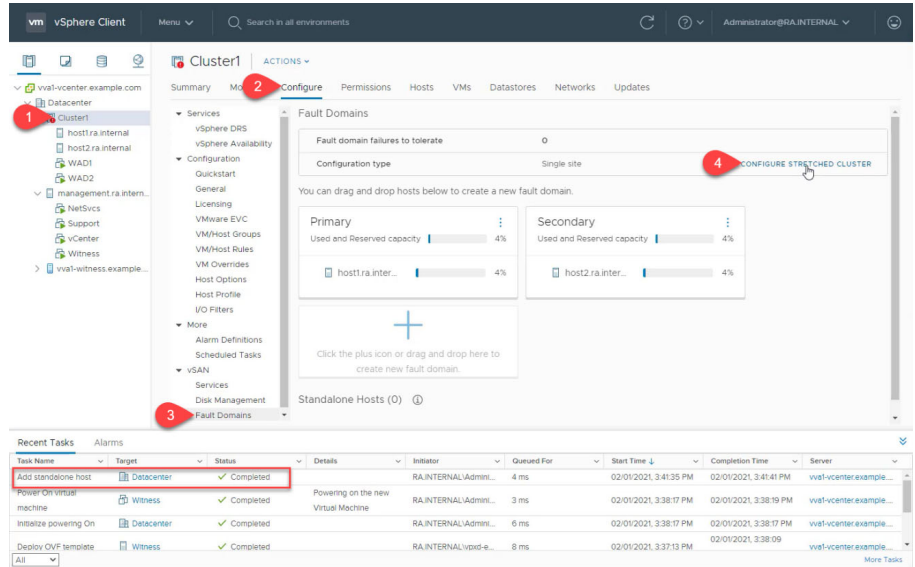
Ready to complete  
Click Finish to add the host

|               |                                  |
|---------------|----------------------------------|
| Name          | vval-witness.example.com         |
| Location      | Datacenter                       |
| Version       | VMware ESXi 6.7.0 build-15160138 |
| License       | License 1                        |
| Networks      | VM Network                       |
| Datastores    |                                  |
| Lockdown mode | Disabled                         |
| VM location   | Management                       |

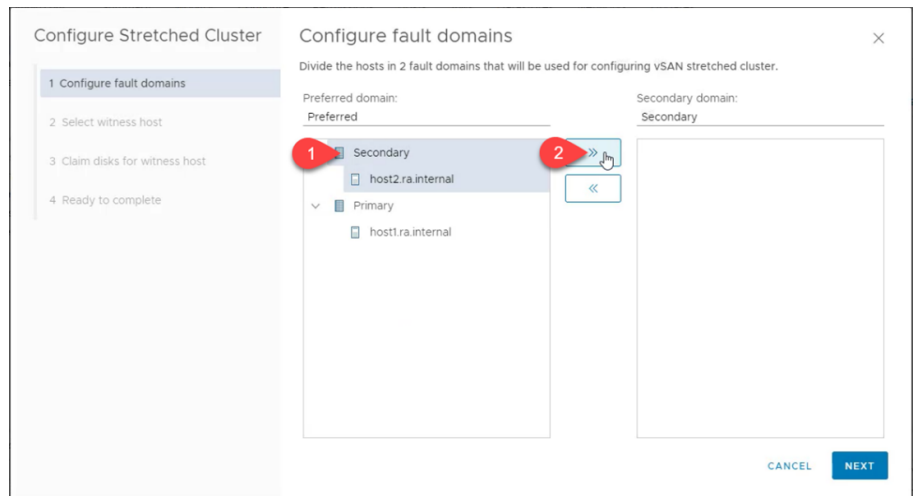
CANCEL BACK **1** FINISH



11. When the Add Standalone Host task completes, perform the following steps.
  - a. Select Cluster and navigate to the Configure tab.
  - b. From the configuration list, select Fault Domains.
  - c. Select Configure Stretched Cluster.



12. Select Secondary (fault domain) and then click the double arrow (>>) button. This moves the secondary fault domain to the right pane.

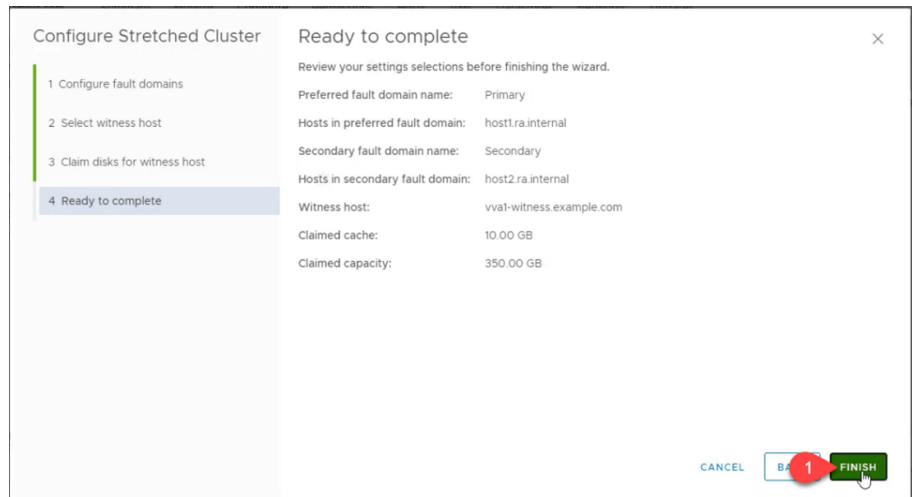


13. Verify that host 1 is in the primary fault domain field and host 2 is in the secondary fault domain field. Then select Next

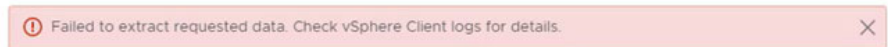
14. Select the new witness host from the inventory list, which launches the Configure Stretched Cluster wizard to run a compatibility check. Verify that the check succeeds and then select Next.

