

VersaVirtual Appliance

Catalog Numbers 9300-VV1000EC, 9300-VV1000EN, 9300-VV1000RC, 9300-VV1000RN, 9300-VV2000EC, 9300-VV2000EN, 9300-VV2000RC, 9300-VV2000RN



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.

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).

	Preface	
	Summary of Changes	7
	Abbreviations	7
	Additional Resources	8
	Chapter 1	
Features	Overview	9
	Chapter 2	
Install and Start the VersaVirtual Appliance	Install the VersaVirtual Appliance in a Rack	11
	Install the Bezel	12
	Chapter 3	
Integrate the Network	Connect the Appliance to the Network	15
	Use the Default VLAN/Subnet Address	15
	Layer 2 Network Address Translation (L2NAT) and Layer 3 NAT (L3NAT) Methods	16
	Change the IP Address Schemes	17
	Domain Name System (DNS) Forwarding	58
	Chapter 4	
Manage the System	Domain Name System (DNS) Requirements	61
	Forward DNS Requests	62
	Configure the Management Computer	63
	Modify the Hosts File	66
	Install VersaVirtual Licenses	69
	Change the Default Password	75
	Chassis Management Controller (CMC)	75
	Baseboard Management Controller (BMC)	76
	VMware vSphere	77
	Virtual Machines	82
	Configure Active Directory Authentication	85
	Update the Hardware Compatibility List	89
	Add a Distributed Port Group	92
	Add a Virtual Machine	95
	Import an OVA Template	102
	Install VSE Software	105
	Chapter 5	
System Shutdown and Startup	Shut Down the VersaVirtual Appliance	107
	Scripted Shutdown	107
	Manual Shutdown	110
	Start Up the System	116

Notes:

Notes:

Notes:

This manual is a user guide for a Rockwell Automation® VersaVirtual™ Appliance. It provides procedures to the following:

- Install the VersaVirtual Appliance
- Establish VersaVirtual Appliance connections
- Configure the VersaVirtual Appliance
- Start up and shut down the system

Summary of Changes

This manual contains new and updated information as indicated in this table.

Topic	Page
Replaced the graphic with the first bullet point in step 2.	16
Replaced 'Witness' with 'Management' in step 2 in the Change the IPv4 Settings and VLAN ID of the Witness Host subsection.	36
Added second sentence and graphic to step 3 in the Migrate the Kernel Back to vdSwitch0 subsection.	47
Added steps 4...10 to the Migrate the Kernel Back to vdSwitch0 subsection.	47
Added steps 1...3 to the Support subsection.	54
Added step 3 to the Change the Firewall subsection.	57
Replaced 'systemct1' with 'systemctl' in step 10 in the Domain Name System (DNS) Forwarding section.	59
Replaced 'one service and two host management controllers' with 'one Management, one Witness, and two cluster Hosts' in the first sentence of the VMware vSphere section.	77
Replaced 'two host management controllers' with 'two cluster hosts and the Witness host' in step 10 of the VMware vSphere section.	79
Added the Witness host URL address in step 10 of the VMware vSphere section.	79

Abbreviations

The following abbreviations are used in this publication.

Abbr	Meaning	Abbr	Meaning
AD	Active Directory	NAT	Network Address Translation
BMC	Baseboard Management Controller	NM	Network (I/O) Module
CMC	Chassis Management Controller	NTP	Network Time Protocol
DCUI	Direct Console User Interface	OVF	Open Virtualization Format
DNS	Domain Name System	SSH	Secure Shell
FQDN	Fully Qualified Domain Name	SSO	Single Sign-on
GUI	Graphical User Interface	VA	Virtualization Appliance
HA	Host Address	vCPU	Virtual Central Processing Unit
HCL	Hardware Compatibility List	VLAN	Virtual Local Area Network
HDD	Hard Disk Drive	VM	Virtual Machine
HSRP	Hot Standby Router Protocol	VSE	Virtual Support Engineer
LDAP	Lightweight Directory Access Protocol		

Additional Resources

These documents contain more information to related products from Rockwell Automation.

Resource	Description
VersaVirtual Appliance Installation Instructions, publication GMSN-IN001	Provides basic product installation information on the Rockwell Automation VersaVirtual Appliance.
Stratix® Managed Switches User Manual, publication 1783-UM007	Provides information to set up, connect, configure, and troubleshoot Stratix 5410 switches.
Stratix 5950 Security Appliance User Manual, publication 1783-UM010	Provides information to set up, connect, configure, and troubleshoot Stratix 5950 security appliances.
Cisco Firepower® Device Manager, publication Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0	Explains how to configure the Cisco Firepower Threat Defense by using the Firepower Device Manager web-based configuration interface included on Firepower Threat Defense devices.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines to install a Rockwell Automation® industrial system.
Product Certifications website, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at

<https://www.rockwellautomation.com/global/literature-library/overview.page>.

Features

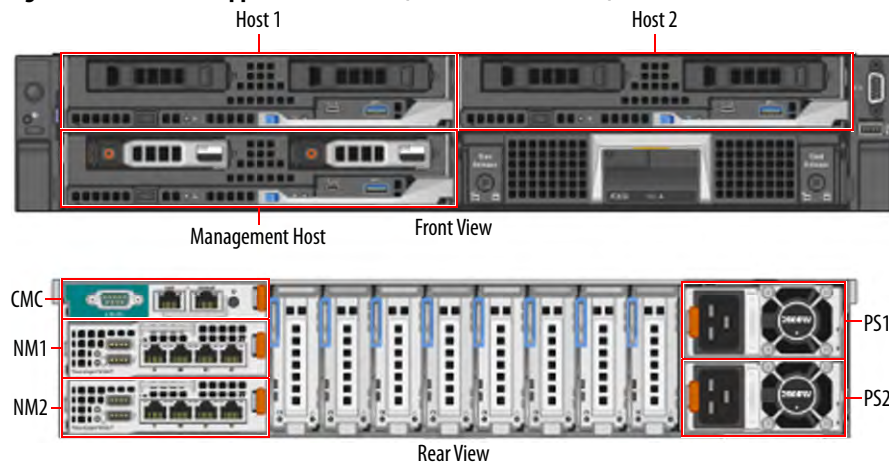
Overview

The Rockwell Automation® VersaVirtual™ Appliance is a hyperconverged (compute, networking, and storage) appliance for entry-level virtualization in a managed environment. The VersaVirtual Appliance comes fully factory-configured with support services to minimize customer on-site configuration. The VersaVirtual Appliance is available in two models, VV1000 and VV2000. The VV1000 is ideal for non-critical production applications, while the VV2000 is ideal for critical production applications.

The following specifications show the difference between the two models.

Attribute	Cat. Nos. 9300-VV1000xx	Cat. Nos. 9300-VV2000xx
No. of hosts	1	2
Processor (CPU)	Intel® Xeon® Silver 4114, 2.2 GHz	
Network (Ethernet) connection ports	2 x 10 Base-T (trunk) 1 x 1000 Base-T (management)	
HDD storage capacity	2 TB	
RAM	96 GB	128 GB
Cooling fan	1	
Operating system software	VMware vSphere® Standard	
Input power	100...240V AC, 50/60 Hz, dual	
Operating temperature range	10...35 °C (50...95 °F)	
Mounting options	Rack	

Figure 1 - VersaVirtual Appliance Overview (VV2000 model shown)



Notes:

Install and Start the VersaVirtual Appliance

Topic	Page
Install the VersaVirtual Appliance in a Rack	11
Install the Bezel	12

The VersaVirtual™ Appliance must be installed in a rack mount. After you install the VersaVirtual Appliance in a rack mount and connect peripherals, you must install the front bezel, which is included.

Install the VersaVirtual Appliance in a Rack

To rack mount the VersaVirtual Appliance, perform the following steps.

- IMPORTANT** Before you install your VersaVirtual Appliance in a rack, perform the following steps:
- Review and follow any safety guidelines that are included in the rack installation instructions.
 - Remove the shipping brackets on the appliance.

1. Install the VersaVirtual Appliance in a rack with the supplied hardware.
2. Connect the CMC and I/O modules to the back of the appliance.



3. Connect the appliance to a power source with the supplied power cord. Secure the power cables with the retention strap.



4. Apply power with the power button on the front of the appliance.

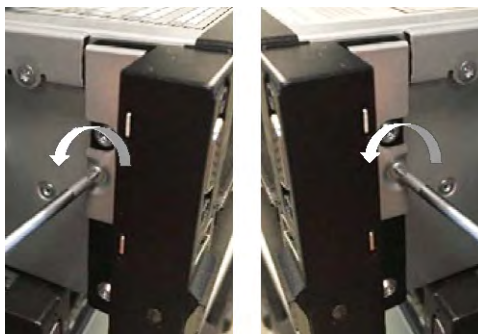


Install the Bezel

To install the bezel on the front of the VersaVirtual Appliance, perform the following steps.

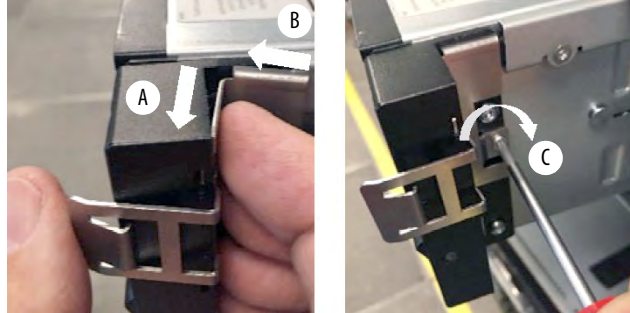
TIP To perform the following steps, you need a T8 Torx screwdriver.

1. Locate and remove the screw on each side and near the front of the appliance.



Place the screws aside to reinstall later.

2. Locate the two tabs that ship with the bezel.
3. Install each tab.
 - a. Slide the two slots of the tab into the corresponding slots (A).
 - b. Rotate the tab so the tab is flush against the appliance frame and the hole of the previously removed screw is visible (B).
 - c. To secure the bezel to the appliance frame, reinstall the screw (C).



4. Align clips on both sides to upper slots on the bezel.
5. Install the bezel.



Notes:

Integrate the Network

Topic	Page
Connect the Appliance to the Network	15
Domain Name System (DNS) Forwarding	58

This chapter details how to integrate your VersaVirtual™ Appliance into your network.

IMPORTANT	<p>To integrate your VersaVirtual Appliance into your network, you need the following connections.</p> <p>For chassis management:</p> <ul style="list-style-type: none"> • An Ethernet connection at least 1 Gb speed <p>For application and hypervisor traffic:</p> <ul style="list-style-type: none"> • Two Ethernet connections at least 1 Gb speed; 10 Gb is recommended
------------------	--

Connect the Appliance to the Network

The following are supported methods for integrating your appliance into the network.

- [Use the Default VLAN/Subnet Address](#)
- [Layer 2 Network Address Translation \(L2NAT\) and Layer 3 NAT \(L3NAT\) Methods](#)
- [Change the IP Address Schemes](#)

Use the Default VLAN/Subnet Address

The default configuration of the VersaVirtual Appliance places the management interfaces on VLAN 3249 with IP subnet [192.168.249.0/24](#).

The ports on the back of each network module (NM) are labeled 9, 10, 11, and 12. Port 12 on each NM must be connected to a 1 GbE or 10 GbE switch port, and must be configured as a trunk. The 1 GbE port on the Chassis Management Controller (CMC) must be connected to an access port configured for VLAN 3249.

To use the default VLAN/subnet address, perform the following steps.

IMPORTANT The equipment for the following two steps is a Cisco® Catalyst® 3850 (model no. WS-C3850-12S-S) core switch and a Cisco Catalyst 3850 server access switch (model no. WS-C3850-24XU-S).

1. Add VLAN 3249 with subnet [192.168.249.0/24](#) to the network.
2. Assign the router address [192.168.249.1](#).
 - Add the following in the core router.

```
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 Network
router(config-if)#exit
router(config)#end
router#wr
```

- Add the following in the server switch.

```
switch#config term
switch#config terminal
switch(config)#vlan 3249
switch(config-vlan)#name VersaVirtual
switch(config)#interface Tel/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 3249
switch(config-if)#interface range Tel/2-3
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan all
switch(config)#end
switch#wr
```

Layer 2 Network Address Translation (L2NAT) and Layer 3 NAT (L3NAT) Methods

L2NAT and L3NAT methods can be used to avoid reconfiguring the default IP and VLAN/subnet addresses in the VersaVirtual Appliance.

Use L2NAT With a Stratix® 5410 Switch

Where the VersaVirtual Appliance is connected to a Stratix 5410 switch, L2NAT can be used.

```
l2nat instance VVA
instance-id 1
permit all
fixup all
outside from host 10.0.0.1 to 192.168.249.1 gateway
inside from range 192.168.249.7 to 10.0.0.42 13

Apply to the uplinks from the 5410 to the rest of the network.

Interface range Te1/27-28
L2nat VVA 3249
```

For additional information about the Stratix 5410 switch, refer to the NAT section of publication [1783-UM007](#), Stratix Managed Switches User Manual.

Use L3NAT With a Stratix 5950 Switch or Cisco Firepower® Device Manager

If there is a Stratix 5950 switch upstream of the VersaVirtual Appliance, then refer to publication [1783-UM010](#), Stratix 5950 Security Appliance User Manual, for L3NAT configuration.

If there is a Cisco Firepower Device Manager switch upstream of the appliance, then refer to Chapter 7, Network Address Translation (NAT), of the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0](#), for L3NAT configuration.

Change the IP Address Schemes



ATTENTION: Changes to the default VLAN or management IP addresses are technically involving and risk rendering part or all the VersaVirtual Appliance non-functional.

Rockwell Automation recommends that the following IP address changes be performed by either an authorized service provider or Rockwell Automation field labor.

This section instructs how to change the IP address scheme for VersaVirtual Appliance. It modifies the IP address, subnet mask, default gateway and, where applicable, VLAN configurations.

IMPORTANT To complete the following steps, vcenter.ra.internal must be resolvable to the current IP address of the VMware vCenter Server® at each step of the process. The easiest way to do so is to modify the hosts file, which is explained in [Modify the Hosts File on page 66](#).

Identify a New VLAN (if necessary)

If you would like to change the VLAN ID from 3249, you must identify and document this VLAN.

Change the Switch Interfaces

Verify that you have administrator access to the switch into which the VersaVirtual Appliance is plugged. If VLANs are being changed, they must be changed on the switch interface.

The following list is the 13 default IP addresses for the appliance.

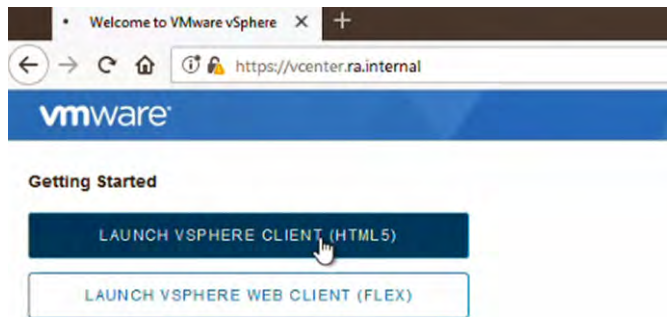
192.168.249.7	nm1.ra.internal	nm1	#FN410T	Network I/O Module
192.168.249.8	nm2.ra.internal	nm2	#FN410T	Network I/O Module
192.168.249.9	cmc.ra.internal	cmc	#FX2	Chassis Management Controller
192.168.249.10	management-bmc.ra.internal	management-bmc	#FC640	Service Baseboard Management Controller
192.168.249.11	host1-bmc.ra.internal	host1-bmc	#FC640	Host 1 Baseboard Management Controller
192.168.249.12	host2-bmc.ra.internal	host2-bmc	#FC640	Host 2 Baseboard Management Controller

192.168.249.13	management.ra.internal	management	#FC640	Service Host vSphere Management
192.168.249.14	host1.ra.internal	host1	#FC640	Host 1 vSphere Management
192.168.249.15	host2.ra.internal	host2	#FC640	Host 2 vSphere Management
192.168.249.16	witness.ra.internal	witness	#VM	vSAN Witness Virtual Appliance
192.168.249.17	netsvcs.ra.internal	netsvcs	#VM	Network Services Virtual Appliance
192.168.249.18	vCenter.ra.internal	vCenter	#VM	vCenter Server Virtual Appliance
192.168.249.19	support.ra.internal	support	#VM	Remote Support Virtual Appliance

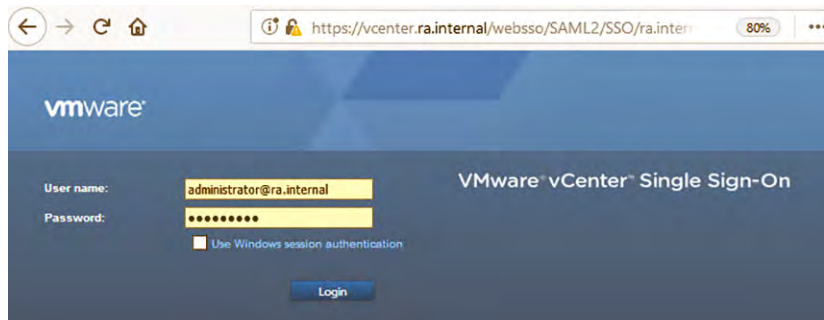
Put the vSAN Hosts in Maintenance Mode

To put the vSAN hosts in maintenance mode, perform the following steps.

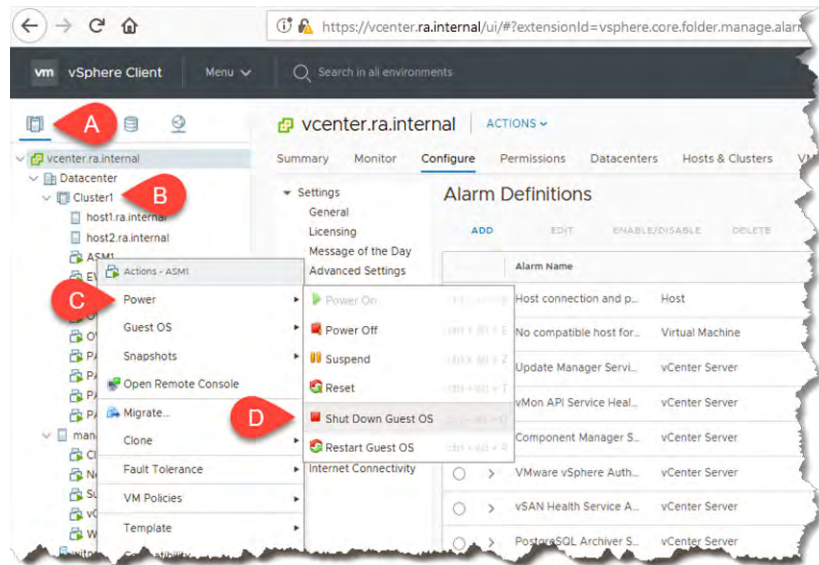
1. Access the following VMware® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).



3. Log into the VMware® vCenter® as administrator@ra.internal with the system-wide password.



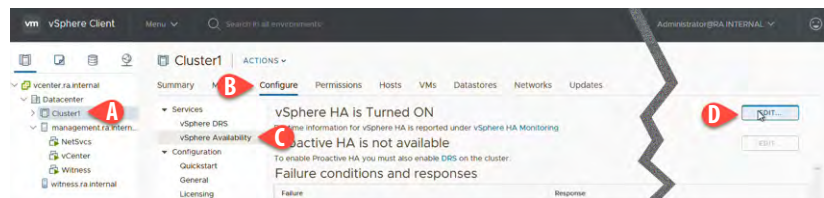
4. Navigate to the Hosts and Clusters view (A).
Expand Cluster1 (B), and shut down any virtual machines on the vSAN cluster (C and D).



5. When prompted, click Yes to confirm Guest Shut Down.



6. On the main Navigation pane, highlight Cluster1 (A).
7. On the Cluster 1 pane, click the Configure tab (B).
8. From the Services pull-down menu, select vSphere Availability (C).
9. Click the Edit button across from vSphere HA is Turned ON (D).
10. Click the Edit button across from vSphere HA is Turned ON (D).

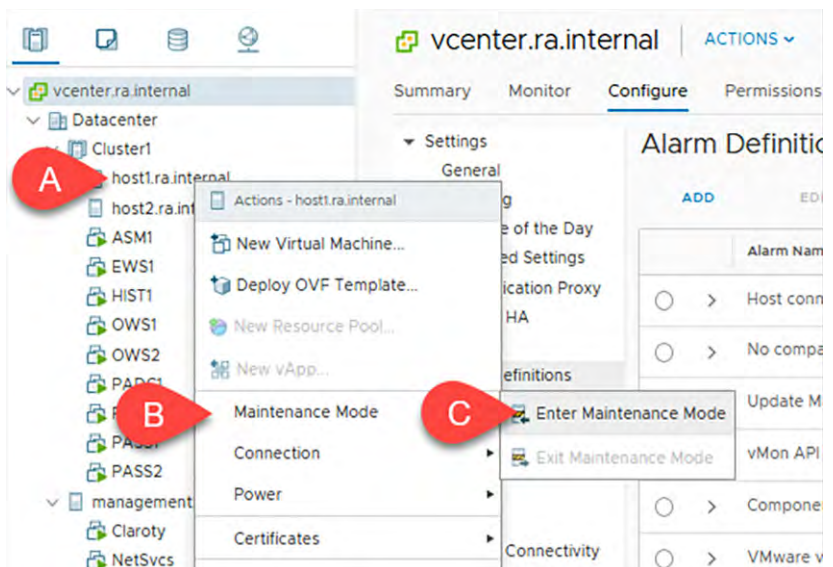


- On Edit Cluster Settings, disable vSphere HA (E).



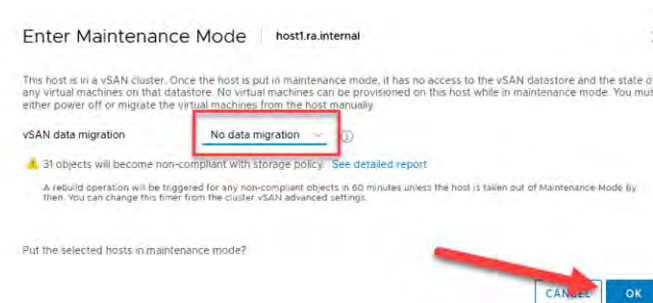
Click OK (F).

- Right-click on host1.ra.internal (A).
Select Maintenance mode (B) > Enter Maintenance Mode (C).

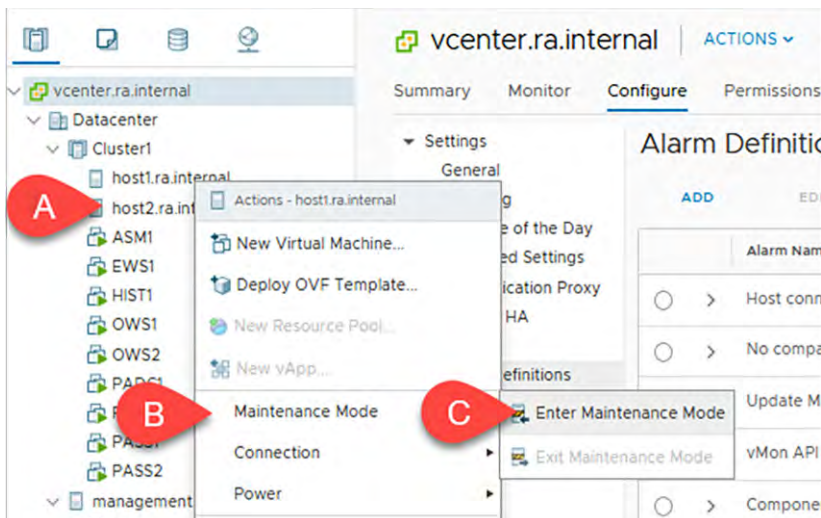


- On Enter Maintenance Mode, select no data migration from the vSAN data migration pull-down menu.

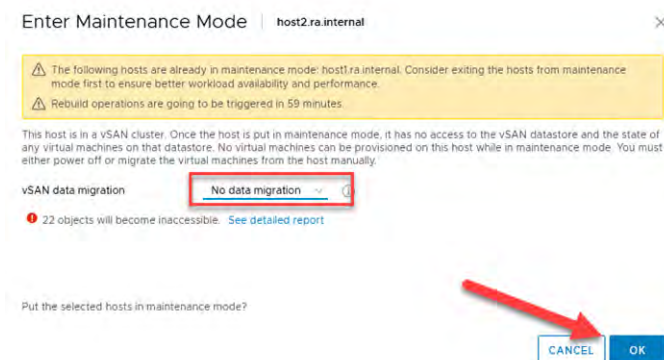
Click OK.



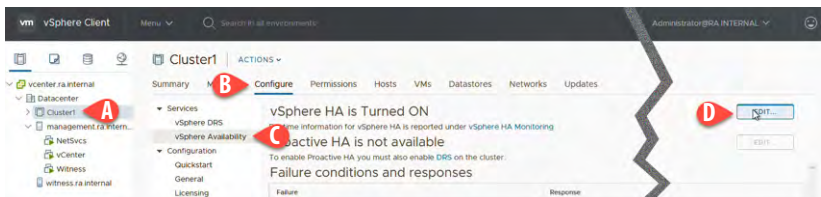
14. Right-click on host2.ra.internal (A).
Select Maintenance mode (B) > Enter Maintenance Mode (C).



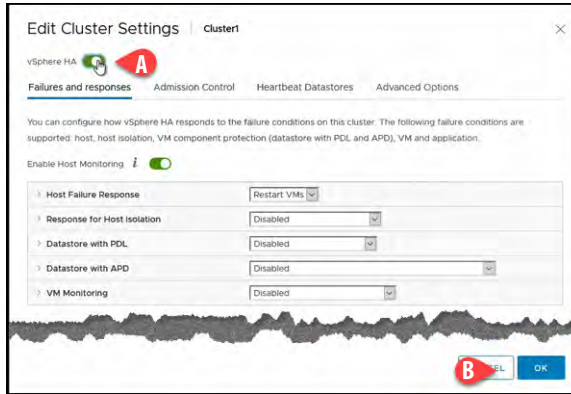
15. On Enter Maintenance Mode, select no data migration from the vSAN data migration pull-down menu.
Click OK.



16. On the main Navigation pane, highlight Cluster1 (A).
17. On the Cluster 1 pane, click the Configure tab (B).
18. From the Services pull-down menu, select vSphere Availability (C).
19. Click the Edit button across from vSphere HA is Turned ON (D).



- 20. On Edit Cluster Settings, turn on vSphere HA (A).



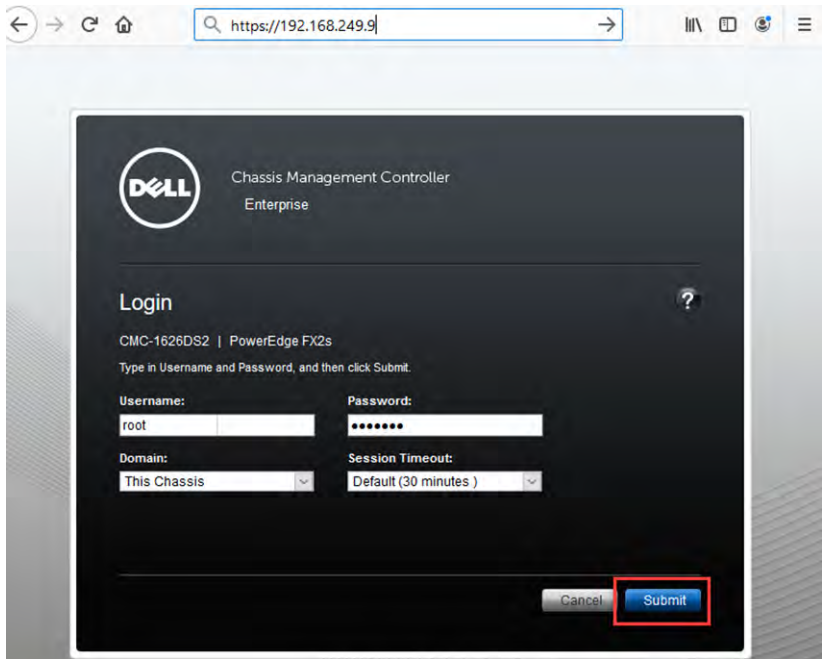
Click OK (B).

Modify the Chassis IPv4 Settings

Chassis Management Controller

- 1. Access the Chassis Management Controller (CMC) through a browser at <https://192.168.249.9>.

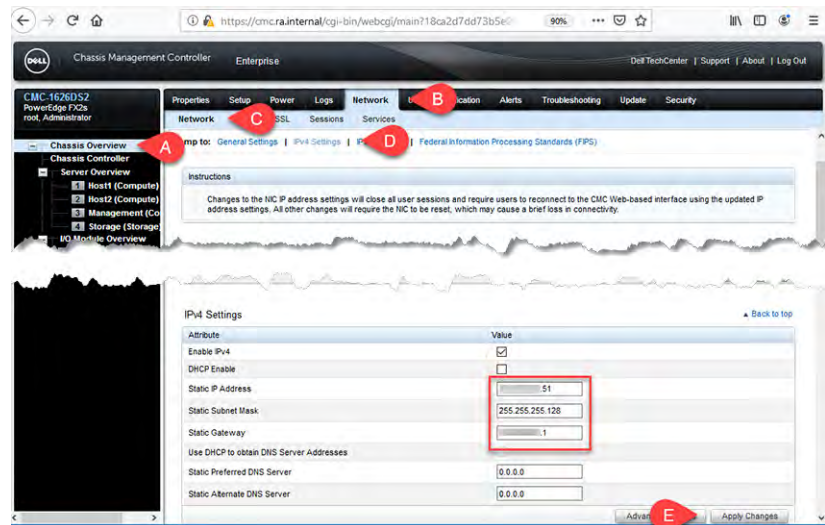
Log in as root with the system-wide password, and click Submit.



2. Navigate to Chassis Overview (A) > Network (B and C) > IPv4 Settings (D).

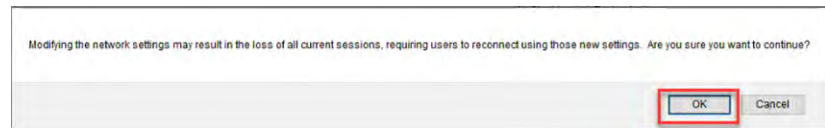
In the Static IP address field, enter the desired Static IP Address, Static Subnet Mask, and Static Gateway.

Click Apply Changes (E).

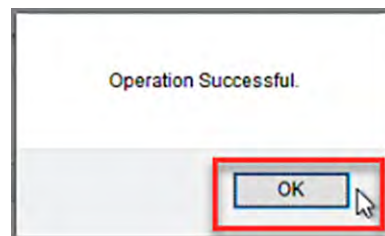


You subsequently lose connectivity to the CMC.

3. Click OK to the current sessions warning.



4. Click OK to the Operation Successful window.



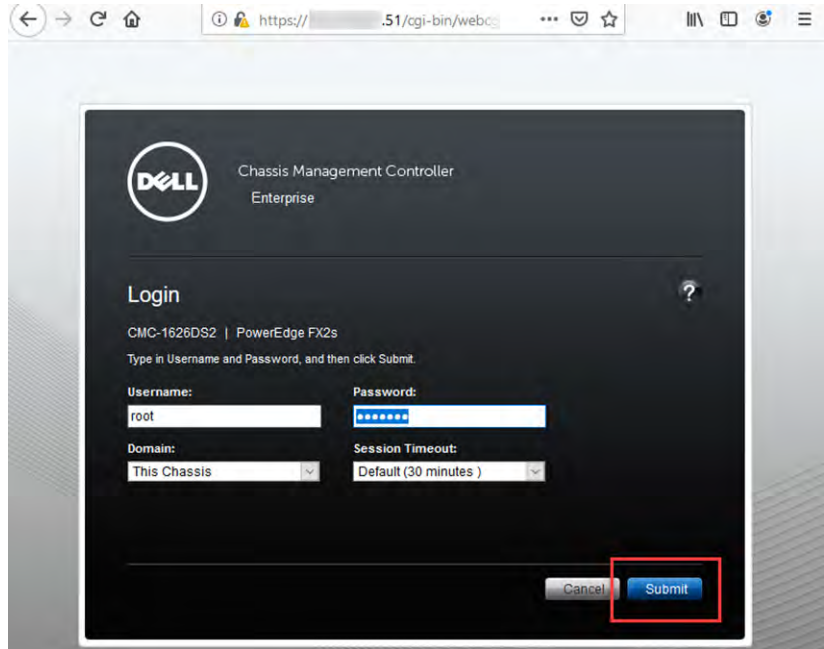
If you changed the VLAN, you must then log into the switch to which the CMC is plugged. To access the desired VLAN, configure the interface to where the CMC is plugged in.

The following is an example of a configuration for a Cisco switch.

```
config t
int te2/0/19
switchport access vlan 801
```

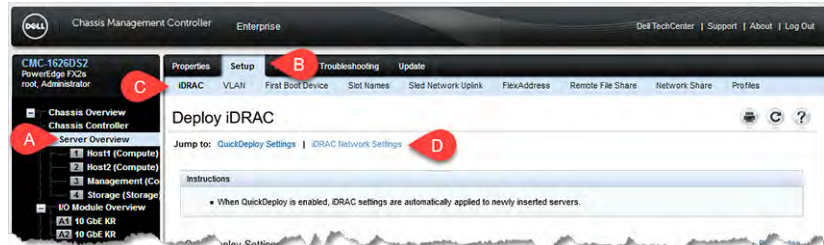
```
3253 VLAN3253 active
US-FAC3-DS-01#config t
Enter configuration commands, one per line. End with CNTL/Z.
US-FAC3-DS-01(config)#int te2/0/19
US-FAC3-DS-01(config-if)#switchport access vlan 801
US-FAC3-DS-01(config-if)#
```

5. In a browser, access the CMC with the new IP address.
Log in as root with the system-wide password, and click Submit.

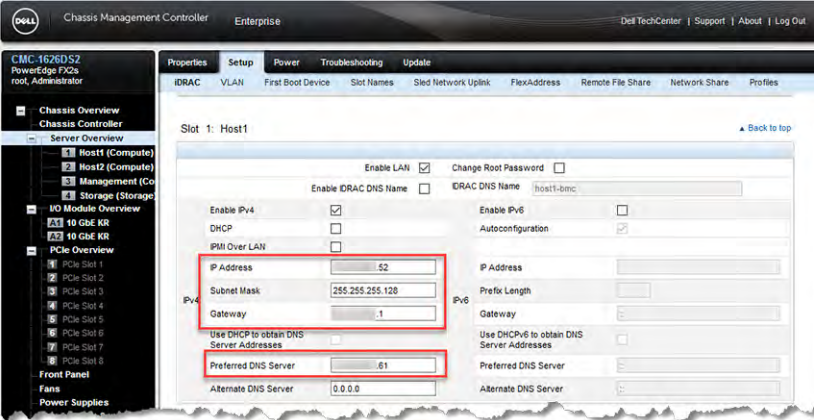


Baseboard Management Controllers

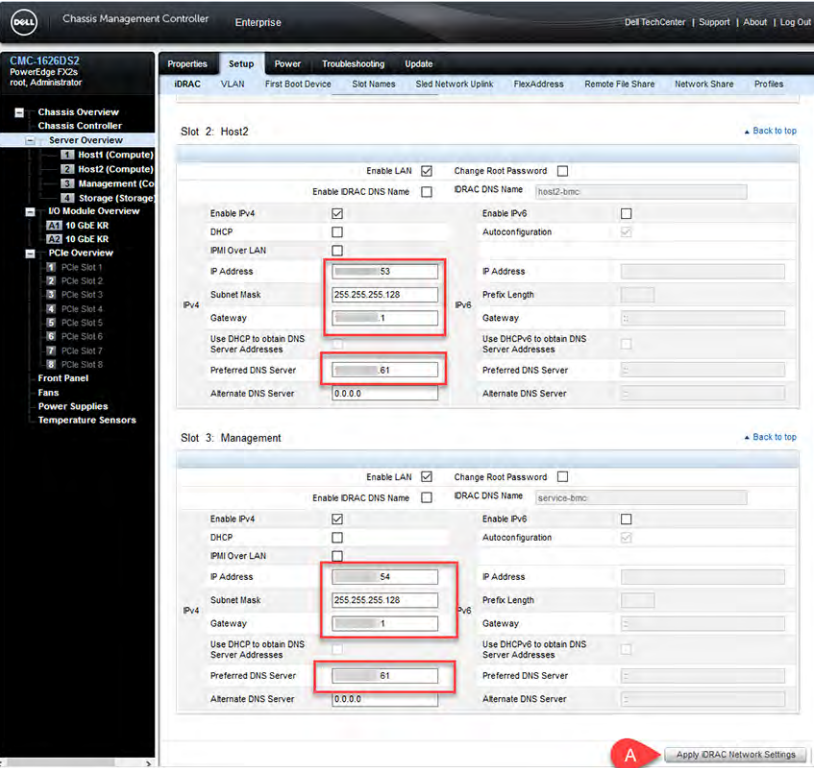
1. If you are not already there, access the Chassis Management Controller (CMC) through a browser.
Log in as root with the system-wide password, and click Submit.
2. Once inside the CMC, navigate to Server Overview (A) > Setup (B) > iDRAC (C) > iDRAC Network Settings (D).