15. Select the cache and capacity tier disks. Confirm that there is only one of each, then select Next to continue.

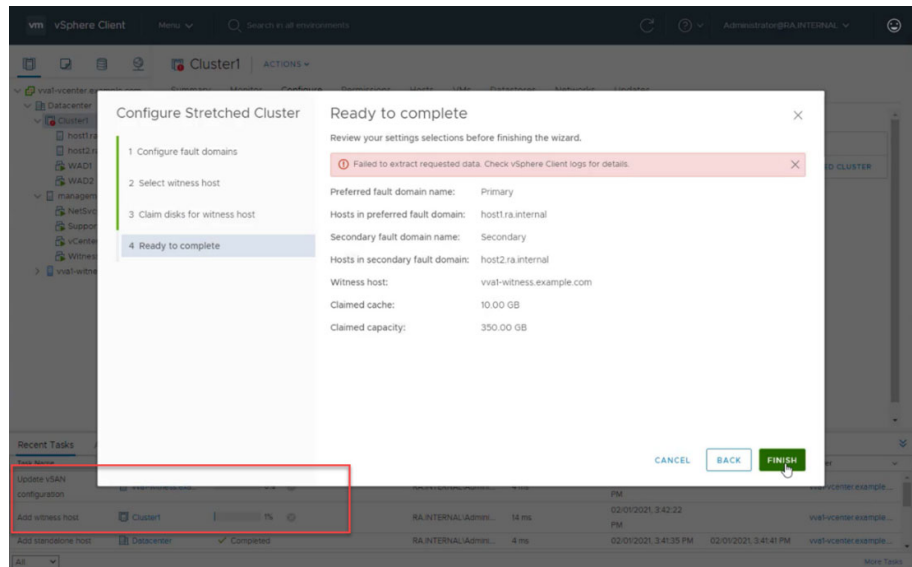
## 16. Verify the configuration information and then select Finish.



## 17. After you select Finish, you might receive the following error:



## 18. This error message might be false. If you receive it, verify the task sign in the background.



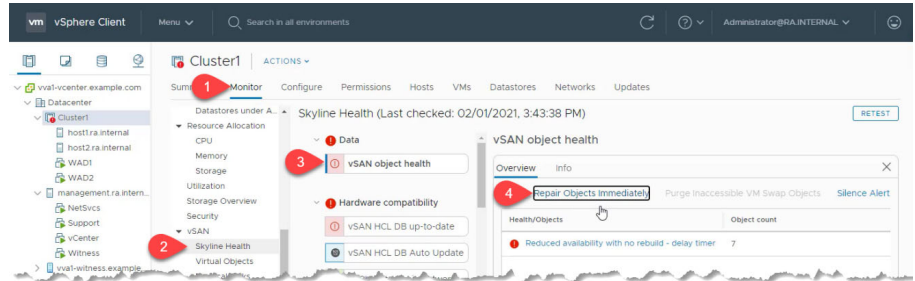
If there is an Add witness host and Update vSAN configuration task in the task list, close the wizard by clicking the X in the upper right and then wait for the tasks to complete.

19. To rebuild the virtual objects, perform the following steps.
  - a. Select the Monitor tab, and navigate to vSAN > Skyline Health.
  - b. Select the vSAN object health alert.

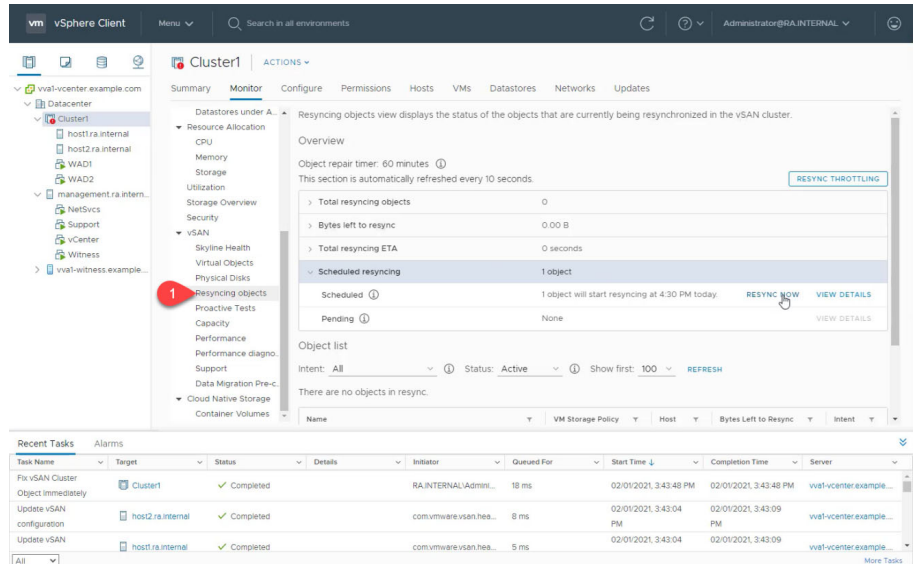
Performance counter objects are degraded, even on systems without VMs.

- c. To start the rebuild, select Repair Objects Immediately.

It can take several minutes to complete this process, depending on the number of affected objects.



20. To monitor resynchronization, select vSAN > Resyncing objects.



Wait for the resynchronization to complete before continuing.

## Rename Cluster Hosts

To rename the cluster hosts, you must remove each host from the vSAN cluster individually. If you perform these steps, your system redundancy will be temporarily degraded. To reduce the risk of data loss due to a component failure during this procedure, shut down and back up any VMs that run on the unit.

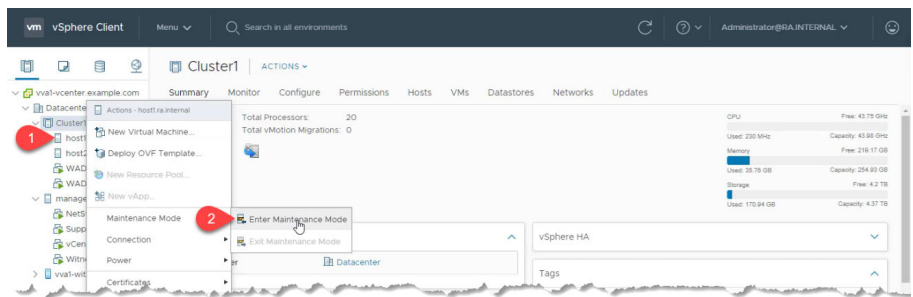
**IMPORTANT** Any VMs that are running during this procedure continue to run. However, the unit will run without redundancy and will stop running if a cluster host or disk fails during the procedure.