- 3. At Slot 1: Host1, reconfigure the desired IP Address, Subnet Mask and Gateway and Preferred DNS Server (DNS becomes the new IP address of the NetSvcs virtual machine).



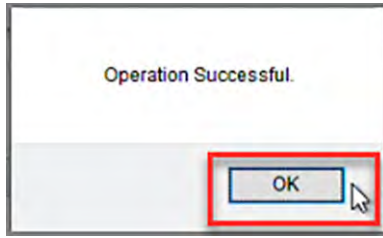
- 4. Scroll down and modify the IP Address, Subnet Mask, Gateway, and Preferred DNS server for Slot 2: Host2 and Slot 3: Management. Click Apply iDRAC Network Settings (A).



- 5. At the warning, click OK.



- Click OK to the Operation Successful window.



Network Modules

- If you are not already there, access the Chassis Management Controller (CMC) through a browser.
Log in as root with the system-wide password, and click Submit.
- Once inside the CMC, navigate to I/O Module Overview (A) > Setup (B) > Deploy (C).

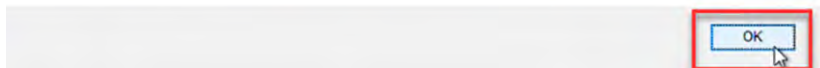
Under Configure I/O Module Network Settings > Slot A1 change the IPv4 settings to the desired IP address, Subnet Mask, and Gateway.

Click Apply (D).



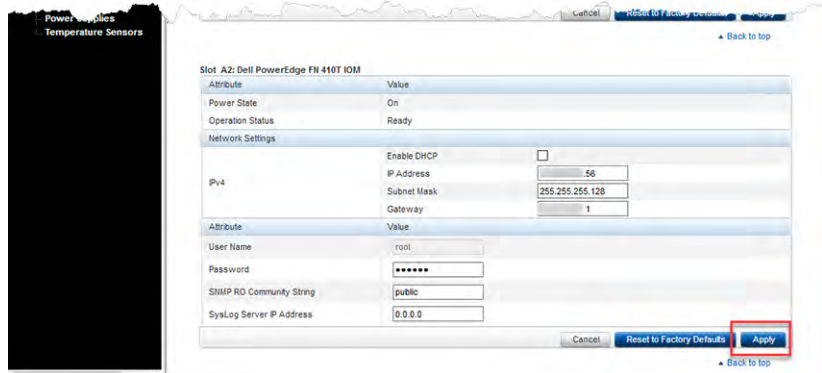
- At the operation status, click OK.

The requested operation has started. The operation will take some time to complete, failures can be viewed in the CMC Log.



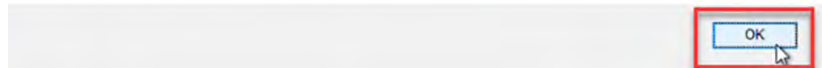
TIP The IPv4 configuration reverts to the old settings. Changes are not reflected immediately.

- Under Configure I/O Module Network Settings Slot A2, change the IPv4 settings to the desired IP address, Subnet Mask, and Gateway. Click Apply.

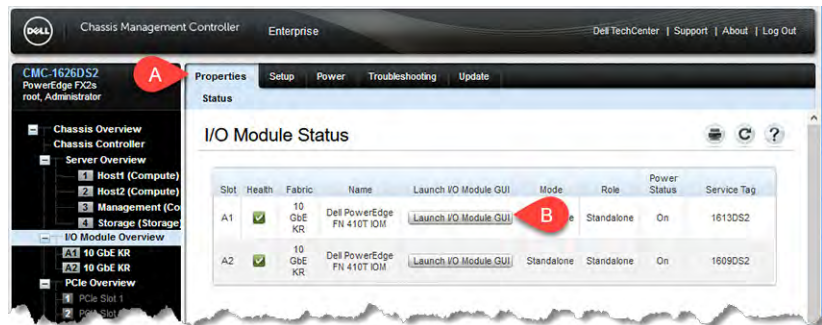


- At the operation status, click OK.

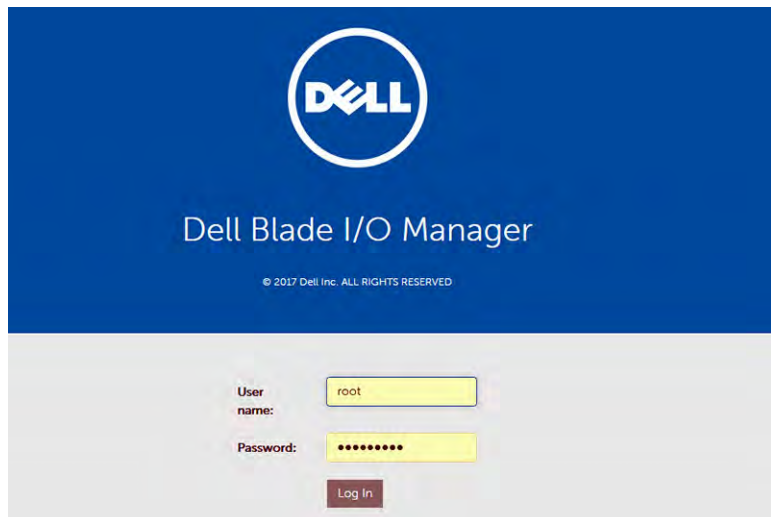
The requested operation has started. The operation will take some time to complete, failures can be viewed in the CMC Log.



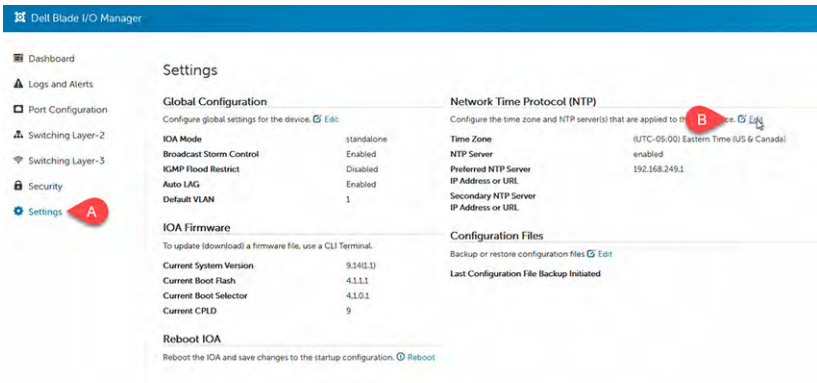
- Navigate to the Properties tab of the I/O Module Overview (A).
For Slot A1, click Launch I/O Module GUI (B).



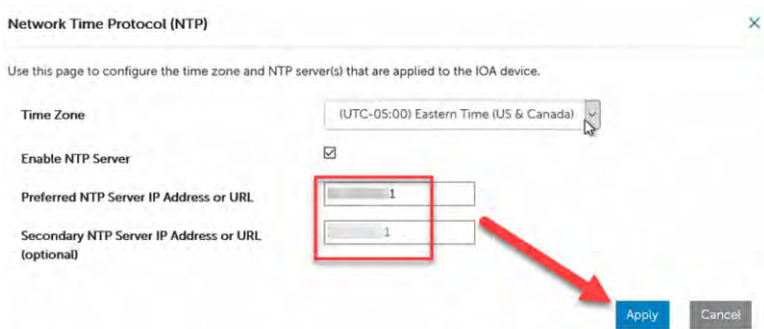
- On the Dell Blade I/O Manager, log in as root with the system-wide password.



8. Navigate to Settings (A) and click Edit (B).



9. On Network Time Protocol, change the Preferred and Secondary NTP servers to the desired IP addresses (usually the gateway or .1).
Click Apply.



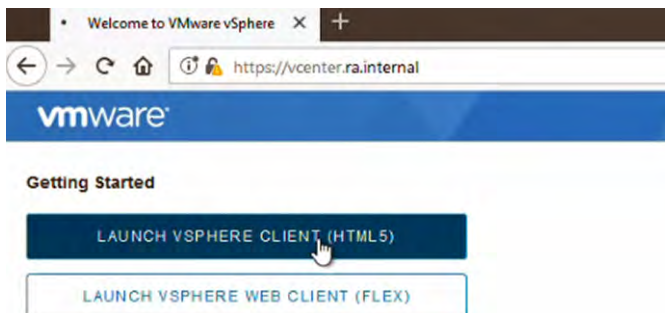
10. For I/O module 2, repeat [step 2](#)...[step 8](#).

Modify the Host IP Addresses

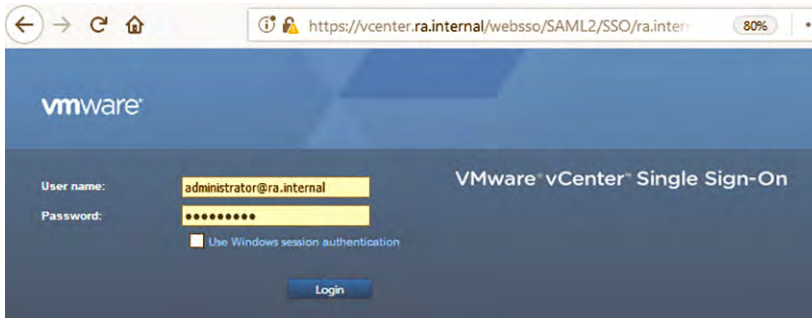
Migrate the Kernels of the vSAN ESXi hosts

To change the VLAN ID on the two vSAN hosts (host1 and host2), the VMKernel0 must be migrated from the Distributed Switch to the Standard switch. Otherwise the VLAN ID appears dimmed on the host. This is accomplished through vCenter.

1. Access the VMware® vSphere® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).

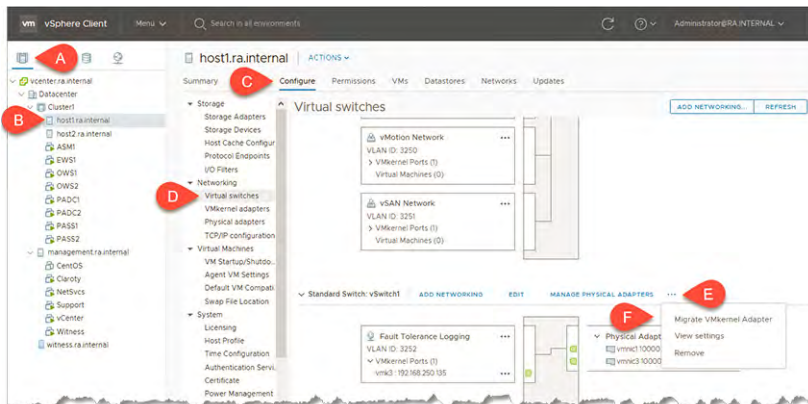


- Log into the VMware® vCenter® as administrator@ra.internal with the system-wide password.

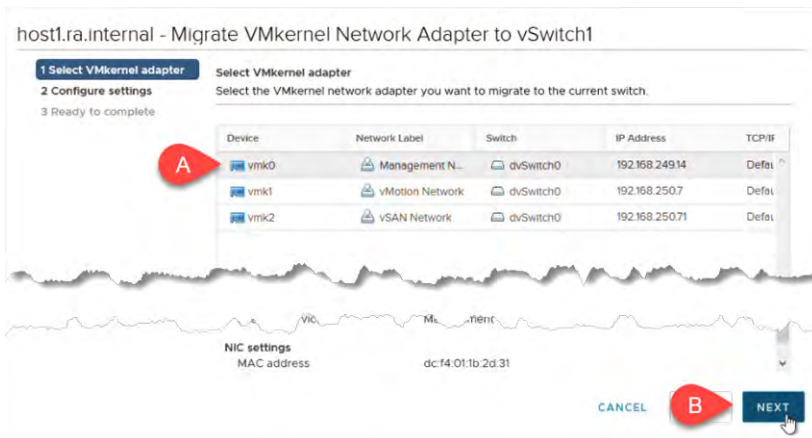


- Navigate to the Hosts and Clusters tab (A).
Select host1.ra.internal (B) > Configure (C) > Networking > Virtual Switches (D).

Scroll down to the Standard Switch: vSwitch1 and click the ellipsis (E) next to Manage Physical Adapters. Select Migrate VMkernel Adapter.



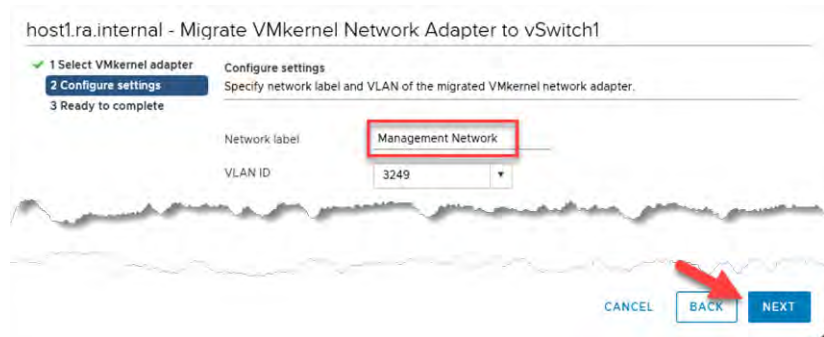
- Select VMkernel adapter vmk0 (A) and click Next (B).



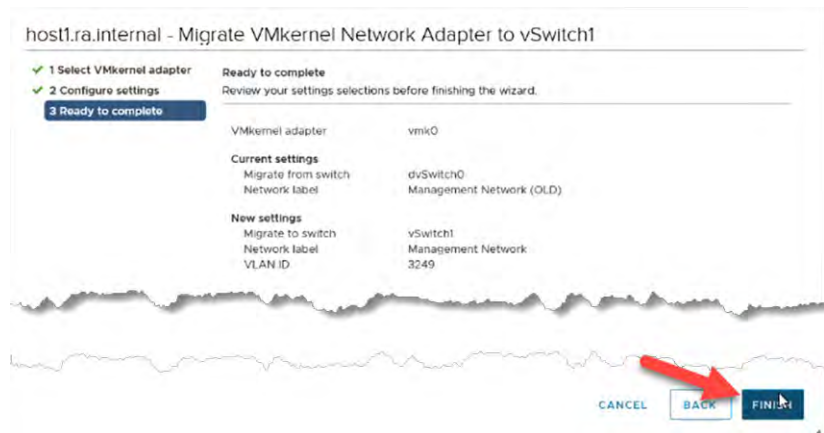
- Name the Network Label “Management Network”.

IMPORTANT Don't change the VLAN ID yet.

Click Next.



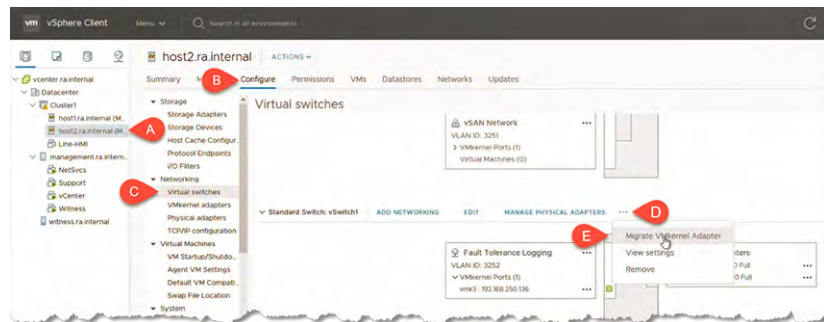
7. Review your settings and click Finish.



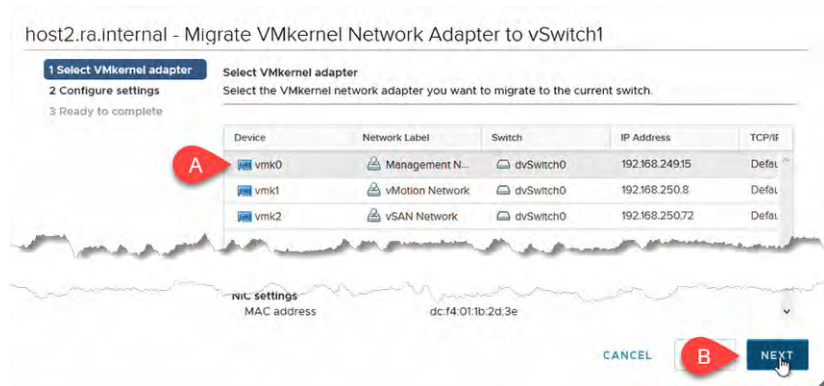
8. Repeat the process for Host2.

Select host2.ra.internal (A) > Configure (B) > Networking >> Virtual Switches (C).

Scroll down to the Standard Switch: vSwitch1 and click the ellipsis (D) next to Manage Physical Adapters. Select Migrate VMkernel Adapter (E).



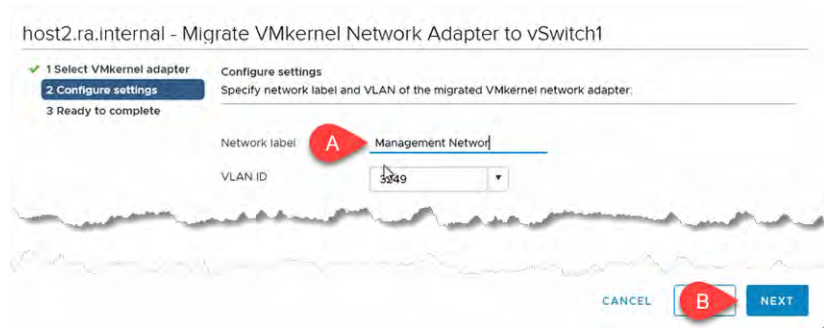
9. Select VMkernel adapter vmk0 (A) and click Next (B).



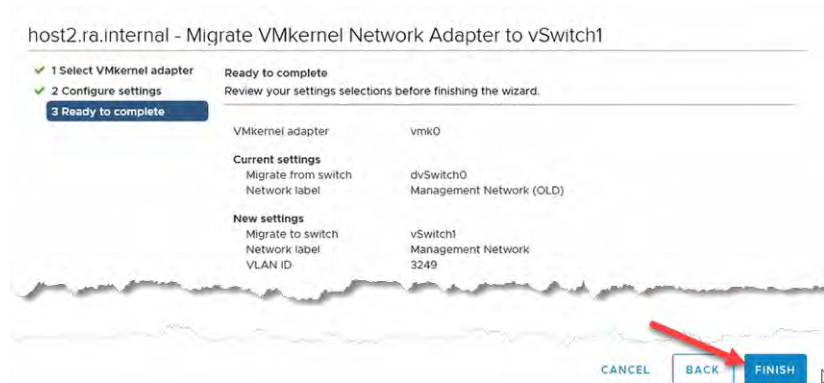
10. Name the Network Label "Management Network" (A).

IMPORTANT Don't change the VLAN ID yet.

Click Next (B).

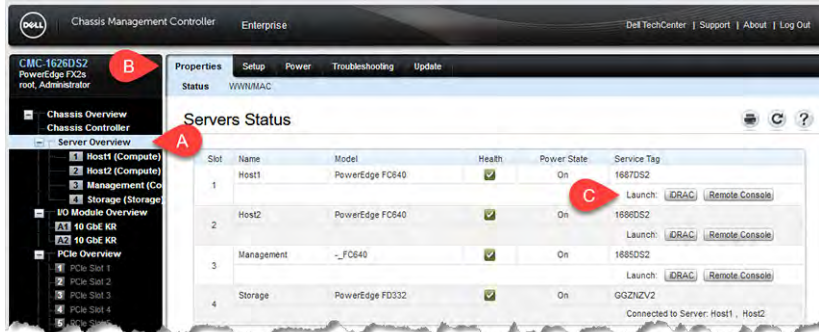


11. Review your settings and click Finish.



Change IP Settings of the ESXi Hosts

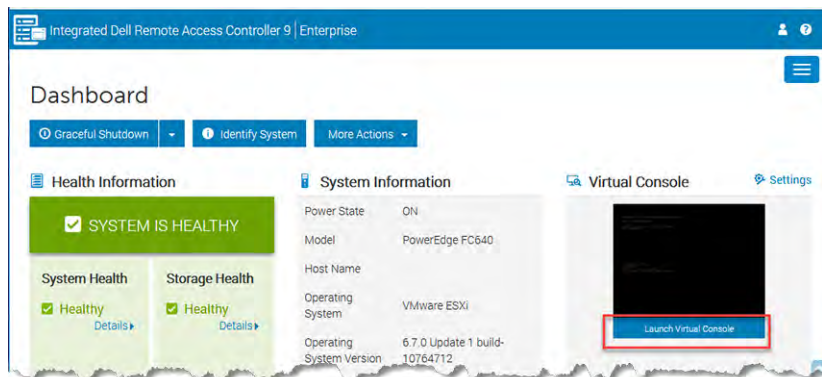
1. Switch to the CMC, navigate to Server Overview (A) > Properties (B). On Servers Status, click Launch: iDRAC (C) for Host1.



The Remote Access Controller opens in a separate tabbed browser.

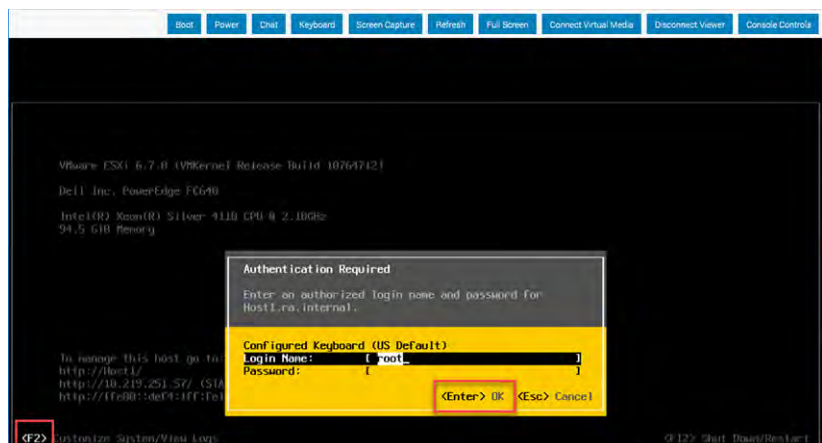
TIP If prompted, disable your popup blocker.

2. Click Launch Virtual Console.



3. Click inside the console and press the F2 key, which prompts for credentials.

Log in with root and system password, and then press Enter.

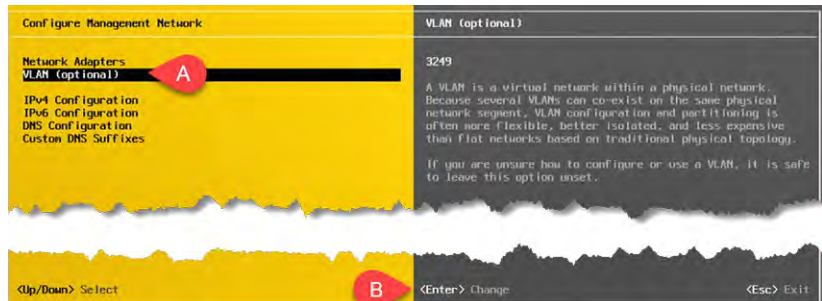


- In the ESXi Direct Console User Interface (DCUI), navigate to Configure Management Network (A) and press Enter (B).

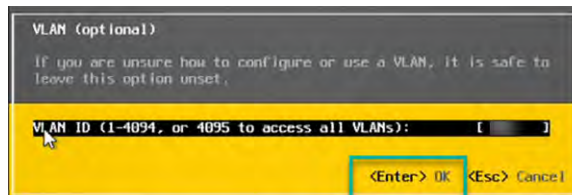
TIP Your mouse does not work in the ESXi console. You must navigate entirely with your keyboard.



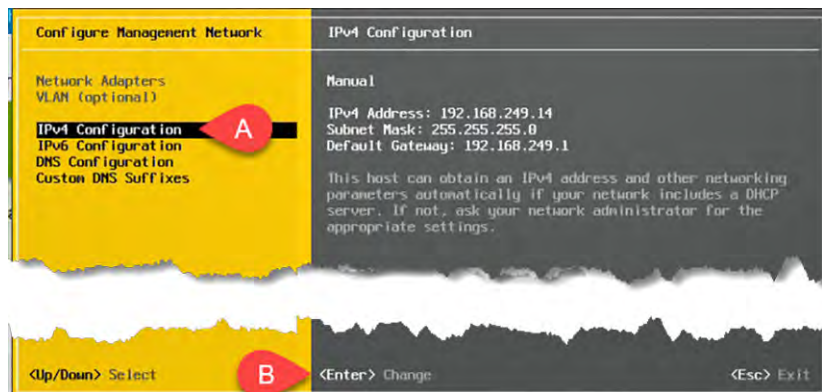
- Select VLAN (optional) (A) and press Enter (B).



- Replace VLAN ID 3249 with the desired VLAN ID and press Enter.

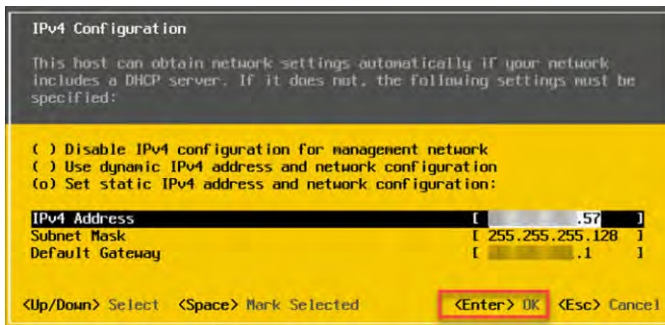


- Select IPv4 Configuration (A) and press Enter (B).

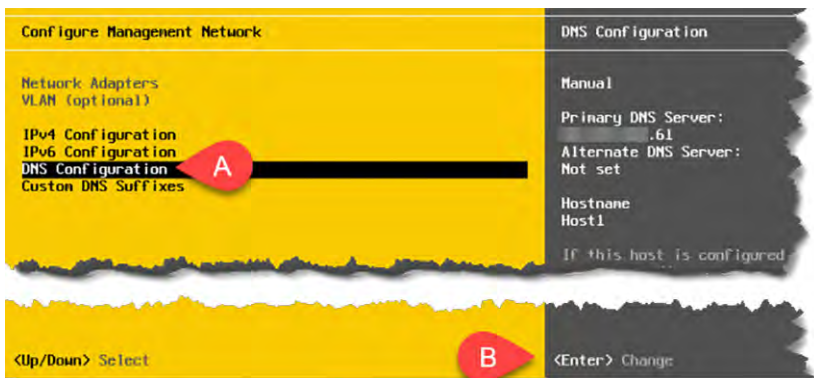


8. With the Up and Down arrow keys, change the IPv4 settings to the desired configuration.

Press Enter when complete.

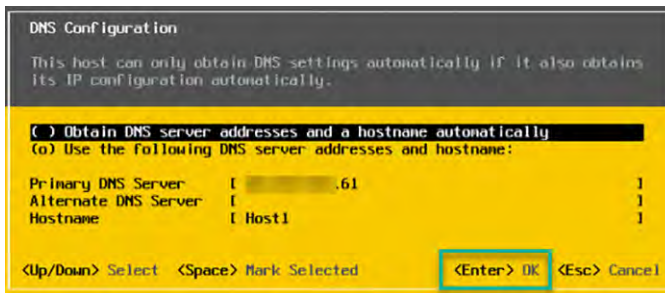


9. Select DNS configuration (A) and press Enter (B).

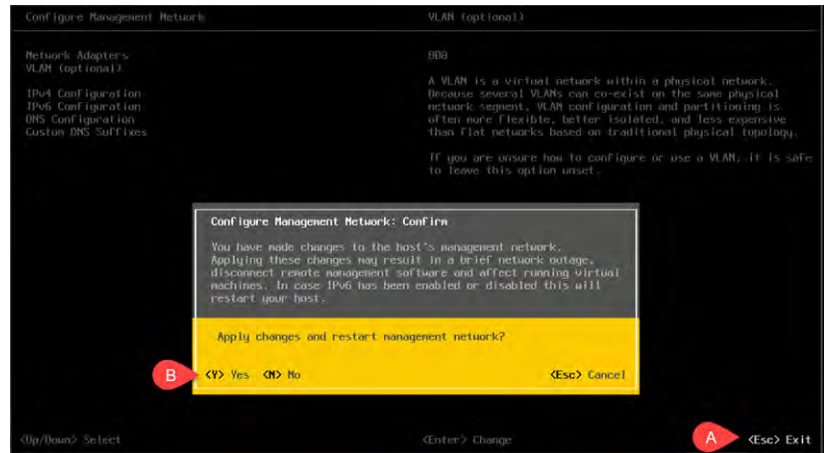


10. Enter the new IP address of the NetSvcs (DNS).

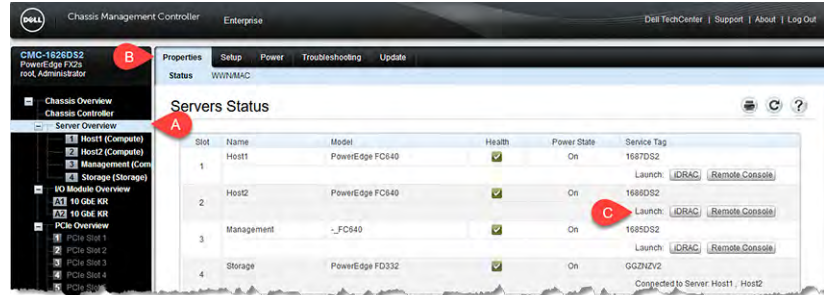
When completed, press Enter.



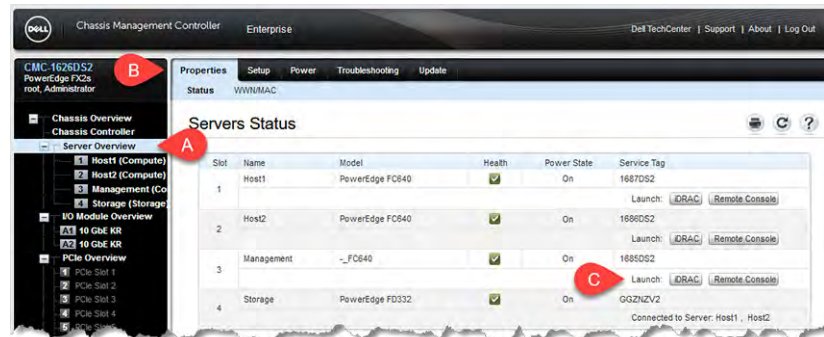
11. To exit, press the Esc key (A) and then press Y (B) to confirm your changes.



12. Switch to the CMC, navigate to Server Overview (A) > Properties (B). On Servers Status, click Launch: iDRAC (C) for Host2.



13. Starting on [page 32](#), repeat [step 2](#)... [step 11](#) for Host2.
14. Switch to the CMC, navigate to Server Overview (A) > Properties (B). On Servers Status, click Launch: iDRAC (C) for Management.



15. Starting on [page 32](#), repeat [step 2](#)... [step 11](#) for Management.

IMPORTANT

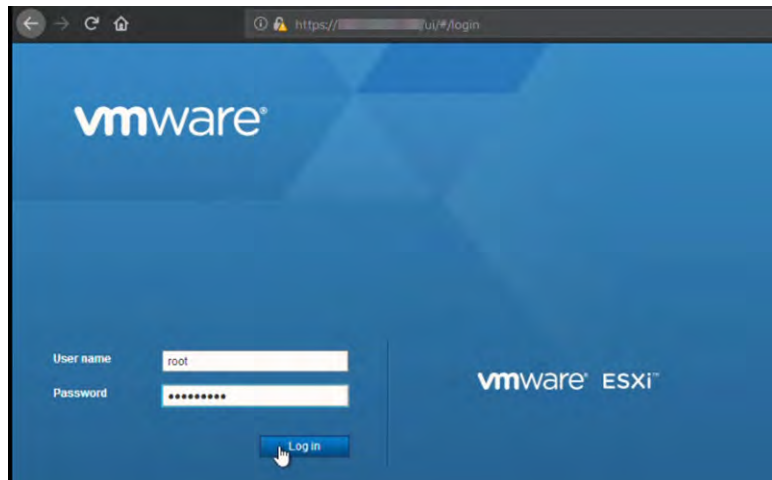
Because the Management host uses a Standard vSwitch, it is not necessary to access vCenter.

Change the IPv4 Settings and VLAN ID of the Witness Host

Because the Witness host is nested, the DCUI console can be accessed through the ESXi web interface.

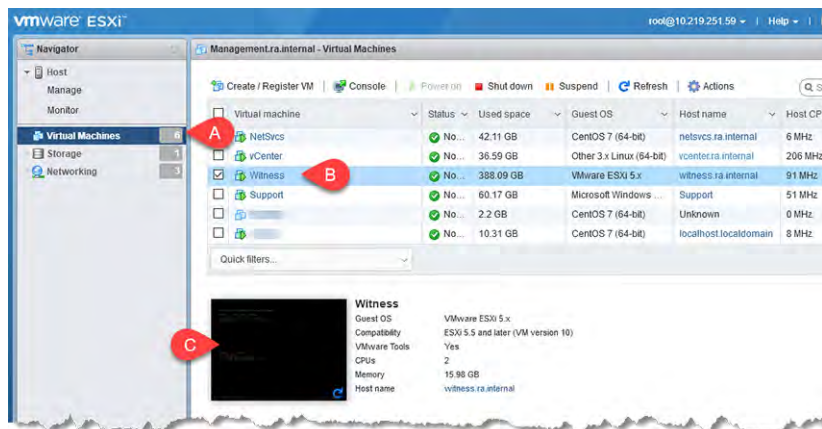
1. Open a browser and navigate to the new IP address of the Management host.

Log in with root and the system-wide password.



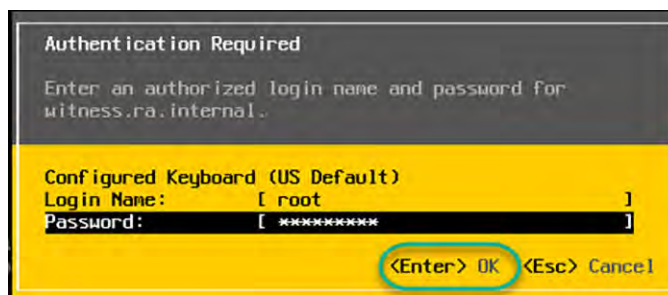
2. In the Management host, navigate to Virtual Machines (A) and select Witness (B).