### Rename Host 1

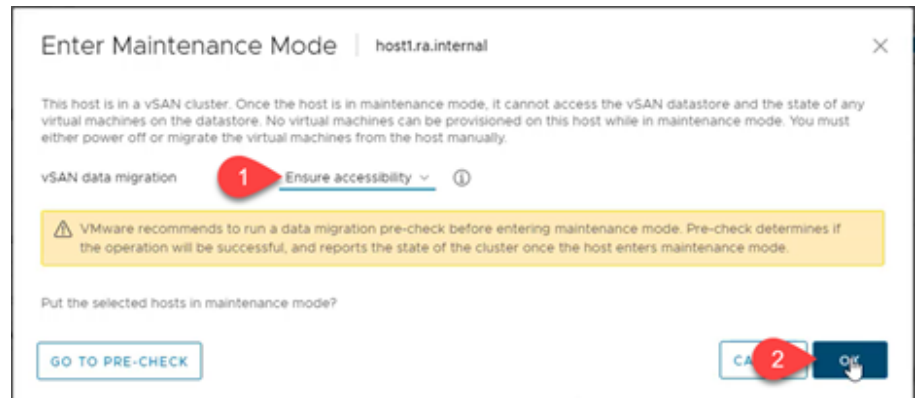
#### Enter Maintenance Mode on Host 1

To enter maintenance mode on host 1, perform the following procedures.

1. Open a web browser and navigate to the VMware vCenter Client:
2. <https://vcenter.ra.internal>
3. Sign in with the following credentials.  
Username: administrator@ra.internal  
Password: <system-specific password>
4. Select Login.
5. Right-click Host1 and select Maintenance Mode > Enter Maintenance Mode



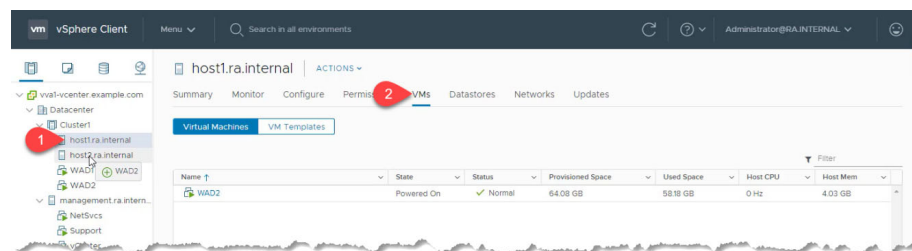
6. Select Ensure accessibility and then select Ok.



7. If there is an active VM on Host 1, a warning is displayed.



8. Select Ok.  
 9. If there is an active VM on Host 1, select Host 1 and then navigate to the VMs tab.  
 10. Select and drop each active VM from host 1 to host 2.



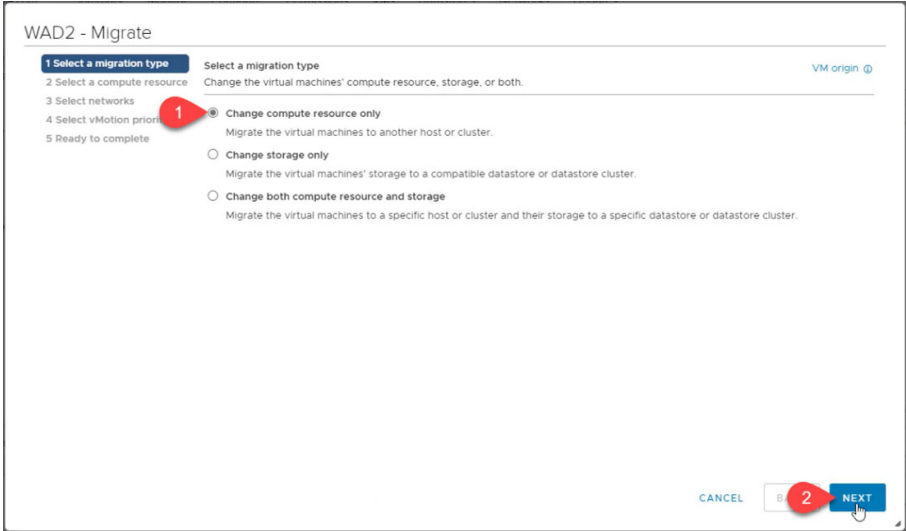
To move multiple VMs between hosts, hold down the shift key and select the VMs you wish to move, then move the selected VMs to the other host as needed.