Click the thumbnail (C) to open the Witness browser console.



3. When the console opens, press the F2 key.

Log in with root and the system password, and then press Enter.

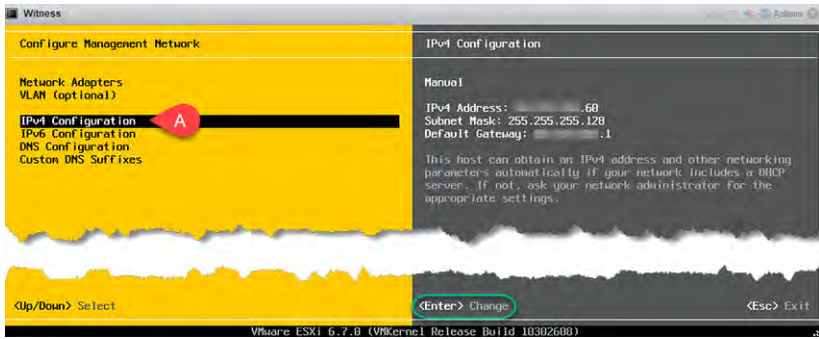


- In the ESXi DCUI, navigate to Configure Management Network (A) and press Enter (B).

TIP Your mouse does not work in the ESXi console. You must navigate entirely with your keyboard.

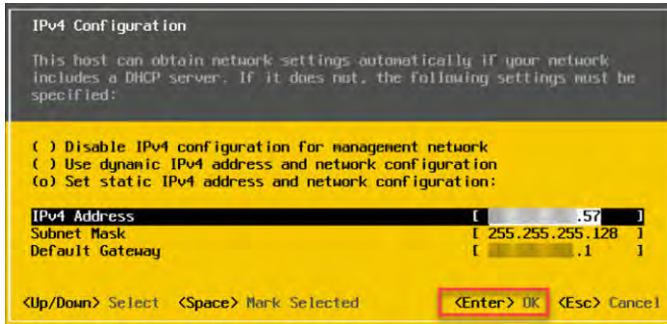


- Select IPv4 Configuration, and press Enter.

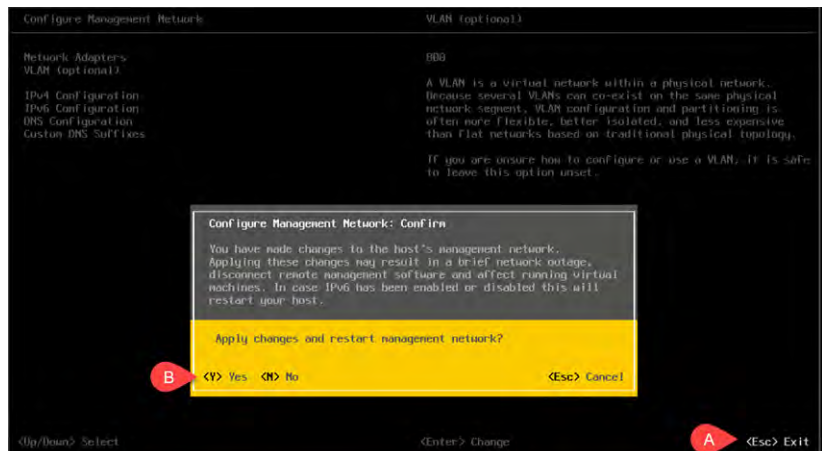


- With the Up and Down arrow keys, change the IPv4 settings to the desired configuration.

When completed, press Enter.



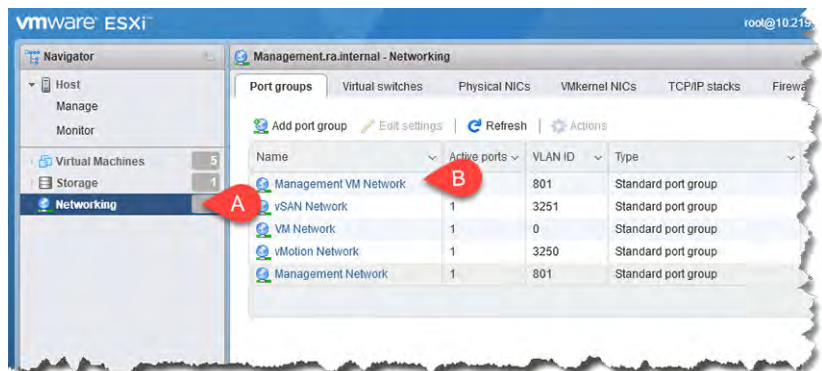
- To exit, press the Esc key (A) and then press Y (B) to confirm your changes.



- Close the Web Console.

You must change the VLAN ID of the Witness host in the ESXi Web GUI.

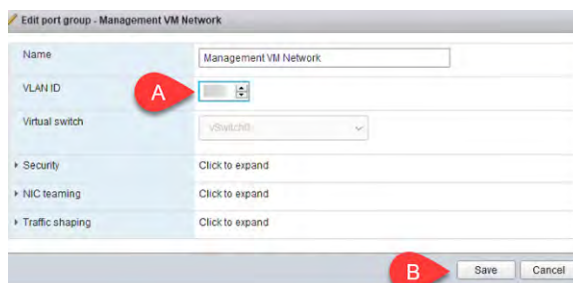
- Navigate to Networking (A) and select Management VM Network (B).



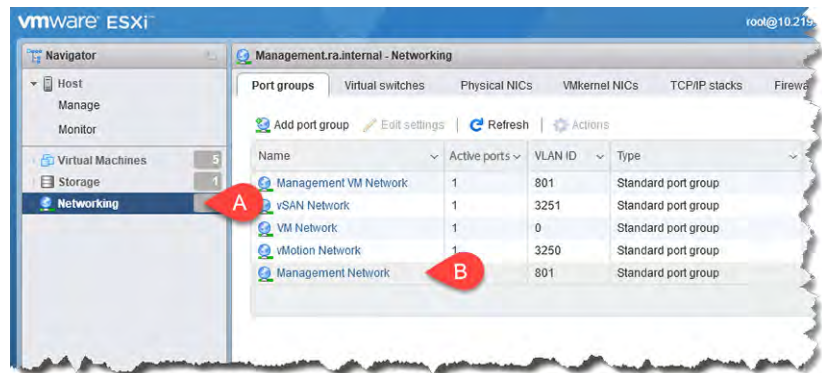
- Click Edit settings.



- Change the VLAN ID (A) to the desired value, and then click Save (B).



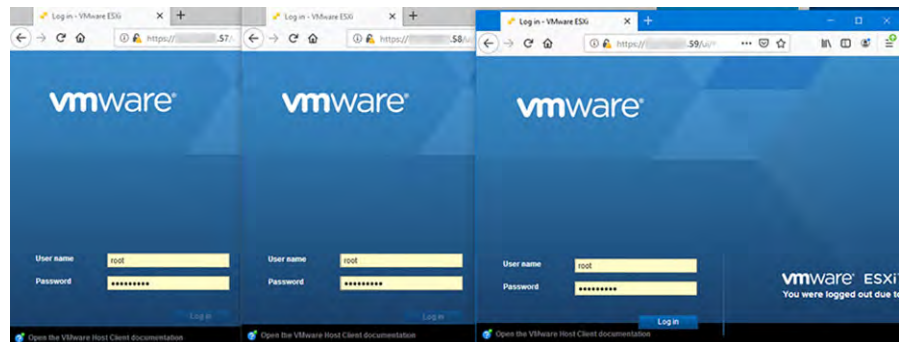
12. Return to Networking (A) and select Management Network (B).



13. Repeat [step 10](#) and [step 11](#) to change the VLAN ID for the Management Network.

Verify Connectivity

From your workstation, open a browser and navigate to all three hosts with the new IP addresses. If you have proper configuration and connectivity, the login screen with the user name/password prompt is visible for each host.



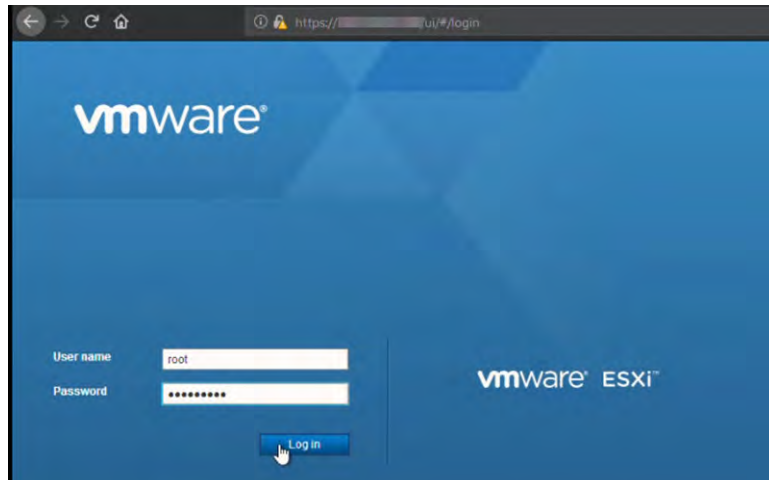
Modify the Virtual Machine IP Addresses

The NetSvcs Virtual Machine

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

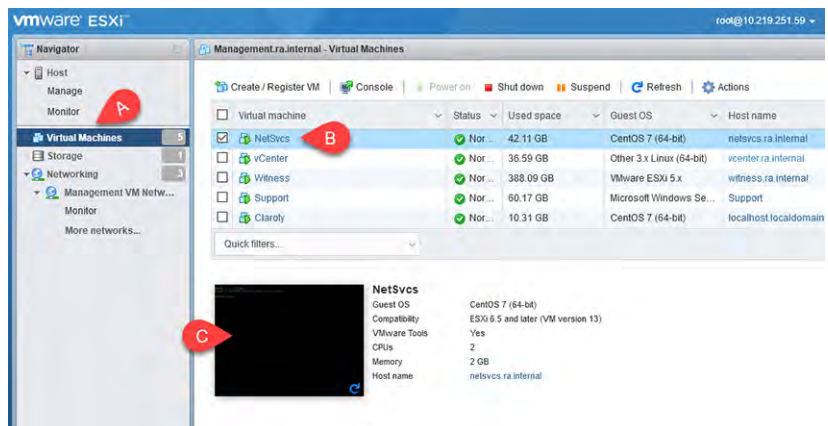
1. Open a browser and navigate to the new IP address of the Management host.

Log in with root and the system-wide password.

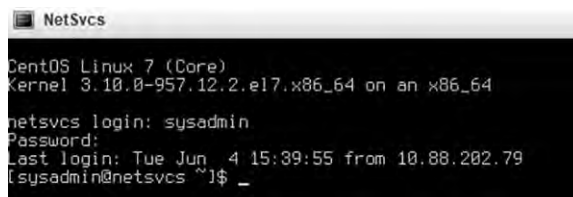


2. From the Inventory Navigator, select Virtual Machines (A), and then select the NetSvcs virtual machine (B).

Click anywhere in the thumbnail to open the NetSvcs DCUI (C).



3. Log in to the CentOS as sysadmin with the system password.



- Bring down the Ethernet interface with the following command:

```
nmcli connection down ethernet0
```

```
[sysadmin@netsvcs ~]$ nmcli connection down ethernet0
Connection 'ethernet0' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[sysadmin@netsvcs ~]$
```

- Modify the interface to configure the correct IP Address, CIDR mask, and gateway with the following command:

```
nmcli connection modify ethernet0 ipv4.addresses xx.xx.xx.xx/25 ipv4.gateway xx.xx.xx.xx
```

```
[sysadmin@netsvcs ~]$ nmcli connection modify ethernet0 ipv4.addresses .61/25 ipv4.gateway
[sysadmin@netsvcs ~]$
```

- Activate the following interface:

```
nmcli connection up ethernet0
```

```
[sysadmin@netsvcs ~]$ nmcli connection up ethernet0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
[sysadmin@netsvcs ~]$
```

- Verify that the IP address changed by typing: 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
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:eb:54:17 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.127/25 brd 192.168.1.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feeb:5417/64 scope link
        valid_lft forever preferred_lft forever
sysadmin@netsvcs ~]$
```

- Test (ping) your connection to the gateway.

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=1.29 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=1.19 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=1.16 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=254 time=1.25 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4002ms
rtt min/avg/max/mdev = 1.169/1.227/1.290/0.059 ms
[sysadmin@netsvcs ~]$
```

Change the DNS Settings in NetSvcs VM

- While still in the NetSvcs VM, type the following command:

```
sudo vim /etc/unbound/unbound.conf
```

```
[sysadmin@netsvcs ~]$ sudo vim /etc/unbound/unbound.conf
```

- First edit the unbound.conf file by replacing the default network with the new IP scheme.

3. If possible, and for simplicity, leave the last octet.

Type: `:%s/192.168.249/[IPAddress]/g`

Where [IPAddress] is the first three octets of the site-specific management network address.

```

NetSvcs
server:
access-control: 127.0.0.0/8 allow
access-control: 10.0.0.0/8 allow
access-control: 172.16.0.0/12 allow
access-control: 192.168.0.0/16 allow
cache-max-ttl: 14400
cache-min-ttl: 300
hide-identity: yes
hide-version: yes
interface: 0.0.0.0
minimal-responses: yes
num-threads: 4
prefetch: yes
qname-minimisation: yes
reset-roundrobin: yes
use-caps-for-id: yes
verbosity: 1

local-zone: "ra.internal." static
local-data: "nm1.ra.internal" IN A 192.168.249.7"
local-data: "nm2.ra.internal" IN A 192.168.249.8"
local-data: "cmc.ra.internal" IN A 192.168.249.9"
local-data: "management-bmc.ra.internal" IN A 192.168.249.10"
local-data: "host1-bmc.ra.internal" IN A 192.168.249.11"
local-data: "host2-bmc.ra.internal" IN A 192.168.249.12"
local-data: "management.ra.internal" IN A 192.168.249.13"
local-data: "host1.ra.internal" IN A 192.168.249.14"
local-data: "host2.ra.internal" IN A 192.168.249.15"
local-data: "witness.ra.internal" IN A 192.168.249.16"
local-data: "netsvcs.ra.internal" IN A 192.168.249.17"
local-data: "vcenter.ra.internal" IN A 192.168.249.18"
local-data: "support.ra.internal" IN A 192.168.249.19"

local-data-ptr: "192.168.249.7" nm1.ra.internal"
local-data-ptr: "192.168.249.8" nm2.ra.internal"
local-data-ptr: "192.168.249.9" cmc.ra.internal"
local-data-ptr: "192.168.249.10" management-bmc.ra.internal"
local-data-ptr: "192.168.249.11" host1-bmc.ra.internal"
local-data-ptr: "192.168.249.12" host2-bmc.ra.internal"
local-data-ptr: "192.168.249.13" management.ra.internal"
local-data-ptr: "192.168.249.14" host1.ra.internal"
local-data-ptr: "192.168.249.15" host2.ra.internal"
local-data-ptr: "192.168.249.16" witness.ra.internal"
local-data-ptr: "192.168.249.17" netsvcs.ra.internal"
local-data-ptr: "192.168.249.18" vcenter.ra.internal"
local-data-ptr: "192.168.249.19" support.ra.internal"

forward-zone:
name: ""
forward-addr:
forward-addr:

:%s/192.168.249/[IPAddress]/g
    
```

4. Press Enter to search the file for the string “192.168.249” and replace it with the appropriate subnet for the site.
5. After the substitutions have successfully completed, edit the fourth octet (if necessary) by pressing i to enter INSERT mode. Make necessary changes with arrow keys. To leave INSERT mode, press the ‘Esc’ key.

Verify that no other changes to the forward-addr entries at the bottom are required.

TIP Sites that reuse an existing Windows Active Directory or are deployed without a Windows Active Directory on the Operational Technology network require that the forward-addr field change to the upstream DNS server.

6. Type: `wq`
7. Press Enter afterwards to write and then quit.
8. Enter the following command:

```

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

No feedback is returned if the services restart successfully.

- Enter the following command:

```
[sysadmin@netsvcs ~]$ systemctl status unbound
unbound.service - Unbound recursive Domain Name Server
Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled)
Active: active (running) since Tue 2019-05-21 12:59:25 EDT; 15s
Process: 4994 ExecStartPre=/usr/sbin/unbound-anchor -a /var/lib/u
Process: 4994 ExecStartPre=/usr/sbin/unbound-checkconf (code=exit
Main PID: 5002 (unbound)
CGroup: /system.slice/unbound.service
└─5002 /usr/sbin/unbound -d

May 21 12:58:35 netsvcs.ra.internal systemd[1]: Starting Unbound re
May 21 12:58:35 netsvcs.ra.internal unbound-checkconf[4994]: unbound
May 21 12:59:25 netsvcs.ra.internal systemd[1]: Started Unbound rec
May 21 12:59:25 netsvcs.ra.internal unbound[5002]: [5002:0] notice:
May 21 12:59:25 netsvcs.ra.internal unbound[5002]: [5002:0] notice:
May 21 12:59:25 netsvcs.ra.internal unbound[5002]: [5002:0] notice:
May 21 12:59:25 netsvcs.ra.internal unbound[5002]: [5002:0] info: s
[sysadmin@netsvcs ~]$ _
```

Look for active (running) and status=0/SUCCESS.

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

If neither are found, then return to [step 1](#) on [page 41](#) and repeat the procedure.

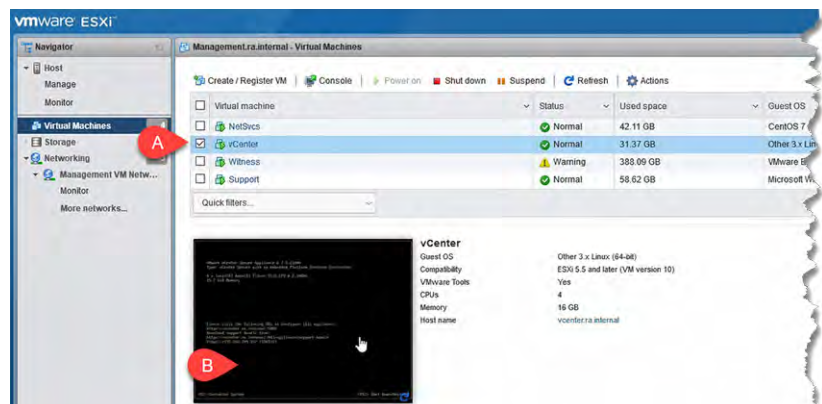
- Type:Logout
- Press Enter to close the NetSvcs DCUI.

IMPORTANT Best practice calls for changing the DNS server on your local workstation to the new IP address of the NetSvcs VM.

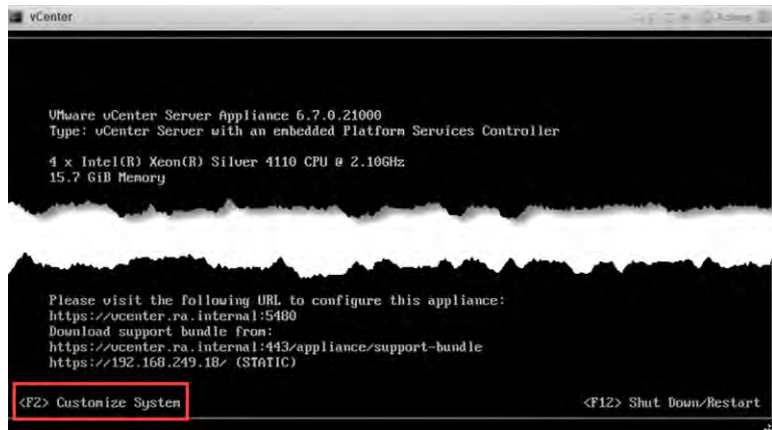
vCenter

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

- In the ESXi Web GUI, select vCenter (A) and click on the thumbnail to launch the vCenter DCUI. (B)



- When the vCenter DCUI opens, press the F2 key.

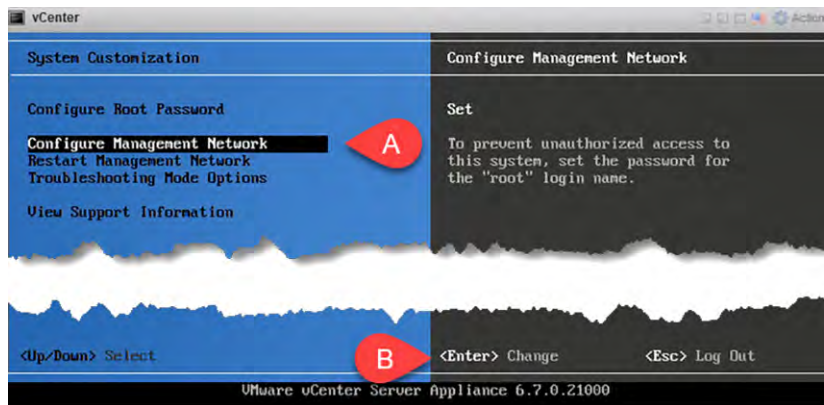


Log in with root and the system password, and then press Enter.



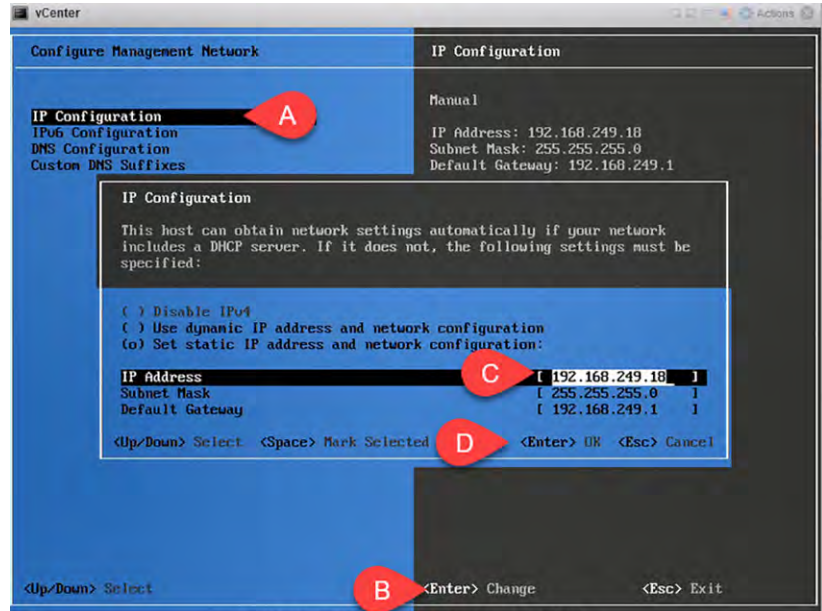
- In the vCenter DCUI, navigate to Configure Management Network (A) and press Enter (B).

TIP Your mouse does not work in the vCenter console. You must navigate entirely with your keyboard.



4. Select IP Configuration (A) and press Enter (B).
5. Use the down arrow to edit the IP address, Subnet Mask, and Gateway (C) to your desired settings.

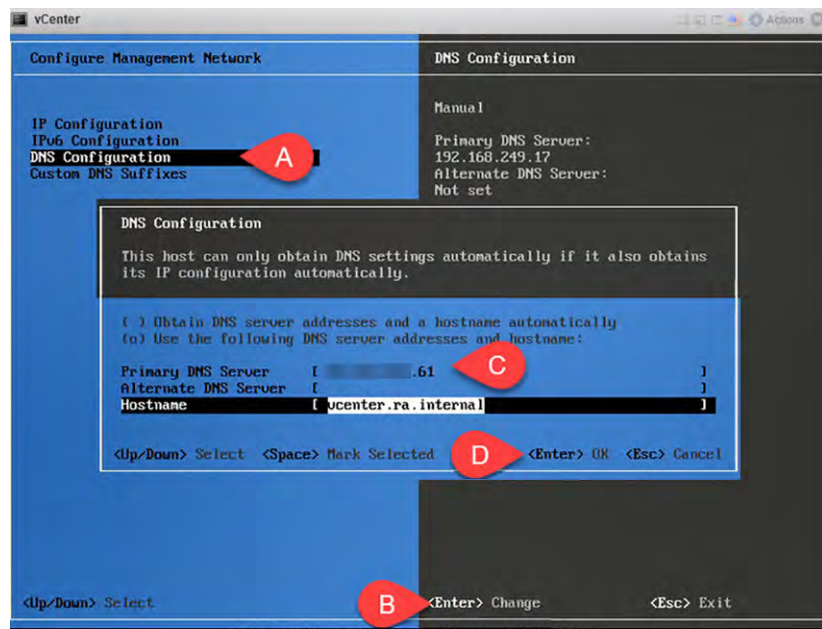
When completed, press Enter (D).



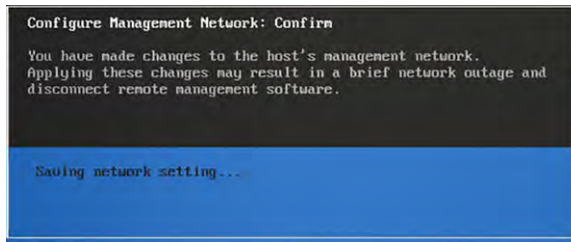
6. Select DNS Configuration (A) and press Enter (B).
Change the Primary DNS Server to your desired setting (C).

IMPORTANT Do not change the host name.

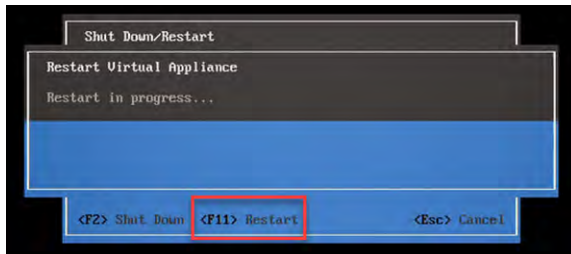
When completed, press Enter (D).



7. To save network settings, press Y.



8. To log off, press Esc .
9. To restart vCenter, press F12. You need to authenticate.
10. To restart, press F11.

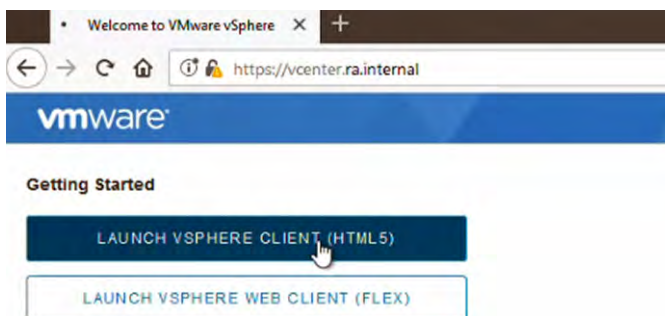


The restart process typically takes 10...15 minutes.

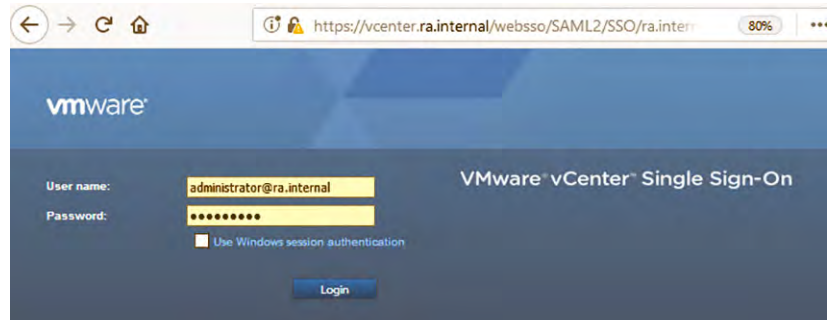
Migrate the Kernel Back to vdSwitch0

IMPORTANT To complete the following steps, vcenter.ra.internal must be resolvable to the current IP address of the VMware vCenter Server® at each step of the process. The easiest way to do so is to modify the hosts file, which is explained in [Modify the Hosts File on page 66](#).

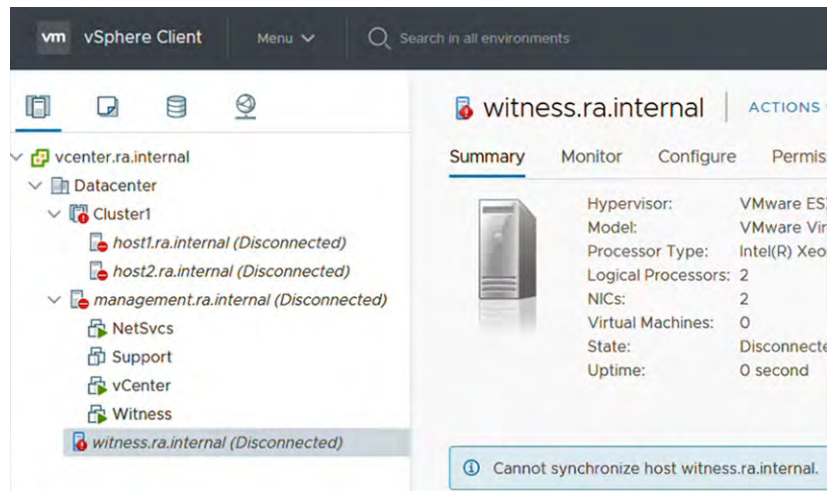
1. Access the following VMware® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).



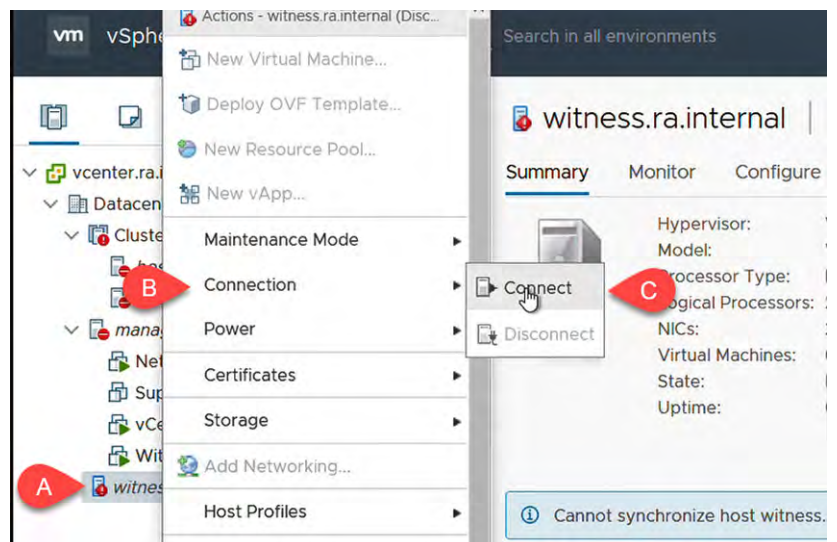
- Log into the VMware® vCenter® as administrator@ra.internal with the system-wide password.



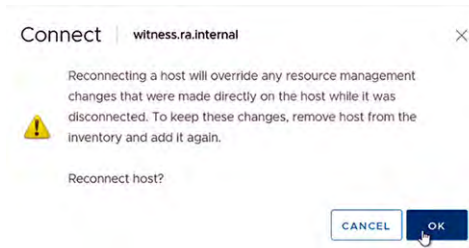
You will notice that the hosts have become disconnected.



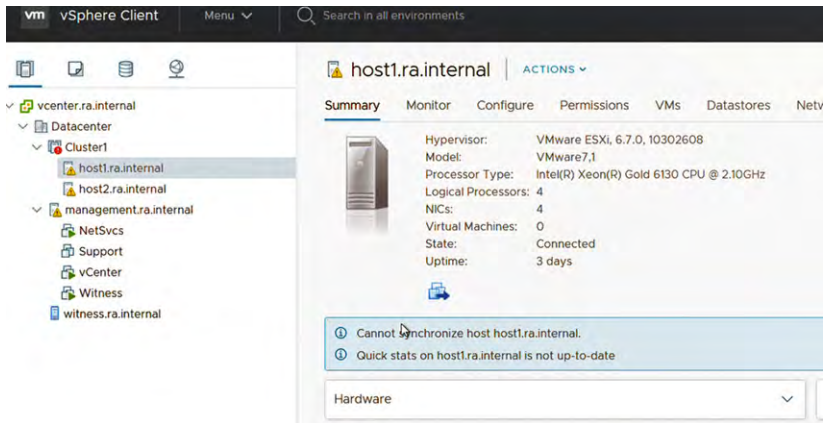
- On Witness host (A), right-click and select Connection (B) > Connect (C).



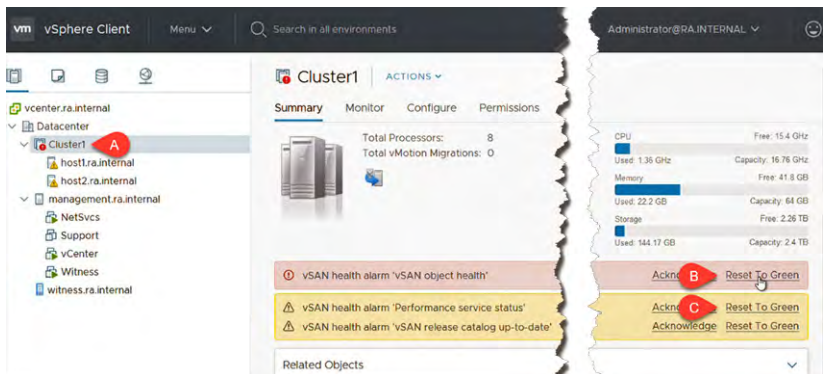
5. A connection alert box appears. Click OK.



6. Please repeat the connection process for the Management host and hosts 1 and 2 until all hosts are properly connected.

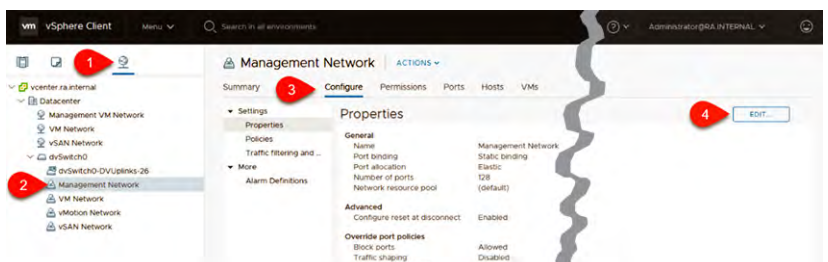


7. Highlight Cluster1 (A), and clear all vSAN health items (B and C).

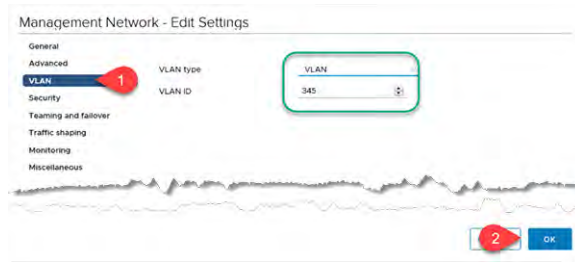


8. Navigate to the networking tab (1) > dvSwitch0 > Management Network (2).

Go to the Configure tab (3) and click Edit (4).



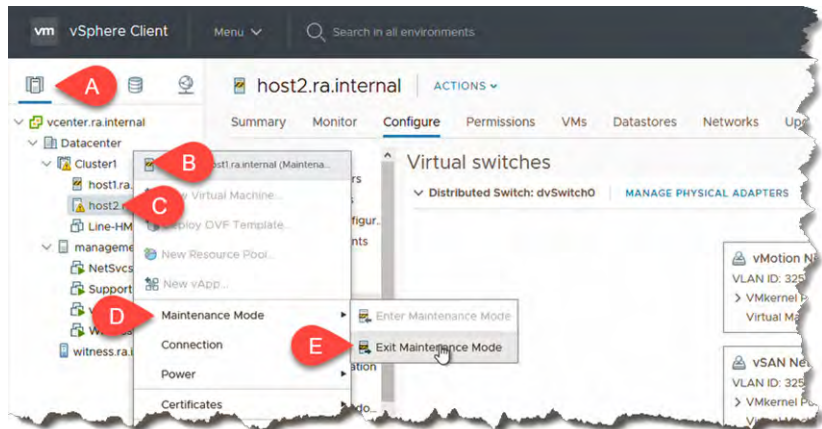
9. Click the VLAN tab and change the VLAN ID to the desired new VLAN. Click OK.



10. Repeat steps 2 and 3 for the VM Network port group.

11. Navigate to Hosts and Clusters (A) > Cluster1 (B).

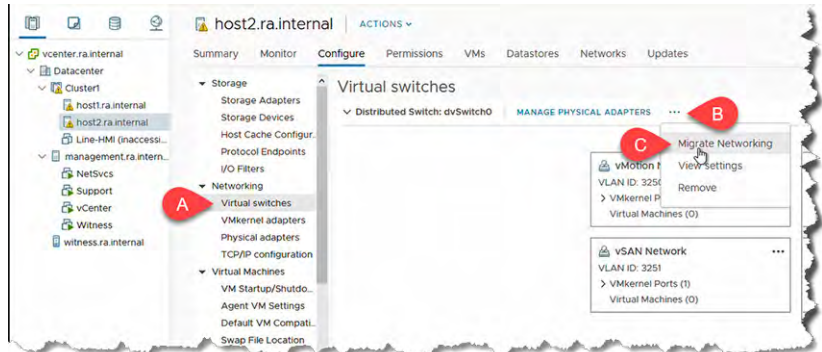
Right-click on host2 (C) > Maintenance Mode (D) > Exit Maintenance Mode (E).



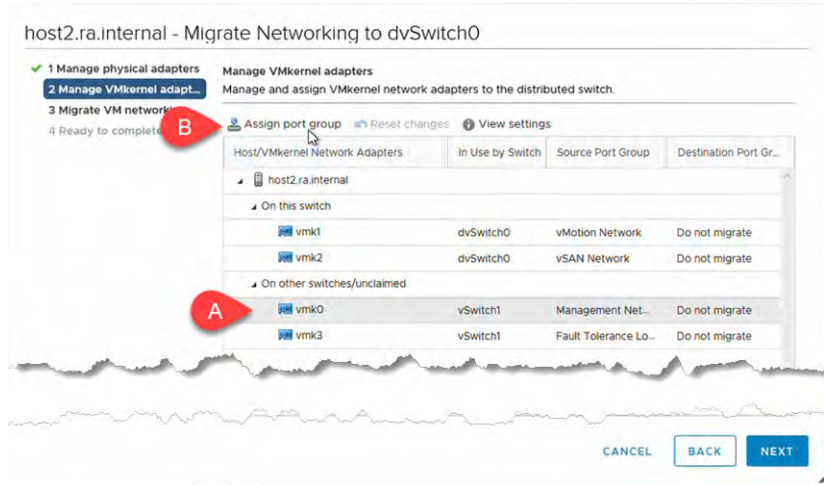
12. Repeat [step 1](#) for host1.

13. On host2, go to Networking > Virtual Switches (A).

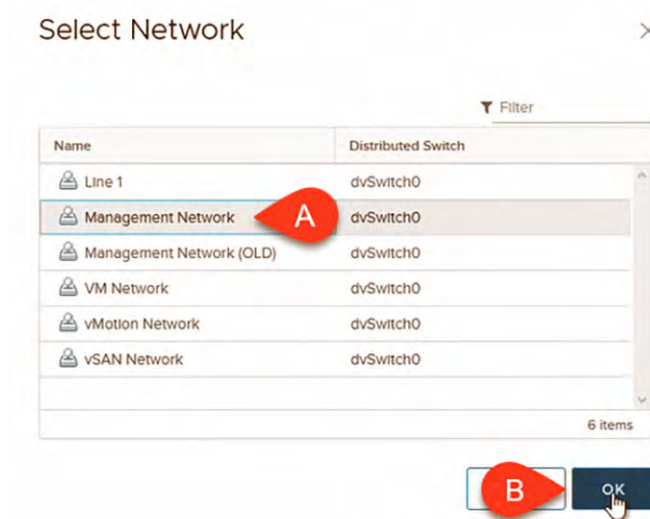
At dvSwitch0, click the ellipsis (B) and select Migrate Networking (C).



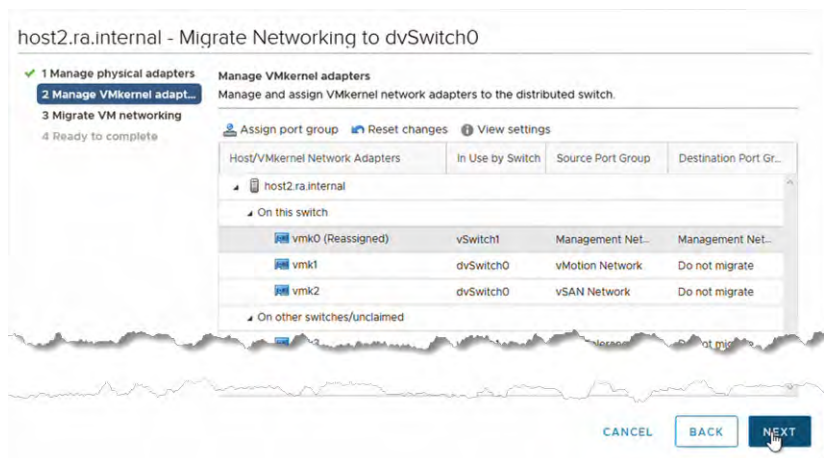
- On Manage VMkernel adapters, select vmk0 (A) and click Assign port group (B).



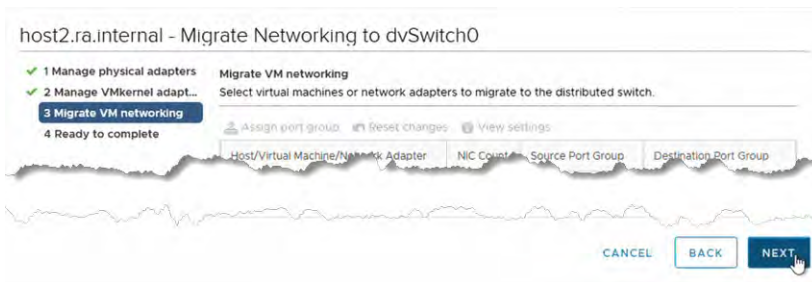
- Select Management Network (A) and click OK (B).



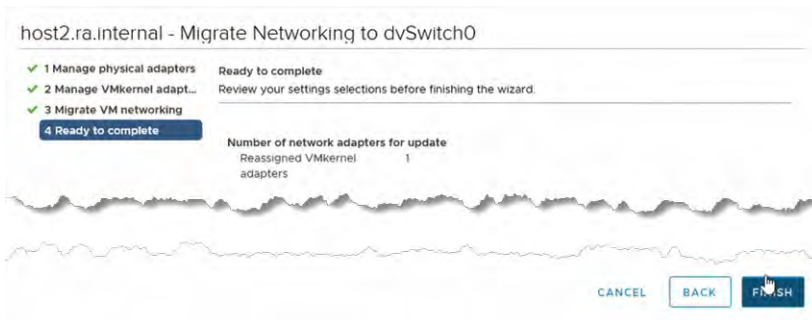
- Click Next.



- On step 3, click Next.



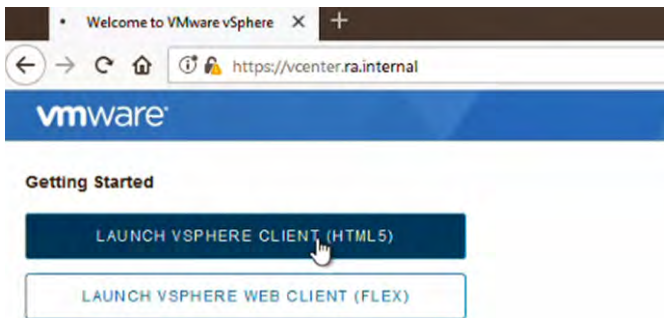
- On step 4, click Finish.



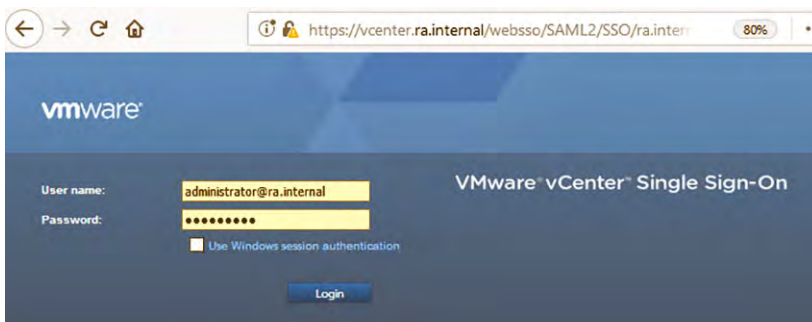
- Repeat [step 13](#)...[step 18](#) to migrate the kernel on host1.

Change the Host Address (HA) Isolation Addresses

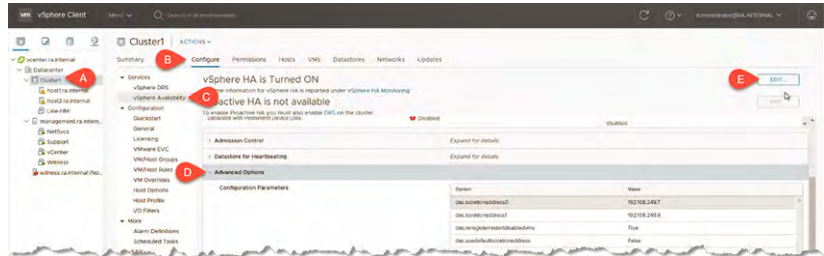
- Access the following VMware® website: <https://vcenter.ra.internal>.
- Under Getting Started, click Launch vSphere Client (HTML5).



- Log into the VMware® vCenter® as administrator@ra.internal with the system-wide password.



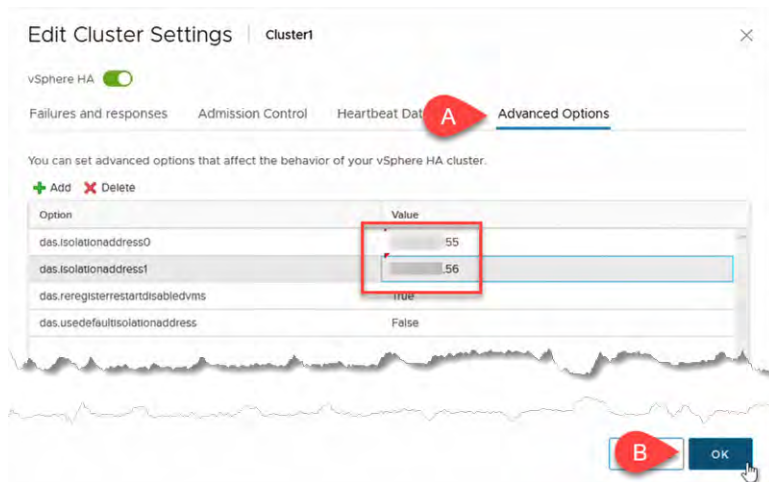
- In vCenter, navigate to Cluster1 (A) > Configure (B) > Services > vSphere Availability (C) > Advanced Options (D) > Edit (E).



- Go to the Advanced Options tab (A).

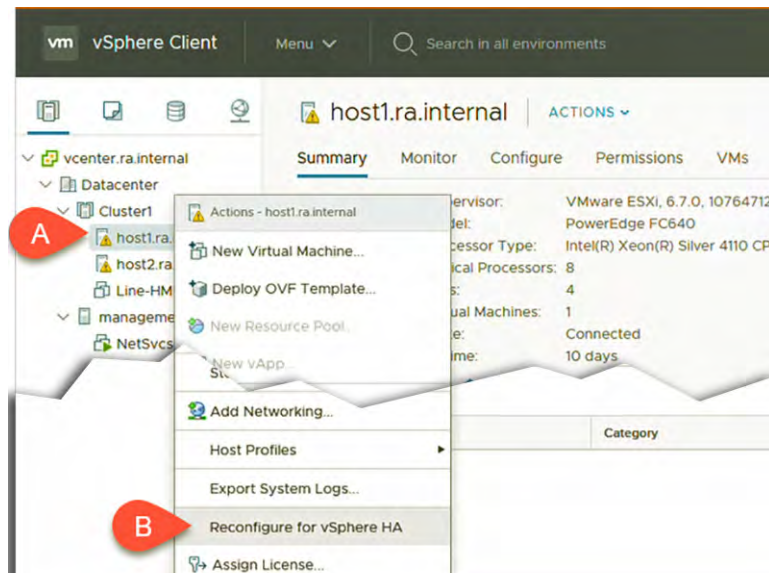
Click inside the das.isolationaddress Values and change the IP addresses to the new IP address of the I/O Network modules.

Click OK (B).



- Right-click on host1 (A) and click Reconfigure for vSphere HA (B).

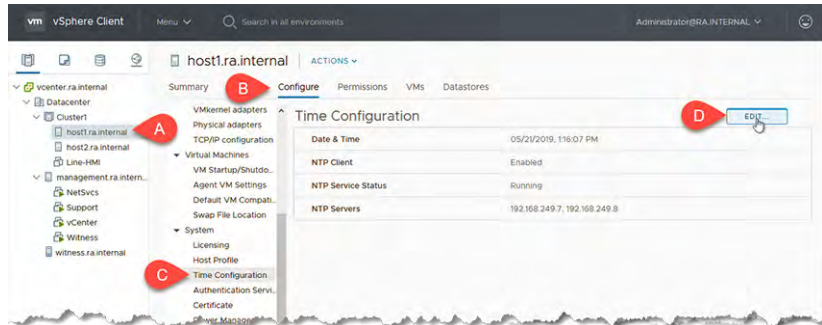
After a moment, the warning clears.



- Repeat [step 6](#) for host 2.

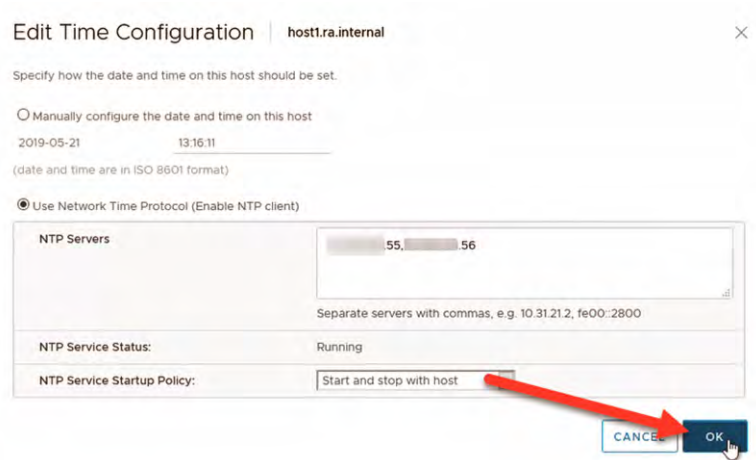
Change the Time Configuration

1. On host1 (A), navigate to the Configure tab (B) > System > Time Configuration (C) > Edit (D).



2. Replace the existing NTP servers with the new IP addresses of the two network modules.

Click OK.



3. Repeat [step 1](#) and [step 2](#) for host2, the Management host, and the Witness host.

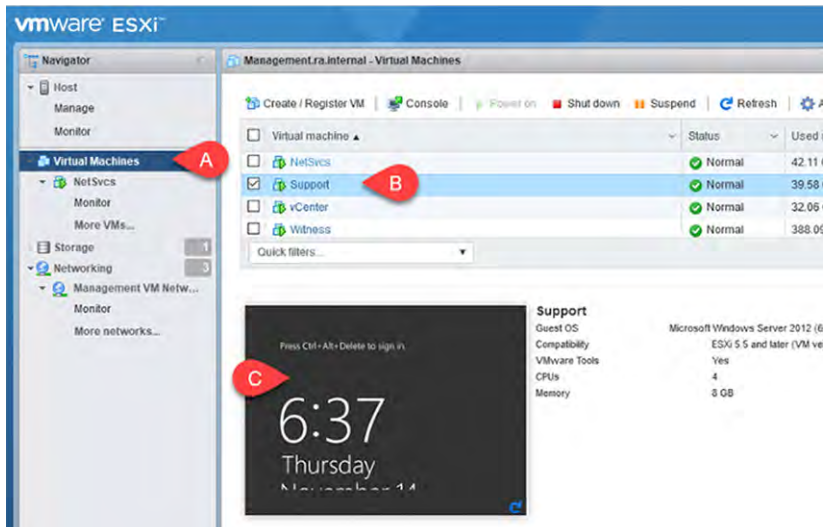
Support

1. Open a browser and navigate to the Management host site at <https://management.ra.internal>.

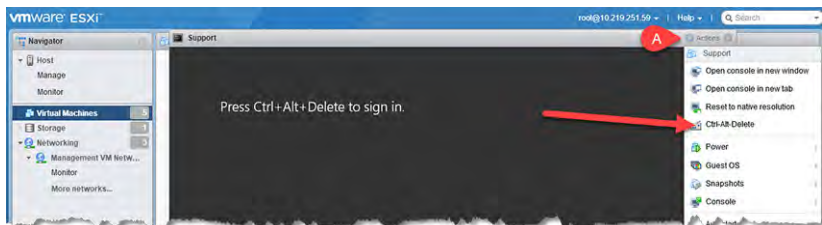
Log in with root and the system-wide password.



2. Under the Navigator pane, highlight Virtual Machines (A).
3. In the Virtual Machines pane, select Support (B), and then click on the Support thumbnail (C) to launch a browser console.



4. Log in to Support as administrator and the system password.



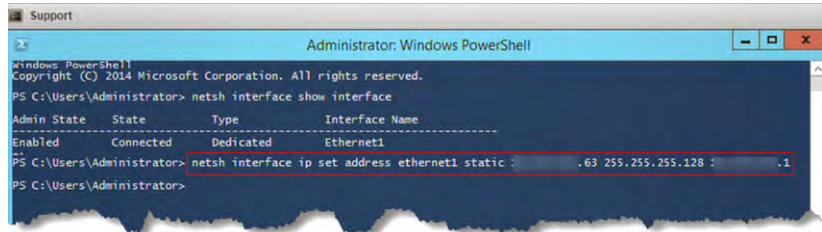
5. Launch the Microsoft® PowerShell application from the task bar.



- Change the IP address by typing the following command:

```
netsh interface ip set address ethernet1 static x.x.x.x
255.255.255.x x.x.x.x
```

Where the x's are your desired IPv4 settings.




- Set the DNS server by typing the following command:

```
Netsh interface ip set dnsservers ethernet1 static x.x.x.x
```

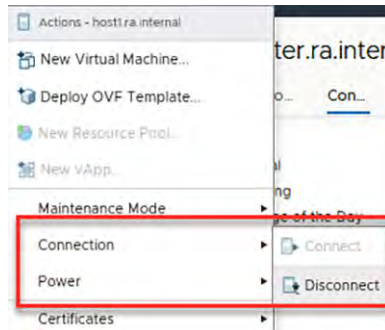
Where x is the IP address of the NetSvcs VM.
- Sign out of the Support VM.

Disconnect Hosts

If you see a warning from vCenter that it cannot synchronize the host, then the four hosts must be disconnected and then reconnected.

 Cannot synchronize host witness.ra.internal.

- Right click host1. Go to Connection > Disconnect.

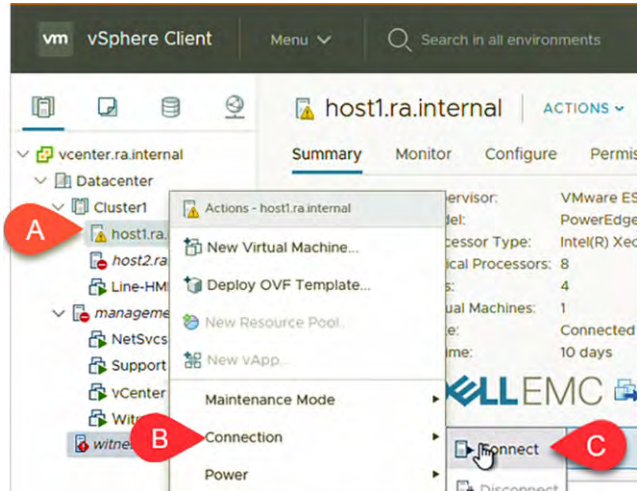


- To disconnect the host, click OK.

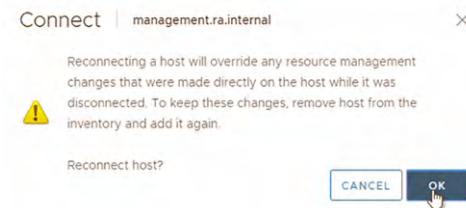


- Repeat steps 2 and step 3 on all four hosts.

4. After all four hosts are disconnected, right-click on host1 (A). Go to Connection (B) > Connect (C).



5. Click OK at the warning.

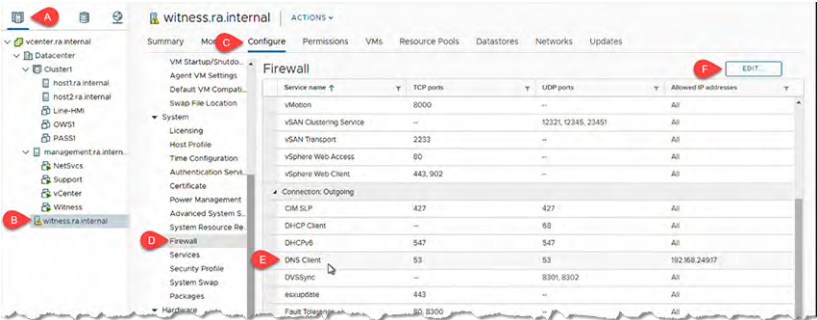


6. Repeat [step 4](#) and [step 5](#) for all four hosts.

Change the Firewall

- 1. From the Witness host (B) in Hosts and Cluster view (A), navigate to Configure (C) > System > Firewall (D).

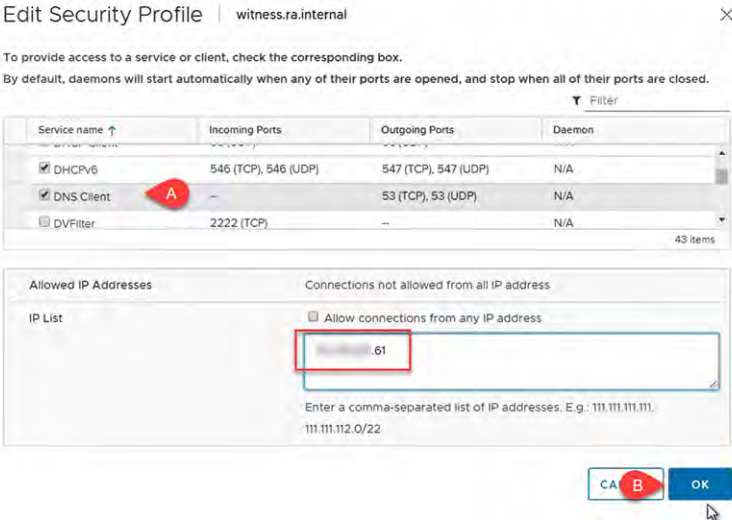
In the Outgoing connections, locate and select the DNS Client service (E). Then click Edit (F).



- 2. Scroll down to DNS client (A) and select it.

In the IP List field, change the IP address to the new NetSvcs (or DNS server) IP address.

Click OK (B).



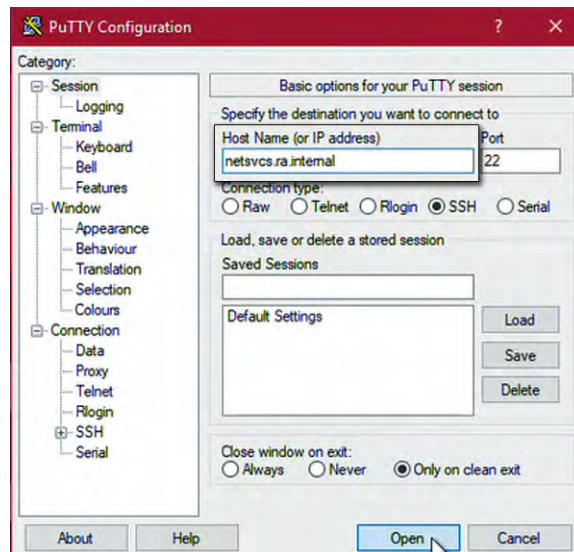
- 3. Repeat steps 1 and 2 for the other three hosts.

Domain Name System (DNS) Forwarding

The included DNS server can be configured to forward DNS queries to an upstream DNS server as a prerequisite to enable Active Directory authentication in vCenter or enable VMware Update Manager functionality. These changes are made from the console of the NetSvcs VM, which can be accessed either via Secure Shell (SSH) or from the vSphere Web Client. Instructions below use SSH via PuTTY for Windows®.

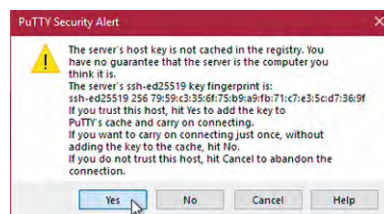
To use the PuTTY application, perform the following steps.

1. Open the application on your personal computer.
2. On the PuTTY configuration screen, add `netsvcs.ra.internal` as the host name.

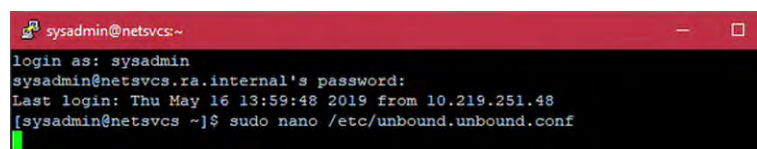


3. Click Open.

A security alert appears.

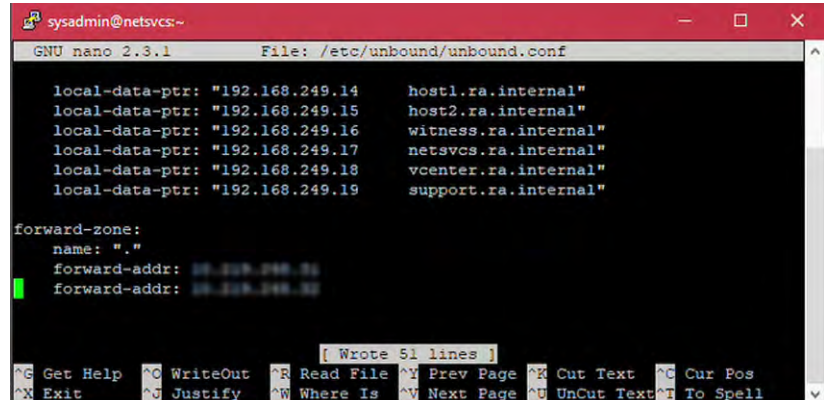


4. Click Yes.
5. On the PuTTY log in screen, type the following.
 - For login: `sysadmin` [Enter]
 - For password: `<system specific password>` [Enter]
 - For the \$ prompt: `sudo nano /etc/unbound/unbound.conf` [Enter]



6. To scroll down to the end of the file, use the arrow key on your keyboard.

7. For the forward-zone, change the forwarder IP address to a number more specific to your network.



```

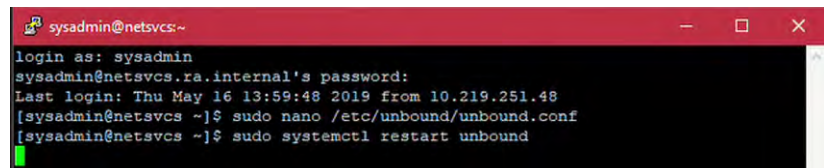
sysadmin@netvcs:~
GNU nano 2.3.1 File: /etc/unbound/unbound.conf
local-data-ptr: "192.168.249.14 host1.ra.internal"
local-data-ptr: "192.168.249.15 host2.ra.internal"
local-data-ptr: "192.168.249.16 witness.ra.internal"
local-data-ptr: "192.168.249.17 netvcs.ra.internal"
local-data-ptr: "192.168.249.18 vcenter.ra.internal"
local-data-ptr: "192.168.249.19 support.ra.internal"

forward-zone:
name: "."
forward-addr: 10.219.251.81
forward-addr: 10.219.249.81
[ Wrote 51 lines ]
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell

```

TIP If there are additional DNS servers on the network, additional 'forward-addr:' lines can be added.

8. To save the file, press Ctrl + O on your keyboard.
9. To exit the file, press Ctrl + X on your keyboard.
You are returned to the shell (\$) prompt.
10. At the \$ prompt, type `sudo systemctl restart unbound` [Enter].



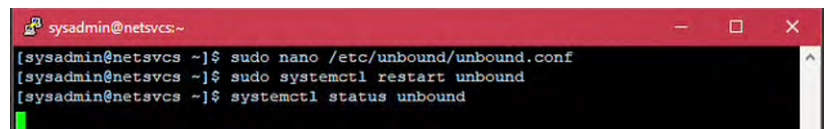
```

sysadmin@netvcs:~
login as: sysadmin
sysadmin@netvcs.ra.internal's password:
Last login: Thu May 16 13:59:48 2019 from 10.219.251.48
[sysadmin@netvcs ~]$ sudo nano /etc/unbound/unbound.conf
[sysadmin@netvcs ~]$ sudo systemctl restart unbound

```

The command restarts the system.

11. To verify that the system restarted, type `systemctl status unbound` [Enter].

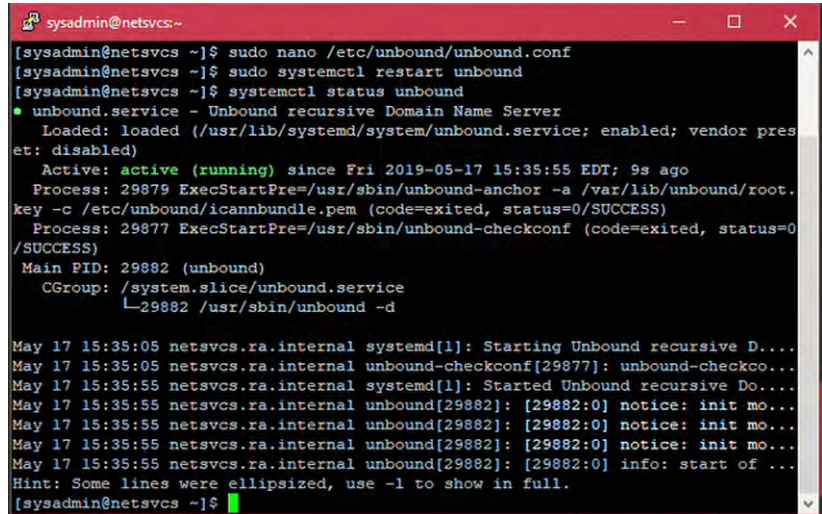


```

sysadmin@netvcs:~
[sysadmin@netvcs ~]$ sudo nano /etc/unbound/unbound.conf
[sysadmin@netvcs ~]$ sudo systemctl restart unbound
[sysadmin@netvcs ~]$ systemctl status unbound

```

12. A detailed startup log appears to verify that a restart was successful with the file that you created.