11. If you move multiple VMs, an alert is displayed to confirm the action.

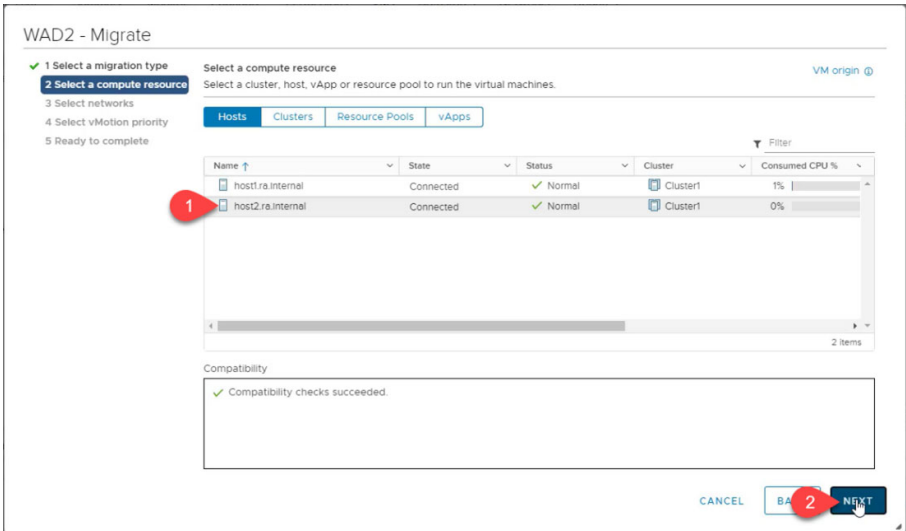


12. To proceed, select Yes.

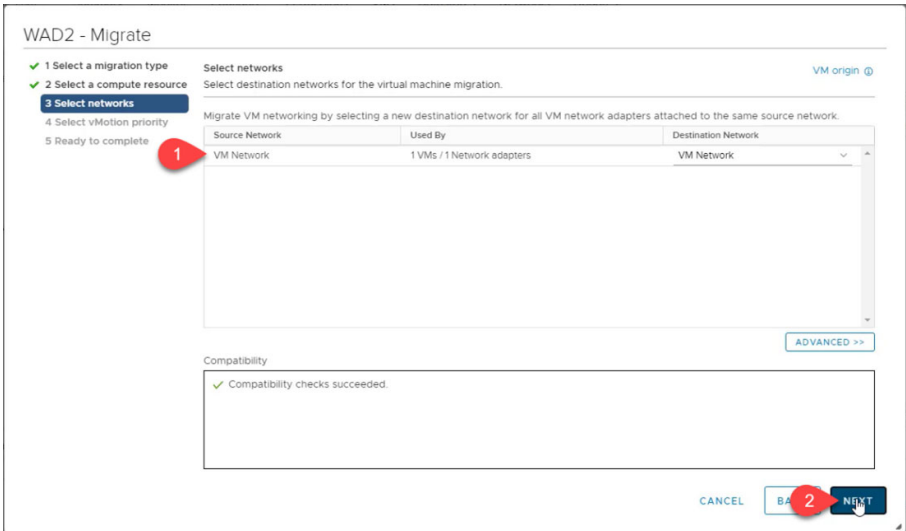
13. The Migration wizard is displayed. Select Change compute resource only and then select Next.



14. Verify that host 2 is selected then select Next.



15. Verify the VM Network connection mapping and select Next.



## 16. Select Schedule vMotion with high priority then select Next.

WAD2 - Migrate

✓ 1 Select a migration type  
 ✓ 2 Select a compute resource  
 ✓ 3 Select networks  
 4 Select vMotion priority  
 5 Ready to complete

Select vMotion priority  
Protect the performance of your running virtual machines by prioritizing the allocation of CPU resources.

☒ Schedule vMotion with high priority (recommended)  
 vMotion receives higher CPU scheduling preference relative to normal priority migrations. vMotion might complete more quickly.

☐ Schedule normal vMotion  
 vMotion receives lower CPU scheduling preference relative to high priority migrations. You can extend vMotion duration.

CANCEL **2** NEXT

## 17. When ready to migrate the VM(s), select Finish.

WAD2 - Migrate

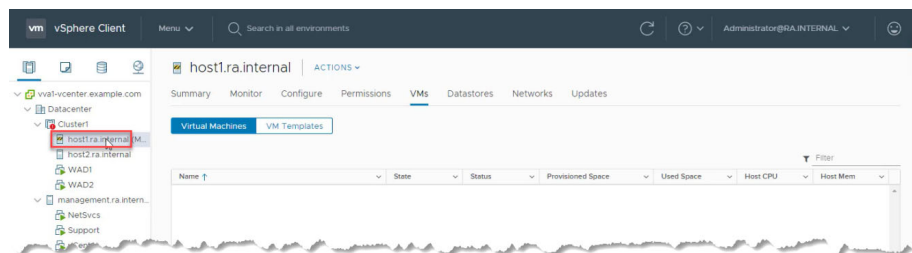
✓ 1 Select a migration type  
 ✓ 2 Select a compute resource  
 ✓ 3 Select networks  
 ✓ 4 Select vMotion priority  
 5 Ready to complete

Ready to complete  
Verify that the information is correct and click Finish to start the migration.

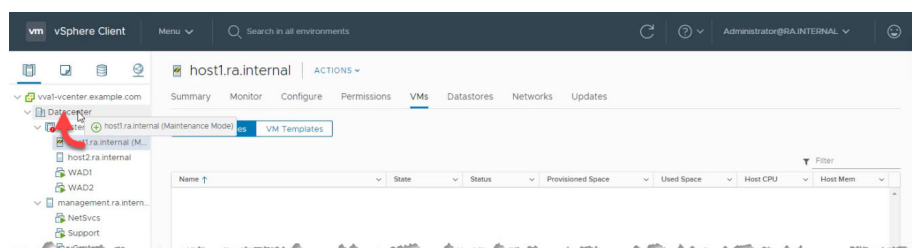
|                  |                                                           |
|------------------|-----------------------------------------------------------|
| Migration Type   | Change compute resource. Leave VM on the original storage |
| Virtual Machine  | WAD2                                                      |
| Cluster          | Cluster1                                                  |
| Host             | host2.ra.internal                                         |
| vMotion Priority | High                                                      |
| Networks         | No network reassignments                                  |