```
sysadmin@netvcs:~  
[sysadmin@netvcs ~]$ sudo nano /etc/unbound/unbound.conf  
[sysadmin@netvcs ~]$ sudo systemctl restart unbound  
[sysadmin@netvcs ~]$ 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 2019-05-17 15:35:55 EDT; 9s ago  
     Process: 29879 ExecStartPre=/usr/sbin/unbound-anchor -a /var/lib/unbound/root.key -c /etc/unbound/icannbundle.pem (code=exited, status=0/SUCCESS)  
     Process: 29877 ExecStartPre=/usr/sbin/unbound-checkconf (code=exited, status=0/SUCCESS)  
    Main PID: 29882 (unbound)  
   CGroup: /system.slice/unbound.service  
           └─29882 /usr/sbin/unbound -d  
  
May 17 15:35:05 netvcs.ra.internal systemd[1]: Starting Unbound recursive D...  
May 17 15:35:05 netvcs.ra.internal unbound-checkconf[29877]: unbound-checkco...  
May 17 15:35:55 netvcs.ra.internal systemd[1]: Started Unbound recursive Do...  
May 17 15:35:55 netvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...  
May 17 15:35:55 netvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...  
May 17 15:35:55 netvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...  
May 17 15:35:55 netvcs.ra.internal unbound[29882]: [29882:0] info: start of ...  
Hint: Some lines were ellipsized, use -l to show in full.  
[sysadmin@netvcs ~]$
```

Any errors can be found in the date/time stamped lines at the bottom of the file.

Manage the System

Topic	Page
Domain Name System (DNS) Requirements	61
Modify the Hosts File	69
Install VersaVirtual Licenses	69
Change the Default Password	75
Configure Active Directory Authentication	85
Update the Hardware Compatibility List	89
Add a Distributed Port Group	92
Add a Virtual Machine	95
Import an OVA Template	102
Install VSE Software	105

Domain Name System (DNS) Requirements

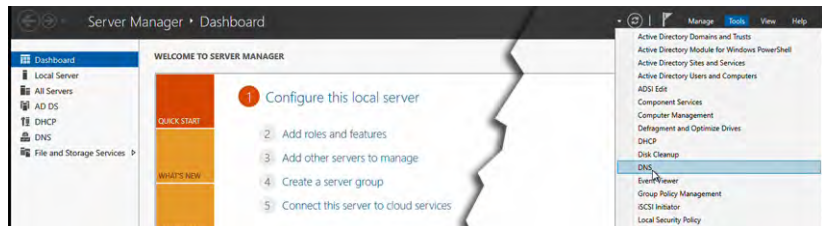
Proper DNS configuration affects access to the VMware vSphere® web client in VersaVirtual, or how you integrate the system with an existing or new Active Directory environment. To access the VMware vSphere web client, one of the following must be completed.

- Configure the Active Directory (AD) to forward DNS requests for the ra.internal domain to the NetSvcs virtual machine default IP address ([192.168.249.17](#)).
- Configure the management computer to use the NetSvcs virtual machine default IP address ([192.168.249.17](#)) as their DNS server.
- Edit the host file on the management computer to add entries for the VersaVirtual™ Appliance.

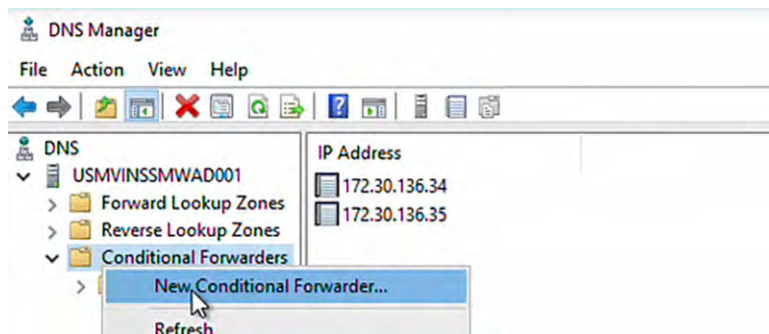
Forward DNS Requests

To add DNS conditional forwarders, perform the following steps.

1. Access the Server Manager.
2. On the Server Manager dashboard, select Tools > DNS.

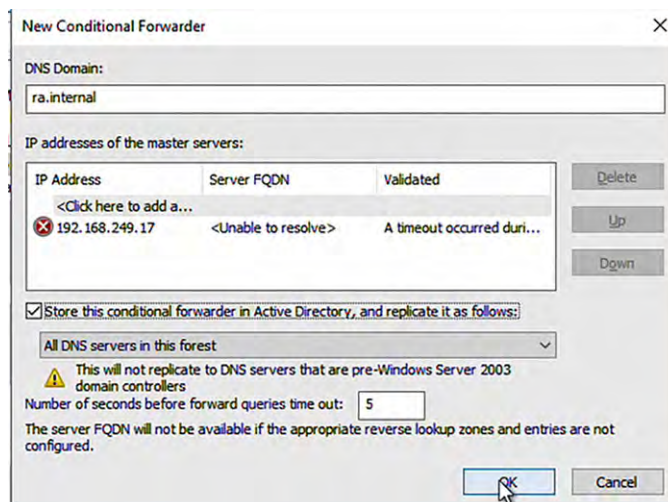


3. Under the Navigation pane on DNS Manager, access and highlight Conditional Forwarders.
4. Right-click on Conditional Forwarders and select New Conditional Forwarder from the pull-down menu.



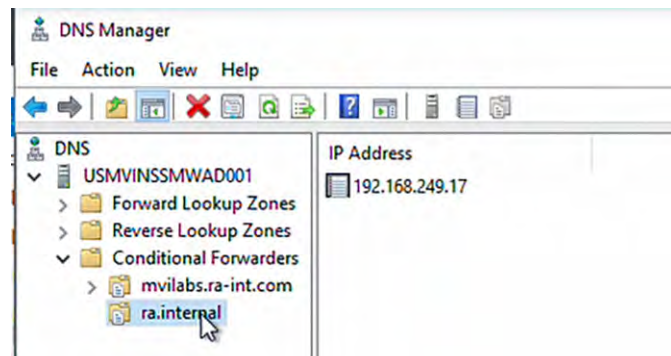
5. On the New Conditional Forwarder box, perform the following:
 - For the DNS Domain, add ra.internal.
 - In the IP address field, click and then add an IP address.
 - Check the 'Store this conditional forwarder in Active Directory ...' box.

TIP When you check this box, the IP address is queried and validated.



6. After the IP address is established and validated, click OK.

On the DNS Navigation pane, ra.internal is now a visible conditional forwarder.



7. To return to the Server Manager dashboard, close the DNS Manager box.

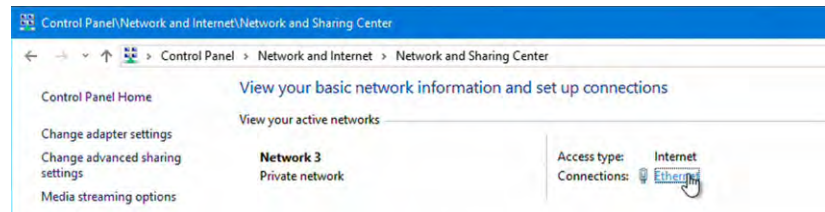


Ra.internal has been added as a DNS conditional forwarder.

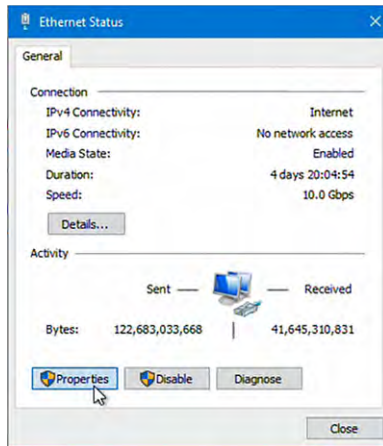
Configure the Management Computer

To add the DNS server address, perform the following steps.

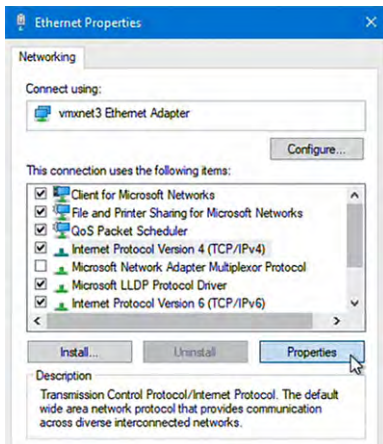
1. From the Start menu of your computer, access the Control Panel.
2. On Control Panel, select Network and Internet.
3. On the Network and Sharing Center, click Ethernet.



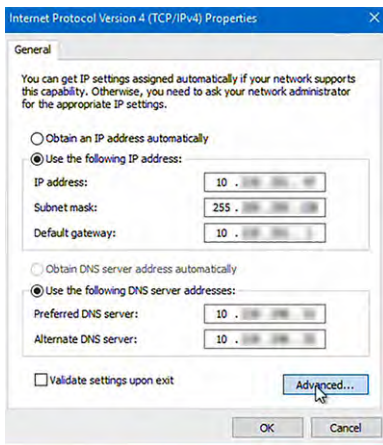
4. On the General tab of Ethernet Status, click Properties.



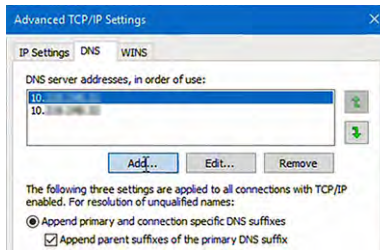
5. On the Networking tab, click Properties.



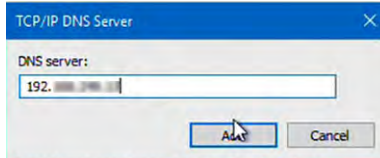
6. On the General tab, click Advanced.



- On the DNS tab, click Add.

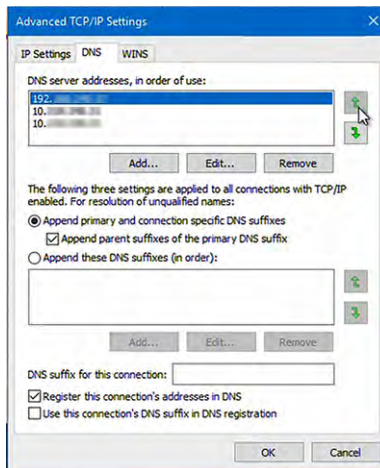


- Type the IP address for your DNS server and click Add.



- On the DNS tab, press the green UP button until the added IP address is at the top of the order.

Once it is at the top of the order, click OK.



- On the General tab, verify that the added IP address is the preferred DNS server address.

Click OK.



11. On the Networking tab, click Close.
12. On the General tab, click Close.
13. Close Networking and Sharing Center.

The DNS Server address is now accessible through the Ethernet port of your computer.

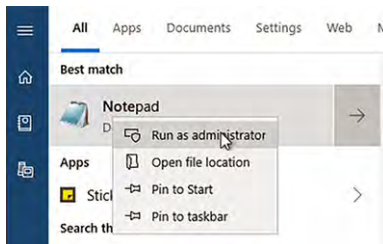
Modify the Hosts File

To add the list of IP addresses for the virtual network, perform the following steps.

1. Copy and paste the following list of IP addresses in the Microsoft® Notepad application. Keep this file open and minimized.

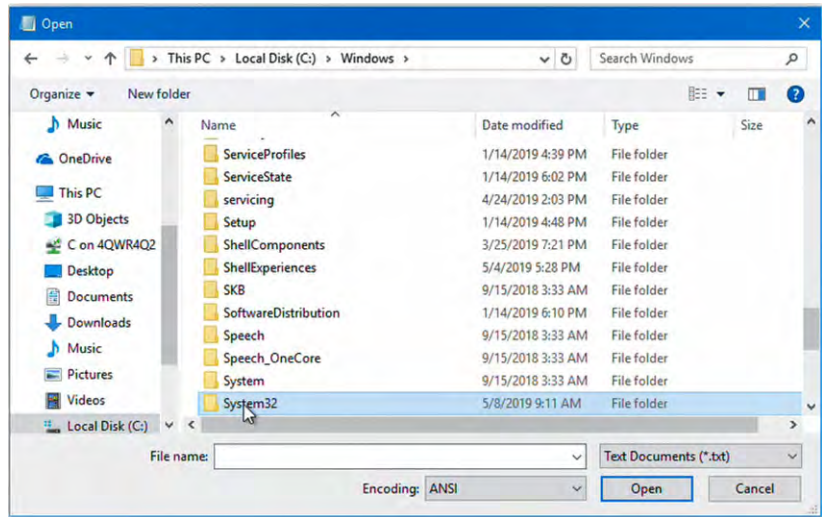
192.168.249.7	nm1.ra.internal	nm1	#FN410T	Network I/O Module
192.168.249.8	nm2.ra.internal	nm2	#FN410T	Network I/O Module
192.168.249.9	cmc.ra.internal	cmc	#FX2	Chassis Management Controller
192.168.249.10	management-bmc.ra.internal	management-bmc	#FC640	Service Baseboard Management Controller
192.168.249.11	host1-bmc.ra.internal	host1-bmc	#FC640	Host 1 Baseboard Management Controller
192.168.249.12	host2-bmc.ra.internal	host2-bmc	#FC640	Host 2 Baseboard Management Controller
192.168.249.13	management.ra.internal	management	#FC640	Service Host vSphere Management
192.168.249.14	host1.ra.internal	host1	#FC640	Host 1 vSphere Management
192.168.249.15	host2.ra.internal	host2	#FC640	Host 2 vSphere Management
192.168.249.16	witness.ra.internal	witness	#VM	vSAN Witness Virtual Appliance
192.168.249.17	netsvcs.ra.internal	netsvcs	#VM	Network Services Virtual Appliance
192.168.249.18	vCenter.ra.internal	vCenter	#VM	vCenter Server Virtual Appliance
192.168.249.19	support.ra.internal	support	#VM	Remote Support Virtual Appliance

2. Access the Notepad application again through Windows > Search.
3. Right-click on the Notepad application icon and select Run as administrator.

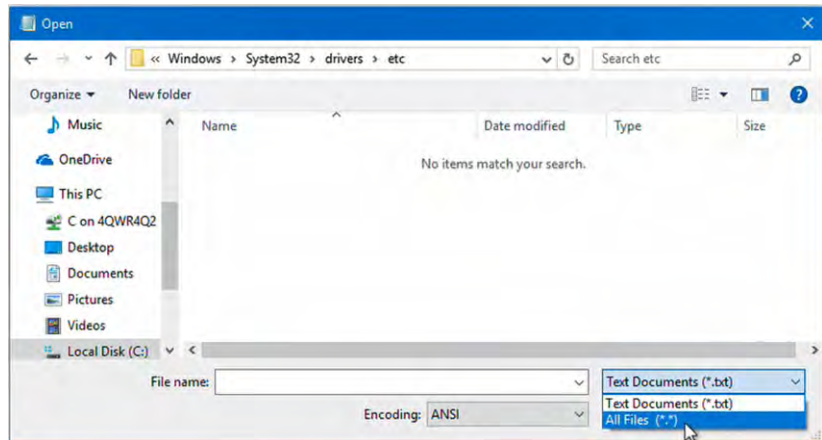


4. After Notepad opens, select File > Open.

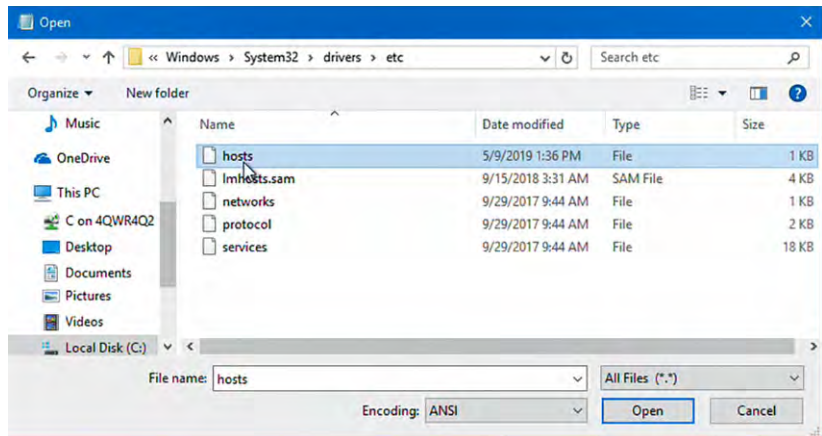
5. Navigate to the following: Local Disk (C:) > Windows > System32.



6. Double-click System32 to open it.
7. From the System32 menu, double-click drivers to open it.
8. From the drivers menu, double-click etc to open it.
9. From the file type pull-down menu, select All Files.



10. From the files that appear, double-click hosts to open it.



The hosts file opens in the Notepad application.

```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# 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:
#
#       102.54.94.97    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
    
```

11. Return to your original Note Pad file with the IP addresses.
12. With your keyboard, press Ctrl + A (select all) and then Ctrl + C (copy).

```

Untitled - Notepad
File Edit Format View Help
192.168.249.7    nm1.ra.internal    nm1    # FM410T    Network I/O Module
192.168.249.8    nm2.ra.internal    nm2    # FM410T    Network I/O Module
192.168.249.9    cnc.ra.internal    cnc     # FX2       Chassis Management Controller
192.168.249.10   management-bmc.ra.internal    management-bmc    # FC640     Service Baseboard Management Controller
192.168.249.11   host1-bmc.ra.internal    host1-bmc    # FC640     Host 1 Baseboard Management Controller
192.168.249.12   host2-bmc.ra.internal    host2-bmc    # FC640     Host 2 Baseboard Management Controller
192.168.249.13   management.ra.internal    management    # FC640     Service Host vSphere Management
192.168.249.14   host1.ra.internal    host1     # FC640     Host 1 vSphere Management
192.168.249.15   host2.ra.internal    host2     # FC640     Host 2 vSphere Management
192.168.249.16   witness.ra.internal    witness    # VM        vSAN Witness Virtual Appliance
192.168.249.17   netsvcs.ra.internal    netsvcs    # VM        Network Services Virtual Appliance
192.168.249.18   vCenter.ra.internal    vCenter    # VM        vCenter Server Virtual Appliance
192.168.249.19   support.ra.internal    support    # VM        Remote Support Virtual Appliance
    
```

13. Return to the hosts file. Place your cursor below the last line of text.
14. With your keyboard, select Ctrl + V (paste).

```

hosts - Notepad
File Edit Format View Help
# 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:
#
#       102.54.94.97    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
192.168.249.7    nm1.ra.internal    nm1    # FM410T    Network I/O Module
192.168.249.8    nm2.ra.internal    nm2    # FM410T    Network I/O Module
192.168.249.9    cnc.ra.internal    cnc     # FX2       Chassis Management Controller
192.168.249.10   management-bmc.ra.internal    management-bmc    # FC640     Service Baseboard Management Controller
192.168.249.11   host1-bmc.ra.internal    host1-bmc    # FC640     Host 1 Baseboard Management Controller
192.168.249.12   host2-bmc.ra.internal    host2-bmc    # FC640     Host 2 Baseboard Management Controller
192.168.249.13   management.ra.internal    management    # FC640     Service Host vSphere Management
192.168.249.14   host1.ra.internal    host1     # FC640     Host 1 vSphere Management
192.168.249.15   host2.ra.internal    host2     # FC640     Host 2 vSphere Management
192.168.249.16   witness.ra.internal    witness    # VM        vSAN Witness Virtual Appliance
192.168.249.17   netsvcs.ra.internal    netsvcs    # VM        Network Services Virtual Appliance
192.168.249.18   vCenter.ra.internal    vCenter    # VM        vCenter Server Virtual Appliance
192.168.249.19   support.ra.internal    support    # VM        Remote Support Virtual Appliance
    
```

15. From the File menu, select Save.

The IP addresses are now part of the hosts file.

Install VersaVirtual Licenses

This section covers how to install licenses within 90 days of the VersaVirtual Appliance purchase.

IMPORTANT A VersaVirtual Appliance is shipped with a 90-day evaluation period, which provides operation without a license. To continue uninterrupted service, Rockwell Automation recommends that you install a license before the 90-day evaluation period ends.

Other application licenses, such as for Microsoft®, are not included with the VersaVirtual Appliance.

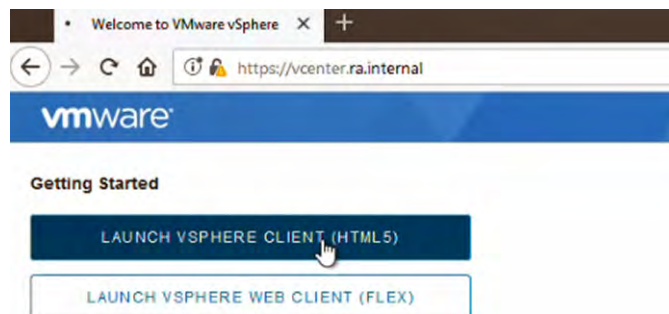
To install licenses after 90 days, search for instructions on the Rockwell Automation Knowledgebase site at https://www.rockwellautomation.com/en_US/support/overview.page. Use VersaVirtual as your search criteria.

The following licenses are supplied.

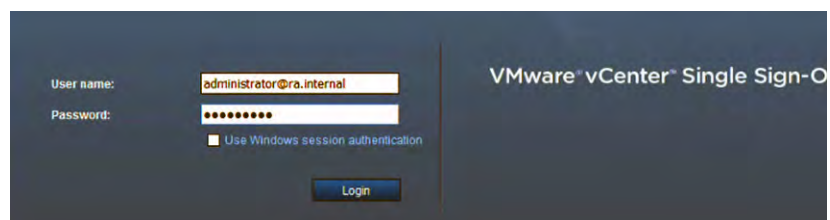
Application	Cat. Nos.	Cat. Nos.
	9300-VV1000EC, 9300-VV1000EN, 9300-VV1000RC, 9300-VV1000RN	9300-VV2000EC, 9300-VV2000EN, 9300-VV2000RC, 9300-VV2000RN
VMware vCenter Server® Foundation	√	√
VMware vSphere® Standard	√	√
VMware vSAN™ Standard		√

To install VersaVirtual Appliance licenses, perform the following steps.

1. Access the following VMware® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).

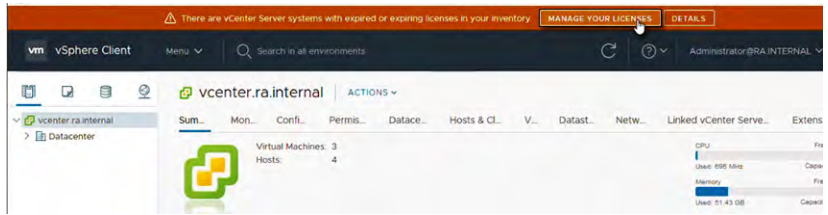


3. Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>

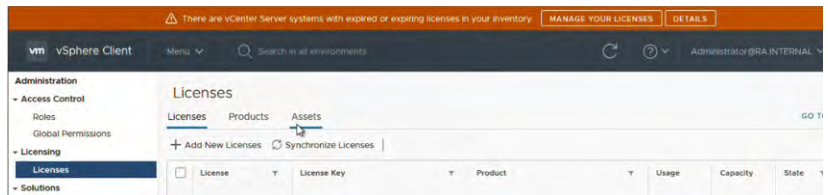


4. Click Login.

- On the home page, click Manage Your Licenses at the top of the page.

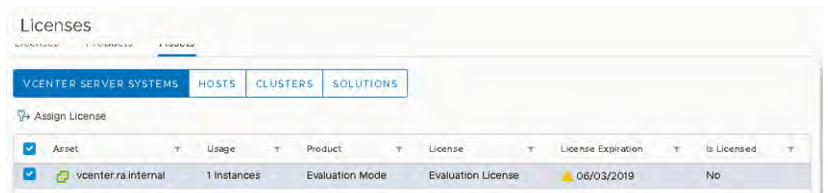


- On Licenses, select the Assets tab.



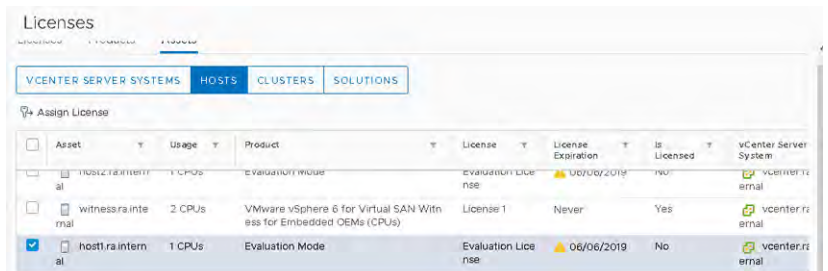
- On Assets, vCenter Server Systems is the default tab.

Verify that vcenter.ra.internal is checked and highlighted.



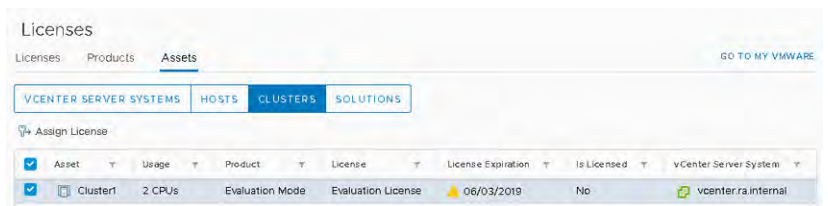
- Click Hosts.

On Hosts, verify that host1.ra.internal is checked and highlighted.

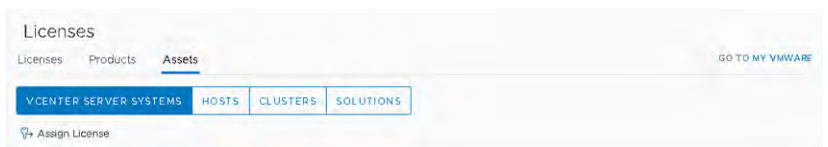


- Click Clusters.

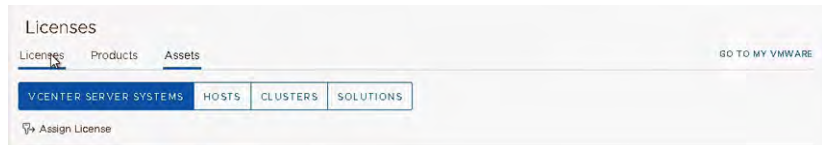
On Clusters, verify that Cluster1 is checked and highlighted.



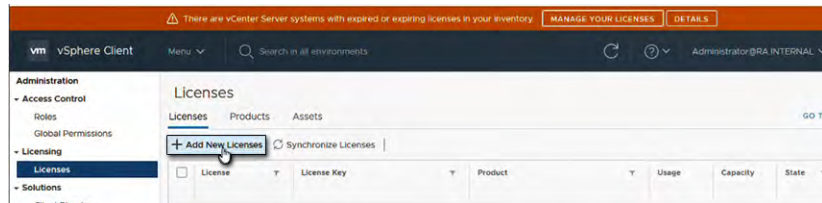
- Click vCenter Server Systems.



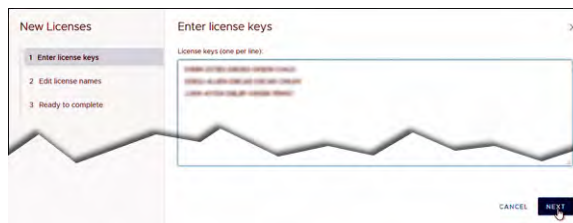
- On vCenter Server Systems, select the Licenses tab.



- On Licenses, click Add New Licenses.

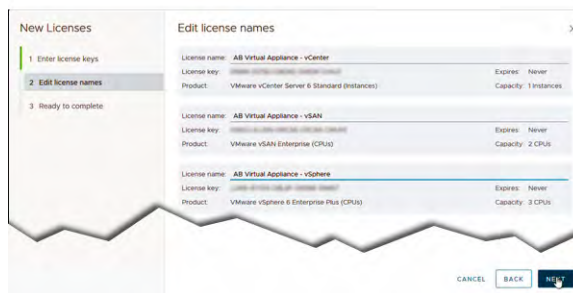


- Enter the license keys that were supplied with your appliance purchase.



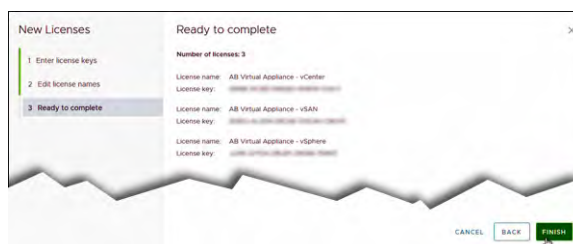
After they are entered, click Next.

- Rename each license key to a more suitable name.



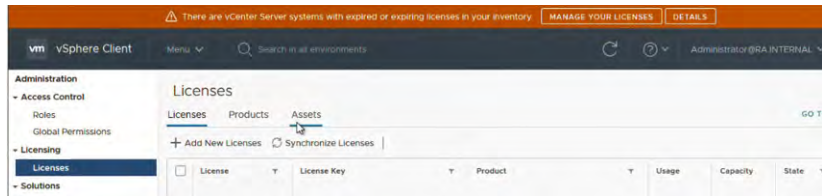
After you rename each key, click Next.

- Verify that each license key has a suitable new name.
If any corrections are needed, then click Back and repeat step 14.

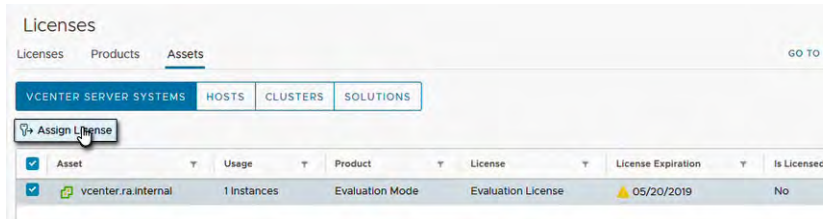


If the new license names are acceptable, then click Finish. You are returned to the Licenses page.

16. Select the Assets tab.



17. With the vcenter.ra.internal asset checked and highlighted, click Assign License.



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



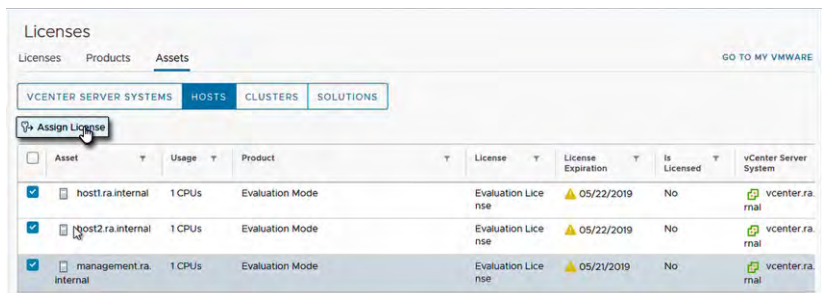
Click OK. You are returned to the Assets page.

19. Click Hosts.

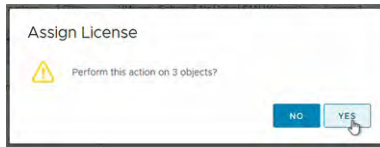
20. On Hosts, verify that the following three assets are checked:

- host1.ra.internal
- host2.ra.internal
- management.ra.internal

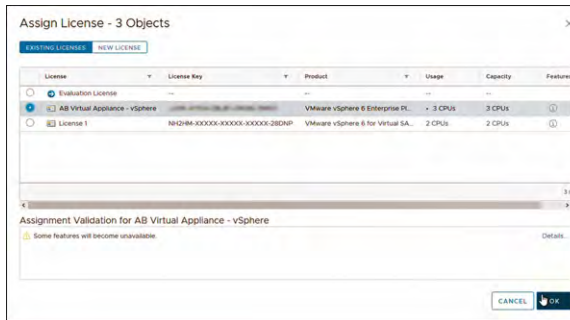
21. With the three assets selected, click Assign License.



22. You receive an alert about assigning one license to three objects.
Click Yes.

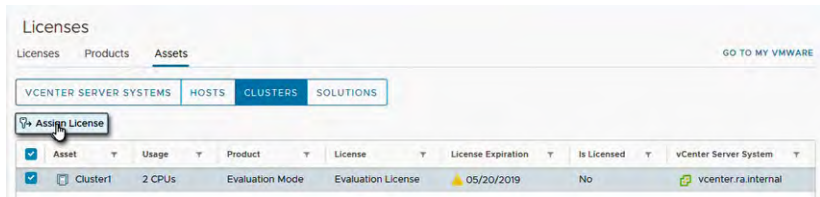


23. On Assign License - three Objects, verify that the new vSphere Standard license key is available and selected.

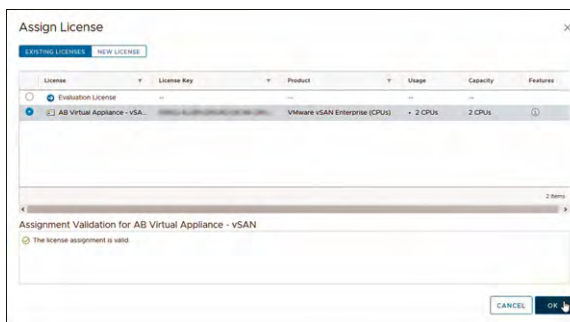


Click OK. You are returned to the Hosts page.

24. Click Clusters.
25. With the Cluster1 asset checked and highlighted, click Assign License.

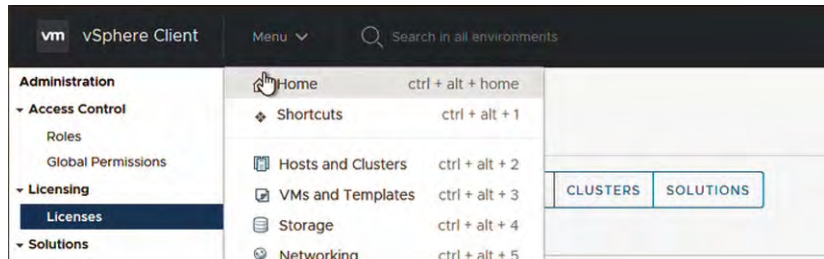


26. On Assign License, verify that the new vSAN Standard license key is available and selected.

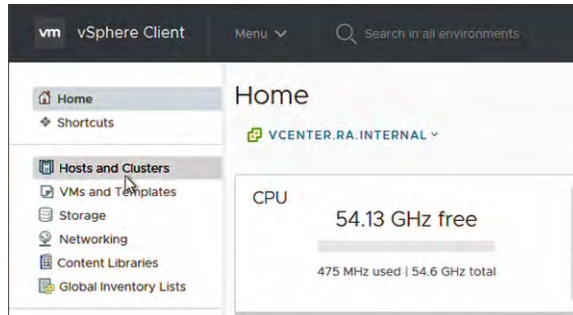


Click OK. You are returned to the Clusters page.

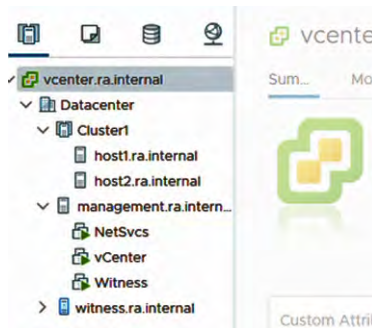
27. Select Menu > Home.



28. Under the Home navigation pane, select Hosts and Clusters.

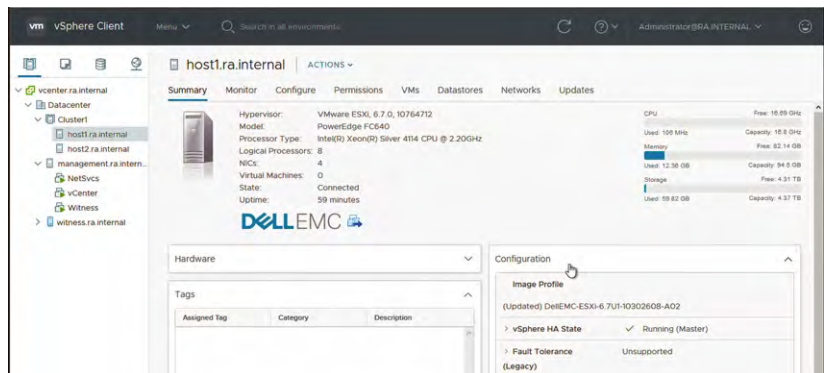


29. Expand the vertical hierarchy for Hosts and Clusters to see the devices where you have assigned licenses.



30. Check each device where licenses were assigned to confirm that those licenses are shown.

In this example, it is for host1.ra.internal.



Repeat any steps in this section where a license is not visible.

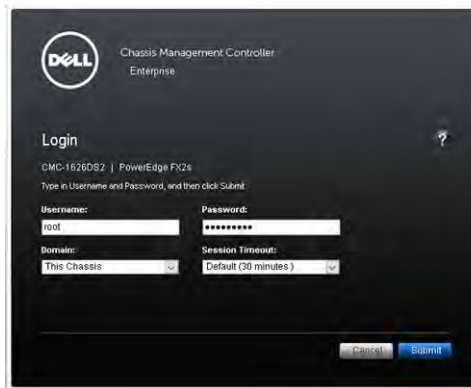
Change the Default Password

This section details where the system password must be changed in the VersaVirtual Appliance.

Chassis Management Controller (CMC)

To change the system password in the CMC, perform the following steps.

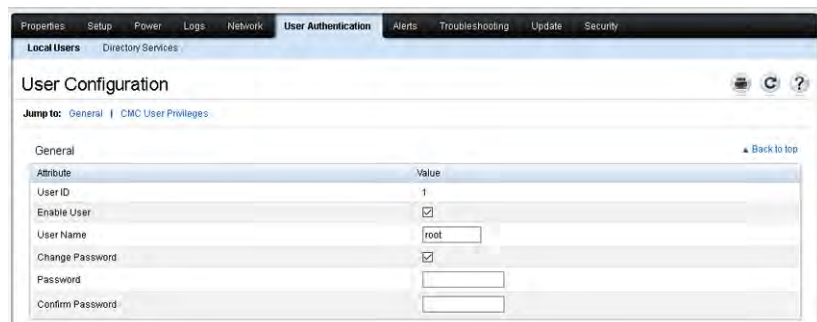
1. Log into <https://192.168.249.9> with the following:
 - User name: root
 - Password: <system-specific password>.



2. Click Submit.
3. Navigate to the User Authentication tab.
4. Click the number next to the 'root' user name.



5. Select the Change Password box.



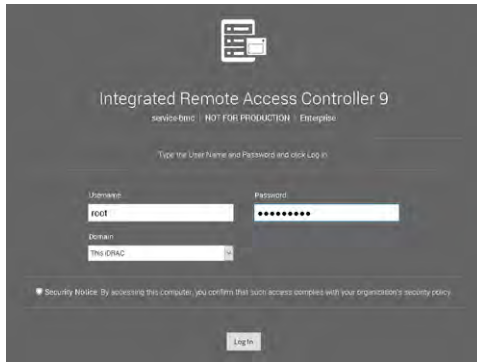
6. Enter the new password in the Password and Confirm Password fields.
7. Click Apply.
8. Log off from the CMC website, and verify that you can log in with the new password.

Baseboard Management Controller (BMC)

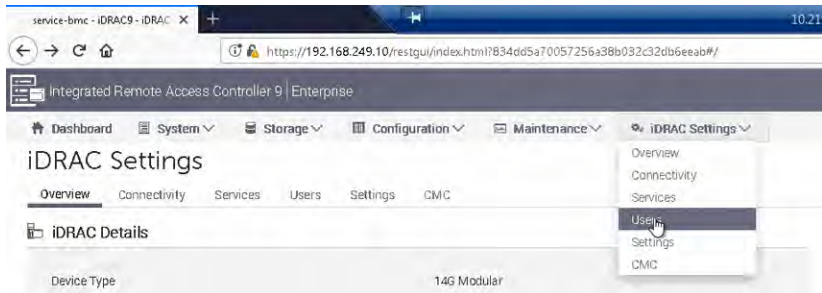
For the BMC, there is one service and two host management controllers with each appliance. To change the system password in each one, perform the following steps.

TIP Step 1 is to access the service management controller. See [step 8 on page 77](#) for the URL addresses that you must log into each host management controller.

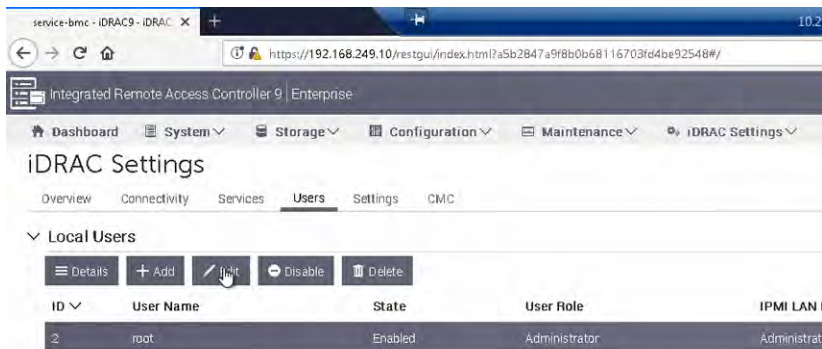
1. Log into <https://192.168.249.10> with the following:
 - User name: root
 - Password: <system-specific password>



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



3. On the iDRAC Settings page, select the root user and click Edit.



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



5. When finished, click Save.
6. When the success window appears, click OK.



7. Log off from the BMC website, and verify that you can log in with the new password.
8. Repeat steps 1...7 for each of the two host management controllers. For step 1, use these URL addresses for each host controller:
 - Host 1: <https://192.168.249.11>
 - Host 2: <https://192.168.249.12>

VMware vSphere

For the VMware vSphere, there is one Management, one Witness, and two cluster Hosts. To change the password in each one, perform the following steps.

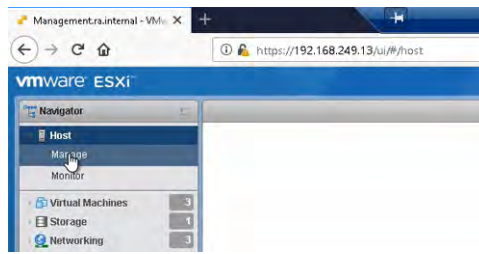
TIP Step 1 is to access the service management controller. See [step 8](#) on [page 77](#) for the URL addresses that you must log into each host management controller.

1. Log into <https://192.168.249.13> with the following:
 - User name: root
 - Password: <system-specific password>

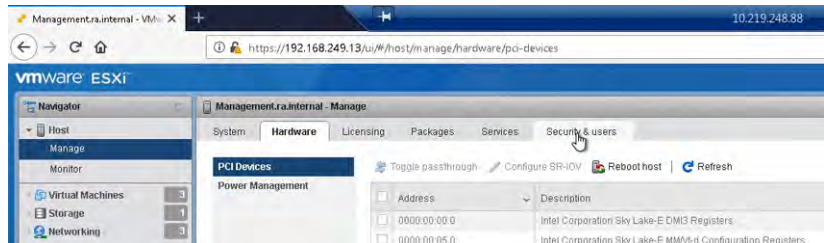


2. Click Login.

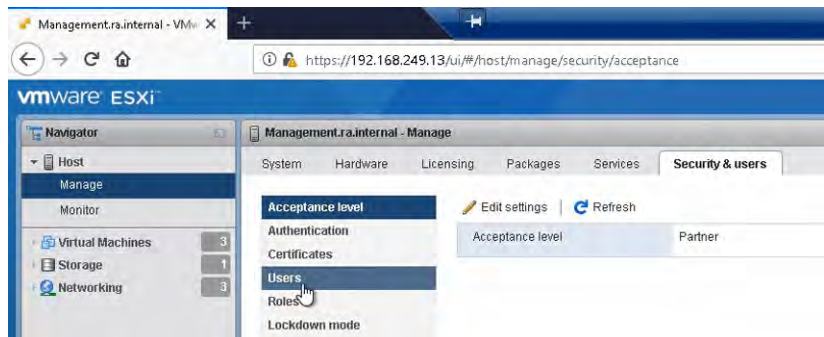
- Under the Navigator pane, click Manage.



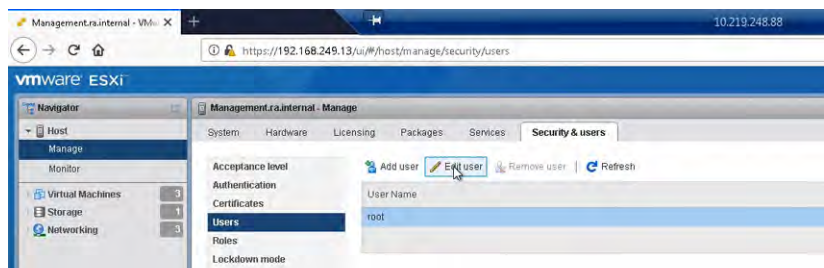
- On the Manage page, select the Security and Users tab.



- Under the Acceptance Level navigation pane, select Users.



- Select 'root' and click Edit user.



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



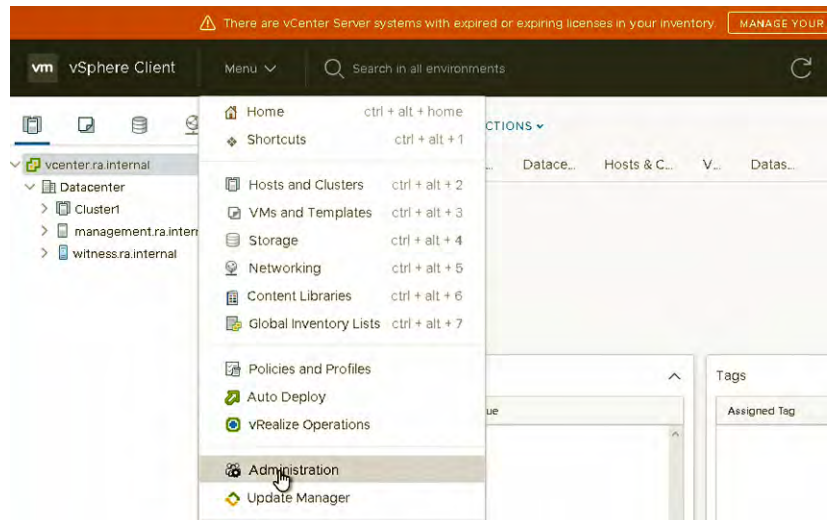
- When finished, click Save.

9. Log off from the VMware ESXi website, and verify that you can log in with the new password.
10. Repeat steps 1...9 for each of the two cluster hosts and the Witness host.
For step 1, use these URL addresses for each ESX host:
 - Host 1: <https://192.168.249.14>
 - Host 2: <https://192.168.249.15>
 - Witness: <https://192.168.249.16>

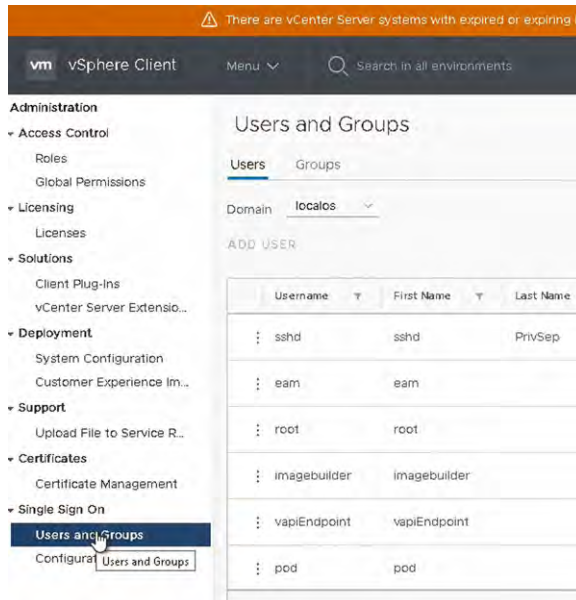
vCenter

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

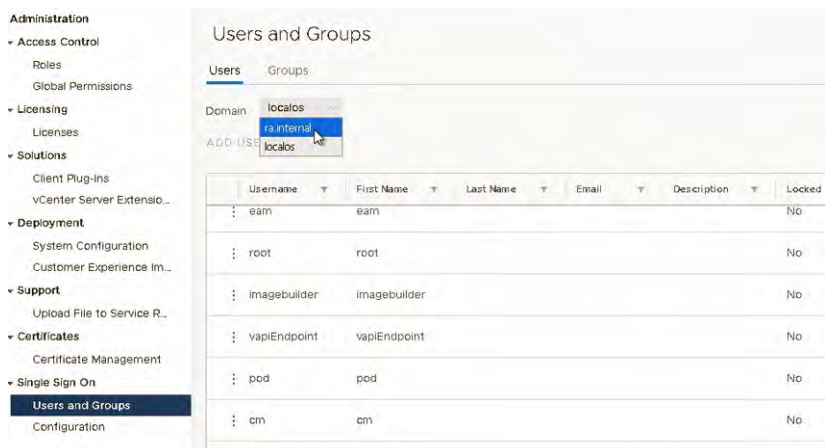
1. Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>
2. On the home page, select Menu > Administration.



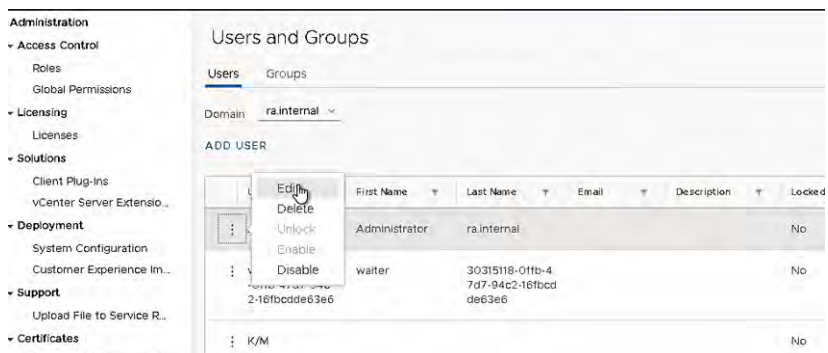
- Under the Administration navigation pane, select Single Sign On > Users and Groups.



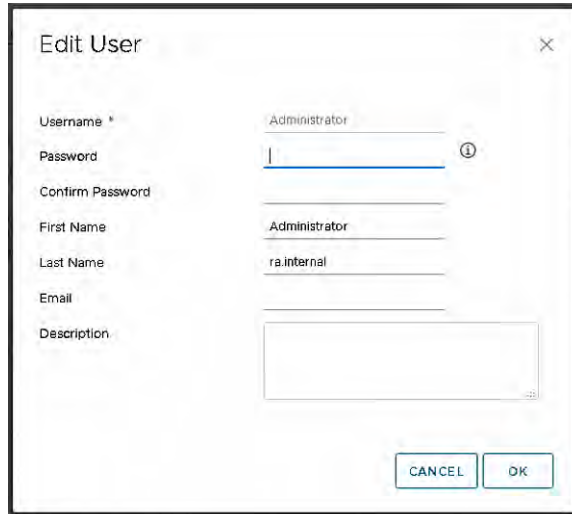
- From the Domain pull-down menu, verify that ra.internal is selected.



- Under the ra.internal domain users, select the Administrator row.
- Click the ellipsis next to the Administrator account.
- From the popup menu, select Edit.



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



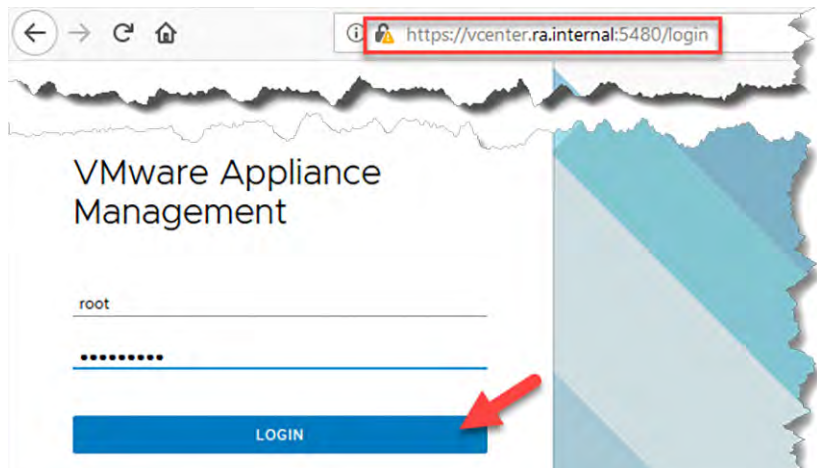
9. When finished, click OK.
10. Log off from the vCenter website, and verify that you can log in with the new password.

vCenter Appliance

To change the password in vCenter Appliance, perform the following steps.

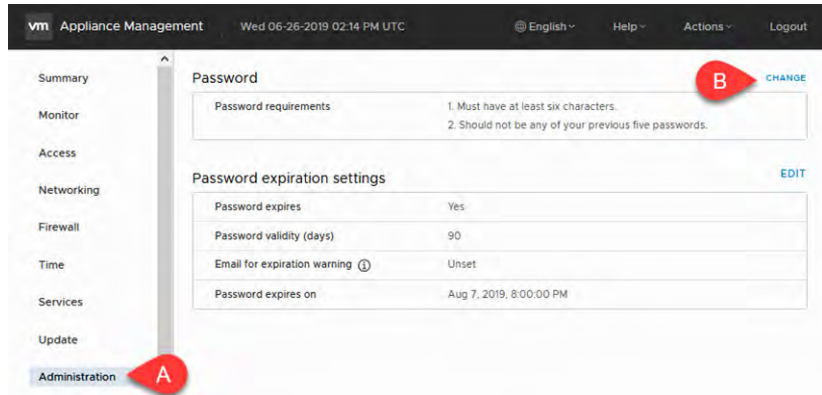
1. In a web browser, enter <https://vcenter.ra.internal:5480/login>.

Note port 5480.



2. Log in to the appliance with root and the system-wide password.

3. In the left column, navigate to Administration (A).
4. On Password, click Change (B).



5. Enter and confirm the New Password.



6. Click Save.
7. Log off the vCenter Appliance, and verify that you can log in with the new password.

Virtual Machines

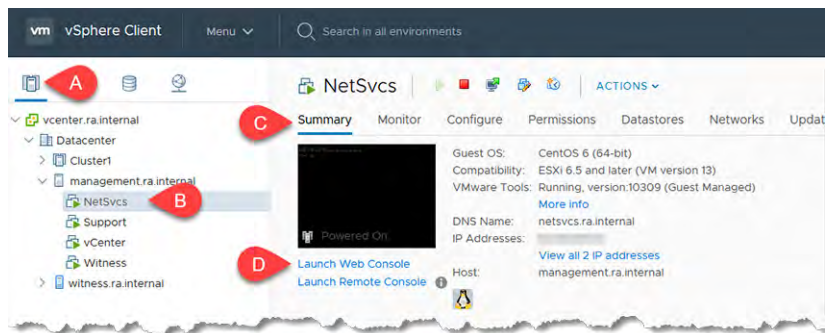
For virtual machines, you must change the password in two areas.

NetSvcs

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

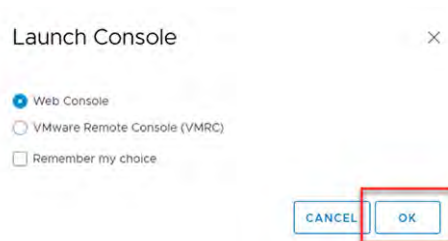
1. Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>

2. On the Hosts and Clusters view (A), expand management.ra.internal and select NetSvcs (B).
3. On the Summary tab (C), click Launch Web Console (D).

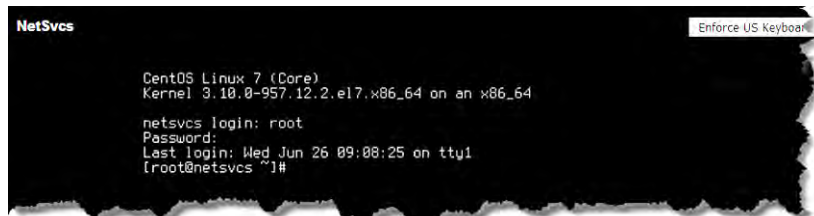


4. On Launch Console, click OK.

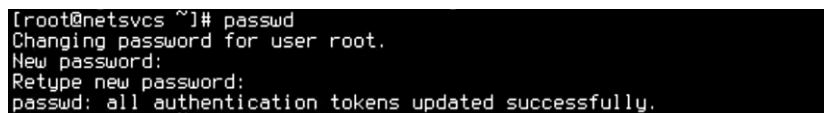
TIP Accept the default Web Console unless you have VMRC already installed.



5. On the CentOS screen, log in as root with the system-wide password.



6. Enter the new password and retype.

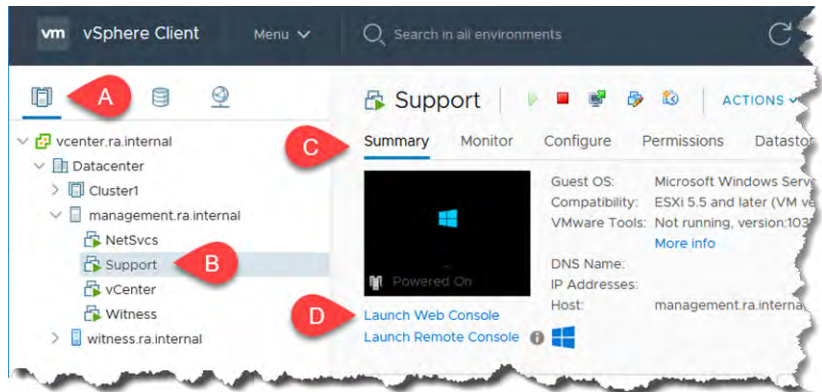


7. Log in as sysadmin and repeat [step 5](#)...[step 7](#).
CentOS prompts user for the current password.
8. When finished, enter log off or press Control+D.

Support

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

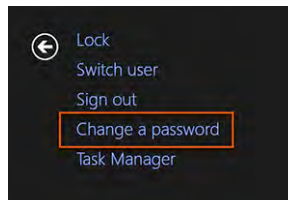
1. Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>
2. On the Hosts and Clusters view (A), expand management.ra.internal and select Services (B).
3. On the Summary tab (C), click Launch Web Console (D).



4. In the upper right corner of the console, click Send Ctrl+Alt+Delete.

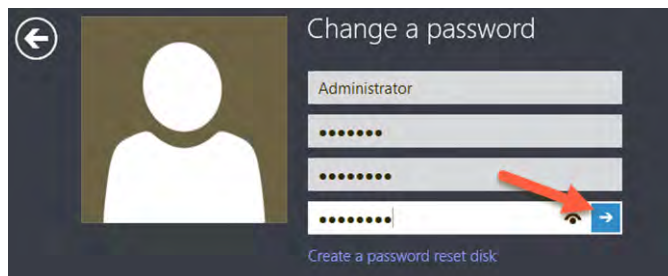


5. Once logged in, press Ctrl+Alt+Delete again, and then click Change a Password.



6. Enter the current password, enter the new password twice to confirm the change.

When finished, click the blue arrow.



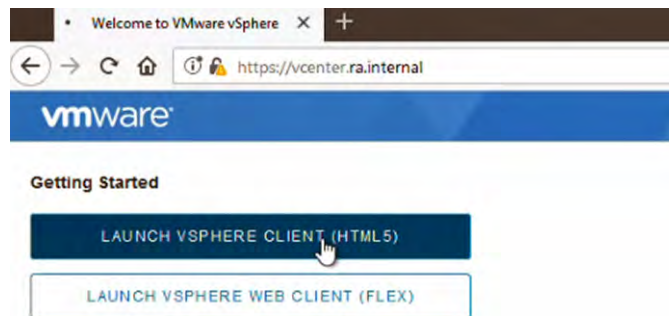
7. Log off Microsoft Windows, and verify that you can log in with the new password.

Configure Active Directory Authentication

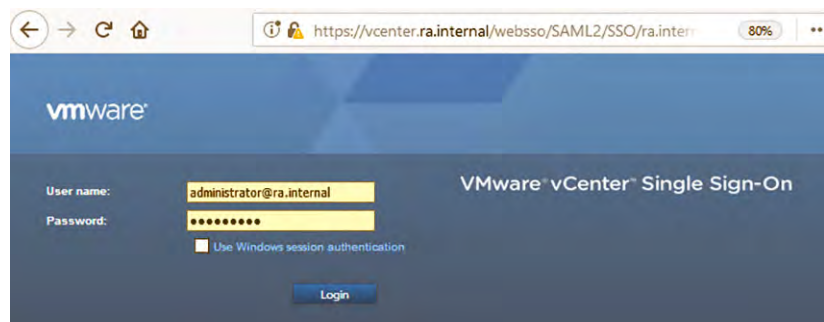
If you want to use domain users to manage VMware vCenter with Active Directory credentials, you can create a Lightweight Directory Access Protocol (LDAP) identity source to manage vCenter.

To create the LDAP identity source, perform the following steps.

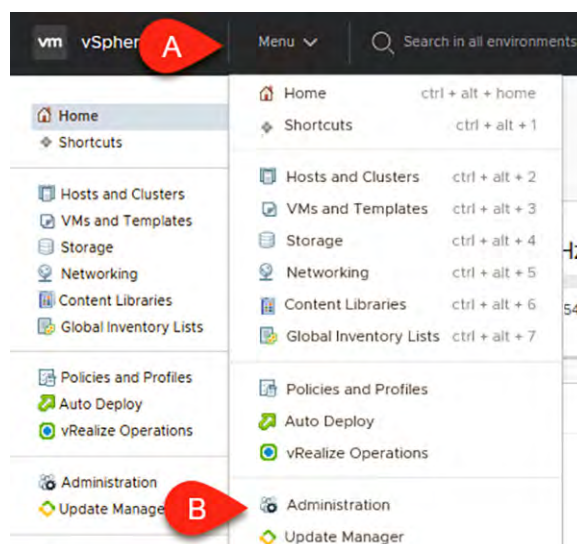
1. Access the VMware® vSphere® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).



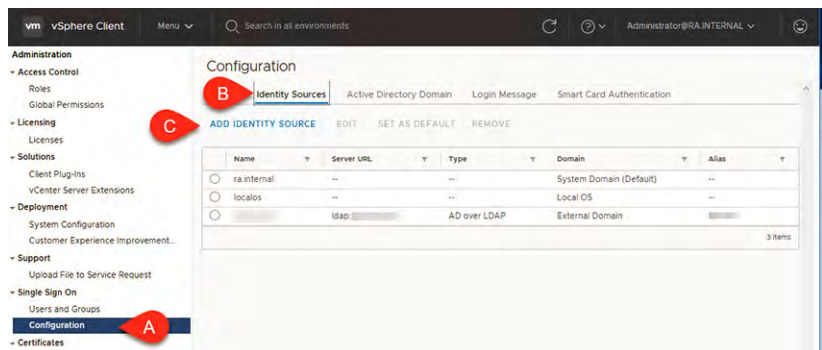
3. Log into the VMware® vCenter® as administrator@ra.internal with the system-wide password.



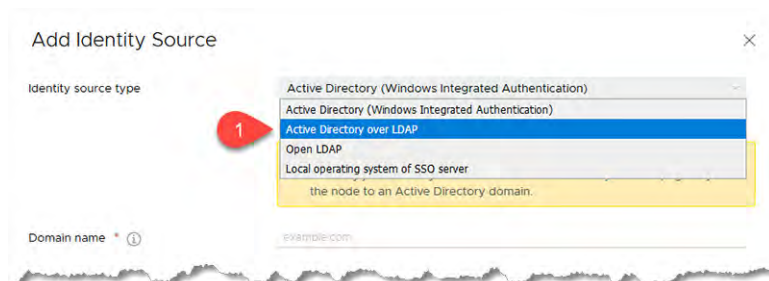
4. In the vSphere Web Client, select Menu (A) > Administration (B).



5. In the Administration navigation view, select Configuration (A).
 - a. On Configuration, click the Identity Sources tab (B).
 - b. On Identity Sources, click Add Identity Source (C).



6. In the Add Identity Source wizard, select Active Directory as an LDAP server.



7. In the Domain name field, add the following.
 - a. For **Name**, enter the domain name (DN).
 - b. 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='.

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

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

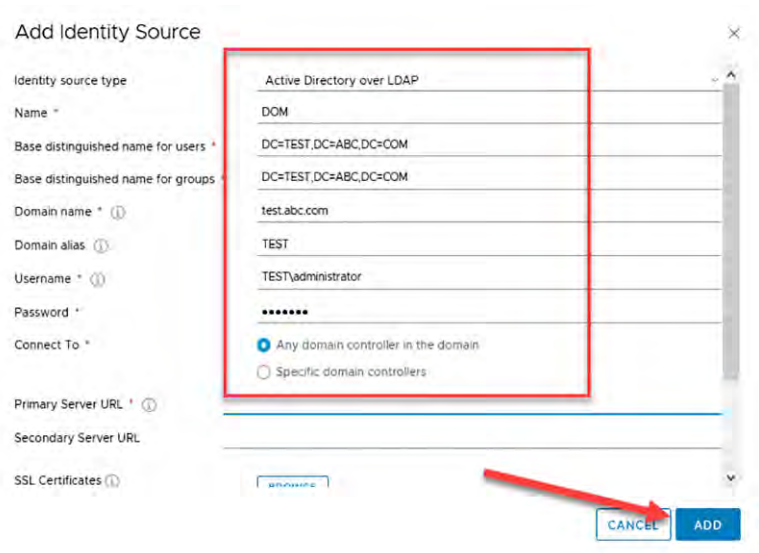
TIP This string is not case-sensitive. For more information, see [https://msdn.microsoft.com/en-us/library/aa366101\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa366101(v=vs.85).aspx).

- c. For the **Base DN for groups**, enter the same DN string as above.
- d. For **Domain name**, enter the FQDN.
- e. For **Domain Alias**, enter the NetBIOS alias of the domain. By default, it is the first portion of the FQDN.

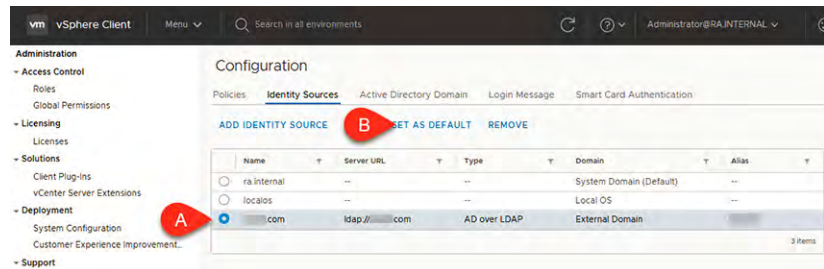
For example: If the FQDN is 'example.com', enter the NetBIOS alias of 'Example'.

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

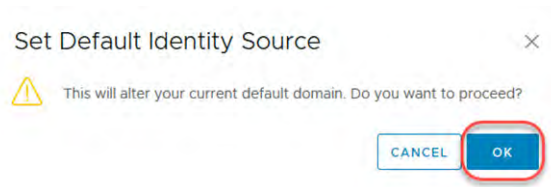
- f. For **Username**, enter a domain user account that has administrative privileges in the domain.