CANCEL **1** FINISH

## 18. When VM migration is complete, the host exits maintenance mode.



## 19. To remove Host 1 from the cluster, select it and drop it into Datacenter.

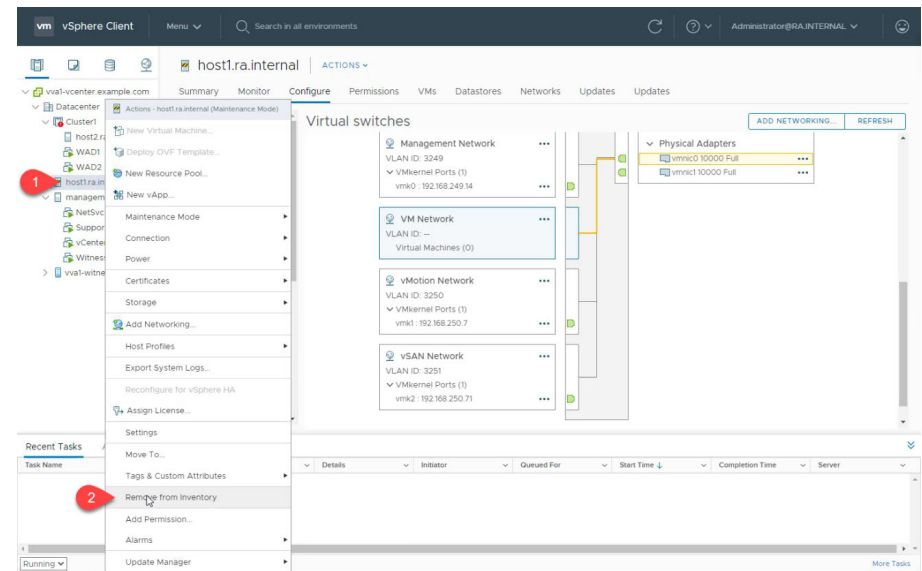




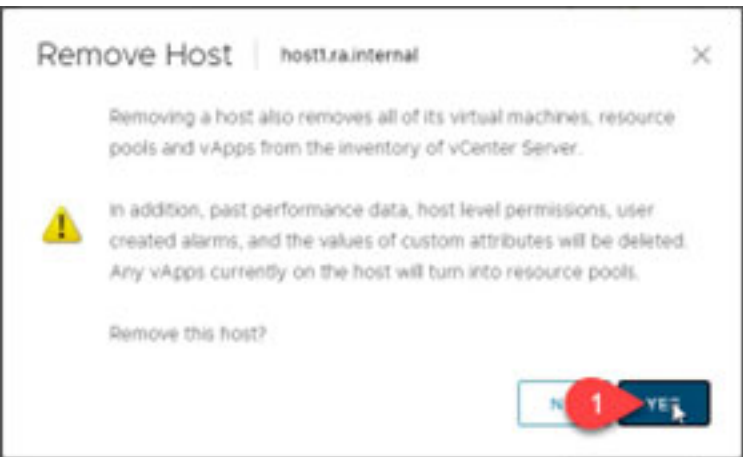
Remove Host 1 from VMware vCenter Inventory

To remove host 1 from the VMware vCenter inventory, perform the following procedures.

1. Right-click on Host 1 and select Remove from Inventory.



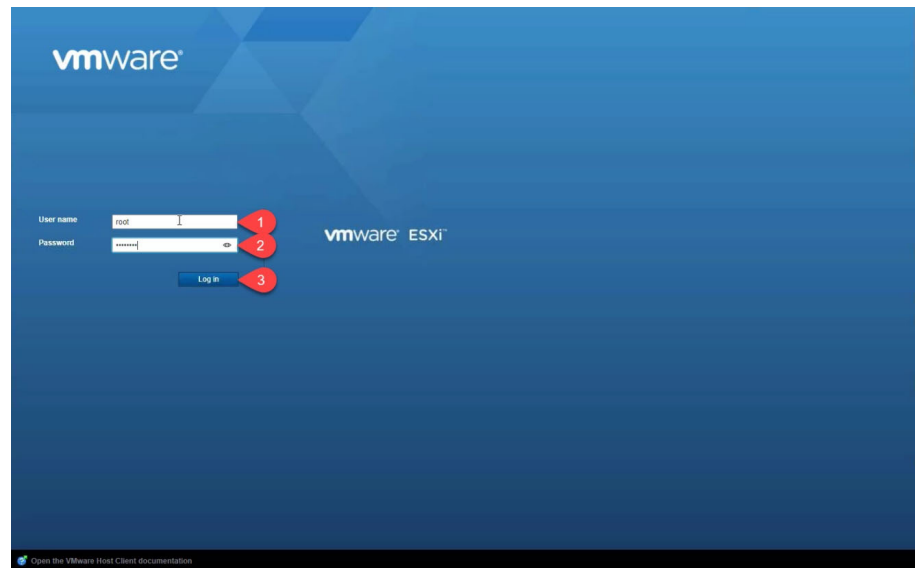
2. A remove host alert is displayed. To continue, select Yes.



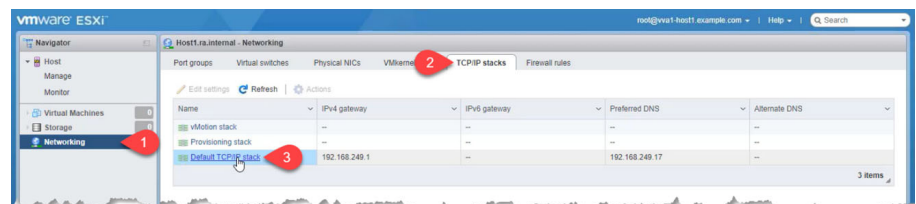
## Reconfigure Host 1

To reconfigure host 1, perform the following procedures.

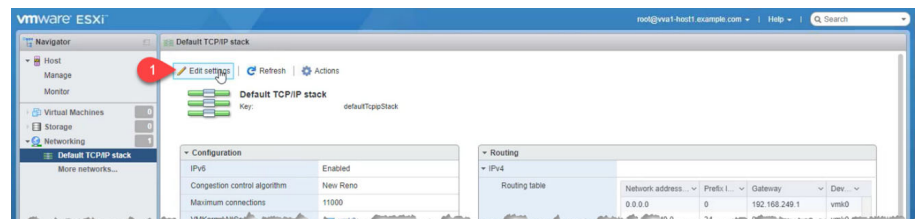
1. Open a new web browser tab or window and navigate to the local management interface for Host 1. The default addresses for the interface are as follows:  
https://host1.ra.internal/ui  
or  
https://192.168.249.14/ui
2. Sign in with the following credentials.  
Username: root  
Password: <system-specific password>
3. Select Login.



4. In the left navigator, select Networking, then select the TCP/IP stacks tab, and then select Default TCP/IP stack.



5. Select Edit settings.



- Change the host name, domain name, and search domains to the desired values, then select Save.

**Edit TCP/IP configuration - Default TCP/IP stack**

Specify how the host should obtain its settings for this TCP/IP stack.