- g. Enter the password for the administrative user.
- h. Click Add.



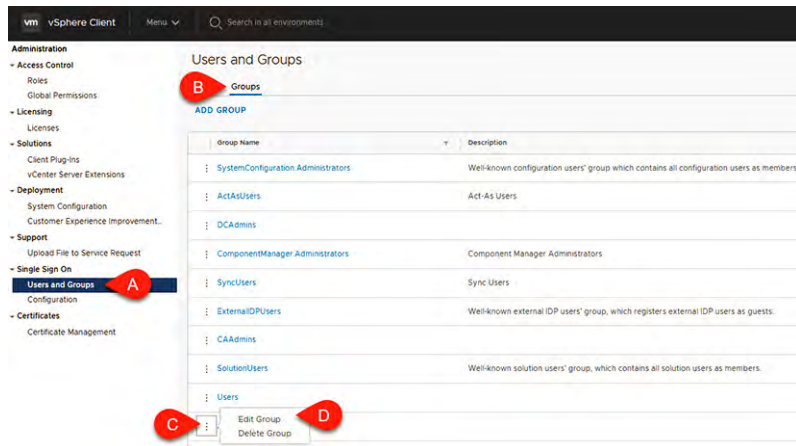
- 8. Select the newly created Identity Source (A), and then click Set as Default Domain (B).



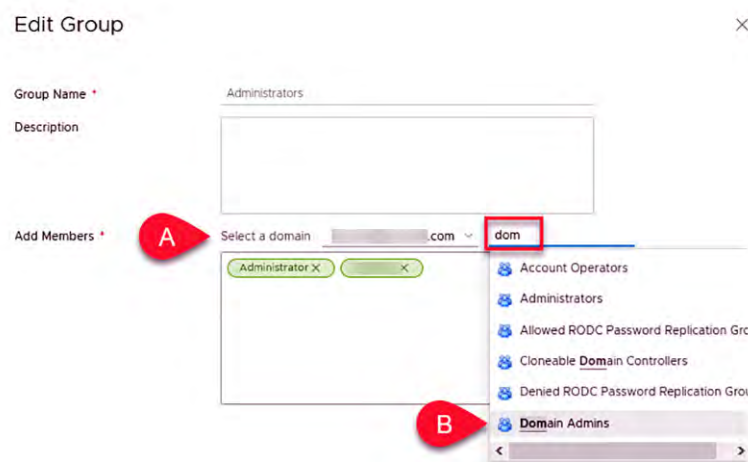
- 9. A warning appears; click OK.



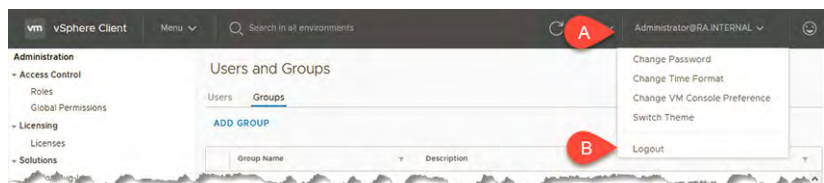
10. In the Administration navigation view, select Users and Groups (A).
 - a. On Users and Groups, click the Groups tab (B).
 - b. On Groups, click the ellipse next to the Administrators group (C).
 - c. From the pull-down menu, select Edit Group (D).



11. In the Edit Group window:
 - a. From the Select a Domain pull-down menu, select the newly added Windows Active Directory (A).
 - b. In the search field, type 'dom' and select the Domain Admins user group from the search finds (B).

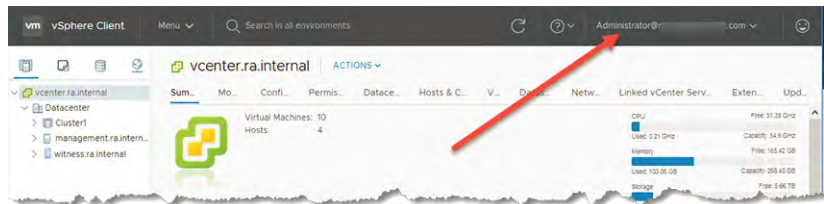


12. Click OK.
13. Click the user name in the top right of the window (A).
 - From the pull-down menu, select Logout (B).



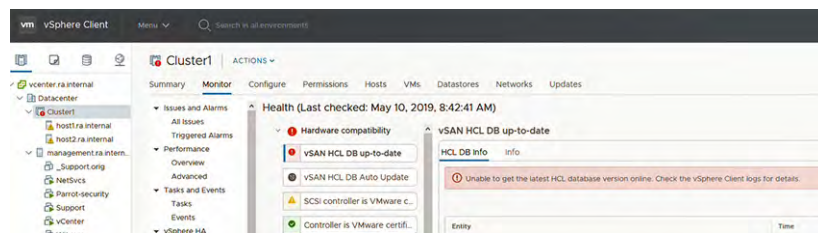
- At the vSphere web client login prompt, use your new Domain Admin credentials to log in.

Verify that the authentication is successful.



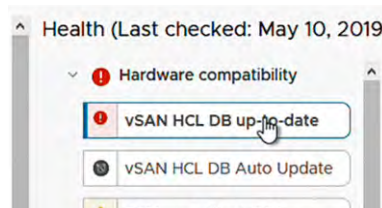
Update the Hardware Compatibility List

You must manually update the Hardware Compatibility List (HCL) if you receive an error that the VersaVirtual Appliance cannot automatically access the most current version. A current HCL is critically important to the stability of vSAN environments.

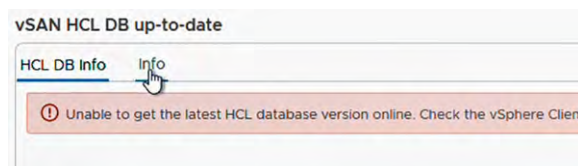


To update to the most current HCL version, perform the following steps.

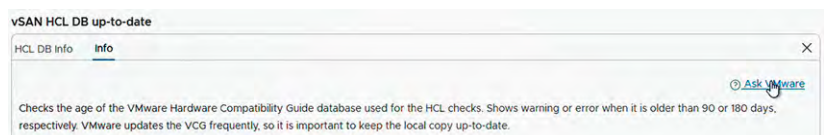
- Click the alert about the outdated vSAN HCL DB.



- Click the Info tab.



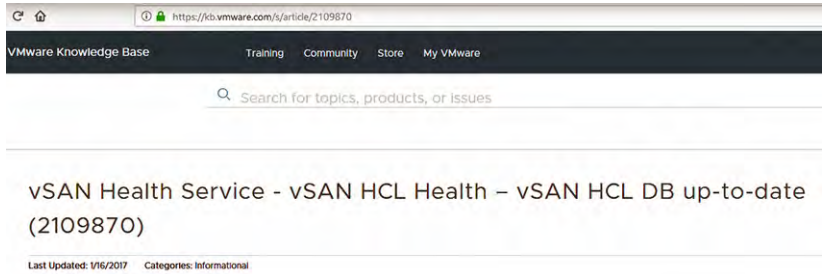
- On Info, click Ask VMware.



TIP

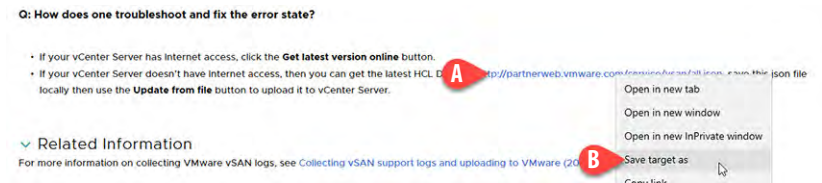
The following address accesses the same VMware Knowledge Base article: <https://kb.vmware.com/s/article/2109870>

You are now on the VMware Knowledgebase site about the outdated HCL issue.

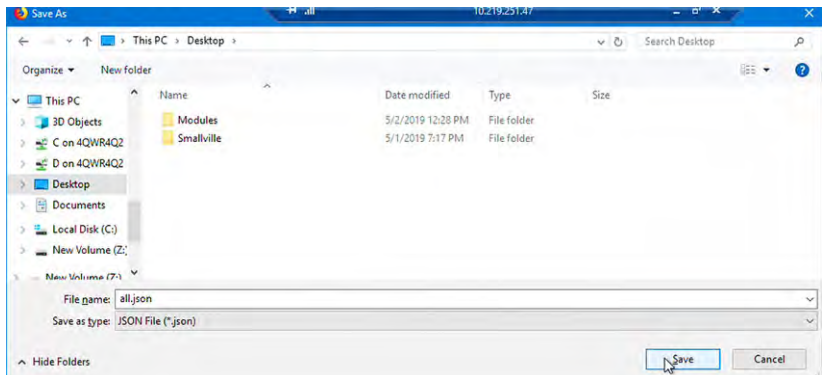


4. Scroll down to the content that includes a link to an updated database (for a JSON file).
5. Highlight the provided URL address (A).

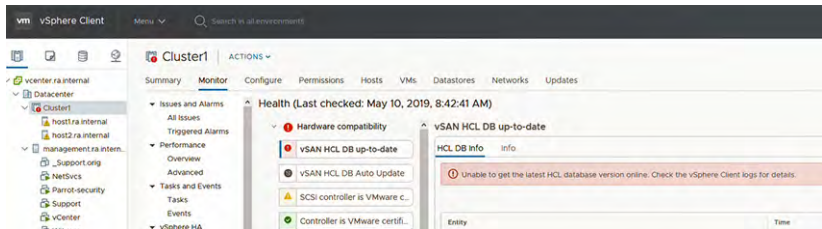
Depending on your browser, right-click on the link and select Save Link As or Save Target As (B).



6. Navigate to your computer desktop and click Save.

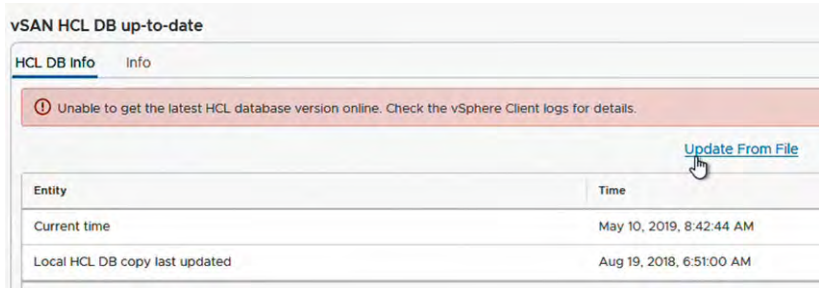


7. Return to vSphere Client.

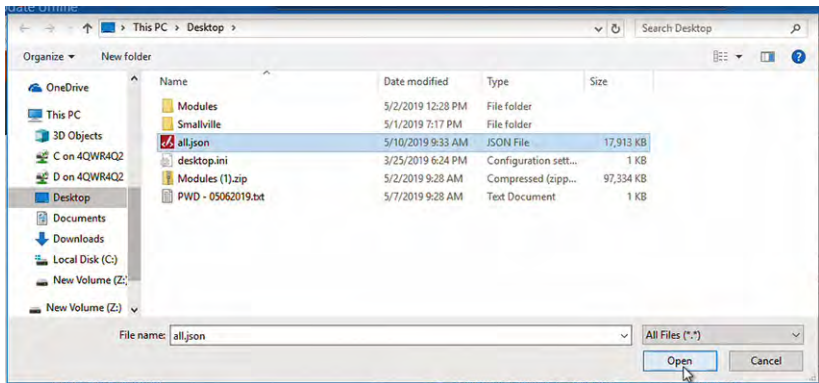


8. Click the HCL DB Info tab.

- On HCL DB Info, click Update from File.



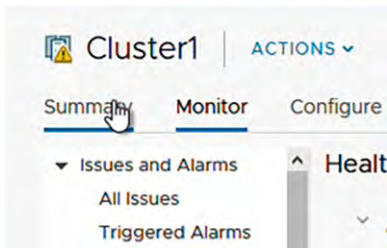
- Navigate to your computer desktop. Highlight the downloaded JSON file and click Open.



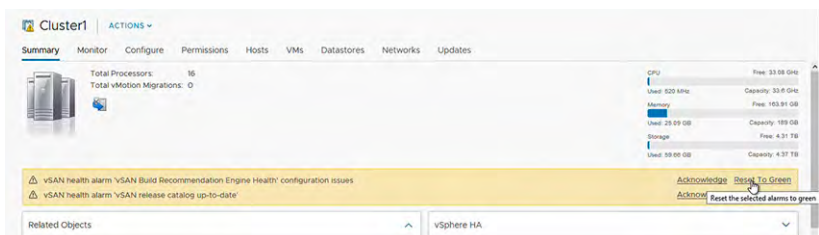
Once updated, the Entity reflects the update.



- On Cluster1, click the Summary tab.



- For each alert line highlighted in yellow, click the corresponding Reset to Green.



Each host under Cluster1 shows an alert because the updated JSON file is stored ‘on non-persistent storage’ (your computer’s desktop).

You can ignore these warnings.

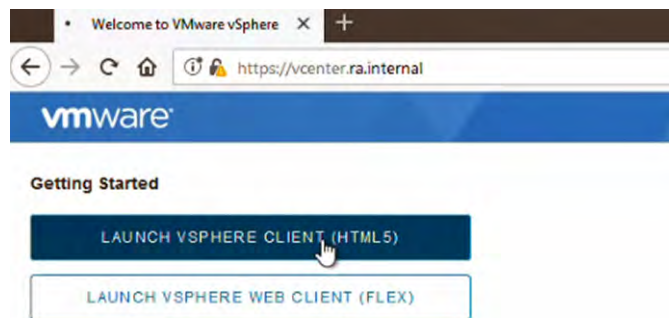


The VersaVirtual Appliance now has the most current HCL.

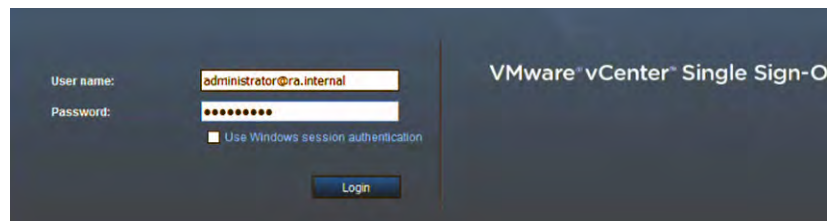
Add a Distributed Port Group

To add a distributed port group, perform the following steps.

1. Access the following VMware website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).

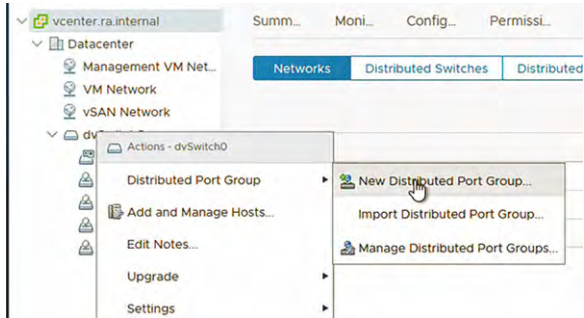


3. Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>



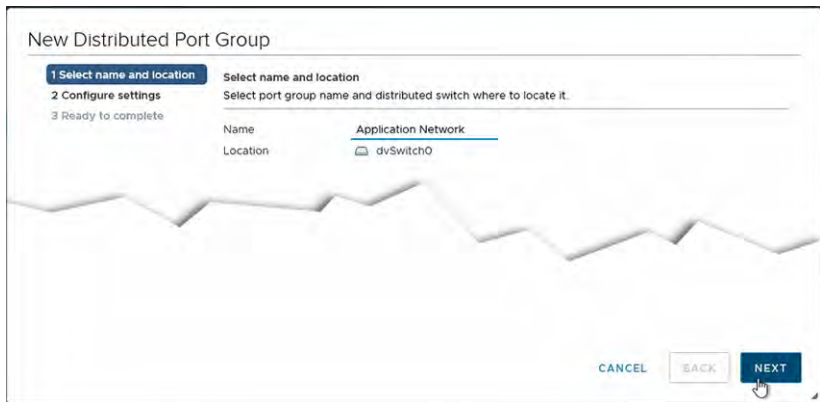
4. Click Login.

- On the main Navigation pane, right-click on dvSwitch0 and select Distributed Port Group > New Distributed Port Group.

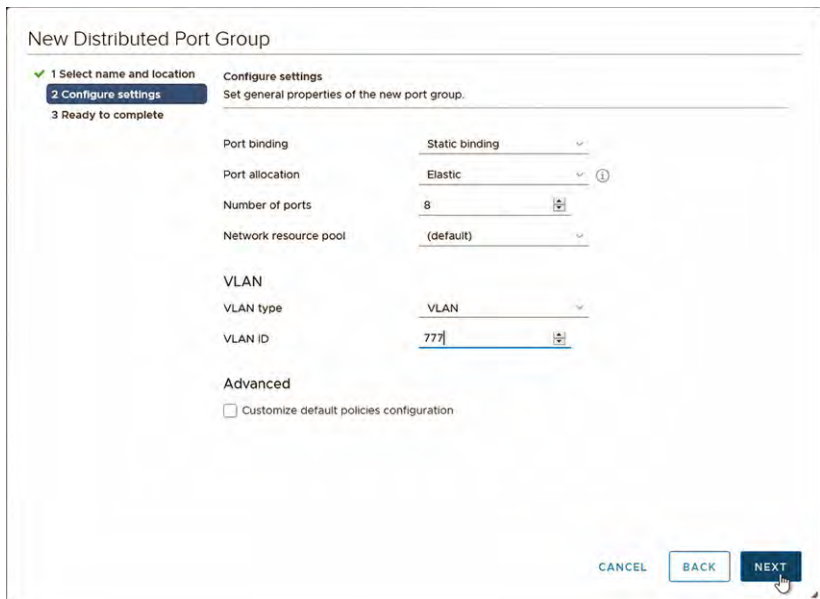


- On step 1 of New Distributed Port Group, add a name for your new port group (Application Network is only used for this example).

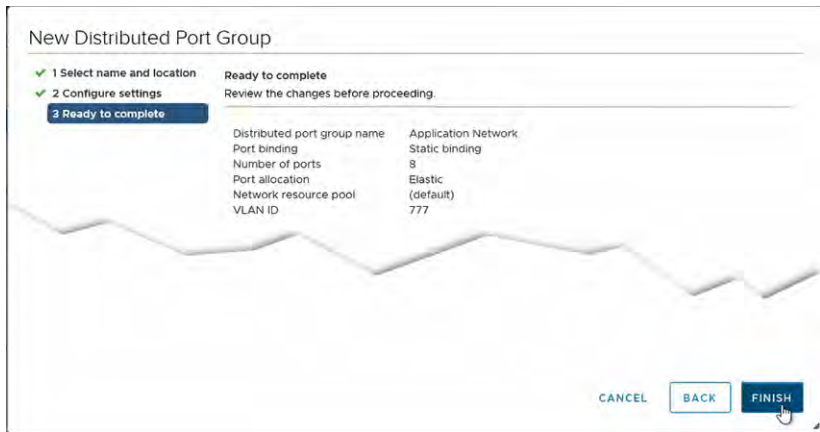
Click Next.



- On step 2, select the following:
 - For VLAN type, select VLAN from the pull-down menu.
 - For VLAN ID, select a number appropriate for your application.



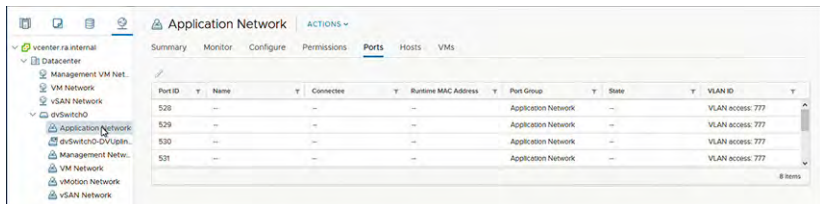
8. On step 3, review your additions and changes.
If satisfied with your choices, click Finish.



On the Navigation pane, the new distributed port group (Application Network) is now visible under dvSwitch0.

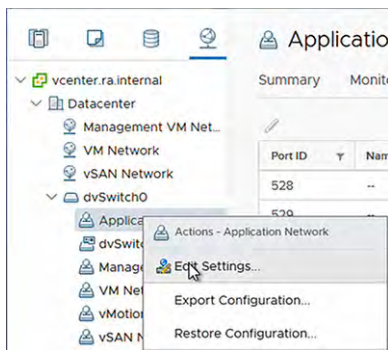
9. Highlight Application Network.

If not already visible, click the Ports tab on the Application Network page.

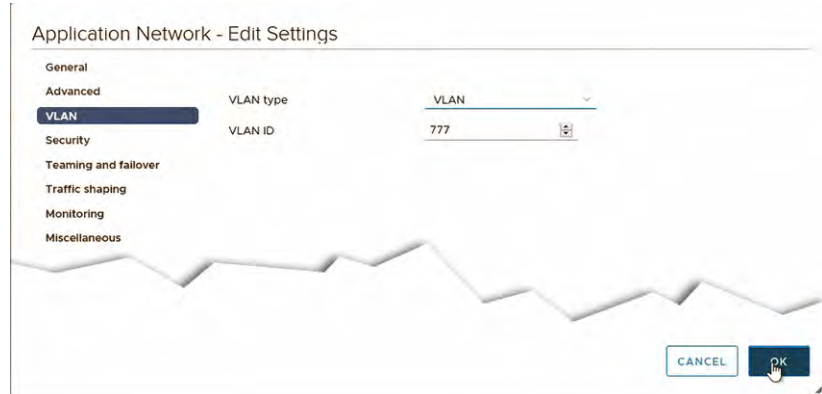


10. Verify that each port shows the same VLAN ID number that you added in [step 7](#).

11. With Application Network still highlighted, right-click and select Edit Settings.



- Verify that the VLAN ID is the same as what you added in [step 7](#) on [page 93](#).

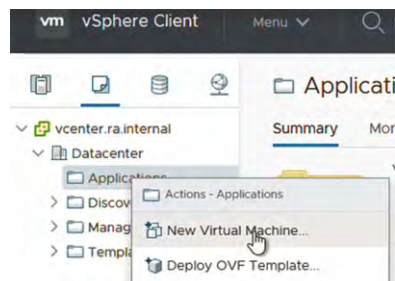


- Click OK after the number is changed or verified.

Add a Virtual Machine

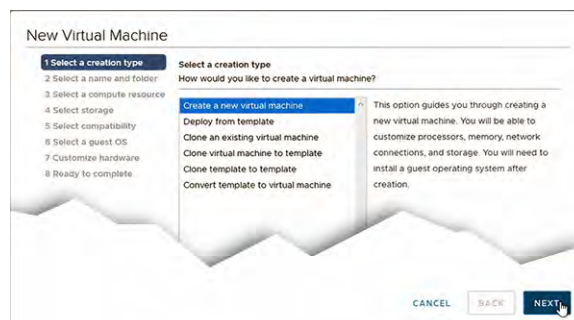
To add a virtual machine, perform the following steps.

- Log into the vCenter web GUI with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>
- On the Actions Navigation pane, right-click on Applications and select New Virtual Machine from the pull-down menu.

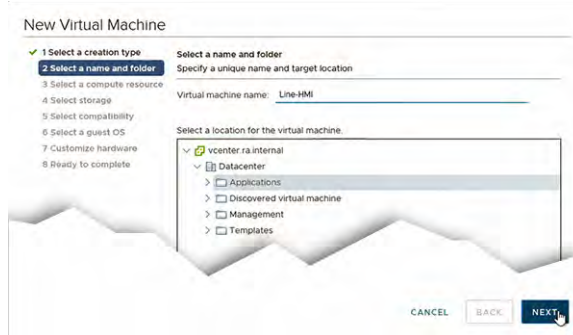


- For step 1 of New Virtual Machine, verify that 'Create virtual machine' is highlighted.

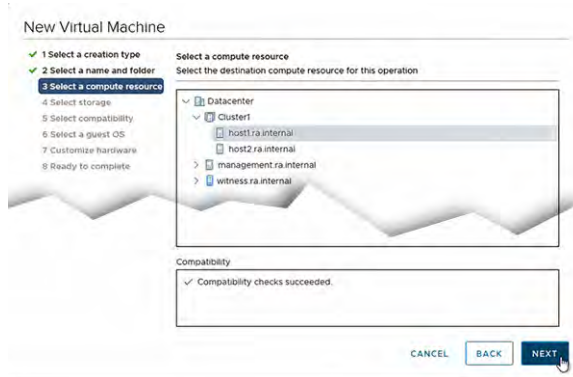
Click Next.



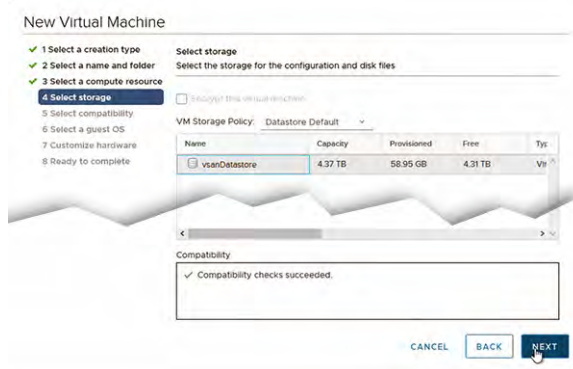
4. For step 2, perform the following:
 - a. Name your new virtual machine
 - b. Select the Applications folder as the new virtual machine location
 - c. Click Next.



5. For step 3, perform the following:
 - a. Select host1.ra.internal as the compute resource location.
 - b. Verify that the compatibility check is successful.
 - c. Click Next.



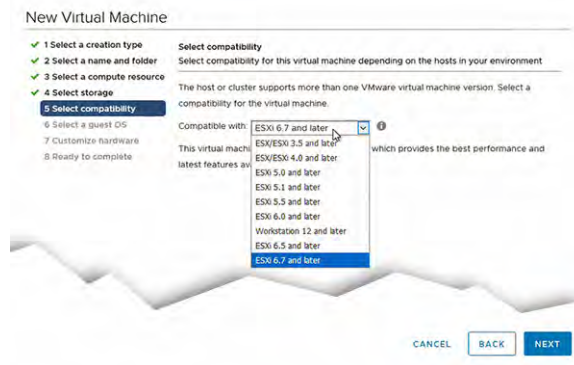
6. For step 4, perform the following:
 - a. Select vSanDatastore for your data storage location.
 - b. Verify that the compatibility check is successful.
 - c. Click Next.



- For step 5, select the version of VMware ESXi software from the pull-down menu that is most compatible for your application. In this example, the most current version of 6.7 is selected.

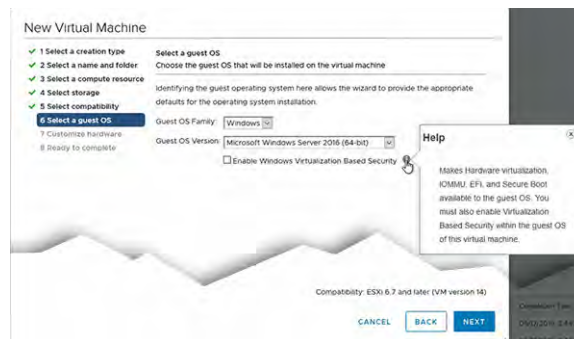
IMPORTANT After the new virtual machine is deployed, you cannot change the compatibility to an earlier version, only to a newer version.

Click Next.



- For step 6, select the operating system and version that you are using.

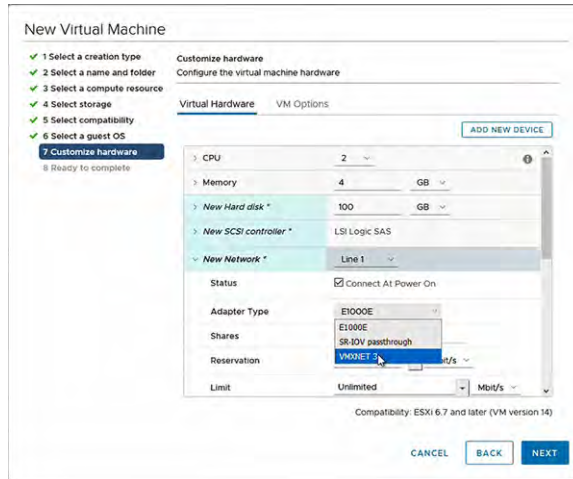
Click Next.



- For step 7, configure any fields so the new virtual machine is set up for your application.

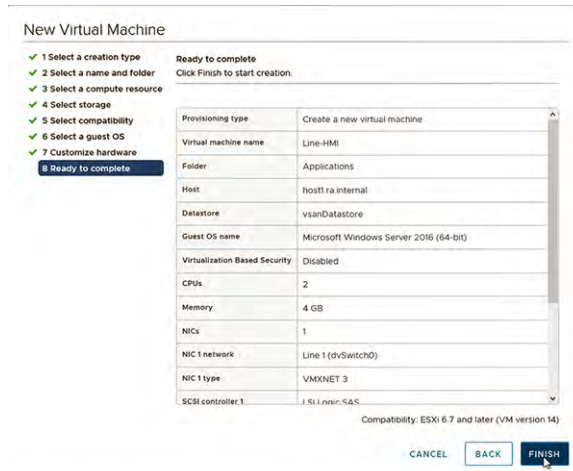
IMPORTANT The default setting for adapter type is E1000E. From the pull-down menu, select VMXNET 3, which is recommended.

Click Next.

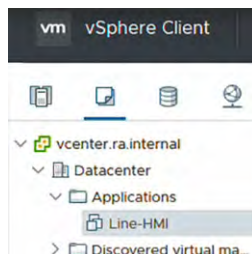


- For step 8, review the information that you added for your new virtual machine.

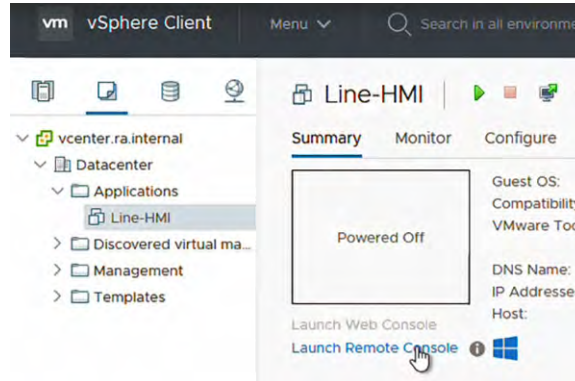
If you must modify any information, click Back. If you are satisfied with the information, click Finish.



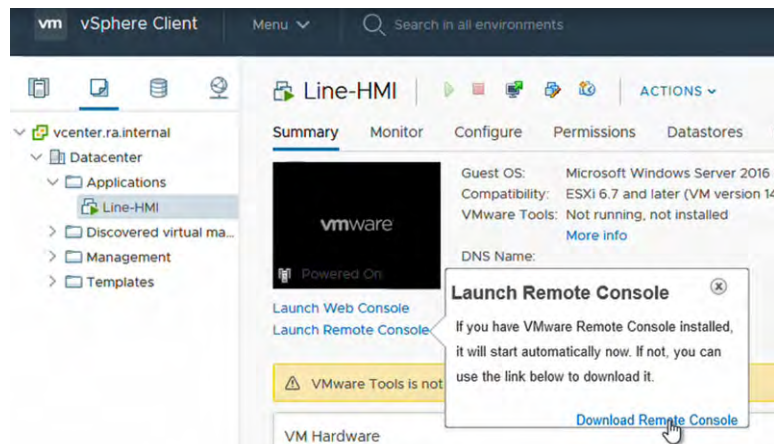
The new virtual machine is now visible under Applications in the Actions Navigation pane.



- On the Summary tab of the new virtual machine, click Launch Remote Console.

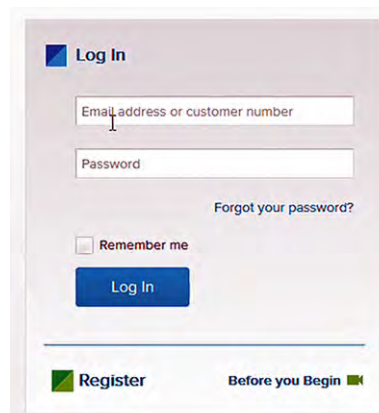


A popup window appears about the VMware Remote Console installation.



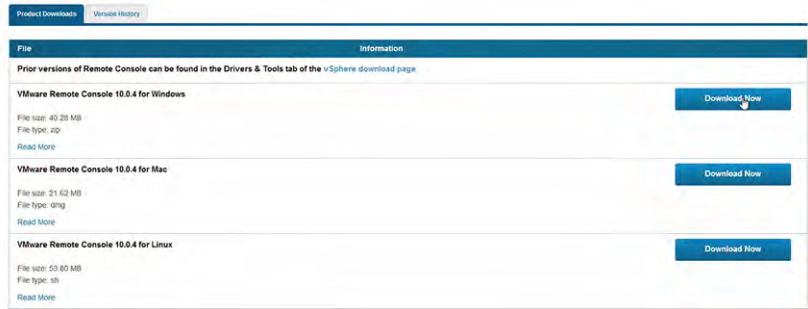
- To install, click Download Remote Console.
- Log into VMware with your email address or customer number, and password.

IMPORTANT If not already done, you must create a VMware account to log into the site and download the remote console. To create an account, click Register on the Log In screen.

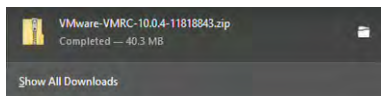


After you log in, you are automatically directed to the Remote Console Download page.

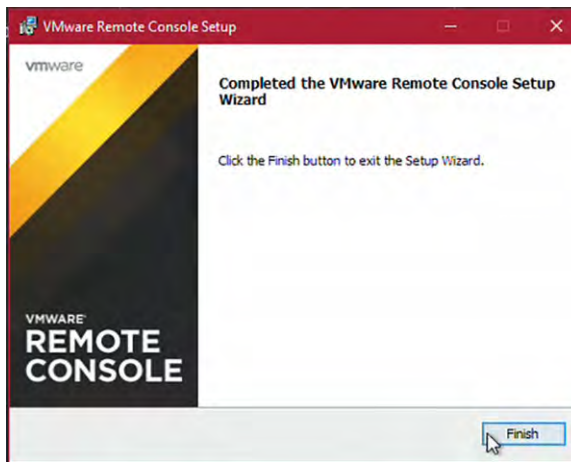
- 14. Click Download Now.



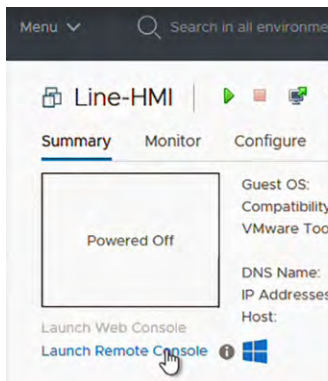
The downloaded file is a WinZip file.



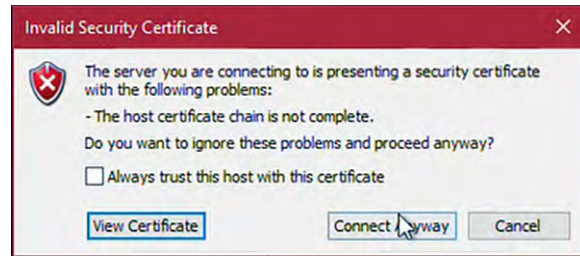
- 15. Open the WinZip file and launch the EXE application file.
The VMware Remote Console Install Wizard appears.
- 16. Accept the end-user license agreement and install the software application.
- 17. Click Finish when the installation is complete.



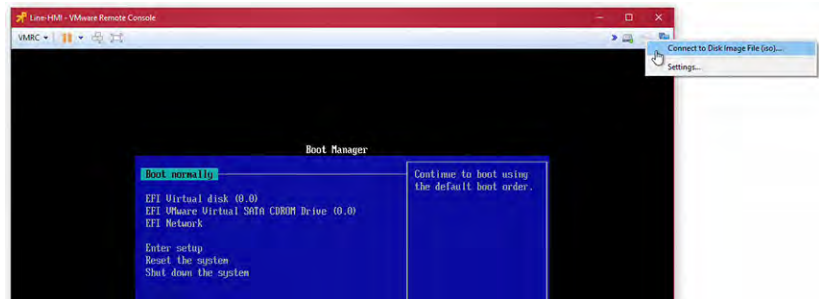
- 18. Launch the VMware Remote Console application.



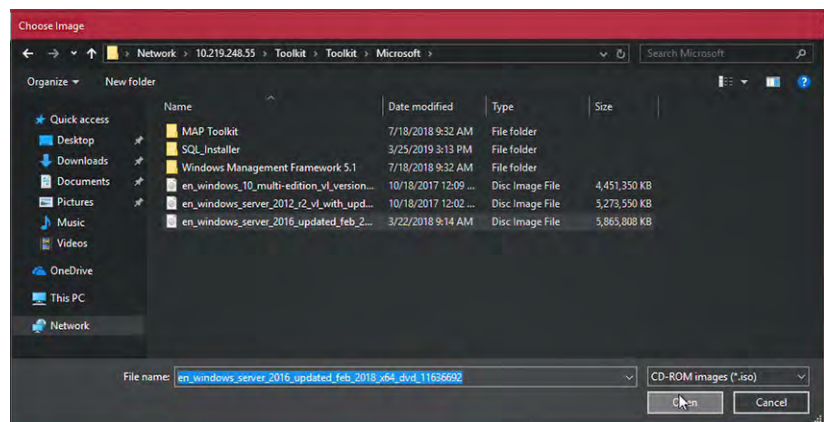
TIP If you receive an invalid security certificate warning, click Correct Anyway.



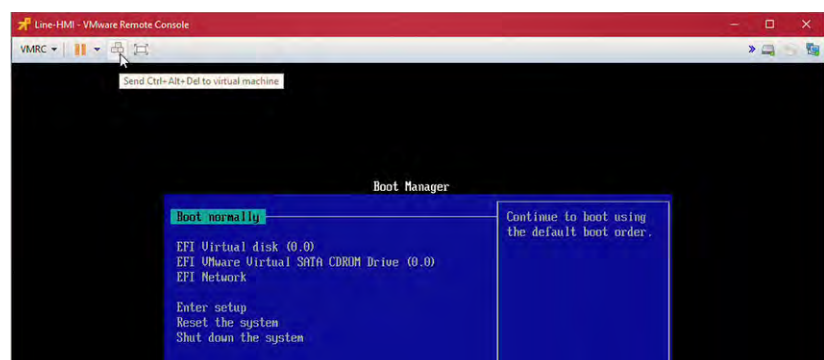
19. On the Boot Manager screen, click the disk image on the quick access toolbar and select 'Connect to Disk image file (iso).'



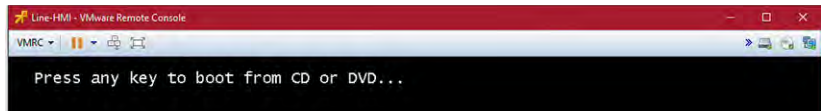
20. Navigate to the network address for available disk image files.
21. Highlight the most current disk image file and click Open.



22. On the Boot Manager screen, click the Send Ctrl+Alt+Delete icon on the quick access toolbar.



- As instructed, press any key to start the Windows installation.



The setup screen appears for the chosen Windows OS.

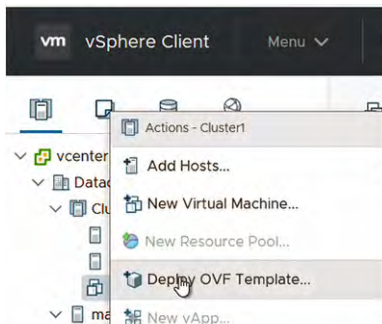
- Follow the various screen prompts to install Windows.

The new virtual machine is successfully added to your network.

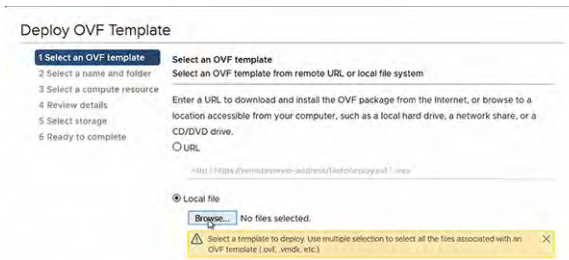
Import an OVA Template

To import an OVA template, perform the following steps.

- Log into <https://192.168.249.18> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>
- On the Main Navigation pane, right-click on Clusters and select Deploy OVF Template from the pull-down menu.

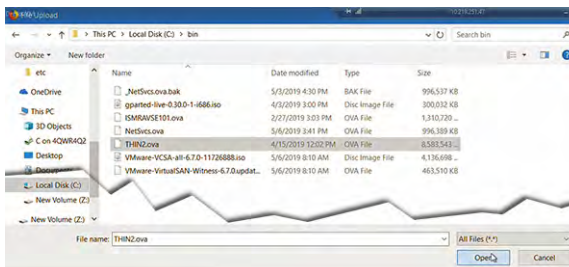


- On step 1 of Deploy OVF Template, click Local File, and then Browse.

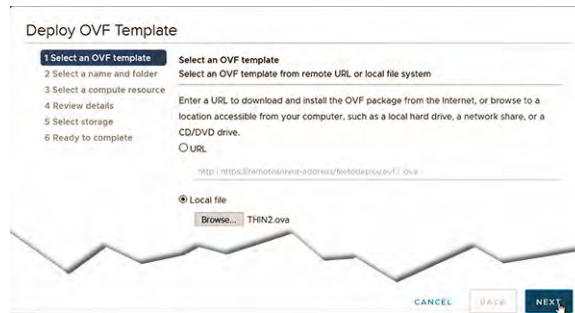


- Navigate to the bin folder on your personal computer and select an OVA file specific to your application.

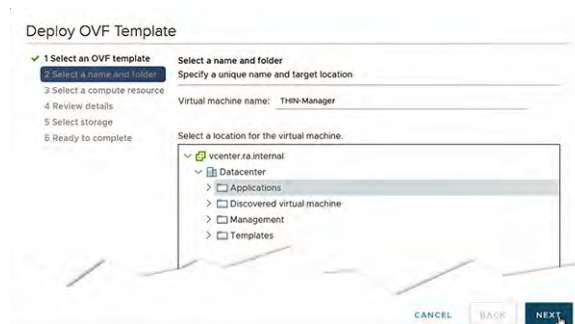
Click Open.



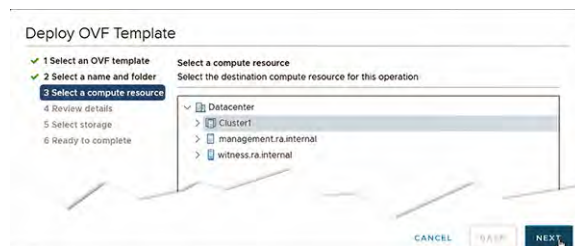
- The OVA file that you chose appears next to the Browse button. Click Next.



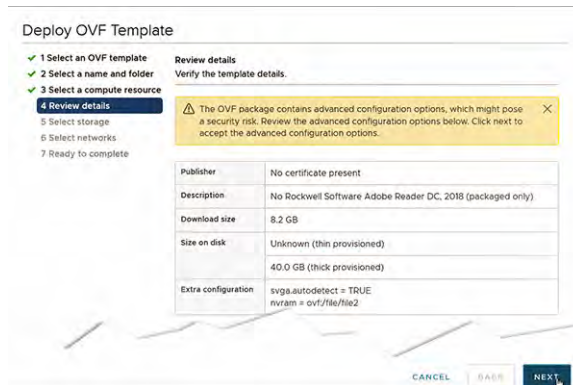
- On step 2, perform the following:
 - Change the virtual machine name to something more specific to your application.
 - Select the location for the virtual machine.
 - Click Next.



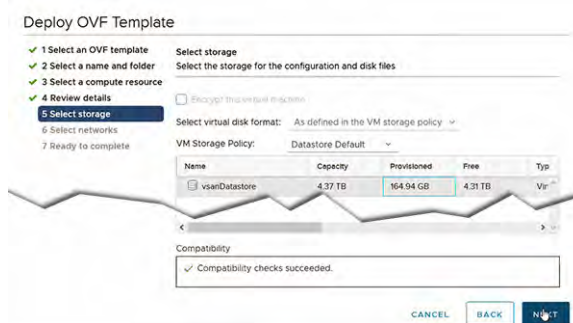
- On step 3, select the resource for this operation. Click Next.



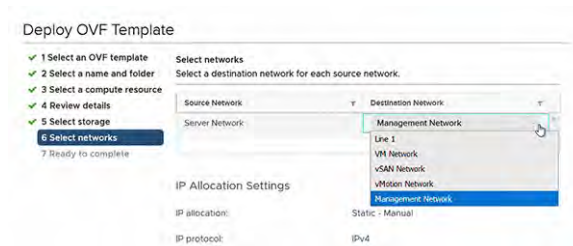
8. On step 4, review the details of the template that you chose. Click Next.



9. On step 5, select the storage for the OVA file. Click Next.

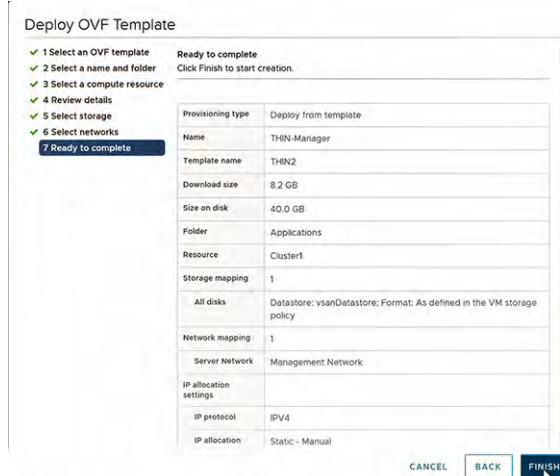


10. On step 6, select the desired port group from the pull-down menu underneath the Destination Network. Click Next.

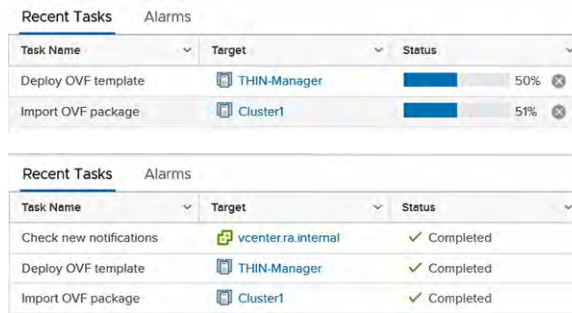


- On step 7, verify the selections that you made.

If you must modify any information, click Back. If you are satisfied with the information, click Finish.



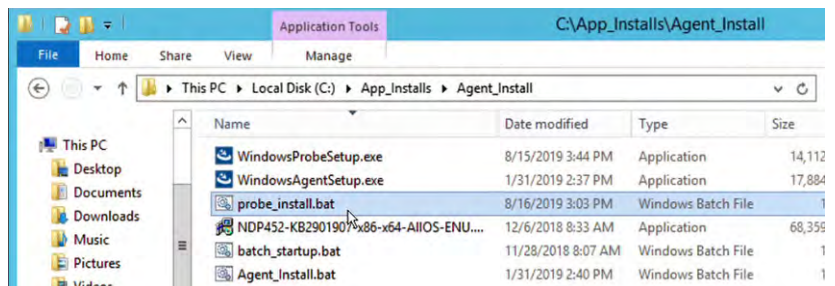
- On the Recent Tasks panel of Cluster1, you can verify if the OVF template was deployed correctly and completed.



Install VSE Software

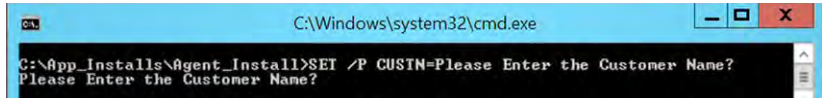
To install the VSE remote access and monitoring service software, perform the following steps.

- To access this software, follow step 1...step 4 in [Support on page 84](#).
- Open Windows Explorer.
- Navigate to C:\App_Installs\Agent_Install.
- Locate the probe_install.bat file and double-click it.



The batch file opens in the Windows Command Prompt program.

- 5. When prompted, enter your supplied customer name and then press Enter.

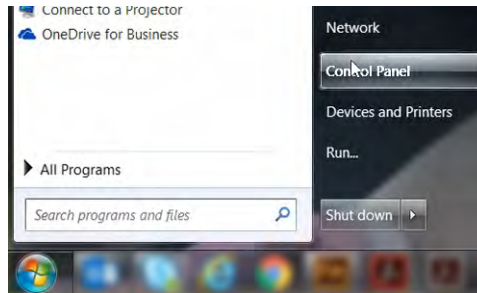


- 6. When prompted, enter your supplied customer ID and then press Enter.

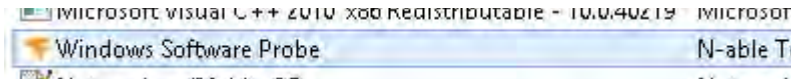


When the installation is finished, the Command Prompt program closes.

- 7. Verify that the installation was successful.
 - a. Under Microsoft Windows® Start, select Control Panel.



- b. In Control Panel, select Programs and Features.
 - c. Verify that Windows Software Probe is in the list of installed programs.



- d. Close the window.

System Shutdown and Startup

Topic	Page
Shut Down the VersaVirtual Appliance	107
Start Up the System	116

This section addresses the methods by which you can shut down and start up the VersaVirtual™ Appliance.

Shut Down the VersaVirtual Appliance

You can shut down the VersaVirtual Appliance through a script or manually.

IMPORTANT For consistency and expediency, Rockwell Automation recommends that you use the scripted method.

Scripted Shutdown

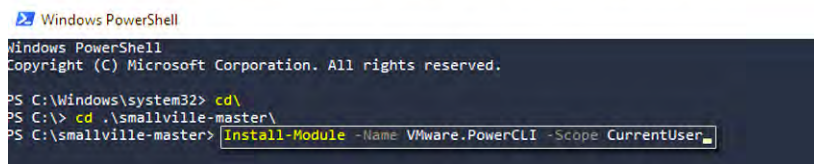
To shut down the VersaVirtual Appliance through a script, perform the following steps.

1. Download the latest shutdown script from the Rockwell Automation Knowledgebase site at https://www.rockwellautomation.com/en_NA/support/overview.page.

Use VersaVirtual as your search criteria.

2. From the Windows® Start menu, launch Windows PowerShell.
3. To import modules so PowerShell can function properly, type the following.