☐ Use DHCP DNS services from the following adapter  
vms3

☒ Manually configure the settings for this TCP/IP stack

Host name: vva1-host1

Domain name: example.com

Primary DNS server: 192.168.249.17

Secondary DNS server:

Search domains: example.com  
One search domain per line

Routing

IPv4 gateway: 192.168.249.1

IPv6 gateway:

Advanced settings

Congestion control algorithm: New Reno

Maximum number of connections: 11000

Save Cancel

- Verify that the DNS configuration for Default TCP/IP stack contains the desired new values.

vmware ESXi

Successfully updated configuration for Default TCP/IP stack

Default TCP/IP stack

Configuration

IPv6: Enabled

Congestion control algorithm: New Reno

Maximum connections: 11000

VMkernel NICs: vms3, vms0, vms1, vms2

DHCP: Disabled

DNS configuration

Host name: vva1-host1

Addresses: 192.168.249.17

Domain name: example.com

Search domains: example.com

Routing

IPv4

| Network address | Prefix L | Gateway       | Dev  |
|-----------------|----------|---------------|------|
| 0.0.0.0         | 0        | 192.168.249.1 | vms0 |
| 192.168.249.0   | 24       | 0.0.0.0       | vms0 |
| 192.168.250.0   | 25       | 0.0.0.0       | vms1 |
| 192.168.250.128 | 25       | 0.0.0.0       | vms3 |
| 192.168.250.64  | 25       | 0.0.0.0       | vms2 |

IPv6

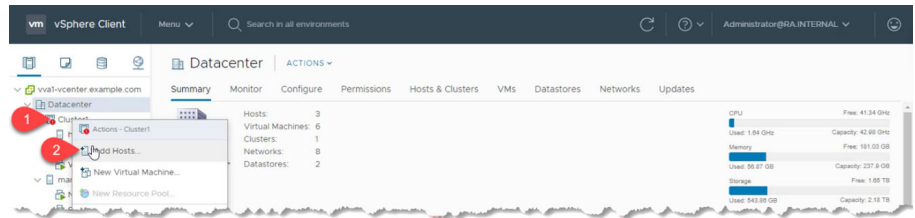
| Network address | Prefix L | Gateway      | Dev  |
|-----------------|----------|--------------|------|
| Default         | 64       | Local subnet | vms0 |
| Default         | 64       | Local subnet | vms3 |
| Default         | 64       | Local subnet | vms1 |

When finished, close the web browser.

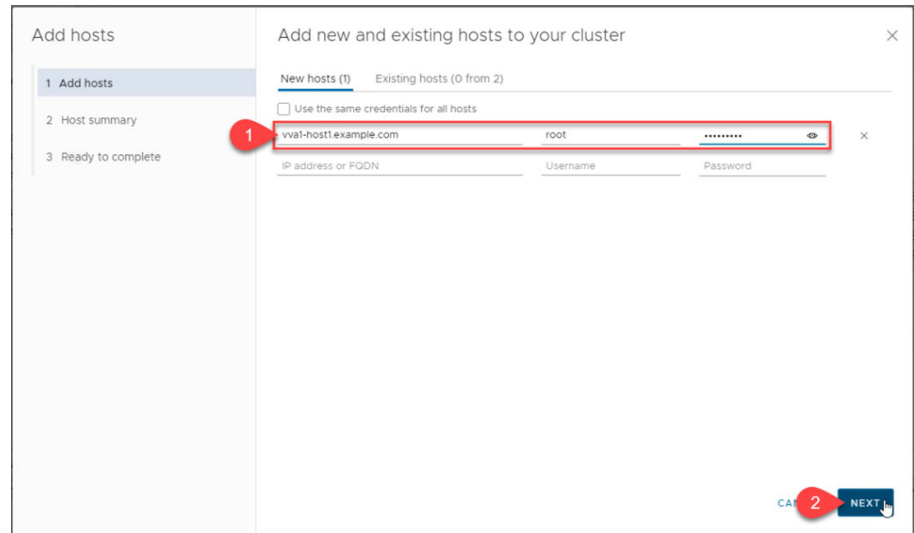
## Add Host 1 Back to VMware vCenter Inventory

To add host 1 back to the VMware vCenter inventory, perform the following procedures.

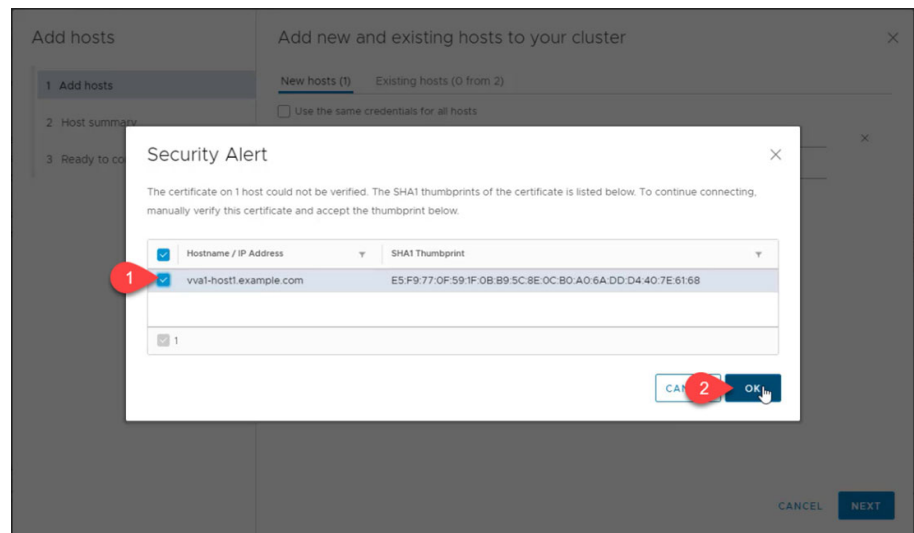
1. In the vSphere Client, right-click Cluster1 and select Add Hosts...



2. Enter the new fully qualified domain name, user name, and password, then select Next.



3. Enter the following credentials.  
Username: root  
Password: <system-specific password>
4. A certificate alert is displayed for host 1. Select Ok.



5. Confirm the host summary information and select Next.

Add hosts

1 Add hosts

2 Host summary

3 Ready to complete

Host summary

| Hostname / IP Address    | ESX Version | Model                     |
|--------------------------|-------------|---------------------------|
| > vva1-host1.example.com | 6.7.0       | Dell Inc. PowerEdge FC640 |

CANCEL

Back

1

NEXT

6. Select Finish

Add hosts

1 Add hosts

2 Host summary

3 Ready to complete

Review and finish

1 new hosts will be connected to vCenter Server and moved to this cluster:  
vva1-host1.example.com

CANCEL

Back

1

FINISH

Wait for all running tasks to complete. It might take several minutes for the system to complete all tasks.

Rename Host 2

To rename Host 2, repeat the procedures that are listed in the [Rename Host 1](#) section.

## Rebalance Virtual Machines across the Cluster

After you rename the cluster hosts, all VMs run on host 1.

If you want to separate applications for primary and secondary VMs, the cluster must be rebalanced manually.

## Remove Obsolete Information from NetSvcs

After you rename the cluster hosts, Rockwell Automation recommends that you remove the original host name entries from the NetSvcs DNS configuration. To do so, perform the following steps.

1. Connect to a terminal session on the NetSvcs VM, either through the VM remote console or through SSH.

Rockwell Automation recommends that you use SSH with an editor such as Microsoft® Visual Studio® Code so you can edit the DNS server configuration files offline and paste changes from the editor into the configuration file.

2. Once connected, edit the ra.conf file with the following command:

```
sudo nano /etc/unbound/local.d/ra.conf
```

```
[sysadmin@vval-netsvcs ~]$ sudo nano /etc/unbound/local.d/ra.conf
```

3. In the editor, remove the old records for forward and reverse entries.
4. If only the host name needs to be changed, remove the old local-zone section records.
5. If you change the domain name, the entire local-zone section for ra.internal can be removed.
6. To save the file, press CTRL-O and then ENTER.
7. To exit the editor, press CTRL-X.
8. With the file updated, enter the following command:

```
sudo systemctl restart unbound
```

It can take several minutes to complete and does not return a confirmation or other information.

9. Once complete, verify the system status by entering the command:

```
systemctl status unbound
```

Look for active (running) status.

```
[sysadmin@vval-netsvcs ~]$ sudo systemctl restart unbound
[sysadmin@vval-netsvcs ~]$ systemctl status unbound
● unbound.service - Unbound recursive Domain Name Server
 Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled; vendor preset: disabled)
 Active: active (running) since Thu 2023-06-22 13:00:42 EDT; 21s ago
 Process: 2622408 ExecStartPre=/usr/sbin/unbound-checkconf (code=exited, status=0/SUCCESS)
 Main PID: 2622567 (unbound)
 Tasks: 4 (limit: 11341)
 Memory: 14.1M
 CGroup: /system.slice/unbound.service
 └─2622567 /usr/sbin/unbound -d
```

## Final ra.conf

Following is an example of the ra.conf after the components have been renamed.

---

```

access-control: 192.168.249.17/24 allow
access-control: 192.168.249.49/25 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.50.194/16 allow
access-control: 169.254.190/16 allow
access-control: 130.151.185.147/22 allow
access-control: 169.254.110.230/16 allow
access-control: 127.0.0.1/8 allow
unblock-lan-zones: yes
local-zone: example.com. transparent
 local-data: vva1-npu.example.com. IN A 192.168.249.13
 local-data-ptr: 192.168.249.13 vva1-npu.example.com
 local-data: vva1-host1.example.com. IN A 192.168.249.14
 local-data-ptr: 192.168.249.14 vva1-host1.example.com
 local-data: vva1-host2.example.com. IN A 192.168.249.15
 local-data-ptr: 192.168.249.15 vva1-host2.example.com
 local-data: vva1-witness.example.com. IN A 192.168.249.16
 local-data-ptr: 192.168.249.16 vva1-witness.example.com
 local-data: vva1-NetSvcs.example.com. IN A 192.168.249.17
 local-data-ptr: 192.168.249.17 vva1-NetSvcs.example.com
 local-data: vva1-vCenter.example.com. IN A 192.168.249.18
 local-data-ptr: 192.168.249.18 vva1-vCenter.example.com
 local-data: vva1-Support-Probe.example.com. IN A
 192.168.249.19
 local-data-ptr: 192.168.249.19 vva1-Support-Probe.example.com
forward-zone:
 name: .
forward-addr: 192.168.249.1

```

---

## Final steps

After you have updated the naming scheme, Rockwell Automation strongly recommends that you perform a controlled system shut down and restart after you follow the procedures that are outlined in chapter 5 of the [VersaVirtual User Manual](#) and the knowledge base [Answer QA45441](#). Performing the procedures that are outlined in these documents helps the VMware vCenter startup properly. Doing so also helps confirm that the newly deployed witness VM is added to the management node auto-start list.



**Notes:**

## A

**Abbreviations** 5  
**About this Publication** 5  
**Active Directory** 5, 45, 46  
     vCenter  
         manage with Active Directory  
         user accounts 45  
**AD** 5, 46  
**Add Host Names to Virtual Network** 17  
**Additional Resources** 7  
**Apply** 82

## B

**Baseboard Management Controller** 5  
**baseline specifications** 6  
     input power 6  
     memory 6  
     mounting options 6  
     network (Ethernet) connection ports 6  
     operating system 6  
     operating temperature range 6  
     processor (CPU) 6  
     storage controllers 6  
     usable storage 6  
**bezel**  
     align 13  
     install 12  
**BMC** 5  
**Boot Optimized Server Storage** 5  
**Boot Optimized Storage Subsystem (BOSS)** 6  
**BOSS** 5, 6  
**bracket**  
     rack mount 12

## C

**certificate thumbprint** 115  
**change the IP address of vCenter** 79  
**Change the IP Address Schemes** 69  
**Change the IPv4 Settings of the Witness Host** 70  
**Change vCenter IP address via Appliance Manager** 79  
**cluster** 63  
     hosts 122  
     rebalance 131  
     vSAN 69  
**cluster hosts**  
     rename 122  
**clusters** 59  
**cold start temperature** 6  
**command**  
     modify the interface 77  
     verify IP address 77  
**command thumbnail** 76

### commands

bring down Ethernet interface 77  
ping 77

### compatibility check

### component

### compute resource

### configuration

IPv4 72

### configuration size

### configure management network

### connect network cables

### Connect the Appliance to the Network

### Connect the Power Cables

### Connecting the Network Cables

### console

DCUI 70

### copper transceiver modules

### core router

## D

### DCUI

ESXi 71

NetSvcs 76

### DCUI console

### deploy vSAN Witness virtual machine

### destination network

### Direct Console User Interface

### disk image

### DN

### DNS

reconfigure records 95  
update NetSvcs settings 78

### Domain Admin

### domain name

### Domain Name System

### domain name system

### Download Center

### Download firmware

### Download Firmware, AOP, EDS, and Other Files

6

## E

### ESXi

DCUI 71

web interface 70

## F

### Features

### final ra.conf

### FQDN

### Fully Qualified Domain Name

### fully qualified domain name

**G**

**Graphical User Interface** 5  
**GUI** 5

**H**

**HA** 5  
**Hard drive** 5  
**Hardware Compatibility List** 5, 49  
**HCL** 5, 49, 51  
    DB 49  
**HD** 5  
**High Availability** 5  
**host**  
    add standalone 118  
    NPU 70, 76, 107  
    Witness 70  
**Host 1** 122  
    rename 122  
**Host 2** 130  
    rename 130  
**host file**  
    local 96  
    update 96