```
Install-Module -Name VMware.PowerCLI -Scope CurrentUser
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd\
PS C:\> cd .\smallville-master\
PS C:\smallville-master> Install-Module -Name VMware.PowerCLI -Scope CurrentUser
```

Press Enter.

4. To permit unsigned scripts, reset the PowerShell execution policy.

IMPORTANT For security reasons, it is important to set the scope to the current process, which helps prevent unauthorized scripts from executing after deployment is complete.

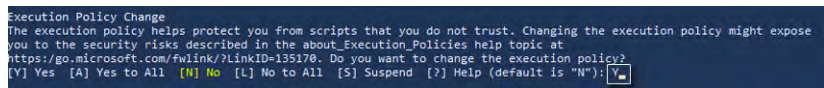
- a. Type the following, and then press Enter.

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
```



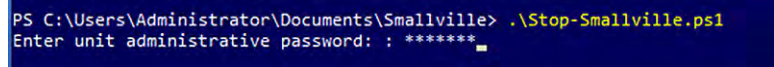
An Execution Policy Change alert appears.

- b. To change the policy, press Y and then press Enter.

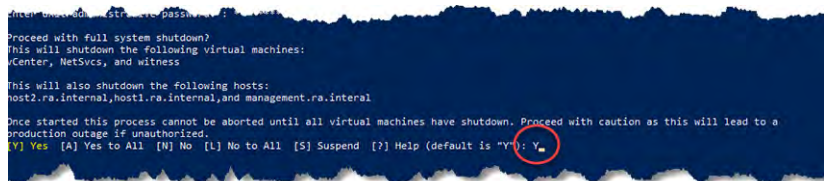


5. At the PowerShell prompt, type the following:

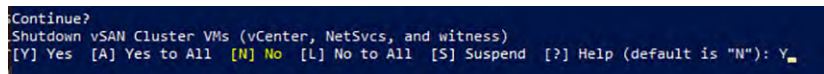
```
.\Stop-Smallville.ps1
```



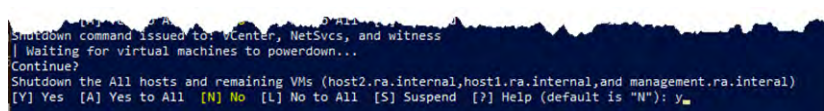
6. When prompted, enter the system-wide password.
7. When asked to proceed, type Y for Yes.



8. When prompted to continue, type Y for Yes again.

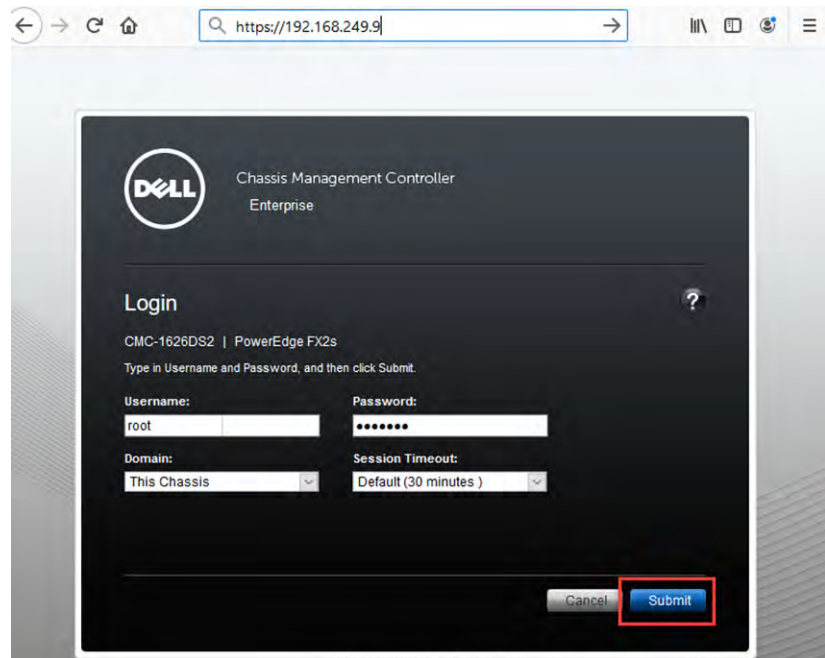


9. When prompted again to continue, type Y for Yes.

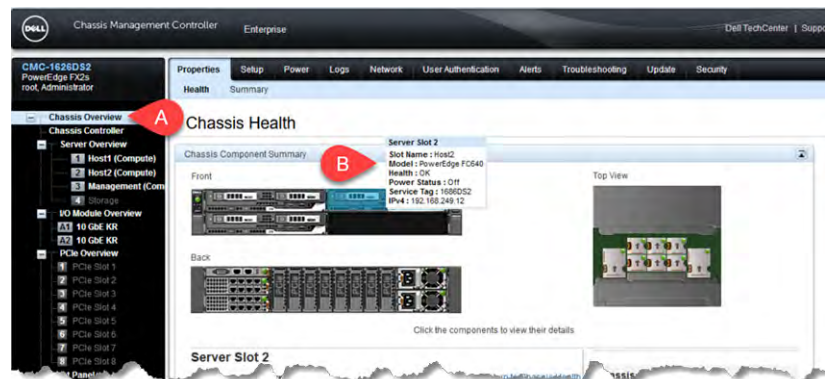


10. Access the Chassis Management Controller (CMC) through a browser at <https://192.168.249.9>.

Log in as root with the system-wide password, and click Submit.



11. On Chassis Overview (A), hover your mouse pointer over each host (B) to verify that all three hosts are powered off.
12. Verify that the green lights on the three hosts are turned off.



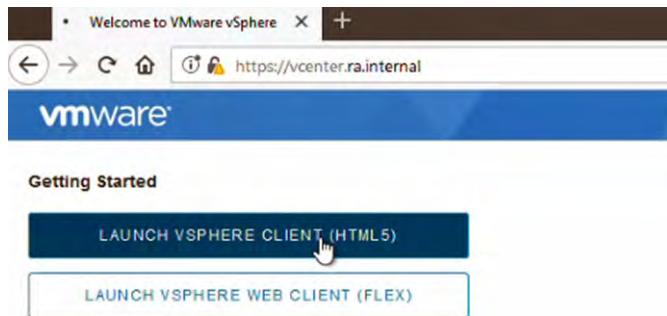
All virtual machines and hosts shut down.

Manual Shutdown

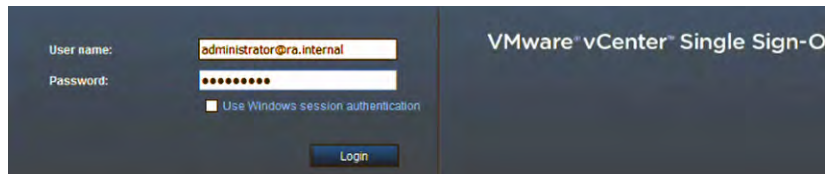
To shut down the VersaVirtual Appliance, perform the following steps.

Shut Down the vSAN Virtual Machines

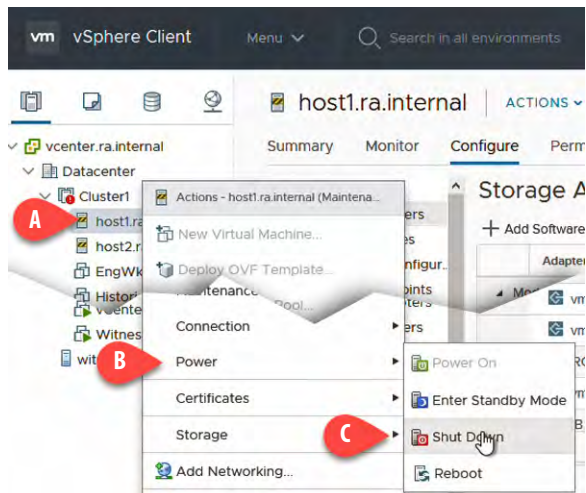
1. Access the following VMware® website: <https://vcenter.ra.internal>.
2. Under Getting Started, click Launch vSphere Client (HTML5).



3. Log into <https://vcenter.ra.internal/ui> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>



4. On the main navigation pane, click the Hosts and Clusters icon.
5. Expand Cluster1 to see all its virtual machines.
6. Right-click on a virtual machine name (A).
7. From the pull-down menu, select Power (B) > Shut Down (C).



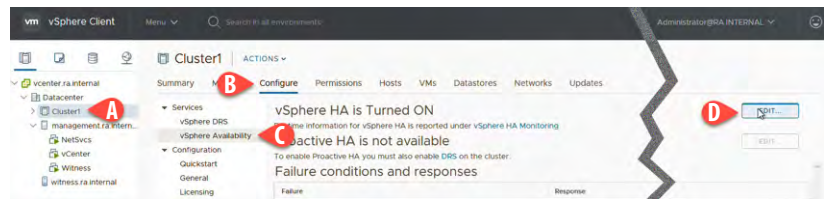
8. Repeat steps 6 and 7 for each virtual machine that is part of Cluster1.

Shut Down the vSAN Cluster

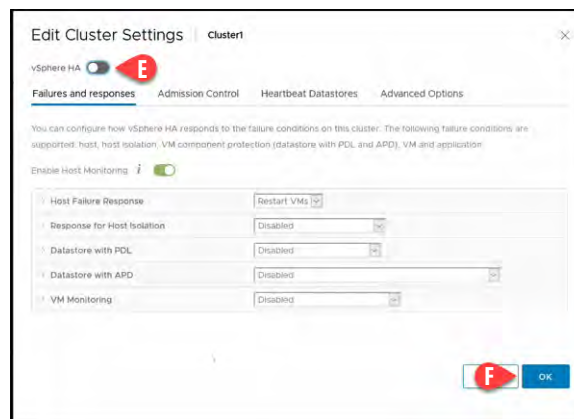
IMPORTANT You must first perform the steps in [Shut Down the vSAN Virtual Machines on page 110](#) before you perform these steps.

The following steps assume that you have shut down all vSAN virtual machines and you remain logged into the VMware website.

1. On the main Navigation pane, highlight Cluster1 (A).
2. On the Cluster 1 pane, click the Configure tab (B).
3. From the Services pull-down menu, select vSphere Availability (C).
4. Click the Edit button across from vSphere HA is Turned ON (D).



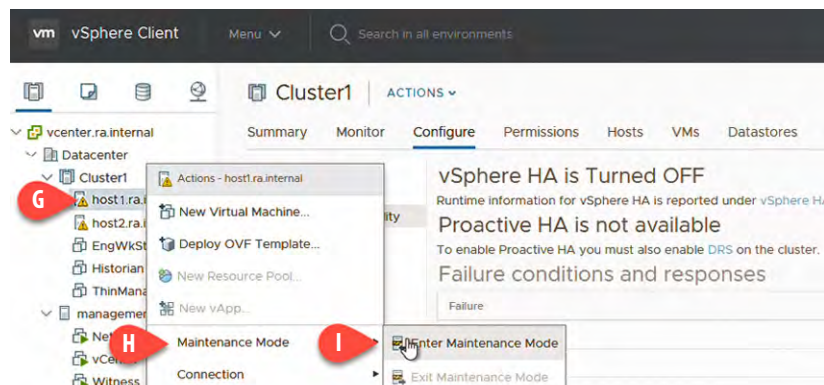
5. On Edit Cluster Settings, disable vSphere HA (E).



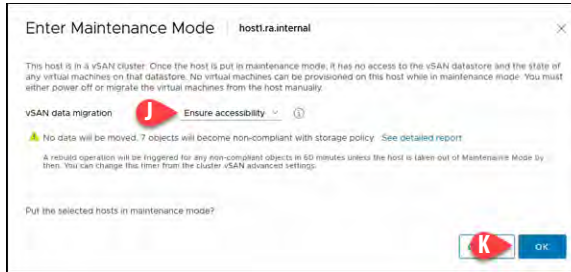
Click OK (F).

6. Under the expanded Cluster1 hierarchy of the main Navigation pane, right-click host1.ra.internal (G).

From the pull-down menu, select Maintenance Mode (H) > Enter Maintenance Mode (I).



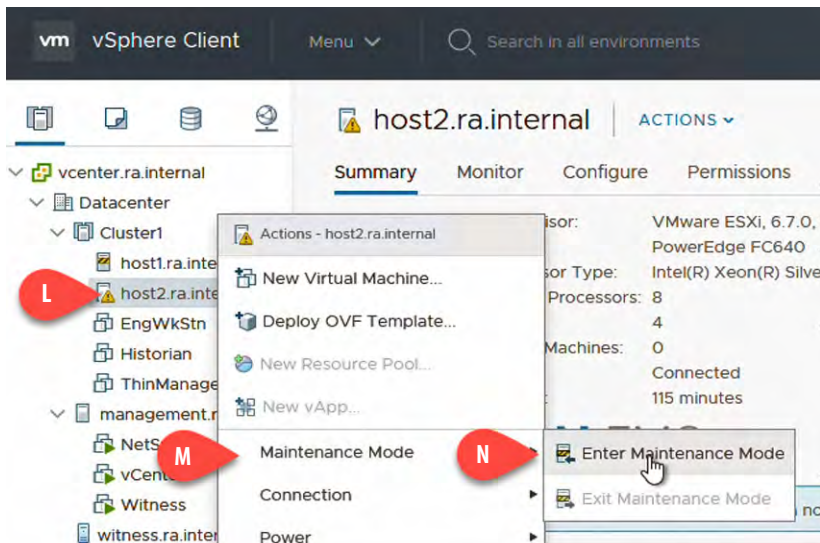
- On the Enter Maintenance Mode, select 'Ensure accessibility' from the pull-down menu (J).



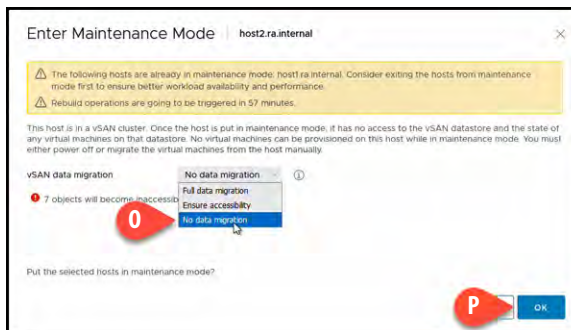
Click OK (K).

- Under the expanded Cluster1 hierarchy of the main Navigation pane, right-click host2.ra.internal (L).

From the pull-down menu, select Maintenance Mode (M) > Enter Maintenance Mode (N).



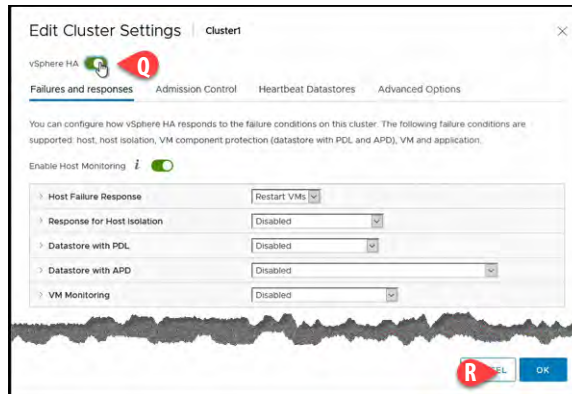
- On the Enter Maintenance Mode, select 'No data migration' from the pull-down menu (O).



Click OK (P).

- Repeat steps 1...4 on page 111.

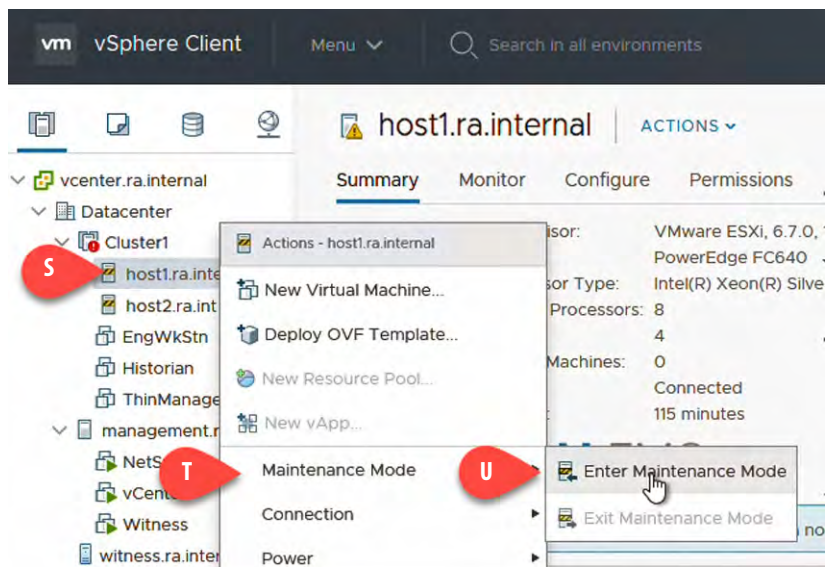
11. On Edit Cluster Settings, turn on vSphere HA (Q).



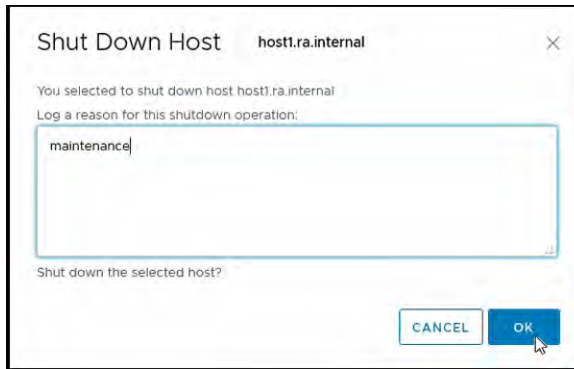
Click OK (R).

12. Under the expanded Cluster1 hierarchy of the main navigation pane, right-click host1.ra.internal (S).

From the pull-down menu, select Maintenance Mode (T) > Enter Maintenance Mode (U).

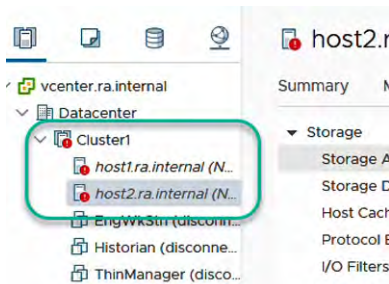


- On Shut Down Host, provide a reason for the shutdown.



Click OK.

- Repeat steps 12 and 13 for host2.ra.internal so both hosts are powered off.



Shut Down the vSphere Service Management Host

To shut down the service management host in VMware vSphere®, perform the following steps.

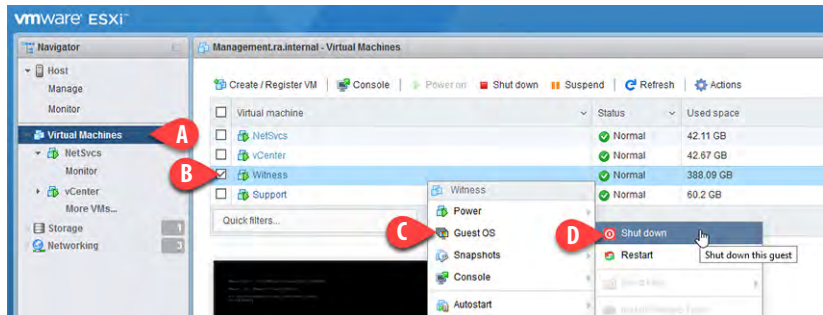
- Log into <https://192.168.249.13> with the following:
 - User name: root
 - Password: <system-specific password>



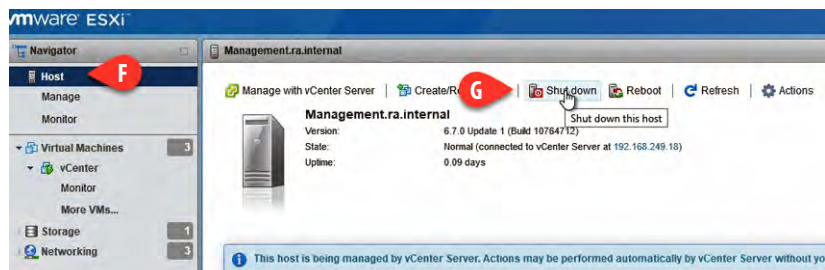
- Click Login.

3. Under the main Navigator pane, click Virtual Machines (A).
4. On the Management pane, highlight the virtual machine Witness (B).
5. Right-click Witness.

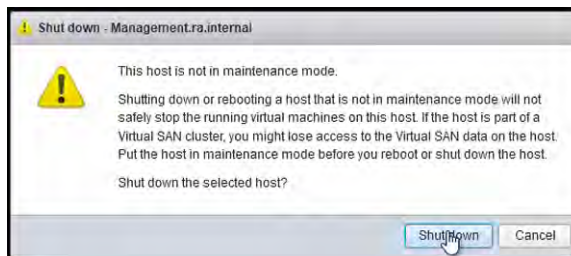
From the pull-down menus, select Guest OS (C) > Shut Down (D).



6. On the main Navigator pane, click Host (F).
7. On the Management pane, click Shut down (G).



8. A shutdown warning appears. Click Shutdown.



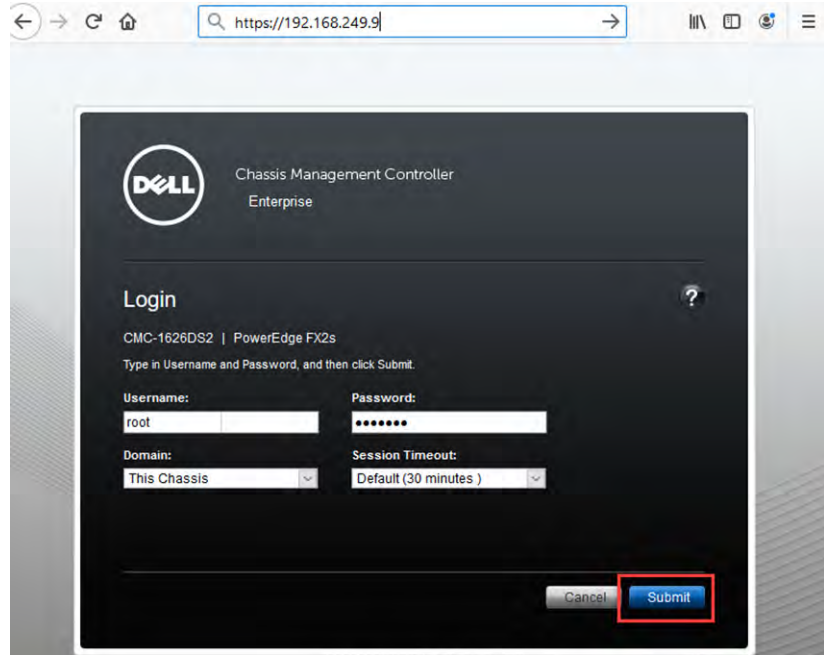
The service management host commences shutting down.

Start Up the System

To restart the system after a shutdown, perform the following steps.

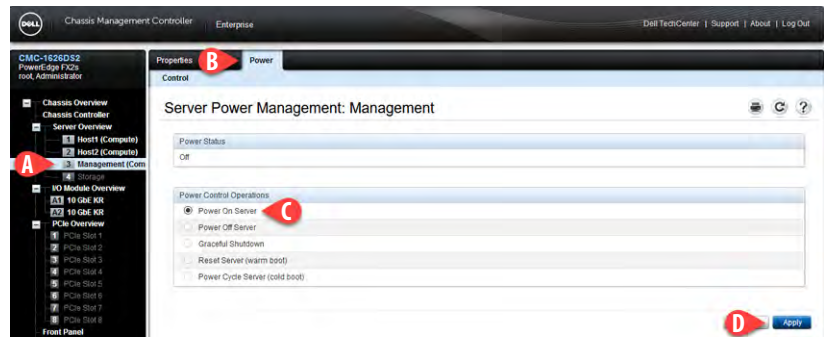
1. Access the Chassis Management Controller (CMC) through a browser at <https://192.168.249.9>.

Log in as root with the system-wide password, and click Submit.

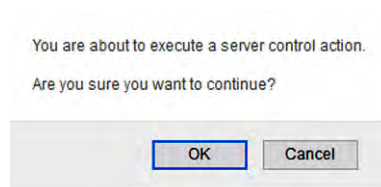


The Chassis Management Controller (CMC) home page appears.

2. On the Navigation pane, select Chassis Overview > Server Overview > Management (Compute) (A).
3. On the Management pane, select the Power tab (B).
4. Under Power Control Operations, select Power On Server (C).
5. Click Apply (D).

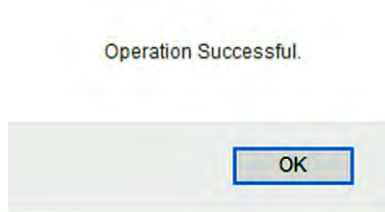


6. An alert appears. Click OK.

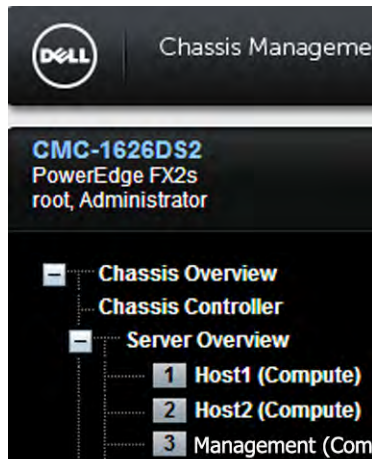


A confirmation appears when completed.

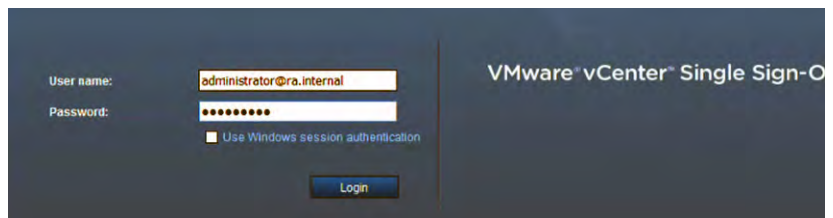
7. Click OK.



8. Repeat steps 3...7 for Host1 and Host2 under the Navigation pane.



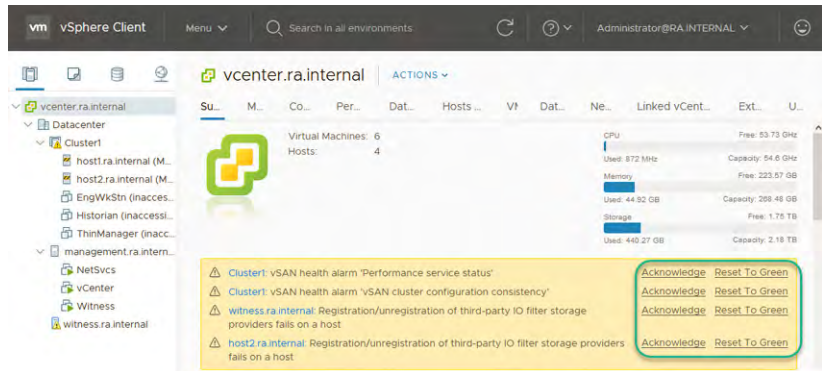
9. Log off CMC.
10. After approximately 10...15 minutes, log into <https://vcenter.ra.internal/ui> with the following:
 - User name: administrator@ra.internal
 - Password: <system-specific password>



11. Click Login.

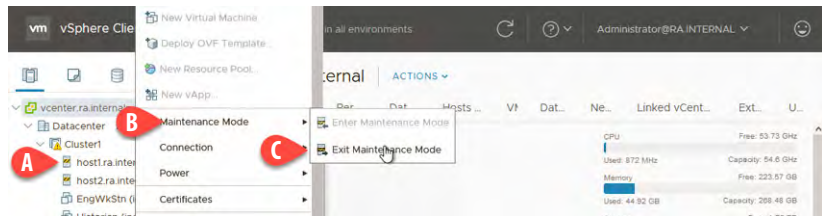
On the vCenter home page, several vSAN health warnings are visible.

12. For each warning, click Reset to Green.



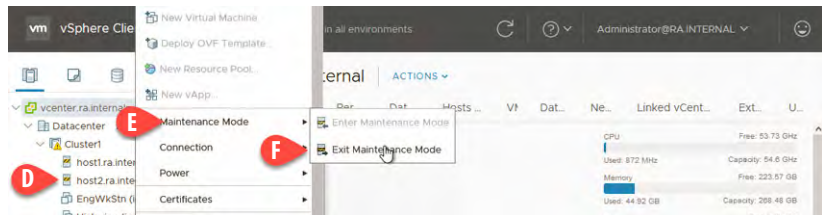
13. On the Navigation pane, click host1 (A).

14. Right-click on host1, and select Maintenance Mode (B) > Exit Maintenance Mode (C).



15. On the Navigation pane, click host2 (D).

16. Right-click on host2, and select Maintenance Mode (E) > Exit Maintenance Mode (F).

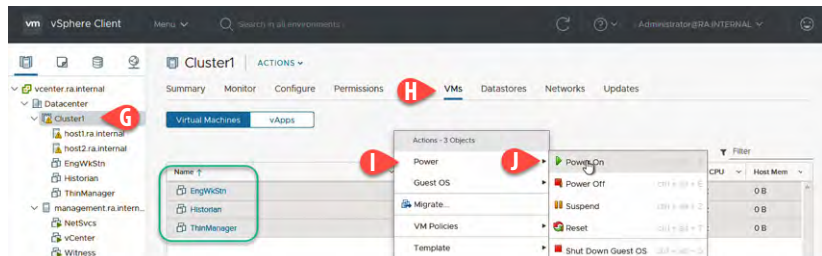


17. On the Navigation pane, click Cluster1 (G).

18. On the Cluster 1 main page, select the VMs tab (H).

19. On the VMs page, select and highlight the virtual machines that you want to turn on.

20. Right-click the selected virtual machines and select Power (I) > Power On (J).



All connection hosts in the VersaVirtual Appliance system are now started.

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Access the online site or dial 1-440-431-2500 for technical support.	https://rockwellautomation.custhelp.com/app/ismrequest
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	https://www.rockwellautomation.com/site-selection.html

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at https://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-c.pdf.

Rockwell Automation maintains current product environmental information on its website at <http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>.

Allen-Bradley, Rockwell Automation, Rockwell Software, Stratix, VersaVirtual, and Virtual Support Engineer are trademarks of Rockwell Automation, Inc.

Cisco, Catalyst, and Firepower are trademarks of Cisco Systems, Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

SolarWinds and N-central are trademarks of SolarWinds Worldwide, LLC.

VMware, vCenter Server, vSphere, and vSAN are trademarks of VMware, Inc.

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-UM001D-EN-P - November 2019

Supersedes Publication GMSN-UM001C-EN-P - September 2019

Copyright © 2019 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.