**I**

**identify ports and components** 10  
**identity sources** 45  
    add 45  
**iDRAC** 11, 15  
    ports 11, 15  
    reset IP addresses 74  
    settings 75  
**input power** 6  
**insertion mode** 78  
**install**  
    bezel 12  
**Install the Bezel** 12  
**Install the VersaVirtual Appliance in a Rack** 9  
**install the VersaVirtual Appliance in a rack** 9  
**Install the VersaVirtual in a Rack** 9  
**Integrate the Network** 15, 69  
**Integrated Dell Remote Access Controller** 11, 15  
**interface**  
    default addresses 127  
**IPv4** 72  
    configuration 72

**J**

**JSON** 50  
**JSON file** 50

**L**

**LDAP** 46  
**local hosts file** 96

**M**

**maintenance mode**  
    host1 122  
**maintenance mode** 122  
    enter 122  
**management network** 71  
    configure 71  
**Management VM Network** 82  
**memory** 6  
**mounting options** 6

**N**

**Nano Processing Unit** 10  
**nano processing unit** 66  
**NetBIOS** 47  
**NetSvcs** 97, 131  
    add new name information to DNS  
        server hosted by NetSvcs 97  
    DCUI 76  
    remove obsolete information 131  
    rename 100  
**NetSvcs virtual machine** 76  
**network (Ethernet) connection ports** 6  
**New VLAN Tag** 74  
**NPU** 10, 66  
    host 76  
    reset IP address 72  
**NPU host** 70, 107  
**NTP** 112  
    servers 112

**O**

**operating system** 6  
**operating temperature range** 6  
**OVA** 59, 62  
    file 60  
**OVA file** 62  
**OVA template** 59  
    import 59  
**OVF** 59, 107  
    configuration size 110  
    template 59, 107  
**OVF template** 59, 63, 107  
    deploy 107

**P**

**performing a controlled shut down and startup**  
    133  
**ping** 77  
**ports**  
    iDRAC 11, 15  
**ports and components** 10  
**power cables** 12  
    connect 12  
**processor (CPU)** 6

## R

- ra.conf** 98
  - update 99
- rack mount**
  - bracket 12
- rack-mount VVA** 9
- rebalance cluster** 131
- rebalance virtual machines across cluster** 131
- rebuild virtual objects** 121
- redploy vSAN Witness virtual machine** 104
- remote console** 57
- rename all VersaVirtual Appliance** 95
- rename cluster hosts** 122
- rename Host 1** 122
- rename Host 2** 130
- rename NetSvcs** 100
- rename process** 97
- rename vCenter** 101
- rename VersaVirtual Appliance components** 95
- renaming components**
  - final steps 133
- repair objects** 121
- Reset IP address of NPU** 72
- Restart Nano Processing Unit** 67
- Restart vSAN Cluster** 68
- router**
  - core 15

## S

- Shutdown Nano Processing Unit** 66
- Shutdown vSAN Cluster** 65
- Shutting Down the vSAN Cluster** 69
- SSO** 81
- storage controllers** 6

## U

- unregister and remove existing witness** 104
- Update Access and Trunk Port** 74
- Update IP Addresses on vSAN Hosts** 85
- Update NetSvcs DNS Settings** 78
- Update NetSvcs IP** 76
- usable storage** 6
- Use the Default VLAN/Subnet Address** 15

## V

- vCenter** 50, 69
  - remote console 57
  - rename 101
- vCenter client** 122
- Versa Virtual Appliance** 65
- VersaVirtual Appliance**
  - rename 95
- VersaVirtual Appliance components**
  - rename 95
- virtual local area network** 15, 69

## virtual machine

- NetSvcs 76

## virtual machines

- rebalance 131

## virtual objects

- VLAN 15, 69

- default 15

## VLAN ID

## VM

- compute resource 61
- new virtual machine 52
- rebuild 121
- repair 121

## VMkernel NICs tab

## VMware

- Customer Connect 56
- remote console 56

## VMware ESXi

## vSAN

- 49, 69
- cluster 69
- register new witness 114
- Witness 107

## vSAN Witness

- deploy new virtual machine 107
- redploy virtual machine 104

## vSanDatastore

## vSphere

- web client 45, 48

## VVA

- 49, 65, 95
- identify ports and components 10
- install in rack 9
- rename components 95
- shut down and startup 65

## W

## Windows Active Directory

## Witness

## witness

- register new vSAN 114

## Witness host

## wtiness

- unregister and remove 104

**Notes:**



# Rockwell Automation Support

Use these resources to access support information.

|                                                         |                                                                                                         |                                                                  |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Technical Support Center</b>                         | Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates. | <a href="http://rok.auto/support">rok.auto/support</a>           |
| <b>Local Technical Support Phone Numbers</b>            | Locate the telephone number for your country.                                                           | <a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a> |
| <b>Technical Documentation Center</b>                   | Quickly access and download technical specifications, installation instructions, and user manuals.      | <a href="http://rok.auto/techdocs">rok.auto/techdocs</a>         |
| <b>Literature Library</b>                               | Find installation instructions, manuals, brochures, and technical data publications.                    | <a href="http://rok.auto/literature">rok.auto/literature</a>     |
| <b>Product Compatibility and Download Center (PCDC)</b> | Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.      | <a href="http://rok.auto/pcdc">rok.auto/pcdc</a>                 |

## Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at [rok.auto/docfeedback](http://rok.auto/docfeedback).

## Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, expanding human possibility, and Rockwell Automation are trademarks of Rockwell Automation, Inc.

Cisco is a trademark of Cisco Systems, Inc.

EtherNet/IP is a trademark of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

**rockwellautomation.com** — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication GMSN-UM003A-EN-P - October 2023

Copyright © 2023 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.